McAfee Intrusion Prevention System

IntruShield 1200 and 1400 Appliances—Pioneering and Industry-Leading, Next-Generation Network Intrusion Prevention Solutions

Features and Details

What Is Intrusion Prevention?

Intrusion prevention is the discovery of, and response to, unauthorized action undertaken with the intent of hindering, damaging, incapacitating, or breaching the security of your network. An intrusion prevention system (IPS) detects and responds to attempted intrusions into a system or network, and complements firewalls or anti-virus software by thoroughly inspecting the contents of network packets and analyzing for attacks embedded within what a firewall might perceive as seemingly benign network traffic.

The McAfee® IntruShield® IPS system combines high-performance network sensor appliances with next-generation detection techniques to provide deep packet inspection in real time at wire speed. When malicious activity is detected, IntruShield provides a variety of custom responses based on the attack. These actions range from logging the event and sending an alert, to blocking the attack packets so they never reach their intended target.

What Is IntruShield?

IntruShield is the industry’s first architecture that delivers realtime network intrusion prevention and takes IPS to a new level. The IntruShield IPS System is an integrated hardware and software platform based on the IntruShield architecture. The IntruShield IPS delivers comprehensive protection from known, zero-day or first strike, encrypted and denial of service (DoS) attacks, as well as spyware—all in real time and at multi-gigabit speeds.

IntruShield also provides the flexible management capabilities needed to administer the varied security policies required for the individual departments, diverse geographies, and separate functions that make up global businesses, service providers, and vital government agencies.

What Components Comprise the IntruShield System?

The IntruShield System is a network-based IPS that combines network sensor appliances and management software for the accurate detection and prevention of known and zero-day attacks, spyware infiltration and communication, DoS attacks, distributed DoS (DDoS) attacks, and misuse. The IntruShield System consists of the following major components:

- The McAfee IntruShield sensor appliances
- The McAfee IntruShield Security Management System, with its Web-based graphical user interface
- The McAfee IntruShield Update Server (hosted at McAfee)

What Is the Advantage to Network-Based Intrusion Prevention?

A host-based IPS (HIPS) is concerned with what is happening on each individual computer or host and is able to detect such things as repeated failed access attempts or changes to critical system files. A network-based IPS (NIPS) examines all the individual packets flowing through your network. An NIPS like IntruShield is able to conduct stateful traffic and packet inspection in real time, thereby detecting maliciously crafted packets that are targeting your network. An NIPS is able to detect an attack and prevent it from reaching its intended target.

What Kinds of Threats Does IntruShield Detect?

Attacks can generally be summarized into three major categories:
McAfee Intrusion Prevention System
Pioneering and Industry-Leading, Next-Generation Network Intrusion Prevention Solution

- **Reconnaissance**—These include host sweeps, TCP or UDP port scans, e-mail recons, and possibly indexing of public Web servers to find cgi holes
- **Exploits**—Attackers take advantage of hidden features or bugs to gain access to the system. The attacks may be in either encrypted or unencrypted data. Nuisance programs like spyware may also be included
- **DoS Attacks**—In a DoS attack, the attacker attempts to crash a service (or the machine), overload network links, overload the CPU, or fill up the disk. The attacker does not always try to gain information, but to simply act as a vandal to prevent you from making use of your machine

Only IntruShield encompasses all of today’s next-generation IPS technology to allow customers to detect known attacks (using custom signatures), new/zero-day (using anomaly techniques), encrypted attacks (using advanced SSL decryption), and DoS attacks (using hybrid algorithms employing statistical and heuristic methods)—making it the most comprehensive IPS solution available today. The combination of these techniques significantly increases the capability and accuracy of the system, reducing false positives and false negatives. The majority of currently available IPS products are exclusively signature-based, and have little or no anomaly or DoS detection capabilities. In addition, IntruShield also detects attacks with unprecedented accuracy through:

- Full protocol analysis and state tracking with multi-trigger, multi-field pattern matching
- Hardware acceleration to deliver wire-speed detection and prevention
- Its ability to see all the traffic in a variety of deployment modes, including active/active, active/passive, and asymmetrically routed traffic environments

**Does IntruShield Provide Protection against Spyware?**

Intrushield provides a complement to its overall comprehensive threat protection by adding a set of spyware-specific signatures to combat the installation and communication of spyware programs—a problem that has become an increasing concern to enterprise security.

The extension of anti-spyware and other potentially unwanted programs (PUPs) signatures to the IntruShield IPS solution provides a beneficial and complementary overlap to McAfee's strong system protection solutions that provide the most comprehensive proactive protection in the industry against spyware and other PUPs, including adware, dialers, keyloggers, password crackers, and remote-control programs.

