



The Evolution of IPS

Intrusion Prevention (Protection) Systems
aren't what they used to be

Contents

Background	3
Past Case for Standalone IPS.....	3
Organizational Control	3
Best-of-Breed Technology	4
Performance Concerns	4
Benefits of Integrated IPS	4
Reduced Cost	4
Reduced Latency.....	4
Cohesive Security Policy	5
Common Management and Training.....	5
Easier IPS Deployment	5
When Standalone IPS is Necessary	5
Conclusion	5

In the past, IPS was comprised of a dedicated physical layer with dedicated teams protecting a network from intrusion and attack. Today, the IPS strategy is moving toward a software layer integrated into a company's existing gateway infrastructure and managed by a general security team.

Given that IPS has become a fundamental component of 'due care' in IT security, the evolution of IPS provides organizations with viable, and in many cases better, deployment options.

Background

Generally speaking, IPS detects and blocks attacks and threats aimed at data and network resources. IPS functionality can be deployed in two key variants: standalone (or dedicated) and integrated.

Standalone IPS offers:

- A dedicated layer of intrusion prevention in a network
- The ability to be deployed on dedicated, purpose-built sensor appliances

Integrated IPS offers:

- Integrated intrusion prevention throughout the entire security infrastructure
- The ability to be deployed as integrated IPS functionality on existing security enforcement points, typically firewall gateways

Historically, at least until recently, the most common method for deploying IPS has been on standalone appliances. While there were good reasons for this approach, a strong case is developing for deploying IPS as integrated functionality within existing security enforcement points.

Past Case for Standalone IPS

Before addressing the growing trend of integrated IPS, one must understand the strengths and weaknesses of standalone IPS appliances. Several key factors have fueled the past growth of standalone IPS deployments

Organizational Control

Past: For years, IPS functionality fell under the jurisdiction of a group or department different than the group responsible for existing core security enforcement points. Firewalls and VPNs were managed by network administrators, while IPS was managed by separate security functions or new technology groups.

Present: Today, in most organizations, areas related to network and data security now fall under a consolidated "network security" group within the organization. The group responsible for IPS technology is the same group responsible for major network security enforcement points like firewalls.

Best-of-Breed Technology

Past: As IPS technology has developed over the last five years, most organizations wishing to deploy IPS functionality understood that it was a developing technology, and therefore selected standalone IPS appliances because they thought standalone appliances were best-of-breed.

Present: As IPS technology has matured, functionality has been added to core network security gateways such as firewalls. However, all IPS's (be they standalone or integrated) are not created equal, so an organization considering IPS deployment must carefully examine each vendor's protection arsenal and history of protections to determine if they meet the organization's needs. Today, deploying an integrated IPS does not require security tradeoffs. Integrated IPS offering full protection sets and capabilities does exist.

Performance Concerns

Past: In the last few years, organizations interested in integrated IPS still selected standalone IPS solutions because they feared that integrating IPS into the firewall would grind performance to a halt.

Present: Performance is still an important criterion that must be evaluated. Different vendor solutions have difference performance characteristics, which may or may not be adequate for an organization's particular needs. However, an integrated IPS solution with multi-gigabit threat coverage does exist, so performance should no longer be a barrier to choosing and deploying an integrated IPS solution.

Benefits of Integrated IPS

According to many industry analysts, recent IPS deployment trends show a steep increase in the use of integrated IPS. Many of these analysts state that integrating IPS into the firewall is an accelerating trend. Benefits of integrated IPS include:

Reduced Cost

Purchasing and deploying multiple security appliances is typically more costly than deploying an integrated solution, which makes integrated IPS cheaper. Some of the cost savings include direct expenses like equipment purchase, and indirect expenses like training and ongoing management. Consolidation also provides incremental savings of rack space, cabling, cooling and power.

Reduced Latency

IPS and firewall functionality both deal with securing traffic and data flowing through Internet, intranet and extranet environments. Since the firewall already inspects all traffic dealing with its part of the network, it is a logical point for IPS inspection. Well designed integrated solutions actually inspect traffic only once for both functions, thus minimizing the impact caused by inspecting the traffic twice (which happens in typical standalone IPS deployments).

Cohesive Security Policy

Having multiple components for any enforcement solution increases the complexity of the policies and rules. It also multiplies potential points of failure. Such complexity increases the likelihood that some threat or attack will 'slip through the cracks,' or that traffic will be checked multiple times. Neither scenario is desired. An integrated solution drives a single, cohesive security policy.

Common Management and Training

Multiple solutions from various vendors require more complex management and staff training. An integrated solution reduces not only the expense associated with management and training, but also reduces errors and oversights. Because most firewall and IPS functionalities are owned by the same network security group, integrated IPS solutions are in synch with today's organizational structures.

Easier IPS Deployment

Since firewalls are already deployed throughout a modern integrated network, adding IPS functionality to firewalls is financially and organizationally easier than purchasing and installing additional devices.

When Standalone IPS is Necessary

While integrated IPS likely will undergo rapid adoption over the next several years, some scenarios for standalone IPS deployments remain. Standalone IPS is best suited for use in portions of the network where firewalls are not deployed; traffic flowing between certain parts of the network may not go through a firewall enforcement point, so deploying a standalone IPS device in that portion of the network may be desired. Also, if IPS and firewall functionality are handled by different network security groups, practical reasons can justify deploying standalone IPS even if an integrated solution is hypothetically more appropriate.

Conclusion

Whichever solution works for your network, organizations must carefully compare IPS solutions from competing vendors to ensure that they are getting the desired level of security and performance. The Check Point IPS Software Blade, which integrates full IPS functionality into firewalls and other security enforcement points, is leading the way in integrated IPS. This solution was designed from the bottom-up to be a fully-functional integrated IPS offering multi-gigabit threat coverage. What's more, the Check Point IPS Software Blade provides strong protection and the ability to be deployed on existing security enforcement points.

Check Point also offers both an integrated IPS (Check Point IPS Software Blade) and a standalone solution (Check Point IPS-1). Both solutions can be managed with the same integrated management architecture and management console, providing truly integrated management. When it comes to IPS, look no further than the Check Point IPS family.



About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leader in securing the Internet. The company is a market leader in the worldwide enterprise firewall, personal firewall, data security and VPN markets. Check Point's PURE focus is on IT security with its extensive portfolio of network security, data security and security management solutions. Through its NGX platform, Check Point delivers a unified security architecture for a broad range of security solutions to protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. The company also offers market leading data security solutions through the Pointsec product line, protecting and encrypting sensitive corporate information stored on PCs and other mobile computing devices. Check Point's award-winning ZoneAlarm Internet Security Suite and additional consumer security solutions protect millions of consumer PCs from hackers, spyware and data theft. Extending the power of the Check Point solution is its Open Platform for Security (OPSEC), the industry's framework and alliance for integration and interoperability with "best-of-breed" solutions from hundreds of leading companies. Check Point solutions are sold, integrated and serviced by a network of Check Point partners around the world and its customers include 100 percent of Fortune 100 companies and tens of thousands of businesses and organizations of all sizes.

CHECK POINT OFFICES

Worldwide Headquarters

5 Ha'Solelim Street
Tel Aviv 67897, Israel
Tel: 972-3-753 4555
Fax: 972-3-624-1100
email: info@checkpoint.com

U.S. Headquarters

800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391 ; 650-628-2000
Fax: 650-654-4233
URL: <http://www.checkpoint.com>

©2009 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, 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, INSPECTXL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpec, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, 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, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, the totalsecurity logo, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, 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 ForceField, 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, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.