



Check Point IPS-1

Dedicated intrusion prevention for enterprise networks

Contents

Overview	3
Benefits of IPS-1	3
IPS-1 product overview	4
IPS-1 Sensors	5
Multi-mode deployment appliances with failover	5
Hybrid Detection Engine	6
Confidence Indexing	7
Enterprise-class IPS Sensors	7
Customizable signature language	7
IPS-1 Management Server	8
Dynamic Shielding Architecture	8
IPS-1 Management Dashboard	8
Threat-profile views	9
Scalable, centralized management	9
Forensic analysis	10
Vulnerability management	10
Reporting and correlation	11
Conclusion	12

Overview

Even as security managers have focused on securing enterprise networks, new threats continue to emerge. Today, organizations face the challenge of protecting against new waves of attacks with increasing complexity and capability. Protecting against these rising threats is challenging due to a number of factors.

First, many of the attacks today use advanced techniques of self-propagation to infect more efficiently and rapidly. This means that Zero Day attacks are more prevalent and problematic than ever before.

Second, attackers are bypassing conventional firewall policies by utilizing many of the common protocols (HTTP, SMTP) as channels of attack into an organization. Many of these attacks can be carried as part of the payload and often are carried out at the application level. Detecting these attacks requires capabilities like deep packet inspection and protocol analysis.

Finally, with myriad new applications being deployed in the enterprise, security managers often find themselves struggling to keep up. In fact, many newer applications like instant messaging (IM) or Voice over Internet Protocol (VoIP) can be used in an unofficial, unregulated manner by users, making the security team's task of protecting against potential threats even more difficult. Sheer numbers of applications combined with multiple attack vectors means that actually preventing attacks, rather than simply detecting attacks, becomes vital.

Bottom line, securing the enterprise is challenging and complex. Traditional firewalls, virtual private networks (VPNs), and antivirus software are a critical part of any security infrastructure, but they are insufficient in addressing today's security challenges. Intrusion prevention systems (IPS) are not only important but a necessity for the corporate security architecture. This white paper describes the benefits and product capabilities of the Check Point IPS-1™ intrusion prevention solution in addressing enterprise network security.

Benefits of IPS-1

Check Point IPS-1 is the leading solution for dedicated enterprise-scale intrusion prevention. It delivers the following critical benefits in securing the enterprise network:

- **Superior detection**—IPS-1 offers superior detection through the core Hybrid Detection Engine™. This core detection engine enables precise, accurate detection with a low false-positive rate
- **Inline prevention from edge to core**—IPS-1 delivers the broadest range of prevention, ranging from inline rates of 50Mbps to 2Gbps. A 10Gbps product is planned for 2007
- **Enterprise-ready intrusion prevention**—The IPS-1 Management Dashboard provides multiple views into the threat profile of the enterprise. It also offers enterprise management capabilities like “lights out” remote installations/upgrades and automatic signature updates to ensure low-touch manageability. Furthermore, IPS-1 offers scalability and reliability suitable for remote/branch offices and large-scale enterprise deployments

- **Dynamic Shielding Architecture™**—Through its core Dynamic Shielding Architecture, IPS-1 receives endpoint profiling information, performs analysis, and dynamically initiates actions in accordance with the current network profile
- **IPv6 readiness**—IPS-1 fully supports IPv6 networks. This means that future migration to this next-generation Internet protocol will be seamless. It also ensures that any attacks currently obfuscated by channeling through IPv6 will be detected and prevented

IPS-1 product overview

The IPS-1 product is designed for enterprise-scale intrusion prevention through a multi-tiered architecture that delivers unparalleled scalability and reliability. The product architecture is shown below in Figure 1.

