McAfee IntruShield Network IPS Appliances

Proven and industry-leading, next-generation intrusion prevention solution. Industry's first *risk-aware* IPS delivering best-in-class proactive prevention of zero-day and DoS attacks, spyware, malware, botnets, and VoIP threats.

The risks to organizations, enterprises, and service providers continue to grow as the rising number of new vulnerabilities, and the speed and sophistication of attacks that exploit those vulnerabilities, pose an ever-increasing threat to your business. The rise and evolution of new hybrid attacks that use multiple techniques to attack your network infrastructure means that enterprises of all sizes must constantly defend themselves against these shifting threats.

Traditional, reactive security technology alone cannot ensure network availability, integrity, and data confidentiality. Due to the inadequate ability of traditional technology to provide proactive threat detection and prevention, businesses remain vulnerable to sophisticated and highly targeted new (zero-day) and Denial of Service (DoS) attacks, as well as spyware, malware, and Voice over IP (VoIP) threats. Businesses need to defend their critical network infrastructure by deploying advanced, proactive protection against vulnerability-based threats and attacks. Furthermore, companies of every size are under intense regulatory and audit pressure to ensure the privacy of confidential data and decrease business risk.

For comprehensive, proactive network protection against a broad range of today's threats and attacks, enterprises and organizations need to deploy next-generation intrusion prevention. The proven and award-winning McAfee® IntruShield® network intrusion prevention system (IPS) delivers the most comprehensive, accurate, and scalable threat protection. IntruShield helps enterprises, service providers, and small- and medium-sized businesses (SMBs) assure the availability and security of critical network infrastructure through proactive and comprehensive threat prevention.

The McAfee IntruShield IPS Solution

IntruShield's family of award-wining, next-generation IPS appliances enables enterprises, service providers, and SMBs to reduce business risk by deploying the industry's most comprehensive and proven network IPS solution. Its purpose-built platforms proactively protect endpoints and critical network infrastructure from known, zero-day, DoS, and encrypted attacks, as well as threats like spyware, VoIP vulnerabilities, botnets, malware, network worms, Trojans, and peer-to-peer applications.

IntruShield's unparalleled technology preemptively blocks attacks before they reach their intended targets, while providing absolute accuracy and mission-critical performance for all network environments. Its integrated protection and easy-to-manage platform delivers broad asset protection, maximized business availability, reduced liability, and security-cost avoidance. And IntruShield's powerful policy enforcement, advanced forensics, and comprehensive reporting capabilities help businesses comply with audit and regulatory requirements.

IntruShield is the industry's first *risk-aware* IPS solution, enabling enterprises, SMBs, and service providers to deploy prioritized risk management through intelligent, highly targeted threat prevention. By integrating with market-leading McAfee Foundstone® vulnerability management (VM) solutions—as well as open-source VM systems such as Nessus—IntruShield reduces business risk, increases operational efficiencies, and maximizes security by providing the ability to identify and block the most relevant threats and attacks targeting your network.

IntruShield's built-in VoIP protection, spyware prevention, and advanced Web-client protection maintains business-critical applications, reduces IT costs, and secures confidential information by blocking spyware, malware, botnets, and VoIP threats. Its unrivaled encrypted-threat protection provides real-time prevention of encrypted attacks, while its ASIC-based architecture, deep packet inspection, and patented shell-code detection deliver unequaled zero-day protection.

The innovative IntruShield architecture is purpose-built for long product life cycles, providing continuous next-generation security and feature enhancements. This allows for continuous protection against the latest threats and vulnerabilities—including spyware, malware, botnets, SYN floods, VoIP threats, and encrypted attacks—while never requiring hardware upgrades. IntruShield's architecture integrates patented signature, anomaly, and DoS/DDoS analysis techniques, enabling highly accurate threat detection and prevention that blocks attacks before they

inflict damage. IntruShield's next-generation technology delivers unparalleled features, including "out-of-the-box" default IPS blocking, pre-configured *Recommended for Blocking* policies, built-in spyware and VoIP protection, virtual IPS, and an integrated internal firewall. And, the IntruShield portfolio of appliances is backed by McAfee—the largest dedicated security company and the most trusted name in the industry.

