



McAfee IntruShield Stands Alone as World's Only Network IPS Solution to Receive New "Multi-Gigabit IPS" Certification by NSS Group

IntruShield receives the only MGIPS-Enterprise certification from among 12 participants

NSS GROUP TEST SUMMARY

In October 2006, McAfee® IntruShield® received the "NSS Approved" designation for multi-gigabyte intrusion prevention systems (MGIPS) from the globally respected NSS Group, outperforming all other vendors and achieving the sole certification in its class.

→ *IntruShield performed flawlessly in NSS testing, achieving results of 100 percent in virtually every major test category—including detection, false-positive resistance, latency, and reliability*

→ *IntruShield signature recognition and blocking was excellent. IntruShield successfully blocked 100 percent of the NSS Group's attacks, evasions, and vulnerabilities with minimal latency and perfect performance*

→ *NSS lauded IntruShield's management and control capabilities as a powerful tool that provides both solid default functions and simple controls for customization. NSS highlighted IntruShield's user-defined signature editor, default in-line IPS policy, global attack response editor, and virtual IPS*

Online review: <http://www.nss.co.uk/certification/mgips/test-reports/MGIPS-0610-MCA.pdf>

NOTABLE QUOTES FROM NSS GROUP

→ *"The performance of the device submitted for testing—the IntruShield 4010—was very impressive, combining excellent security effectiveness with low latency under all traffic loads. It also handled our demanding, extended false-positive, false-negative, and evasion tests easily, and without blocking any legitimate traffic or succumbing to common evasion techniques"*

→ *"Management and control capabilities are outstanding, and the recently updated Java-based GUI is very slick and intuitive to use. McAfee now offers its management system as a turnkey appliance to simplify deployment, and it provides extremely powerful and flexible means of controlling anything from a single device to a large enterprise-wide deployment"*

→ *"The I-4010 also demonstrated outstanding resistance to common evasion techniques, providing total coverage across the board in all our evasion tests, including the very difficult server-to-client HTML evasions"*

→ *"Alerts were kept to a minimum and appeared to be very accurate, making the analyst's job as straightforward as possible. Resistance to false positives also appeared to be very good"*



EXCERPTS FROM TEST

On Security Effectiveness:

- The performance of the I-4010 was outstanding, detecting all of the [high-severity] test cases out of the box and blocking all but one of them (this was blocked following tuning)
- The I-4010 performed extremely well with the Audit and Reconnaissance test suites, catching 100 percent of the Audit and all but five of the Reconnaissance cases after tuning
- DoS and peer-to-peer (P2P) traffic was well covered, and performance in the very difficult server-to-client (S2C) test suite was very good
- Performance in our extensive false-positive tests was outstanding
- Resistance to known evasion techniques was outstanding across the board

On Performance:

- Performance at almost all levels of our load tests was impeccable, with 100 percent of all attacks being detected under all but the most extreme load conditions, and 100 percent of all attacks being blocked under any load conditions

- The sensor remained remarkably unaffected by high levels of Dedicated Denial of Service (DDoS) attacks, too, offering complete protection for the servers behind it while continuing to pass legitimate traffic through the device with extremely low latency

On Architecture:

- IntruShield 4010 has one of the most robust architectures we have seen in our labs when it comes to handling excessive levels of traffic
- The IntruShield Manager and Console have been designed from the ground up to handle large distributed networks and even managed services environments, and they contain several useful features to make this type of deployment easier to handle
- The granular nature of policy management makes ISM perfect for managed services environments

On Inbound vs. Outbound traffic rules:

- This is an incredibly powerful feature that allows the administrator to refine the differences in how inbound and outbound traffic are inspected

McAfee IntruShield



- **Broad threat prevention**—IntruShield protects infrastructure and endpoints from zero-day, DoS, encrypted, and SYN flood attacks, plus spyware, botnets, malware, Voice over IP (VoIP) vulnerabilities, phishing, and worms
- **Risk-aware intrusion prevention**—IntruShield's prioritized risk management blocks the most relevant threats and attacks on your network
- **Out-of-the-box default blocking**—IntruShield's default *Recommended for Blocking* policy provides proactive blocking for hundreds of attacks straight out of the box
- **Backed by McAfee**—The world's largest and most trusted name in the security industry