Although this is an enhancement to IntruShield’s comprehensive protection, malicious PUPs and applications are best defended at the host with McAfee’s Anti-Spyware Enterprise Edition Module for VirusScan® Enterprise 8.0i. Deploying complementary, multi-layered security solutions provides maximum network and system protection.

**Does IntruShield Provide Firewall Capabilities?**

Yes, IntruShield provides internal firewall capabilities that allow the enforcement of the organizations security policy by blocking traffic between network segments based on protocol or IP address.

**Does IntruShield Replace My Existing Internet Firewall?**

No, IntruShield is not intended to be a replacement for your existing perimeter firewall. IntruShield’s internal firewall technology is focused on providing policy enforcement for the internal segments of the network. By combining virtual IPS, intrusion prevention, and internal firewall capabilities within one system, IntruShield allows for the creation of virtual perimeters within the network. Virtual perimeters provide increased security for critical assets by creating hardened defense zones around critical assets that are located within the greater network.

**How Does a Virtual Perimeter Increase Security?**

Most networks today have extensive defenses—including perimeter firewalls, intrusion detection systems, etc.—deployed around the edges, or perimeter of the network to protect against outside threats. As networks grow to accommodate new demands such as VPN access, wireless access, etc., it is becoming more and more difficult to define—much less protect—all of the potential boundary points on a network. In addition, the majority of successful security compromises are initiated from within the network.
perimeter. Virtual perimeters are a new way of defining the security architecture of a network.

Instead of thinking of the network as a physical or geographic island with a distinct boundary that contains different assets of varying value, it recognizes that the security perimeter must be established around the assets themselves. This approach allows the appropriate level of protection to be applied for the value of the asset itself. A virtual perimeter may be established around a single server, a group of servers, a physical segment, or VLAN; whatever approach best suits the unique needs of the individual network.

Once a virtual perimeter is established around the appropriate asset, IntruShield allows you to tailor the level of protection appropriate to the value of the asset. This unique ability provides extremely focused and much more effective protection than the one-size-fits-all approach required by traditional physical perimeter solutions.

**What Is Virtual IPS and How Does It Benefit Me?**

Typically, IPS systems allow only one aggregate intrusion policy for the monitored network link or physical network segment. A virtual intrusion prevention system (VIPS) provides a flexible approach to protecting your network resources. You can create VIPS management domains for specific departments, geographic locations, or functions within an organization. VIPS significantly enhances the scalability of the IPS solution and allows for highly granular and flexible deployment options, while also enabling the delivery of customized security service offerings.

After establishing these domains you can flexibly define systems or assets and define unique security policies for each asset or groups of assets. With this approach, one IntruShield sensor can replace dozens of legacy IDS/IPS sensors. VIPS is the enabling technology for our virtual perimeter architecture and provides unmatched accuracy and control to the system.

**How Does IntruShield Detect Attacks?**

IntruShield has the most sophisticated and accurate attack detection capability available today. Attacks can only be effectively prevented if they can be reliably and accurately detected. IntruShield’s unparalleled accuracy is achieved using the following techniques:

**Signature Detection Techniques**—Systematically scan network traffic looking for signature patterns of known attacks, comparing these patterns against an extensive database of signatures. This method is very effective against existing attacks, but does not detect zero-day attacks exploiting unknown vulnerabilities.

**Anomaly Detection**—Utilizes protocol, statistical, and application anomaly detection to determine a deviation from normal behavior of network traffic or protocol specification to identify zero-day attacks.

**DoS Attack Detection**—Characterizes normal traffic using pre-programmed thresholds or realtime, self-learning distributions, and then using this data to detect what might constitute a maliciously excessive consumption of network bandwidth, host processing cycles, or other resources.

IntruShield is the only network IPS on the market today that effectively integrates all three of these detection methods, providing protection against the full spectrum of threats and vulnerabilities in a single purpose-built appliance. There are several advantages to combining multiple detection methods on one sensor. Uniting the three detection methods in one product improves the correlation of attack detection across the various methods, increasing the product’s accuracy and ability to effectively protect the assets on the network.

**Can IntruShield Protect against Internal Attacks?**

Yes. Companies and organizations often focus their attention on protecting themselves against external attacks, when in fact insider attacks are both most common and most dangerous.

