McAfee IntruShield Network IPS Sensor

Pioneering and Industry-Leading, Next-Generation Network Intrusion Prevention Solution

The Challenge

The risks to enterprise and service provider security continue to grow, as the number of new vulnerabilities and the speed and sophistication of attacks seeking to exploit those vulnerabilities increase every year. The evolution of new hybrid attacks that use multiple vectors to breach the security infrastructure means that enterprises must defend themselves against a constantly shifting threat.

- *Dynamic Security Risks*—The dynamic nature of today's security threats means that new, hybrid attacks are increasing at an unprecedented pace. Network security gaps leave critical assets vulnerable and increase enterprise and service provider security risks
- *Inadequate Protection with Traditional Security Technology*—Despite significant security investments, enterprises remain vulnerable to sophisticated and *zero-day* attacks due to the inadequate ability of traditional technology to provide proactive threat detection and prevention
- *The Need for Proactive Risk Prevention*—Unfortunately, there is no single product that protects against all threats. To ensure comprehensive security, service providers and enterprises need to adopt a layered approach that delivers proactive risk prevention to accurately detect and block known and zero-day attacks before they inflict damage

The pioneering and proven McAfee® network intrusion prevention (IPS) solution delivers the most comprehensive, accurate, and scalable threat protection, helping enterprises and service providers assure the availability and security of their critical network infrastructure through proactive risk prevention.

The McAfee IntruShield Solution

McAfee IntruShield® network IPS delivers advanced realtime protection against known, zero-day (unknown), and encrypted attacks, as well as spyware. IntruShield delivers the most comprehensive, accurate, and scalable network IPS solution for a broad range of mission-critical environments. As part of the McAfee Protection-in-Depth™ Strategy, it delivers comprehensive and proactive intrusion prevention to protect business availability and critical network infrastructure by detecting and blocking attacks before they inflict damage. Through a full suite of aggregated platforms and solutions that scale from hundreds of Mb/s to multi-gigabit bandwidth rates, its broad protection extends from the network core to the edge and the branch office, and provides enterprise and carrier-class scalability in both large and small enterprise environments.

The innovative IntruShield architecture integrates patented signature, anomaly, and Denial of Service (DoS) analysis techniques, enabling highly accurate and intelligent attack detection and prevention up to multi-gigabit speeds. This unprecedented harnessing of innovative technologies protects even the most demanding networks from the threat of known, zero-day (unknown), and DoS attacks, as well as spyware. IntuShield's next-generation technology delivers industry-first encrypted attack prevention and network IPS and internal network firewall integration, offering the most accurate and comprehensive protection available in the industry.

The IntruShield product family includes the IntruShield 4010, IntruShield 4000, IntruShield 3000, IntruShield 2600, IntruShield 1400, and IntruShield 1200—six powerful and purpose-built network IPS sensor appliances that provide the performance and functionality required to protect high-availability networks—and the IntruShield Security Management (ISM) system, a powerful and scalable security management solution.

Features and Benefits

Comprehensive Protection

- *Realtime Encrypted Attack Prevention*—Industry's first and only network IPS to protect against both clear-text and encrypted attacks, as well as spyware
- *Signature, Anomaly, and DoS Analysis*—Protects against known, zero-day, and DoS attacks
- *IPS and Internal Firewall*—Unprecedented internal system and network infrastructure threat protection and policy enforcement through converged network IPS and internal firewall capabilities
- *Integrated Network and Host IPS Protection*—Provides breakthrough integration by enabling host (McAfee Entercept®) and network (IntruShield) IPS security event aggregation and coordination on a single IntruShield Manager console
- *High-Availability Deployment Options*—Enables virtualization and unmatched proactive IPS protection for broad range of high-availability environments

Accurate Protection

- *Depth-of-Analysis*—IntruShield's purpose-built platform enables stateful traffic analysis by providing thorough parsing of more than one hundred protocols, over 3,000 high-quality multi-token/multi-trigger signatures, and advanced evasion resistance to deliver unmatched accuracy for mission-critical, in-line prevention
- *Virtual IPS and Internal Firewall*—IntruShield's unique virtualization capability extends to both IPS and internal firewall, enabling highly customized and granular security policies for a dramatic reduction in false positives
- *Intrusion Intelligence*—Powerful capabilities provide detailed, accurate, and reliable information related to intrusion identification, relevancy, direction, impact, and analysis