Features and Benefits

Comprehensive protection

- **Broad threat prevention**—IntruShield's purpose-built IPS appliances deliver the most comprehensive threat prevention by proactively protecting endpoints and network infrastructure from known, zero-day, DoS, and encrypted attacks, as well as threats like spyware, VoIP vulnerabilities, malware, botnets, network worms, Trojans, and peer-to-peer applications
- **Built-in anti-spyware protection**—Provides enhanced security by integrating multi-layered protection against spyware, adware, dialers, keyloggers, password crackers, and remote-control programs. IntruShield's spyware protection helps reduce IT costs, prevents potential privacy breaches, and protects confidentiality by proactively preventing the download of these unwanted programs, while blocking spyware communication and propagation
- **Built-in advanced Web-client protection**—Proactively protects Web browsers and desktops from cyber-attacks, spyware, botnets, and other forms of malware. It prevents the download of unwanted programs, while protecting against unauthorized network access. IntruShield's built-in Web-client protection complements McAfee's Perimeter and System Protection solutions by providing an additional layer of network protection
- **Next-generation DoS prevention**—The industry's most advanced, next-generation DoS prevention technology delivers comprehensive, real-time protection against sophisticated DoS attacks, cyber-attacks, and cyber extortion. Multi-layered threshold, profile-based, and SYN-cookie technology—in combination with IntruShield's unrivaled virtual IPS capabilities—deliver highly granular protection against a broad spectrum of DoS attacks, including DoS, DDoS, and SYN flood attacks
- **Infrastructure protection**—Provides preemptive, zero-day vulnerability protection against threats and attacks that target mission-critical routers, switches, perimeter firewalls, and DNS servers. Provides the only effective means to protect critical network infrastructure during "windows of vulnerability"

The IntruShield 4010

The IntruShield 4010 (I-4010) is suited for deployment at the core of large enterprise, data center, or service provider networks. The high port-density Gigabit Ethernet interfaces provide the performance and operational redundancy required to secure a high-availability network infrastructure, along with economies-of-scale needed by large enterprises, data centers, and service providers.

- Twelve Gigabit Ethernet detection ports
- One Fast Ethernet management port
- Optional redundant hot-swappable power supply
- Purpose-built for high performance, high availability, and low latency
- Up to 2 Gbps performance

The IntruShield 4000

The IntruShield 4000 (I-4000) is suited for deployment at the core of enterprise, data center, or service provider networks. The Gigabit Ethernet interfaces provide the performance and operational redundancy required to secure a high-availability network infrastructure.

- Four Gigabit Ethernet detection ports
- One Fast Ethernet management port
- Optional redundant hot-swappable power supply
- Purpose-built for high performance, high availability, and low latency
- Up to 2 Gbps performance

The IntruShield 3000

The IntruShield 3000 (I-3000) is suited for deployment at the core of large enterprise, data center, or service provider networks. The high port-density Gigabit Ethernet interfaces provide the performance and operational redundancy required to secure a high-availability network infrastructure, along with economies-of-scale needed by large enterprises, data centers, and service providers.

- Twelve Gigabit Ethernet detection ports
- One Fast Ethernet management port
- Optional redundant hot-swappable power supply
- Purpose-built for high performance, high availability, and low latency
- Up to 1 Gbps performance

McAfee®

- **Unrivaled botnet prevention**—Industry's only network-based security solution to provide comprehensive, layered, and proactive blocking of malicious distributed botnets. IntruShield protects against the growing threat of botnets by identifying them as a distinctive category of attack and proactively blocking their installation, communication and activation through the Internet
- **VoIP vulnerability protection**—IntruShield's integrated VoIP security proactively protects mission-critical VoIP infrastructure and applications by accurately detecting and blocking known, zero-day, and DoS attacks. IntruShield protects against underlying VoIP protocol vulnerabilities, while preserving VoIP application and voice-quality integrity
- **Encrypted attack prevention**—Industry's first and only network IPS to securely and proactively protect against both clear-text and encrypted attacks. IntruShield's advanced, real-time SSL decryption and inspection technology dramatically increases network security coverage by protecting critical e-commerce infrastructure
- **IPS and internal firewall**—Integrated network IPS and stateful internal firewall capabilities deliver unrivaled internal system protection, network infrastructure protection, and enterprise-wide policy enforcement

