McAfee IntruShield 1200 and 1400 Network IPS Appliances

Proven and industry-leading, next-generation intrusion prevention for the small and medium-sized business customer

No business is immune to security threats, no matter how large or small. In today's dynamic threat environment, the risks to small and medium-sized organizations continue to grow as the rising number of new vulnerabilities, and the speed and sophistication of attacks exploiting those vulnerabilities, poses an ever-increasing threat. The increase and evolution of new hybrid attacks that use multiple techniques to attack your network infrastructure means that small and medium-sized businesses must constantly defend themselves against these shifting threats.

Traditional reactive security technology alone cannot ensure network availability, integrity, and data confidentiality. As a result, your business remains vulnerable to sophisticated, targeted, and zero-day attacks due to the inadequate ability of traditional technology to provide preemptive threat detection and prevention. Businesses like yours 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, reduce liabilities, and decrease business risk.

To ensure comprehensive, proactive network protection against a wide range of threats and attacks, you must deploy enterprise-class intrusion prevention. The proven network Intrusion Prevention System (IPS) of McAfee® IntruShield® delivers the most comprehensive, accurate, and scalable threat protection, helping your small or medium-sized business assure the availability and security of critical network infrastructure through proactive threat prevention.

The McAfee IntruShield IPS Solution

McAfee IntruShield's next-generation network IPS delivers advanced, real-time protection against known, zero-day (unknown), and Denial of Service (DoS) attacks, as well as spyware and other potentially unwanted programs. IntruShield also helps control non-business applications by delivering broad protection for instant messaging and peer-to-peer programs. And IntruShield's powerful policy enforcement and comprehensive reporting capabilities help your business comply with regulatory requirements while decreasing risks and liabilities.

With the IntruShield 1200 and 1400 appliances, McAfee's protection extends from your network edge out to your branch offices, providing comprehensive, proactive, and scalable solutions for both small and medium enterprise environments.

Our innovative IntruShield 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 IPS blocking, pre-configured *Recommended for Blocking* policies, built-in spyware and VoIP protection, virtual IPS, and integrated IPS and internal firewall. And, the IntruShield 1200 and 1400 appliances are backed by the largest dedicated security company and the most trusted name in the industry—McAfee.

Features and Benefits

Comprehensive protection

- **Unmatched threat prevention**—IntruShield delivers the most comprehensive and proactive intrusion prevention for maintaining network and business availability by protecting against known, zero-day, and DoS attacks, as well as a wide variety of other threats, including evasions, backdoors, and Trojans
- **Integrated spyware protection**—IntruShield provides enhanced security by integrating multi-layered protection against spyware, adware, dialers, keyloggers, password crackers, and remote-control programs. IntruShield's complimentary spyware protection helps reduce IT costs, prevents potential privacy breaches, and protects confidentiality by detecting and blocking spyware communication and propagation
- **Signature, anomaly, and DoS analysis**—IntruShield's unmatched architecture integrates a variety of the most advanced detection methods available, including signature, application and protocol anomaly, patented shell-code detection algorithms, and DoS statistical analysis. IntruShield's next-generation detection and

McAfee®

prevention engines minimize false-positives and prevent zero-day attacks by delivering the most comprehensive and accurate threat and vulnerability protection available

- **Unparalleled VoIP protection**—IntruShield's integrated VoIP security proactively protects mission-critical VoIP applications by accurately detecting and blocking known, new (zero-day), and DoS attacks, while preserving VoIP application and voice-quality integrity by protecting against underlying VoIP protocol vulnerabilities
- **IPS and internal firewall**—unprecedented internal system protection, network infrastructure protection, flexibility, and enterprise-wide policy enforcement through integrated network IPS and internal firewall capabilities

Accurate protection

- **Proven 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 without affecting legitimate traffic
- **Unprecedented virtual IPS**—IntruShield's unique and flexible virtualization capability extends to both IPS and internal firewall, supporting up to 32 virtual IPS sensors per physical device, each with its own highly customized and granular security policy. Virtualization allows small and medium-sized businesses to easily implement and enforce a broad set of security policies on a single device, thereby increasing flexibility and accuracy, reducing the total number of appliances required, and dramatically reducing total cost of ownership (TCO)
- **Intrusion intelligence**—Powerful capabilities provide accurate and *highly actionable* information and reporting related to intrusion identification, relevancy, direction, impact, and analysis. This allows for quicker IT response times, helps organizations comply with regulatory requirements, and supports seamless migration from reactive intrusion detection to proactive in-line prevention.
- **Backed by McAfee**—Proven protection, unmatched security knowledge and proactive security research from the world's largest dedicated security company