Scalable and Manageable

- *Enterprise-Wide Scalability*—Through a full suite of solutions that scale from hundreds of Mb/s to multi-gigabit bandwidth rates, IntruShield's broad protection extends from the network core to the edge and the branch office and provides mission-critical solutions with proven scalability for all enterprise environments
- *Flexible Deployment*—Unprecedented flexibility of IPS or IDS deployment—including In-Line, Port Clustering, high-availability, Span, and Tap Modes—to suit any network security architecture
- *Automated Realtime Threat Updates*—Innovative, automated process delivers realtime, enterprise-wide signature updates without requiring sensor reboots and provides protection against newly discovered vulnerabilities while eliminating manual updates and network downtime

Comprehensive Threat Prevention

As part of the McAfee Protection-in-Depth Strategy, IntruShield delivers comprehensive intrusion prevention solutions that protect both internal and external network infrastructure from a broad range of threats and attacks—spanning from the network core to the edge and the branch office. By combining broad network environment protection with unprecedented threat prevention technologies—including encrypted attack prevention and internal firewall integration—IntruShield redefines intrusion prevention with the most comprehensive protection from known, zero-day, and encrypted attacks, as well as spyware.

Encrypted Attack Prevention

Information that requires protection via SSL is critical by nature. In today's dynamic threat environment, HTTP is

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 2Gb/s 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 2Gb/s 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 1Gb/s performance

one of the most popular protocols for attackers due to its open availability. Not only is it important to protect the sensitive data that resides on the Web server itself, but modern e-commerce sites typically access information stored on database servers that live at the very core of the network.

Protecting SSL-enabled infrastructure is critical in order to safeguard local Web server data and help prevent potential attack channels into the heart of the trusted network. IntruShield's breakthrough intrusion prevention technology provides comprehensive network protection against both clear-text and encrypted attacks. Its revolutionary ability to decrypt and inspect SSL traffic dramatically increases network security coverage by proactively detecting and blocking encrypted threats.

- *SSL Traffic Inspection*—IntruShield's hardware-accelerated SSL inspection technology allows the sensor to copy, decrypt, and inspect the SSL data stream using the securely stored SSL private key. After converting the SSL data stream into clear text within the sensor, traffic is inspected by IntruShield's protocol and application anomaly, statistical DoS, and signature matching engines. If an alert is not triggered, the original encrypted packet is forwarded with minimal delay
- *SSL Encrypted Attack Prevention*—IntruShield's encrypted threat protection proactively blocks encrypted threats by dropping malicious packets upon detection of an attack
- *SSL Security Forensics*—The IntruShield sensor can be configured to capture and store clear text copies of SSL alert packets on the IntruShield manager. Captured packets are transmitted between the sensor and the manager via an encrypted connection
- *Uncompromising SSL Key Security*—Protection of the SSL private key is vital. In order to ensure private key confidentiality and integrity, the key is securely exported to the IntruShield Manager in encrypted format. The IntruShield Manager re-encrypts the private key with the sensor's public key for local storage. While performing SSL traffic inspection, the IntruShield sensor securely stores the SSL private key in volatile memory, ensuring that no unencrypted copies of the key are permanently stored on the system

IPS and Internal Firewall

Today's firewalls offer perimeter protection. IntruShield pioneers next-generation technology by integrating internal firewall capabilities and network IPS on a single purpose-built platform to deliver industry-first internal network protection. The integration of IPS and internal firewall allows

The IntruShield 2600

The IntruShield 2600 (I-2600) 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 600Mb/s 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 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

for a higher level of protection, while delivering unmatched control, flexibility, and reduced cost of ownership.

IntruShield's virtualization technology extends to both network IPS and internal firewall capabilities. This enables customers for the first time to implement a virtual perimeter around critical resources, delivering an added layer of protection to guard against attacks that successfully penetrate perimeter firewalls or that originate internally. Highly granular virtual perimeters can protect a network segment, a collection of hosts, or even a single system with a unique policy.

Signature, Anomaly, and DoS Analysis

IntruShield's patented and integrated signature, anomaly, and DoS analysis delivers anti-spyware and broad protection against known, zero-day, and DoS attacks. The *Depth-of-Analysis* section provides additional details on this topic.

Integrated Network and Host IPS Protection

McAfee's IPS provides unprecedented integration of its IntruShield network IPS and Entercept host IPS products. Integrated host and network IPSs provide the most comprehensive IPS protection available in the industry, encompassing servers, desktops, and laptops, as well as the network core and edge.

