



February 2005

A white paper  
commissioned by  
Check Point Software  
Technologies

Document #205101

# Improving Security ROI via an Integrated Application Security Solution

*Check Point Proactively Protects More  
Applications at the Perimeter in a  
Single Gateway with Greater Security  
ROI than Cisco or Juniper*

## Statement of Licensing Info and Acceptable Usage

Entire contents © 2005 The Tolly Group, Inc. All rights reserved.

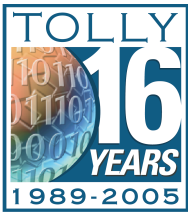
For additional information on acceptable usage of this document (Tolly Group Document #205101) contact The Tolly Group at (561) 391-5610 or via E-mail at sales@tolly.com.



Reproduction of this publication in any form without prior written permission is forbidden. The information contained herein is believed to be accurate and reliable. The Tolly Group shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof.

**All excerpts from this report must be approved by The Tolly Group in advance of publication or use in any public materials.**

## Tolly Group Services



With more than 15 years experience validating leading-edge Information Technology products and services; The Tolly Group has built a global reputation for producing accurate and unbiased evaluations and analysis. We employ time-proven test methodologies and fair testing principles to benchmark products and services with the highest degree of accuracy.



Launched in 2003, The Tolly Group's "Tolly Verified" service provides in-depth, vendor-neutral certification of an array of features, functions and performance characteristics in technology disciplines as diverse as WLAN Switching and Anti-spam. See our "Tolly Verified" Home Page.

Our "Up-to-Spec" service provides the custom testing complement to the "standard", granular tests offered in "Tolly Verified". See our "Up-to-Spec" Home Page.



Plus, unlike narrowly focused testing labs, The Tolly Group combines its vast technology knowledge with focused marketing services to help clients better position product benchmarks for maximum exposure.

This document was authored by:

- Kevin Tolly,  
President/CEO  
The Tolly Group
- Charles Bruno,  
Executive Editor  
The Tolly Group

## Table of Contents

- 4 Exploits Drive Innovation
- 5 Integrated Intrusion Protection
- 9 Depth of Protection via Architecture
- 12 Total Cost of Security
- 14 Intelligent Approach to Security
- 17 Appendix: Detailed Test Results

## List of Figures

- 7 Figure 1. Test Result Table Comparison Between Check Point's VPN-1 NG Series vs. Cisco PIX515E and Juniper NetScreen-204
- 12 Figure 2. Total Cost-of-Ownership Comparison of Single-Site Hybrid Firewall/IPS Solutions

# Improving Security ROI via an Integrated Application Security Solution

## Exploits Drive Innovation

When it comes to enterprise-class network security, firewalls and VPNs have long been firmly established as the fundamental building blocks of security at the network perimeter. With some 65,000 possible TCP points of entry, firewalls do an excellent job of blocking ports that are not needed - but you can't close every port and still conduct business. Hackers know that.

Recognizing the effectiveness of firewalls at blocking access, hackers are skillfully changing direction and embracing a whole new arsenal of innovative security exploits.

Today, hackers attempt to penetrate network perimeters by cleverly hiding "exploits" (i.e. attacks) inside traffic streams of legitimate corporate communications protocols. Today, attacks are carried out across critical applications such as secure Web access (SSL), E-mail (SMTP) and database access (SQL) - to name just a few.

Instead of gaining access to previous network data by attacking open ports, hackers now are using applications as the transport vehicle to gain access to critical data stores. They are going after the applications, since traditional firewalls are not designed to detect and thwart attacks at the application level.

By attacking via applications, hackers hope to achieve any of a variety of goals:

- Deny service to legitimate users (Denial of Service)
- Gain administrator access to servers or clients
- Gain access to back-end information databases
- Install Trojan horse software that bypasses security and enables access to applications
- Install software on a server that runs in "sniffer" mode and captures user IDs and passwords

Security vendors have countered these sophisticated attacks with their own measures, either through development of intrusion detection and prevention systems (IDS/IPS), or via a new form of software intelligence that monitors and understands application behavior and uses that knowledge to guard against attacks and other threats.