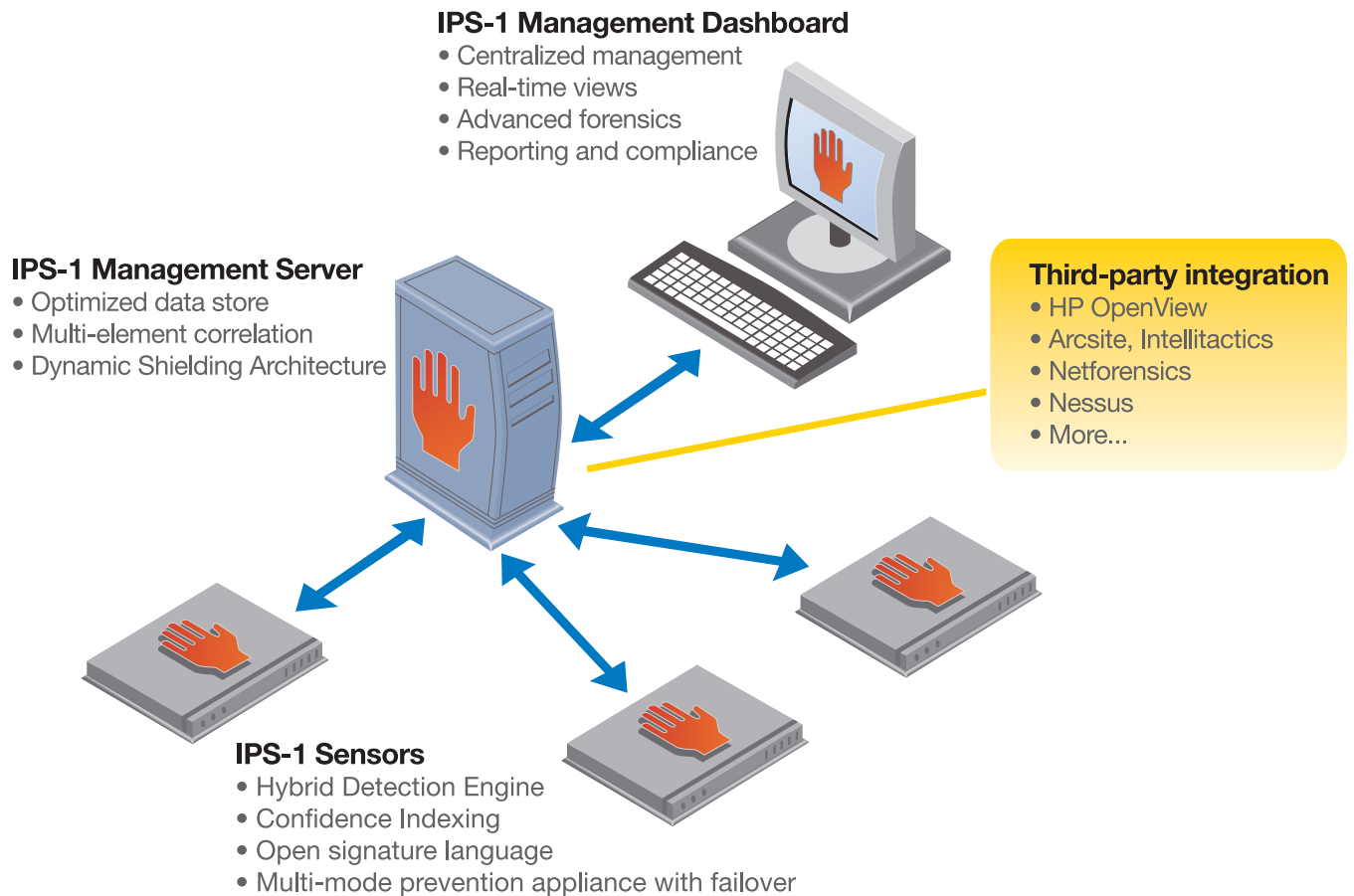


Figure 1. IPS-1 product architecture

The IPS-1 product architecture is composed of three primary components:

- IPS-1 Sensors
- IPS-1 Management Server(s)
- IPS-1 Management Dashboard

Through the multi-tiered product architecture, IPS-1 delivers true scalability for enterprise intrusion prevention. There is a many-to-one relationship between IPS-1 Sensors and the IPS-1 Management Server (i.e., several IPS-1 Sensors may be linked to one IPS-1 Management Server). Accordingly, there is also a many-to-one relationship between an IPS-1 Management Server and a single IPS-1 Management Dashboard (i.e., several IPS-1 Management Servers may be linked to one IPS-1 Management Dashboard).