Unprecedented Detection Accuracy

In today's dynamic threat environment, detection accuracy is critical to network operators. Although false positives from a network IDS may result in unnecessary alerts and create an annoyance for operators, false positives from a network IPS are more critical due to the fact they can result in the blocking of legitimate network traffic. IntruShield's highly accurate attack detection forms the foundation for the most accurate attack prevention solution for today's demanding, mission-critical, in-line IPS deployments.

Depth-of-Analysis

IntruShield delivers unparalleled protection against spyware, as well as known, zero-day, and DoS attacks by integrating stateful signature, anomaly, and DoS statistical analysis for both clear-text and encrypted malicious traffic. IntruShield's stateful traffic analysis and session state maintenance for up to 1 million sessions, as well as its thorough parsing for over one hundred protocols, form the foundation for comprehensive signature, anomaly, and DoS analysis.

Signature Detection and Prevention

IntruShield sensors offer powerful signature analysis to accurately guard against known attacks. Over 3,000 IntruShield signatures are written to protect against known vulnerabilities. By focusing on vulnerabilities as opposed to individual exploits, IntruShield can often detect variations of attacks without requiring new signatures.

- *Stateful Signature Detection Engine*—IntruShield sensors employ a patented stateful signature detection engine. This enables context-sensitive signature detection, leveraging state information within data packets, utilizing multiple token matches, and detecting attack signatures that span packet boundaries or are in an out-of-order packet stream
- *Signature Specification Language*—IntruShield sensors utilize a proprietary, high-level Signature Specification Language. The IntruShield architecture de-couples signatures from the sensor software, enabling quality signatures to be made available with a quicker turnaround
- *Realtime Signature Updates*—IntruShield sensors benefit from an innovative realtime signature update process, where new signatures are automatically pulled by the IntruShield Manager software at the customer site. Based on policy configuration, these signatures can be pushed from the IntruShield Manager to sensors automatically in real time. IntruShield sensors dynamically utilize the latest signatures without requiring reset or reboot for uninterrupted attack protection
- *User-Defined Signatures*—Sensors also leverage custom signatures that users can easily create through IntruShield Manager's intuitive graphical user interface

Anomaly Detection and Prevention

IntruShield's anomaly detection functionality can identify sophisticated zero-day and unknown attacks, significantly improving attack detection rates.

- *Statistical, Protocol, Application Anomalies*—Sensors offer comprehensive anomaly detection by employing statistical, protocol, and application anomaly detection techniques
- *Buffer Overflow Detection*—More than half of new exploits today are buffer overflow attacks. IntruShield's anomaly detection techniques are effective in protecting against this major threat source

Denial of Service Detection and Prevention

IntruShield offers unprecedented accuracy and granularity for DoS detection and delivers the response actions needed to proactively block attacks.

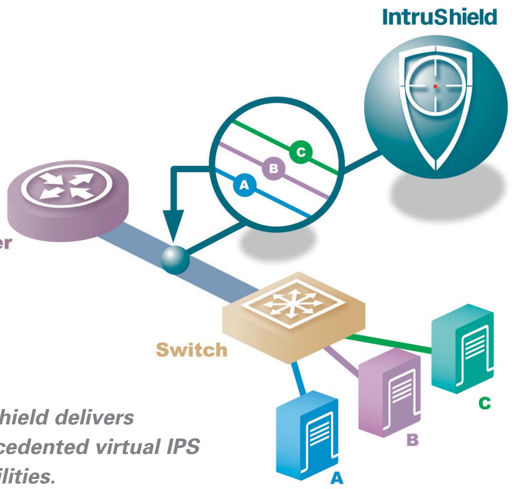
- *Self-Learning Profiles and Threshold-Based Detection*—Sensors offer threshold-based detection as well as self-learning, profile-based DoS detection that uses a patented algorithm to separate even low volumes of attack traffic from large volumes of legitimate traffic

- *Highly Granular DoS Detection*—Sensors deliver unparalleled granularity in DoS detection using profile-based techniques. A profile can be created for a range of IP addresses or even an individual host, and the IntruShield architecture supports several hundred profiles per sensor. Any deviation from normal traffic behavior flags a DoS condition. If a single host/subnet downstream to a gigabit network link comes under attack—with even a couple of Mb/s of traffic—a sensor's granular DoS detection can spot the attack

Virtual IPS and Internal Firewall

IntruShield sensors support an innovative and powerful virtualization concept to segment a single IntruShield sensor into and up to 1,000 virtual sensors, each of which can be completely customized with a granular security policy—including individualized attack selection and associated response actions. A virtual sensor can be defined based on a block of IP addresses, one or multiple VLAN tags, or by specific port(s) on a sensor.