Application Intelligence is a software-based technology that is aware of the protocol in use by an application and is fully aware of the actual and potential limitations of the protocol such that it can identify characteristics exhibited by an exploit. So if exploiting a perceived vulnerability requires coming through a certain firewall port and contains a payload larger than a certain size, the software can be tuned to look for traffic meeting those criteria. If such traffic is found, it can be dropped.

## Integrated Intrusion Protection

Security companies recognize the need to blend firewall and VPN functionality along with so-called "intrusion protection" technology to identify threats and deal with them before they become a nuisance or worse, a debilitating event that adversely impacts business services.

Moreover, integration of the technologies makes sense from a business perspective because it lowers total cost-of-ownership by centralizing multiple functions and management control in a single box. So upfront security deployment costs and ongoing management expenses can be reined in.

With the arrival of standalone IDS/IPS products to market, users often were faced with the prospect of adding a second perimeter security box alongside their already installed, trustworthy firewall/VPN devices. But this added significant cost and complexity to the network. Administrators often found themselves learning yet another management interface and physically managing yet another layer of security devices.

An alternative to the standalone IDS/IPS is a single-box multilayered security device that provides firewall, VPN and intrusion services. Many users fall into the trap of believing that the single-box solutions from various vendors deliver the same level of functionality.

That simply is not the case. There are significant differences that separate security devices and their IDS/IPS capabilities.

In fact, Check Point Software Technologies, Inc., one of the industry's leading security solutions suppliers, commissioned The Tolly Group to conduct a series of tests that demonstrate the effectiveness of the company's Application Intelligence within the Check Point VPN-1 NG Series firewall compared to other offerings and how they handle threatening security exploits. Check Point recognizes that many soft-

### INSPECT Engine Drives Processing

Check Point VPN-1 NG Series devices are based upon the company's patented Stateful Inspection technology and its architecture which relies upon an INSPECT Engine. The INSPECT Engine enforces security policies on host gateways where it resides and extracts info it needs from the various communication layers of traffic it handles.

The INSPECT Engine is dynamically loaded into the operating system kernel, between the Data Link and the Network layers (layers 2 and 3). Since the data link is the actual network interface card (NIC) and the network link is the first layer of the protocol stack (for example, IP), Check Point is positioned at the lowest software layer. By inspecting at this layer, Check Point ensures that the INSPECT Engine intercepts and inspects inbound and outbound packets on all interfaces. No packet is processed by any of the higher protocol stack layers, no matter what protocol or application the packet uses, unless the INSPECT Engine first verifies that the packet complies with the security policy.

Since the INSPECT Engine has access to the 'raw message,' it can inspect all the information in the message, including information relating to all the higher communication layers, as well as the message data itself (the communication- and application-derived state and context). The INSPECT Engine examines IP addresses, port numbers, and any other information required in order to determine whether packets should be accepted, in accordance with the defined security policy.

The INSPECT Engine's ability to look inside a packet enables it to allow certain commands within an application while disallowing others. For example, the INSPECT Engine can allow an ICMP ping while disallowing redirects, or allow SNMP gets while disallowing sets, and so on. The INSPECT Engine can store and retrieve values in tables (providing dynamic context) and perform logical or arithmetic operations on data in any part of the packet.

**For more info on Check Point's Stateful Inspection™ architecture, go to:**

[http://www.checkpoint.com/products/downloads/Stateful\\_Inspection.pdf](http://www.checkpoint.com/products/downloads/Stateful_Inspection.pdf)

ware applications built for the Web environment have not been designed with security as a priority - the debilitating Blaster security exploit is a perfect example. Blaster exploited a widespread vulnerability in Microsoft's Windows operating system by attacking the DCOM (Distributed Component Object Model) interface, which handles messages sent using the RPC (Remote Procedure Call) protocol.

New software vulnerabilities are discovered every day and hackers are continually armed with innovative ways to exploit various parts of the Web environment. Check Point believes its Check Point VPN-1 NG Series with Application Intelligence firewall is the only perimeter security gateway to provide protection for the entire perimeter environment - without requiring the purchase and deployment of a second standalone "intrusion protection" device. (Check Point's Application Intelligence is based upon the company's INSPECT security architecture, see sidebar.)