IPS-1 architecture also offers the benefit of failover functionality to ensure that any unlikely failure of components will not result in impeding network or security operations. For example, secondary IPS-1 Management Servers may be configured redundantly to primary servers. In the event that the primary IPS-1 Management Server fails, the sensors will switch to the secondary servers. Also, all sensors have built-in failover mode that enables pass-through of network traffic if the sensor fails.

IPS-1 Sensors

IPS-1 Sensors offer deep packet inspection of network traffic and combine line-speed performance with accurate detection. IPS-1 offers a complete line of IDS/IPS sensors to meet performance needs from the low-end to high-end multi-gigabit data rates.

IPS-1 Sensor Model	Data Rate IPS/IDS	PS/IDS Networks
IPS-1 Sensor 50C	50/75Mbps	3 total ports for 1 IPS or 3 IDS
IPS-1 Sensor 200C/F	200/250Mbps	3 total ports for 1 IPS or 3 IDS
IPS-1 Sensor 500C/F	500Mbps/1Gbps	4 total ports for 2 IPS or 4 IDS
IPS-1 Power Sensor 1000C/F	1/2Gbps	8 total ports for 4 IPS or 8 IDS
IPS-1 Power Sensor 2000C/F	2/4Gbps	8 total ports for 4 IPS or 8 IDS

The following section describes key security features of the IPS-1 Sensors:

Multi-mode deployment appliances with failover

IPS-1 may be deployed in three different modes—Passive Intrusion Detection Mode, Inline Bridge Mode (also known as Learning Mode), and full Inline Prevention Mode.

- **Passive Intrusion Detection Mode**—as the traditional intrusion detection mode, Passive Intrusion Detection Mode receives traffic off a span port or tap. In this mode, IPS-1 is not inline but receives a copy of the traffic for attack-detection analysis and will raise alerts accordingly
- **Inline Bridge Mode**—when deployed in Inline Bridge Mode (also known as Learning Mode), IPS is deployed inline but it does not actually prevent attack traffic when detected. Instead, it allows all traffic to pass yet raises an alert as if it were in Passive Detection Mode. This mode enables a transition step from detection to prevention where the user may observe the effectiveness of IPS-1 running inline, detecting attacks, and without actually dropping any detected attack traffic. This mode is also useful for the network management team to assess the device's resiliency for placing it in full Inline Prevention Mode
- **Inline Prevention Mode**—IPS-1 is a fully functional intrusion prevention system when deployed in full Inline Prevention Mode. It will prevent malicious traffic when detected

In addition, IPS-1 Sensors have built-in failover capabilities. By simply pointing and clicking, security managers can define whether the sensor will fail unsevered or severed in the event of a power loss or other catastrophic failure. The fail unsevered mode means that when the sensor fails, network traffic will continue to pass through, ensuring network integrity and business operations. This typical default mode ensures continued operations of the network with no impediment or loss of traffic. The fail severed mode results in no pass-through of network traffic. Using this mode enforces a policy that security is more important than traffic flow.