Virtualization is available for both IPS and internal firewall functionality. The breakthrough integration of virtual IPS and internal firewall capabilities empowers enterprises to extend perimeter-grade protection internal to the network. IntruShield enables highly granular security policies for individual network segments, a collection of hosts, or even singular hosts. This allows for the creation of a Virtual Perimeter for protected segments or hosts. IntruShield's Virtual Perimeter technology delivers the industry's first internal network security solution. It mitigates security risks and delivers unprecedented protection for those internal networks that are often left vulnerable due to no or limited security policy enforcement.



IntruShield delivers unprecedented virtual IPS capabilities.

Virtualization capability allows security professionals to implement and enforce a heterogeneous set of security policies with a single IntruShield sensor. Such flexibility allows organizations to effectively meet differing security needs, or allows service providers to offer customized security solutions and SLAs to multiple customers. As well, virtualization further reduces the total number of devices required for a network-wide deployment and reduces total cost of ownership.

Intrusion Intelligence

The dynamic nature of today's security threats means that new, hybrid attacks are increasing at an unprecedented pace. In order to detect and block known and zero-day attacks before they inflict damage, enterprises and service providers need to adopt a strategy of proactive risk prevention. IntruShield's Intrusion Intelligence™ delivers unique features to analyze key characteristics of known and zero-day threats and intrusions. This unprecedented set of features delivers detailed, accurate, and reliable information related to intrusion identification, relevancy, direction, impact, and analysis. This allows carriers and enterprises to migrate from reactive intrusion detection to proactive intrusion prevention to stop attacks before they reach their intended targets.

Enterprise-Wide, Carrier-Class Scalability and Manageability

IntruShield provides unparalleled scalability and manageability to meet the needs of diverse enterprise, carrier, and service provider environments. Through a full suite of aggregated platforms and solutions that scale from hundreds of Mb/s to multi-gigabit bandwidth rates, IntruShield's broad protection extends from the network core to the edge and the branch office and provides mission-critical solutions with proven scalability in all network environments.

Enterprise-Wide Protection

The multi-gigabit performance of the IntruShield 4010 and 4000 sensors makes them suitable for deployment at logical traffic aggregation points at the core of the enterprise network, in data centers or at service provider networks. By deploying sensors in front of the server farm, users can leverage the IntruShield Virtual IPS capability to monitor each aggregation point with multiple customized security policies. What's more, the sensor's high-availability deployment option—using stateful failover between two sensors without requiring any external hardware—provides operational redundancy, prevents any single point of failure, and offers uninterrupted IPS protection. The IntruShield 3000, with up to 1Gb/s performance, also provides a compelling price-performance solution for core network, carrier, and service provider deployments. Both the IntruShield 3000 and IntruShield 4010 offer the industry's highest Gigabit port-density network IPS appliance. The IntruShield 2600, with its Fast and Gigabit Ethernet interfaces, offers a flexible solution for the perimeter of enterprise networks. The IntruShield 1400 delivers a scalable solution for mid-size, branch, and remote offices and the perimeter of enterprise networks. The IntruShield 1200 delivers a scalable solution for mid-size, branch, and remote offices of enterprise networks.

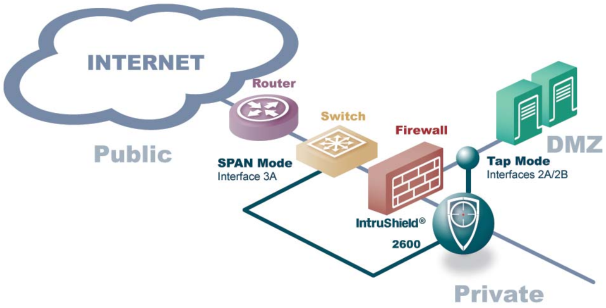
Multi-Gigabit Performance

IntruShield sensors are powered by programmable security-focused hardware. Intrusion detection and prevention are extremely computing-intensive applications, requiring eight to ten times the processing power of a firewall. Specialized silicon is used to speed up almost every function with orders of magnitude improvements in repetitive tasks such as protocol analysis, statistical analysis, string matching, and virtualization. As a result, IntruShield sensors can support thousands of signatures at wire-speed traffic rates without any packet loss, while protecting against known, zero-day, and DoS attacks, as well as spyware. IntruShield delivers compelling price/performance for bandwidth needs ranging from tens of Mb/s to 2Gb/s.