Accurate protection

- ***Risk-aware*** **intrusion prevention**—Risk-aware IPS delivers significant operational efficiencies by providing the ability to intelligently identify and block the most relevant alerts and attacks. Integration with market-leading Foundstone VM solutions automatically identifies and highlights risks. Enables targeted, prioritized risk management by importing and correlating risk-assessment information from Foundstone, as well as open-source VM systems, such as Nessus
- **Signature, anomaly, and DoS analysis**—IntruShield's unmatched architecture integrates a variety of advanced detection methods (including signature, application and protocol anomaly, shell-code detection algorithms, and next-generation DoS/DDoS prevention) to deliver the most accurate protection available against today's threats and attacks
- **Unmatched detection accuracy**—IntruShield performs stateful traffic inspection with thorough parsing of over 100 protocols, while leveraging over 3,000 high-quality, multi-token, multi-trigger signatures to provide the most accurate detection in the industry. IntruShield's unmatched accuracy allows you to confidently block threats and attacks in real time without affecting legitimate traffic

The IntruShield 2700

The IntruShield 2700 (I-2700) offers a flexible IPS for enterprise perimeter deployment. Multiple Fast Ethernet and Gigabit Ethernet interfaces provide effective protection for multiple network segments.

- Two Gigabit Ethernet and six Fast Ethernet detection ports
- Built-in Fast Ethernet network taps
- One Fast Ethernet management port
- Purpose-built for high performance, high availability, and low latency
- Up to 600 Mbps performance

The IntruShield 1400

The IntruShield 1400 (I-1400) offers a cost-effective IPS deployment for mid-size, remote/branch office networks, or at the perimeter of enterprise networks. Centralized Web-based management for enterprise-wide IPS deployments dramatically reduces operational costs.

- Four Fast Ethernet detection ports
- Built-in Fast Ethernet network taps
- One Fast Ethernet management port
- Purpose-built for high performance, high availability, and low latency
- Up to 200 Mbps performance

The IntruShield 1200

The IntruShield 1200 (I-1200) offers a cost-effective IPS deployment for mid-size or remote/branch office networks. Centralized Web-based management for enterprise-wide IPS deployment dramatically reduces operational costs.

- Two Fast Ethernet detection ports
- Built-in Fast Ethernet network taps
- One Fast Ethernet management port
- Purpose-built for high performance, high availability, and low latency
- Up to 100 Mbps performance

McAfee®

- **Backed by McAfee**—Proven protection, unmatched security knowledge, and continuous proactive security research from the world's largest dedicated security company: McAfee, the most trusted name in the industry

Scalable and manageable

- **Out-of-the-box default blocking**—IntruShield is preset for default IPS blocking, and comes pre-configured with a *Recommended for Blocking* policy that provides accurate and proactive blocking for hundreds of attacks straight out of the box. *Recommended for Blocking* signatures are continuously updated by McAfee to provide comprehensive protection against new threats
- **Unprecedented virtual IPS**—IntruShield's unique and flexible virtualization capability extends to both IPS and internal firewall, supporting up to 1,000 virtual IPS sensors per physical device, each with its own highly customized and granular security policy
- **Always on management with automated disaster recovery**—Delivering uninterrupted, highly available management capabilities by providing Active/Standby management-server technology for the IntruShield Security Management (ISM) system. Automated failover and fail-back technology that enables disaster recovery of critical configuration data in the event of failure. Always on management ensures the continuity of critical network protection and supports corporate disaster recovery policies
- **Integrated user authentication**—Integrated user authentication capabilities deliver administrative and user-management efficiencies. Integration provides system operators and users with comprehensive authentication support to external databases, including Radius, LDAP, and TACAS
- **Easy-to-use centralized management**—A single management console delivers simple, centralized, Web-based management of IntruShield appliances and policies. Plus, a rich set of fourteen ready-to-use, pre-defined IPS security policies allow for easy customization. IntruShield's easy-to-use management system reduces complexity, maximizes IT efficiencies, and lowers operational costs. ISM is provided at no cost for management of up to two IntruShield appliances
- **Automated real-time threat updates**—Innovative, automated process delivers real-time signature updates without requiring sensor reboots and provides protection against newly discovered vulnerabilities, while eliminating manual updates and network downtime
- **Advanced intrusion forensics**—Delivers unique forensic features to analyze key characteristics of known and zero-day threats and intrusions. IntruShield's powerful forensic capabilities provide highly actionable and accurate information and reporting related to intrusion identification, relevancy, direction, impact, and analysis
- **Flexible deployment**—Unprecedented flexibility of IPS or intrusion detection system (IDS) deployment (including in-line, port clustering, high-availability, span, and tap modes) to suit any network security architecture. IntruShield's flexible architecture allows enterprises and service providers to automatically migrate from reactive intrusion detection to proactive intrusion prevention