Hybrid Detection Engine

Since effective intrusion prevention is predicated on accurate detection, the most important feature of the IPS-1 Sensors revolves around the Hybrid Detection Engine, which utilizes multiple detection and analysis techniques to detect and defend against potential threats. Some of the key analysis and detection techniques are:

- Exploit-based signatures—detect a known threat by providing a signature match against characteristics of a specific exploit
- Vulnerability-based signatures—detect a potential threat before the release of a known exploit by providing signature validation against a vulnerability's characteristics. This is effective against Zero Day attacks
- Policy-based signatures—detect violations of security policy, including misuse and anomalies
- Protocol validation—protect against Zero Day attacks by detecting anomalies to protocol specifications and usage
- Passive operating system fingerprinting—determines the operating system (OS) of the target host to drive a unique feature known as Smart Reassembly, which enables automatic IP packet reassembly based on the target host's OS. Since each OS may reassemble fragments differently, attackers can take advantage of this difference to launch fragmented attacks that can bypass typical detection methods. IPS-1 uses these fingerprinting to detect such hidden attacks
- Multi-element correlation—detects topologically discrete events that are otherwise similar and raises them as a higher level correlated alert. For example, multiple scans and attack attempts levied across a geographically distributed network, all from the same source IP address will be detected, alerted, and blacklisted, depending on policy
- Dynamic worm mitigation—utilizes statistical alert behavior to identify and automatically quarantine rapidly, self-propagating Zero Day worms

Accurate detection isn't just about detecting attacks. It also involves reducing or eliminating false-positives. As previously noted, IPS-1 has built-in OS fingerprinting. When this feature is turned on, it can be used to minimize false-positives. When IPS-1 detects a potential attack directed to a specific host, it will cross-reference against the host profile to determine if the host is actually vulnerable to the attack. For instance, if a Windows-based attack is directed at a Linux machine, IPS-1 can be configured so that a visual alert is not raised. False-positives are minimized, and administrators are not overwhelmed analyzing attacks that have no material effect on potential targets.

Alert flood suppression is another IPS-1 tool that can make your security team more effective and efficient. In the event of a widespread attack, security managers are often inundated with a flood of essentially identical alerts. This makes it difficult, if not impossible, for security managers to sift through the volume of alerts in a reasonable amount of time. Alert flood suppression will suppress similar alerts with identical source/destination addresses within a specified time window, consolidating that information into a summary alert, eliminating alert flooding.

Confidence Indexing

One of the unique capabilities of IPS-1 is a patent-pending feature known as Confidence Indexing™, which is particularly useful in lowering false-positives in an inline prevention deployment by providing the ability to regulate the level of prevention based on a “confidence score.”

Through Confidence Indexing, IPS-1 associates a confidence score with every event detected. This score indicates the level of assurance that the detected event is a legitimate attack. In the case of a definite signature match, the assigned score may be 90 percent or more, indicating a high level of confidence of malicious traffic. Where there is a potential protocol violation or misuse, the confidence score may be lower, indicating that the protocol violation may be benign and not an indication of attack.

Depending on the risk tolerance of the organization, the administrator can then set IPS-1 to block all detected attacks that have a 90 percent score or higher. This minimizes the risk of false-positives in inline prevention mode and allows the user to regulate the level of prevention appropriate to the organization’s risk profile.

Enterprise-class IPS Sensors

With products that offer from 50Mbps to 2 Gbps throughput, IPS-1 provides a performance range suitable for the smallest organizations to the largest corporations.

As previously mentioned, all sensors come with built-in pass-through failover, ensuring that in the unlikely event of failure, a network interruption will not ensue. Furthermore, IPS-1 Power Sensors (all sensors delivering more than 1 Gbps inline throughput) also offer enterprise functionality with redundant main components such as power supplies, fans, drives, processors, and ports. And IPS-1 Power Sensor main components are hot-swappable, making field service very simple and efficient.

Customizable signature language

IPS-1’s signatures and signature language, called N-Code, is open and available for customers to modify as well as to write their own signatures. Although most customers depend on Check Point to supply signatures, in some cases, there may be a need or desire to modify the signatures to address specific requirements of the organization. At other times, a corporation may employ applications with specific, custom protocols that require deep packet inspection and protocol validation. In these instances, having the option to use this powerful scripting signature language to design effective custom signatures for Check Point’s IPS-1 will prove invaluable.