Flexible Deployment

IntruShield's flexible network deployment enables unmatched threat protection for a broad range of mission-critical network environments, including In-Line, Port Clustering, high-availability, SPAN, and TAP modes. In addition, IntuShield delivers comprehensive infrastructure protection for network routers, switches, VPNs, and gateways.

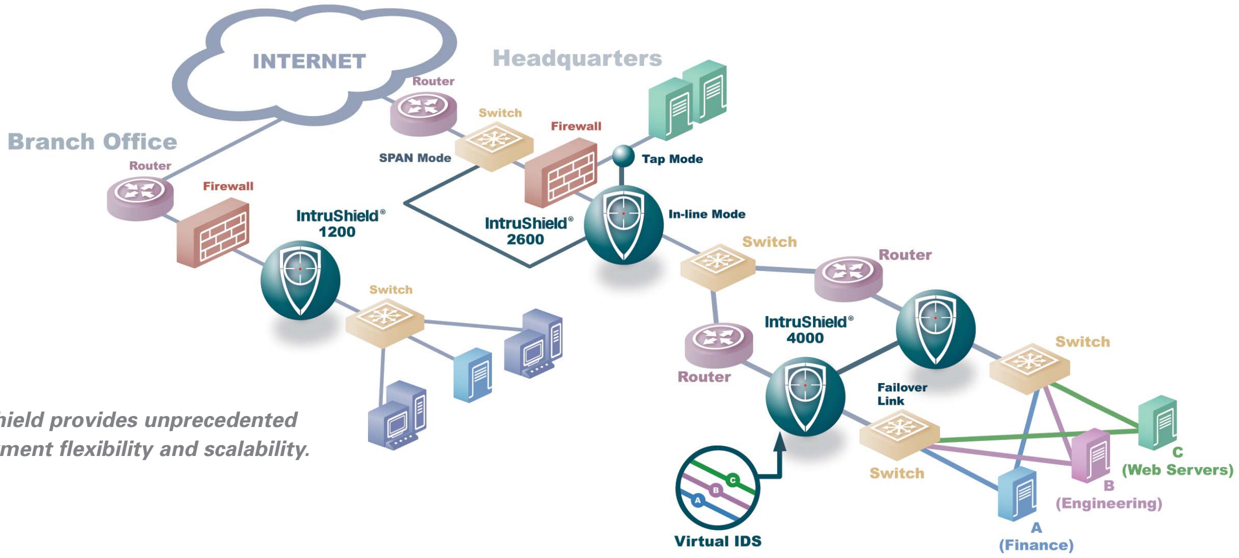
- *In-Line Mode*—IntruShield sensors sit in the data path with active traffic passing through them, mediating the flow of traffic, and dropping malicious packets—based on granular policy—before they reach their intended targets. Wire-speed performance and highly reliable operation prevent IntruShield sensors from becoming bottlenecks
- *Port Clustering*—Port Clustering, or interface grouping, enables traffic monitored by multiple ports on a single system to be aggregated into one traffic stream for stateful intrusion analysis
- *High Availability with Stateful Failover*—IntruShield sensors support high-availability IPS deployments using stateful sensor failover between two sensors, avoiding a single point of failure
- *SPAN and Tap Modes*—The sensor can monitor hubs or the SPAN ports of multiple switches and can inject several response actions, such as TCP resets to terminate malicious connections through the monitoring port itself. In Tap Mode, full-duplex monitoring allows a complete direction-sensitive view of network traffic, enabling stateful analysis of traffic. Dedicated response ports enable indirect response actions, such as initiating TCP resets to terminate malicious connections



Realtime Intrusion Prevention

No security solution is complete unless it can actually stop attacks in real time. Accurate detection is the foundation for the complete set of realtime intrusion prevention options available with IntruShield sensors. These attack response options enable IntruShield sensors to be integrated into network environments with a full spectrum of security policies, ranging from realtime notification to complete blocking of attacks in progress. Upon detecting an attack, IntruShield sensors can: thwart an attack in progress by dropping or blocking a single packet or session; initiate TCP resets or ICMP unreachable message through response ports; reconfigure firewalls to block offending traffic; trigger an alert to the IntruShield Manager; notify security professionals via e-mail, pager, and script alerts; and capture and log packets for detailed analysis. IntruShield offers a full spectrum of security policies even from a single sensor.

