

Q4 2009 NETWORK INTRUSION PREVENTION SYSTEM TEST EXECUTIVE SUMMARY



Today, networks and data are more vulnerable than ever before. An essential part of layered security, network intrusion prevention systems (IPS) must be fast, accurate, and easy to deploy and maintain. During Q4 2009 NSS Labs performed the industry's most rigorous test of leading IPS solutions, including 1,159 validated exploits—the most ever performed in a test. As part of NSS Labs' independent testing information services, this report was produced for our enterprise subscribers. Leading vendors were invited to participate fully at no cost, and NSS Labs received no vendor funding.

All devices were configured and tuned by the respective vendor's technical experts; the time required was recorded for purposes of estimating the ongoing tuning and total cost of ownership (TCO) calculations. Effectiveness and performance results were obtained with the vendor-tuned policies and then again using the default policies to provide readers with a high-low range of possible results.

KEY FINDINGS

- Protection varied widely. The difference between the least and most effective products was 72.2%. The least effective product achieved only a 17.3% block rate, while the most effective product achieved an 89.5% block rate.
- Tuning is required. Organizations that do not tune could be missing numerous "catchable" attacks. The average difference in protection between tuned and default settings was 18%.
- Evasion tripped up most IPS products. Only Sourcefire, IBM, and McAfee successfully resisted all evasion and obfuscation techniques.
- Vendor performance claims are overstated between 12%-50%.
- The lower priced product is rarely the better value; sub-par protection is a poor investment at any price. Organizations should evaluate products based upon their value (protection, performance, and labor costs) within the context of a three-year TCO.

PRODUCT GUIDANCE

NSS Labs' recommendations are based solely on empirical test data, validated over multiple iterations.

	PRODUCTS
RECOMMEND	IBM Proventia® Network IPS GX6116 IBM Proventia Network IPS GX4004 McAfee® M-8000 Sensor McAfee M-1250 Sensor Sourcefire 3D® 4500
NEUTRAL	Cisco™ IPS 4260 Sensor Stonesoft StoneGate™ IPS-6105 Stonesoft StoneGate IPS-1060 Stonesoft StoneGate IPS-1030
CAUTION	TippingPoint® 2500N IPS TippingPoint 660N IPS TippingPoint TP-10 IPS Juniper Networks® IDP800 Juniper Networks IDP600C Juniper Networks IDP250

IPS PRODUCT RATINGS

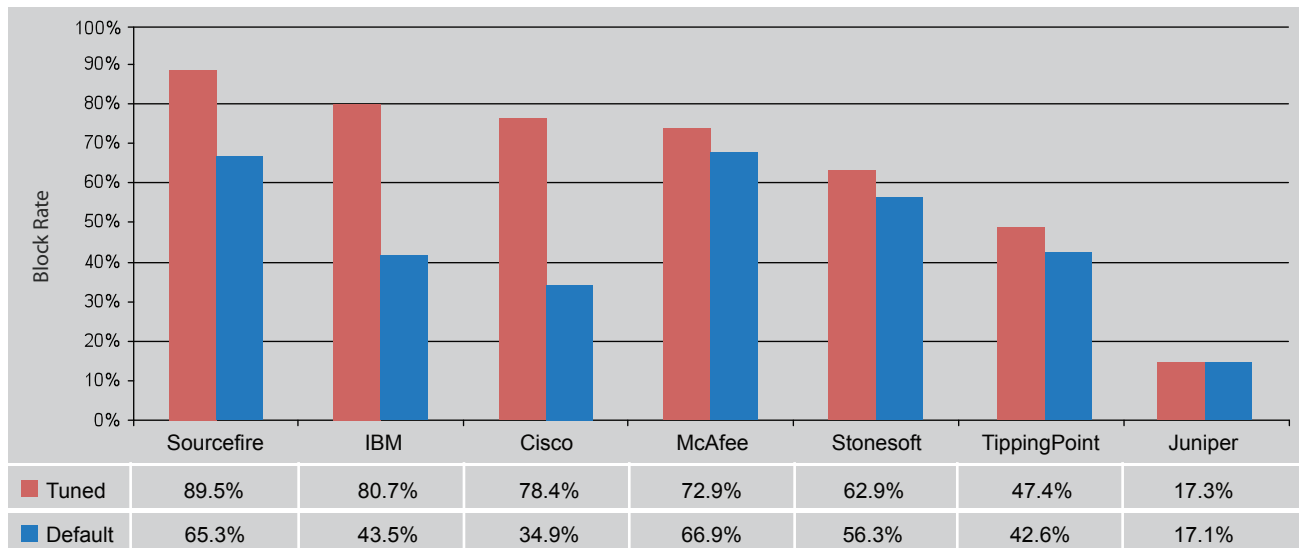


A product's effectiveness is handicapped if it fails to detect obfuscated exploits (evasion), and our product guidance is adjusted to reflect this. This is why the Cisco 4260 did not achieve "Recommended" status despite a respectable block rate.

Product Line	IP Packet Fragmentation	TCP Stream Segmentation	RPC Fragmentation	URL Obfuscation	FTP Evasion	TOTAL
IBM	✓	✓	✓	✓	✓	PASS
McAfee	✓	✓	✓	✓	✓	PASS
Sourcefire	✓	✓	✓	✓	✓	PASS
Cisco	✓	✓	✓		✓	FAIL
Juniper Networks	✓	✓				FAIL
Stonesoft	✓				✓	FAIL
TippingPoint			✓			FAIL

RESISTANCE TO EVASION*

* Although the Sourcefire 3D 4500 failed to detect an RPC Fragmentation evasion attempt in our Q4 2009 test, a fix to the product resolving this issue was subsequently validated by us on February 10, 2010.



BLOCK RATE - DEFAULT VS. TUNED POLICIES

ABOUT NSS LABS

NSS Labs, Inc. is the world's leading independent, information security research and testing organization. Its expert analyses provide information technology professionals with the unbiased data they need to select the right product for their organizations. Pioneering intrusion detection and prevention system testing with the publication of the first such test criteria in 1999, NSS Labs also evaluates firewall, unified threat management, anti-malware, encryption, web application firewall, and other technologies on a regular basis. The firm's real-world test methodology is the only one to assess security products against live Internet threats. As such, NSS Labs tests are considered the most aggressive in the industry and its recommendations and certifications highly coveted by vendors. Founded in 1999, the company has offices in Carlsbad, California and Austin, Texas. For more information, visit www.nsslabs.com.