Award-winning ASIC-based architecture

- **Purpose-built hardware**—IntruShield appliances are purpose-built for mission-critical intrusion prevention, and are engineered using multiple state-of-the-art network processors, co-processors, FPGAs, and general-purpose processors. IntruShield's award-winning architecture incorporates dedicated, high-speed hardware to achieve unmatched accuracy, performance, and proactive protection
- **Investment protection**—Industry's most advanced architecture, purpose-built for long product life cycles, allows for continuous next-generation security and feature enhancements. Continues to provide advanced protection against today's threats, including spyware, malware, DoS, VoIP vulnerabilities, botnets, and encrypted attack protection, while never requiring appliance hardware upgrades
- **Integrated network and host IPS**—Provides breakthrough integration by enabling host (McAfee Host Intrusion Prevention) and network (IntruShield) IPS security-event aggregation and coordination on a single ISM console
- **Industry's highest gigabit port-density appliances**—Combines with IntruShield's virtual IPS capabilities to provide superior price/performance, high scalability, and lower capital expenditure. Supports high-scale deployments and profitable security service delivery
- **High-availability deployment**—Complete, stateful failover capabilities deliver high-availability (HA) configuration between a pair of primary and failover IntruShield appliances. IntruShield's HA configuration feature allows transparent, Layer 7, stateful failover, thereby avoiding a single point of failure

McAfee®

IntruShield Sensor Specifications






Sensor Hardware Components	I-4010	I-4000	I-3000	I-2700	I-1400	I-1200
Network location	Core	Core	Core	Perimeter	Branch office/ perimeter	Branch office
Performance throughput	Up to 2 Gbps	Up to 2 Gbps	Up to 1 Gbps	Up to 600 Mbps	Up to 200 Mbps	Up to 100 Mbps
Maximum concurrent connections	1,000,000	1,000,000	500,000	250,000	80,000	40,000
Ports						
Gigabit Ethernet detection ports	12	4	12	2	—	—
Fast Ethernet (FE) detection ports	—	—	—	6	4	2
Dedicated Fast Ethernet (FE) response ports	2	2	2	3	1	1
Dedicated Fast Ethernet (FE) management ports	Yes	Yes	Yes	Yes	Yes	Yes
External fail-open control ports	6	2	6	1	—	—
Console and aux ports	Yes	Yes	Yes	Yes	Yes	Yes
Built-in network taps	No	No	No	Yes (for FE ports)	Yes	Yes
Fail-open	Optional	Optional	Optional	Yes (for FE ports)	Yes	Yes
Fail-close	Yes	Yes	Yes	Yes	Yes	Yes
Mode of operation						
SPAN port monitoring	Yes	Yes	Yes	Yes	Yes	Yes
Tap mode	Optional	Optional	Optional	Yes (for FE ports)	Yes	Yes
In-line mode	Yes	Yes	Yes	Yes	Yes	Yes
Port clustering	Yes	Yes	Yes	Yes	Yes	Yes
No. of virtual IPS systems	1,000	1,000	1,000	100	32	16
Traffic monitoring on active-active links	Yes	Yes	Yes	Yes	Yes	Yes
Traffic monitoring on active-passive links	Yes	Yes	Yes	Yes	Yes	Yes
Monitoring of asymmetric traffic routing	Yes	Yes	Yes	Yes	Yes	Yes
High availability						
Redundant power	Yes (Optional)	Yes (Optional)	Yes (Optional)	Yes (Optional)	No	No
Device failure detection	Yes	Yes	Yes	Yes	Yes	Yes
Link failure detection	Yes	Yes	Yes	Yes	Yes	Yes
Physical						
dimensions	2RU Rack mountable 17.44 (W) x 3.44 (H) x 23.00 (D)	2RU Rack mountable 17.44 (W) x 3.44 (H) x 23.00 (D)	2RU Rack mountable 17.44 (W) x 3.44 (H) x 23.00 (D)	2RU Rack mountable 17.44 (W) x 3.44 (H) x 23.00 (D)	1RU Rack mountable 17.32 (W) x 1.65 (H) x10.5 (D)	1RU Rack mountable 17.32 (W) x 1.65 (H) x10.5 (D)
Weight	47 lbs.	47 lbs.	47 lbs.	47 lbs.	17 lbs.	15 lbs.
Power	100–240VAC (50/60Hz)					
Power consumption	350w	350w	350w	250w	100w	100w
Temperature	0° to 40° C (Operating) -40° to 70° C (Non-operating)					
Relative humidity (non-condensing)	Operational: 10% to 90% Non-operational: 5% to 95%					
Altitude	0 to 10,000 feet					
Safety certification	UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, IEC 60825, 21CFR1040 CB license and report covering all national country deviations.					
EMI certification	FCC Part 15, Class A (CFR 47) (USA) ICES-003 Class A (Canada), EN55022 Class A (Europe), CISPR22 Class A (Int'l)					