Integrated detection and prevention in a single product enable the flexibility to migrate from intrusion detection to intrusion prevention at a user-selected pace, while preserving enterprise and service provider technology investments.



IntruShield provides unprecedented deployment flexibility and scalability.

McAfee PrimeSupport

McAfee has pursued a strategy of providing best-of-breed technology for each type of security and performance management application—but the Protection-in-Depth Strategy is more than just deploying and implementing best-of-breed solutions today. Prevention is certainly our first priority, but inevitably, you will have to react to a problem.

The McAfee PrimeSupport® program is essential for making the most of your investment in McAfee System and Network Protection Solutions. McAfee's PrimeSupport team has all the right resources and is ready to deliver your needed service solution. PrimeSupport resources include: delivering authorization to access all available maintenance releases and product upgrades, access to a comprehensive suite of additional online self-support capabilities, live telephone support accessible 24/7/365, available assigned support account managers, and a range of software and hardware support solutions that can be tailored to meet your needs.

IntruShield Sensor Specifications

Sensor Hardware Components	*I-4010*	*I-4000*	*I-3000*	*I-2600*	*I-1400*	*I-1200*
Network Location	Core	Core	Core	Perimeter	Branch Office/Perimeter	Branch Office
PerformanceThroughput	Up to 2Gb/s	Up to 2Gb/s	Up to 1Gb/s	Up to 600Mb/s	Up to 200Mb/s	Up to 100 Mb/s
Concurrent Session State Maintenance	1,000,000	1,000,000	1,000,000	250,000	80,000	40,000
Ports						
Gigabit Ethernet Detection Ports	12	4	12	2	—	—
Fast Ethernet Detection Ports	—-	—-	—	6	4	2
Dedicated Fast Ethernet Response Ports	2	2	2	3	1	1
Dedicated Fast Ethernet Management Port	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 Fast Ethernet Ports)	Yes	Yes
Fail-Open	Optional	Optional	Optional	Yes (for Fast Ethernet 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 Fast Ethernet Ports)	Yes	Yes
In-Line Mode	Yes	Yes	Yes	Yes	Yes	Yes
Port Clustering	Yes	Yes	Yes	Yes	Yes	Yes
No. of Virtual 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)	No	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)	1RU Rack-Mountable 17.32 (W) x 1.69 (H) x 17.64 (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	47lbs.	47lbs.	47lbs.	28lbs.	17lbs.	15lbs.
Power	100-240VAC (50/60Hz)	Same for All Models	Same for All Models	Same for All Models	Same for All Models	Same for All Models
Power Consumption	350w	350w	350w	250w	100w	100w
Temperature	0° to 40° C (Operating) -40° to 70° C (Non-operating)	Same for All Models	Same for All Models	Same for All Models	Same for All Models	Same for All Models
Relative Humidity (non-condensing)	Operational: 10% to 90% Non-operational: 5% to 95%	Same for All Models	Same for All Models	Same for All Models	Same for All Models	Same for All Models
Altitude	0 – 10,000 feet	Same for All Models	Same for All Models	Same for All Models	Same for All Models	Same for All Models
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.	Same for All Models	Same for All Models	Same for All Models	Same for All Models	Same for All Models
EMI Certification	FCC Part 15, Class A (CFR 47) (USA) ICES-003 Class A (Canada), EN55022 Class A (Europe), CISPR22 Class A (Int'l)	Same for All Models	Same for All Models	Same for All Models	Same for All Models	Same for All Models

Sensor Software Components		*I-4010*	*I-4000*	*I-3000*	*I-2600*	*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
	Realtime 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
	DoS Profiles	3,000	3,000	3,000	500	128	64
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 Fast Ethernet 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

McAfee® products denote years of experience and commitment to customer satisfaction. The McAfee PrimeSupport® team of responsive, highly skilled support technicians provides tailored solutions, delivering detailed technical assistance in managing the success of mission-critical projects—all with service levels to meet the needs of every customer organization. McAfee Research, a world leader in information systems and security research, continues to spearhead innovation in the development and refinement of all our technologies.