IPS-1 Management Server

IPS-1 Management Server provides data management services for IPS-1. It consists of an optimized, high-performance database where alerts from sensors are stored. Each IPS-1 Management Server can support several IPS-1 Sensors depending on the data rate, the configuration profile, and type of network traffic.

Dynamic Shielding Architecture

The IPS-1 Management Server encapsulates the core of the Dynamic Shielding Architecture, which leverages profiled host information to proactively protect the network. Dynamic Shielding Architecture works as follows:

- Receives host- and network-profiled information, either from active scanning tools like Nessus or passive scanning tools like the Dynamic Network Protection component
- Cross-references that information against the configured signature profiles for IPS-1 and determines appropriate action
- Takes actions, which could range from automatic updates of signature profiles and with the release currently in development, the ability to quarantine a compromised machine

For example, XYZ Corp. has a policy to only run hardened Apache Web servers. As such, the protection profile is configured with that assumption: i.e., Apache signatures are installed. However, shortly after configuration, a rogue Microsoft IIS server is set up in the accounting department—without permission—to run a departmental intranet. Once the rogue server is detected by active network scanning (currently Nessus), the Dynamic Shielding Architecture will drive IPS-1 to:

1. Display an alert to inform the security team of the network change
2. Display an alert of the policy violation (an IIS Web server is a violation of the Apache-only HTTP-server policy)
3. Cross-reference the signature protection profile and determine that the current configuration does not include signatures for IIS and will automatically update the protection profile by pushing IIS signatures out to the sensors

These actions notify the security team of the violation, while providing the best available protection against the rogue server being exploited until the security team has time to investigate the server deployment to determine who deployed it and why.

This proactive adaptation of the protection profile relative to the changing dimensions of the security environment ensures much broader network security than what a standard, static IDS/IPS deployment provides.

IPS-1 Management Dashboard

IPS-1 Management Dashboard provides the user interface to enable the management of an IPS-1 deployment. There are notable differences between the IPS-1 Management Dashboard and standard user interfaces of other intrusion prevention products. Among the key differences are the following features of IPS-1 Dashboard:

Threat-profile views

IPS-1 Dashboard is designed to monitor the security profile of the organization, rather than simply monitor alerts. Besides the standard alert management view common to many IPS dashboards, IPS-1 Dashboard offers multiple threat-profile views (Figure 2). Instead of merely focusing on alerts, the administrator can focus on what really matters—the security profile of the organization or network segment, for which he/she has responsibility.