McAfee®

Sensor Software Components		I-4010	I-4000	I-3000	I-2700	I-1400	I-1200
Stateful traffic inspection	IP defragmentation and TCP stream reassembly	Yes	Yes	Yes	Yes	Yes	Yes
	Detailed protocol analysis	Yes	Yes	Yes	Yes	Yes	Yes
	Asymmetric traffic monitoring	Yes	Yes	Yes	Yes	Yes	Yes
	Protocol normalization	Yes	Yes	Yes	Yes	Yes	Yes
	Advanced evasion protection	Yes	Yes	Yes	Yes	Yes	Yes
	Forensic data collection	Yes	Yes	Yes	Yes	Yes	Yes
	Protocol tunneling	Yes	Yes	Yes	Yes	Yes	Yes
	Protocol discovery	Yes	Yes	Yes	Yes	Yes	Yes
Signature detection	User-defined signatures	Yes	Yes	Yes	Yes	Yes	Yes
	Real-time signature updates	Yes	Yes	Yes	Yes	Yes	Yes
Anomaly detection	Statistical anomaly	Yes	Yes	Yes	Yes	Yes	Yes
	Protocol anomaly	Yes	Yes	Yes	Yes	Yes	Yes
	Application anomaly	Yes	Yes	Yes	Yes	Yes	Yes
DoS detection	Threshold-based detection	Yes	Yes	Yes	Yes	Yes	Yes
	Self-learning profile-based detection	Yes	Yes	Yes	Yes	Yes	Yes
	Maximum DoS profiles	5,000	5,000	5,000	300	120	100
Intrusion prevention	Stop attacks in progress in real time	Yes	Yes	Yes	Yes	Yes	Yes
	Drop attack packets/sessions	Yes	Yes	Yes	Yes	Yes	Yes
	Reconfigure firewall	Yes	Yes	Yes	Yes	No	No
	Initiate TCP reset, ICMP unreachable	Yes	Yes	Yes	Yes	Yes	Yes
	Packet logging	Yes	Yes	Yes	Yes	Yes	Yes
	Automated and user-initiated prevention	Yes	Yes	Yes	Yes	Yes	Yes
Encrypted attack protection	Stops encrypted attacks in real time	Yes	Yes	Yes	Yes	No	No
Internal firewall	Blocks unwanted and nuisance traffic	Yes	Yes	Yes	Yes	Yes	Yes
	Granular security policy enforcement	Yes	Yes	Yes	Yes	Yes	Yes
High availability	Stateful failover	Yes	Yes	Yes	Yes (for FE ports)	Yes	Yes
Management	Command line interface (console)	Yes	Yes	Yes	Yes	Yes	Yes
	Manager communication	Secure channel	Same for all models	Same for all models	Same for all models	Same for all models	Same for all models

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com