Internal attacks present a unique security challenge since they are executed by people you have entrusted with authorized access to your network and who have privileged knowledge of the nature of your network and its architecture, including where your data is stored. By deploying and configuring effectively, IntruShield can help protect you against internal attacks by leveraging the following next-generation technologies:

**IntruShield’s Anomaly/DoS Learning Mode**—Enables you to learn day-to-day network activities, so that normal activity—such as accessing various services and servers—do not trigger attack warnings, only deviations in normal behavior generate an alert.

**IntruShield’s VIPS Feature**—Can monitor multiple network segments with custom policies that provide
protection for each specific environment, enabling you
to have one policy protecting your HR department, for
example, and another protecting your finance
department. A single sensor, capable of monitoring
multiple network uplinks, can provide protection for
multiple uplinks. What’s more, deployment in front of
the servers you want to protect provides unmatched
protection against internal attackers and deployment at
the perimeter deals with external attackers.

Does IntruShield Eliminate the Need for
Host IPS?
No, host and network IPS are complementary, not
competitive technologies. Both approaches are critical
components to the McAfee Protection-in-Depth™
Strategy. IntruShield provides full alert integration with
the award-winning McAfee Entercept® Host IPS to
provide a single, unified view of all the intrusion events
taking place on the network. The advanced system
protection afforded by Entercept Host IPS compliments
the McAfee virtual perimeter architecture and allows
customers to tailor the level of system protection
appropriate to the value of the asset.

Is IntruShield Easy to Install and Configure?
The IntruShield system can be easily installed in
minutes with just a few easy steps, including: installing
the Manager software on your Manager server,
positioning and powering on the sensor, configuring its
network information, adding the sensor to your
Manager configuration, and applying one of the
IntruShield-supplied, pre-configured policies. Your IPS
is then up and monitoring.

What Are the Benefits of Web-Based Access
to the IntruShield Security Management
System?
Secure Web-based access to the IntruShield Security
Management system empowers remote management
of a large number of sensors deployed throughout the
enterprise network. The complete set of tasks
associated with IPS configuration, policy, threat, and
response management functions can be performed
remotely, obviating the need for physical access to
Manager or sensor.

An intuitive Web interface enables security
administrators to install and operate both sensor and
Manager with minimal effort while providing powerful
advanced functionality for demanding users.

Centralized security administration allows users to
define, distribute, enforce, and audit heterogeneous
security policies in a scalable fashion.

How Do I Get Updates for Newly Discovered
Attacks?
For an IPS system to properly detect and protect
against malicious activity, it must be frequently updated
with the latest signatures and software patches
available. Thus, the McAfee team constantly
researches and develops signatures that combat the
latest exploits and attacks. When a new severe-impact
attack is discovered, McAfee will develop and release
a signature update. Since new vulnerabilities are
discovered almost on a daily basis, signature updates
are released twice a month or more frequently if
needed.

How Does Realtime Signature Update Work?
IntruShield sensors benefit from an innovative, realtime
signature update process in which new signatures
made available by McAfee are automatically pulled
from a master update server located at McAfee by the
IntruShield Manager at the customer site. Based on
policy configuration, these signatures can be pushed
by IntruShield Manager to sensors automatically and in
real time. IntruShield sensors dynamically utilize the
latest signatures without requiring reset or reboot, for
uninterrupted attack protection.

Is My Signature Policy Configuration Lost If a
Sensor Fails or System Software/Signature
Set Is Updated?
No, user-defined customized security policy
configuration—such as responses you want to take
when an attack is detected—persists in the IntruShield
Manager. Existing security policy configuration from
the failed sensor can be pushed to a new replacement
sensor in the event of a sensor failure. Customized
policy information is preserved through signature or
software updates as well.

Does IntruShield Support User-Defined
Signatures?
Yes. IntruShield enables users to define their own
signatures for detecting attacks. This process is
facilitated by an easy-to-use graphical tool within the
Manager interface. You can utilize specific fields and
data obtained through IntruShield’s protocol analysis
capabilities, or state information gathered via
IntruShield’s analysis mechanisms.
Using the graphical tool, you can define signatures and group them to define attacks you want to detect. You can use these custom attacks when you configure your security policies, applying them to specific resources and specifying responses when the attack is detected. These user-defined signatures and attacks are unaffected by signature update sets.

What Forensic Analysis Capabilities Are Provided?
IntruShield sensors capture and log packets prior, during, or subsequent to the attack and can redirect traffic to a spare system port for detailed forensic analysis. This captured packet information acts as a record of the actual flow of traffic that triggered the attack. When the data is viewed, it is converted to Libpcap format for presentation. Tools like Ethereal, a network protocol analyzer for UNIX and Windows®, can be used to examine the packet log data for more detailed analysis of the detected event.