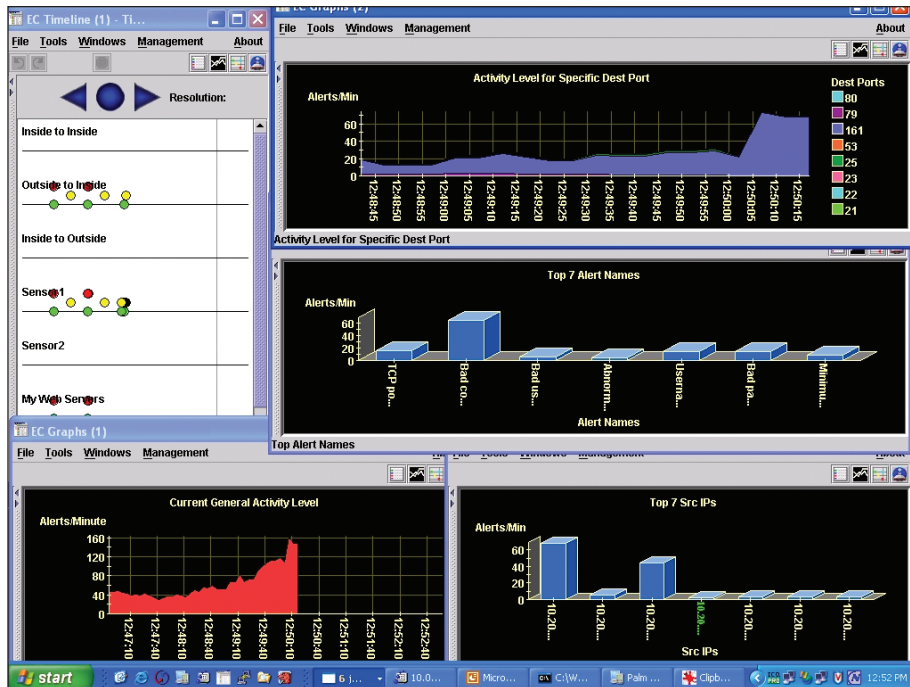


Figure 2. IPS-1 Dashboard threat -profile views

One particularly unique view offered in the IPS-1 Dashboard is the Timeline view (Figure 3), which plots security-related activity over a moving timeline and offers highly effective and efficient graphical threat monitoring. In addition, the Timeline View enables security managers to scroll back in time to review threat activity.

Scalable, centralized management

The size and scope of IPS-1 deployments range from a couple collocated sensors to hundreds of sensors deployed in a global network. Especially in the case of larger deployments, the ability to manage the IPS-1 system is vitally important. Using IPS-1 Dashboard, the administrator may manage the installation, upgrade, configuration, and diagnostics of hundreds of sensors, regardless of location. This low-touch, scalable management is enabled by facilities within IPS-1 Dashboard to create virtual groups for policy management purposes. For instance, a corporate user could manage all branch-office IPS-1 solutions by creating a virtual group of all these appliances. She could then perform policy management by virtual groups, rather than tediously managing policies for each appliance individually.