Ease-of-use and manageability

- **Out-of-the-box default blocking**—IntruShield is pre-set 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
- **Easy-to-use centralized management**—A single management console (McAfee IntruShield Manager) delivers simple, centralized, Web-based management of IntruShield appliances and policies. Plus, a rich set of 14 ready-to-use, pre-defined IPS security polices allow for easy customization. IntruShield's centralized, easy-to-use management reduces complexity, maximizes IT efficiencies, and lowers total cost of ownership. The IntruShield Manager is provided at no cost for management of up to two IntruShield appliances
- **Automated real-time threat updates**—IntruShield's innovative update process delivers automated, real-time signature updates without requiring appliance reboots. Real-time threat updates provide the most proactive protection against newly-discovered vulnerabilities, while eliminating manual updates and network downtime
- **Flexible deployment**—Unprecedented flexibility of IDS or IPS deployment—including in-line, port clustering, high-availability, span, and tap modes—while delivering comprehensive infrastructure protection for network routers, switches, VPNs, and gateways

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 200Mb/s 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 100Mb/s performance

McAfee®

IntruShield Sensor Specifications

Sensor Hardware Components	I-1400	I-1200
Network Location	Branch Office/Perimeter	Branch Office
PerformanceThroughput	Up to 200Mb/s	Up to 100Mb/s
Maximum Concurrent Connections	80,000	40,000
Ports		
Gigabit Ethernet Detection Ports	—	—
Fast Ethernet (FE) Detection Ports	4	2
Dedicated Fast Ethernet (FE) Response Ports	1	1
Dedicated Fast Ethernet (FE) Management Port	Yes	Yes
External Fail-Open Control Ports	—	—
Console and Aux Ports	Yes	Yes
Built-In Network Taps	Yes	Yes
Fail-Open	Yes	Yes
Fail-Close	Yes	Yes
Mode of Operation		
SPAN Port Monitoring	Yes	Yes
Tap Mode	Yes	Yes
In-Line Mode	Yes	Yes
Port Clustering	Yes	Yes
No. of Virtual IPS Systems	32	16
Traffic Monitoring on Active-Active Links	Yes	Yes
Traffic Monitoring on Active-Passive Links	Yes	Yes
Monitoring of Asymmetric Traffic Routing	Yes	Yes
High Availability		
Redundant Power	No	No
Device Failure Detection	Yes	Yes
Link Failure Detection	Yes	Yes
Physical		
Dimensions	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	17lbs.	15lbs.
Power	Same for All Models	Same for All Models
Power Consumption	100w	100w
Temperature	Same for All Models	Same for All Models
Relative Humidity (non-condensing)	Same for All Models	Same for All Models
Altitude	Same for All Models	Same for All Models
Safety Certification	Same for All Models	Same for All Models
EMI Certification	Same for All Models	Same for All Models

McAfee®

Sensor Software Components		I-1400	I-1200
Stateful Traffic Inspection	IP Defragmentation and TCP Stream Reassembly	Yes	Yes
	Detailed Protocol Analysis	Yes	Yes
	Asymmetric Traffic Monitoring	Yes	Yes
	Protocol Normalization	Yes	Yes
	Advanced Evasion Protection	Yes	Yes
	Forensic Data Collection	Yes	Yes
	Protocol Tunneling	Yes	Yes
	Protocol Discovery	Yes	Yes
Signature Detection	User-Defined Signatures	Yes	Yes
	Real-time Signature Updates	Yes	Yes
Anomaly Detection	Statistical Anomaly	Yes	Yes
	Protocol Anomaly	Yes	Yes
	Application Anomaly	Yes	Yes
DoS Detection	Threshold-based Detection	Yes	Yes
	Self-Learning Profile-Based Detection	Yes	Yes
	Maximum DoS Profiles	120	100
Intrusion Prevention	Stop Attacks in Progress in Real Time	Yes	Yes
	Drop Attack Packets/Sessions	Yes	Yes
	Reconfigure Firewall	No	No
	Initiate TCP Reset, ICMP Unreachable	Yes	Yes
	Packet Logging	Yes	Yes
	Automated and User-Initiated Prevention	Yes	Yes
Encrypted Attack Protection	Stops Encrypted Attacks in Real Time	No	No
Internal Firewall	Blocks Unwanted and Nuisance Traffic	Yes	Yes
	Granular Security Policy Enforcement	Yes	Yes
High Availability	Stateful Failover	Yes	Yes
Management	Command Line Interface (Console)	Yes	Yes
	Manager Communication	Same for All Models	Same for All Models

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