I Have Administrators in Different Geographic Locations. How Can I Have Them Share Administrator Tasks Securely?
Security organizations usually are comprised of multiple individuals, and management of the overall system is generally delegated to different people according to some logical categorization—by department, by geographic location, by system (i.e., the e-mail servers, the Web servers), and so on. With IntruShield, you delegate the management of system components by organizing the components logically into admin domains and then granting various management privileges for the domains to your IntruShield users.

What Is a Sensor and How Does It Work?
Most vendors’ IPS sensors are software-based, single-port devices based on PCs or modified Ethernet switches. IntruShield sensors are next-generation devices, designed for performing the compute intensive task of intrusion prevention in real time. IntruShield sensors are high-performance, scalable, and flexible security appliances purpose-built for the accurate detection and prevention of known, zero-day, encrypted, and DoS attacks, as well as detection and protection from spyware.

IntruShield sensors have multiple monitoring ports, use hardware acceleration and a realtime OS to handle traffic at wire speed with improved system reliability.

The sensors efficiently inspect and detect intrusions with a high degree of accuracy, and are flexible enough to adapt to the security needs of any enterprise environment. The primary function of an IntruShield sensor is to analyze traffic on selected network segments and to respond when an attack is detected according to its configured policy. The sensor examines the header and data portion of every network packet, looking for patterns and behavior in the network traffic that indicate malicious activity. The sensor examines packets according to user-configured policies or rule sets that determine what attacks to watch for and how to react with countermeasures if an attack is detected. If an attack is detected, a sensor responds according to its configured policy(s).

Sensors can perform many types of attack responses, including generating alerts, resetting TCP connections, blocking traffic at firewalls, scrubbing malicious packets, and dropping packets entirely before they reach their target.

How Does Purpose-Built Hardware Help?
Network IPS is a very computation-intensive application. It requires about an order of magnitude higher computation power—compared to that of a firewall—to process the same network bandwidth. A purpose-built IPS hardware appliance empowers thorough stateful analysis at multi-gigabit speeds while thousands of signatures are turned on. A combination of signature, anomaly, and DoS analysis techniques—leveraging stateful analysis—boosts IntruShield’s attack detection accuracy. Finally, purpose-built hardware delivers IntruShield’s innovative VIPS and encrypted attack protection functionality.

What Is Stateful Analysis?
Stateful analysis offers network traffic analysis in the context of the protocol and application state. Unlike simple string or pattern matching, which many IPS systems employ, analyzing attacks in the context of the protocol or application state yields better accuracy of attack detection, improving false positives and false negatives.

What Networks Can IntruShield Sensors Monitor?
Both the I-1400 and the I-1200 appliances monitor Fast Ethernet network traffic at high speeds -- 100Mbits for the I-1200 and up to 200Mbits for the I-1400. These best-in-class appliances address the needs of small
and mid-size businesses, as well as branch and remote offices of larger organizations with a full suite of functionality at a price-point ideal for smaller networks.

With IntruShield’s unique Virtual IPS feature, each IntruShield sensor provides the capability of multiple sensors, delivering significant cost efficiencies on an ongoing basis. The I-1400 delivers 32 virtual IPS’ and the I-1200 delivers 16 virtual IPS’ that provide SMBs with the level of sophisticated flexibility and functionality found only in high-end appliances costing an order of magnitude higher than the IntruShield I-1200 and I-1400. Additionally, the Virtual IPS and Internal Firewall features, as well as the IntruShield advanced Management system, enable smaller enterprises to undertake granular, enterprise-wide security policy enforcement—something that is becoming increasingly important to SMBs as a result of increasing security threats and regulatory pressures.

IntruShield also supports High Availability with Stateful Failover—allowing stateful failover between two IntruShield appliances, thereby avoiding a single point of failure and assuring network and business availability for mission-critical environments.

In monitoring mode (i.e., either tap mode or SPAN/hub mode), a single IntruShield sensor can monitor the multiple network links of a high-availability network. Monitoring in-line, two IntruShield sensors with the same configuration (same model, cabling, signature set, and software release), can provide backup capabilities for each other, should one fail.

**Are IntruShield Sensors Reliable?**
IntruShield purpose-built sensors are extremely reliable. They have no internal hard disks and incorporate both redundant fans and redundant power supplies. Full Active-Active and Active-Passive High-Availability configurations are supported. IntruShield sensors are specifically engineered for the most demanding mission-critical enterprise, carrier, and service provider environments.