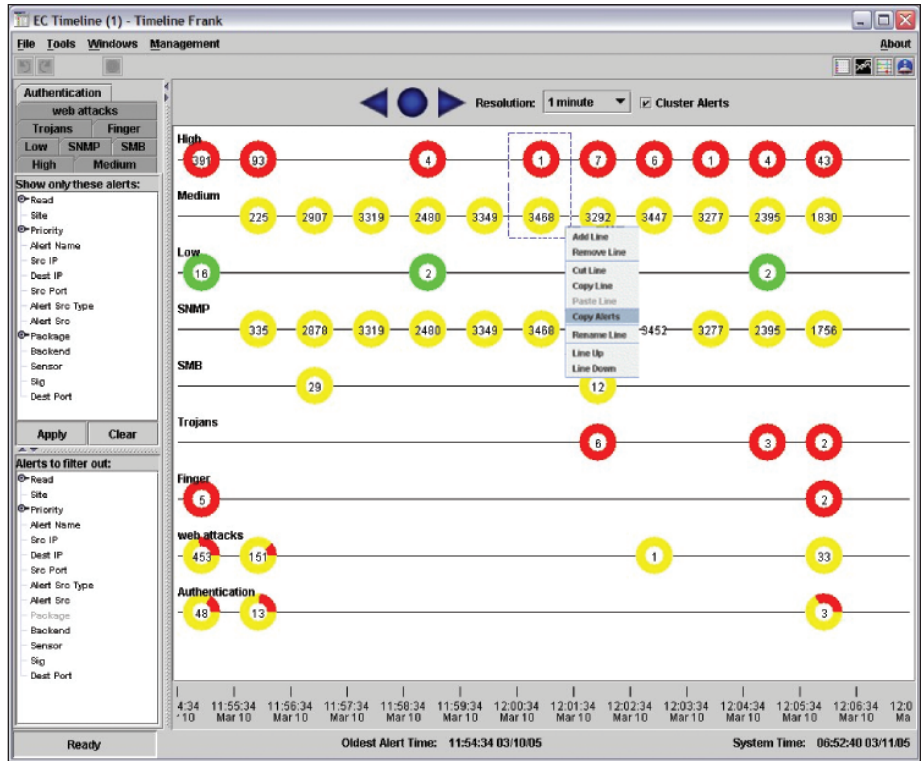


Figure 3. Timeline View

Forensic analysis

IPS-1 features impressive analysis capabilities to quickly help administrators dissect attack data and compile reports on attack and event trends. Through the IPS-1 Management Dashboard, administrators get real-time, high-level graphical views across all sensors as well as the ability to drill-down and group event and alert data to effectively pinpoint attack sources and their scope. Administrators can customize attack graphs and attack-vector timelines, forming their own window to monitor real-time attack and prevention activity. Alert data can be easily sorted into common groups, which are customizable based on user-configurable criteria. Alerts can be grouped by any field such as source IP, attack type, and target vulnerability.

Vulnerability management

IPS-1 also includes vulnerability management capabilities built into the IPS-1 Management Dashboard. This feature, called the IPS-1 Vulnerability Browser (Figure 4), leverages data received from active scanning and enables vulnerability viewing and management from a single dashboard. The Vulnerability Browser combines IPS-1 functions with Nessus vulnerability scanning (a popular, open-source network-scanning tool sponsored by Tenable Networks and used by more than 75,000 organizations worldwide) to enable security managers to quickly identify high-risk security issues, drill-down on details of specific vulnerabilities in the network, and understand which vulnerabilities and services are currently under attack. And, through the IPS-1 Dynamic Shielding Architecture (see Page 8), IPS-1 proactively enables protections against vulnerabilities that are currently exposed, ensuring current vulnerabilities in the network are properly shielded from exploits.

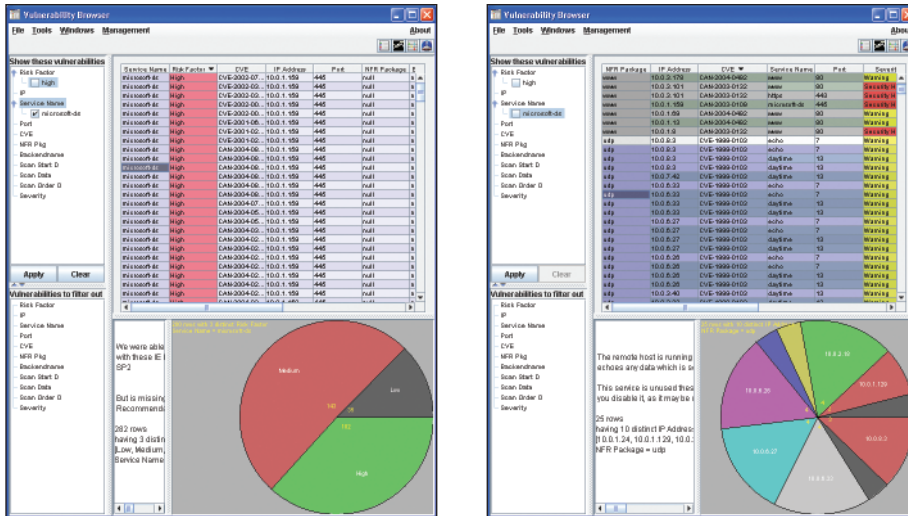


Figure 4. Vulnerability Browser

Reporting and correlation

IPS-1 offers the best of security reporting (see Figure 5) by including more than 40 reports that provide the user a view into the security posture of the organization. Both real time and historical analysis reports are provided.

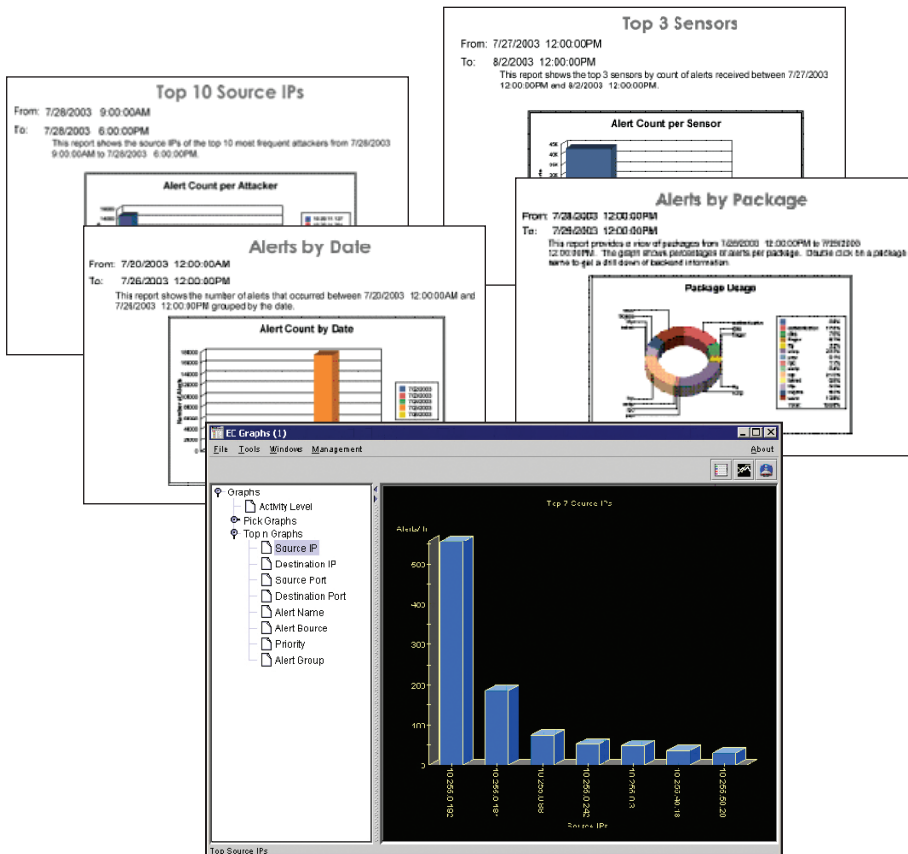


Figure 5. Reporting

IPS-1 Dashboard also provides the correlation functionality uncommon to many conventional IPS dashboards. It allows the creation of real-time charts that are an aggregation of data based on conditional rules defined by the user. These rules are easily defined by pointing and clicking through the graphical interface, rather than scripting, making such functionality accessible to the nonprogrammer.

Conclusion

The wide range of threats that exist today requires a multi-layered defense that spans the perimeter as well as trust points within the corporate network. Intrusion prevention systems need to be able to accurately detect and prevent attacks against IT systems while taking into consideration multiple vectors of a dynamically changing environment.

This dynamically changing IT environment demands that today's intrusion prevention systems go beyond simple attack detection and prevention and offer functionality that 1) dramatically lowers false-positives through granular and customizable detection mechanisms, 2) applies host vulnerability information to intelligently apply the correct prevention action, 3) provides granular forensic analysis to determine the cause and corrective action in the event of an attack, and 4) scales as the enterprise scales—whether that means adapting to new applications, system upgrades, or ever-increasing network performance requirements. And today's intrusion prevention systems need to offer all this while minimizing the administrative overhead required managing the system.

Check Point IPS-1 provides IT organizations with a robust intrusion prevention system that not only meets today's requirements, but also has built in the adaptability and scalability to grow and change as the environment or the business requirements change.

©2003–2007 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-Address Mapping, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 6,496,935, 6,873,988, and 6,850,943 and may be protected by other U.S. Patents, foreign patents, or pending applications.

March 8, 2007 P/N 502462



Check Point
SOFTWARE TECHNOLOGIES LTD.