Other single-box solutions, Check Point says, fall short in terms of protection, or lure users with a single-box solution that contains a subset of the required security functionality. After deployment, users find themselves without requisite coverage - and are forced to buy the vendor's stand-alone box to build a complete perimeter security solution.

Check Point commissioned The Tolly Group in November 2004 to examine the depth of security provided by three single-box solutions: Check Point VPN-1 NG Series Firewall; Cisco Systems PIX 515E firewall and Juniper Networks, Inc.'s NetScreen-204 firewall.

Tolly Group testing illustrates that neither Cisco nor Juniper can provide the breadth of coverage for the range of security vulnerabilities tested in a single-box solution as they don't implement a full-blown intrusion system in their firewall offerings. To get "Check Point-class" protection, customers must deploy a second perimeter device - a dedicated intrusion gateway - at additional capital and operational cost.

Prior to testing, The Tolly Group contacted both Cisco and Juniper in November 2004 in accordance with The Tolly Group's Fair Testing Charter. The Tolly Group invited both companies to participate in the testing. Through the end of November, Cisco did not respond to the testing invitation, while Juniper agreed to participate and provide input. Juniper received the full test methodology but did not comment on it in late November. The Tolly Group sent preliminary test results to Juniper Networks for review and comment; Juniper had not provided feedback by yearend.

All three products were subjected to more than two dozen tests that exposed them to various security exploits common to enterprises of all sizes.

Figure 1, below shows how each of the three products fared for the various security exploits. For detail on each specific test, turn to Appendix on page 17.

Test Results Table Comparison between Check Point's VPN-1 NG Series vs. Cisco PIX 515E and Juniper NetScreen-204					
			Check Point VPN-1 NG Series	Cisco PIX 515E Security Appliance	Juniper NetScreen-204
Test Case	SmartDefense Advisory	Test Name	Result		
1	CPAI-2004-38	Netscape NSS Library Record Parsing Buffer Overflow: Enforcement of SSLv2 Challenge Length	✔	✘	✘
2	CPAI-2004-37	Cisco IOS Malformed OSPF Denial of Service: Enforcement of MD5 authenticated OSPF connections	✔	✘	✘
3	CPSA-2004-03	Attacks on Dynamic Routing Protocols: Enforcement of MD5 authenticated RIP	✔	✘	✘
4	CPSA-2004-03	Attacks on Dynamic Routing Protocols: Enforcement of RIPv2	✔	✔	✔
5	CPSA-2004-03	Attacks on Dynamic Routing Protocols: Enforcement of MD5 Authenticated BGP	✔	✘	✘
6	CPAI-2004-25	SOCKS-based Trojans: Block SOCKSv4	✔	✘	✘
7	CPAI-2004-25	SOCKS-based Trojans: Block unauthenticated SOCKSv5	✔	✘	✘
8	CPAI-2004-21	IRC-based Worms: Enforcement on Non-Standard IRC Ports	✔	✘	✘
9	CPSA-2003-09	Multiple Vulnerabilities in SQL: Extended Stored Procedures (xp_cmdshell) Protections	✔	✘	✘
10	CPSA-2003-09	Multiple Vulnerabilities in SQL: Public Queries (sp_start_job)	✔	✘	✘
11	CPSA-2003-09	Multiple Vulnerabilities in SQL: Block Admin Login without Password	✔	✘	✘
12	CPAI-2004-19	Microsoft SSL Library Remote Compromise Vulnerability: Block Malformed PCT (Protected Communications Transport)	✔	✘	✘
13	CPAI-2004-15	IKE Aggressive Mode Vulnerabilities: Block IKE Aggressive Exchange	✔	✘	✘
14	CPAI-2004-19	OpenSSL Null-Pointer Assignment Vulnerability: Enforcement of SSL Length	✔	✘	✘
15	CPAI-2004-07	Microsoft ASN.1 Remote Code Execution: Enforcement over NTLM (NT LAN Manager)	✔	✘	✘
16	CPAI-2003-04	Microsoft SQL Worm (Slammer): Slammer Test	✔	✘	✘
17	CPAI-2004-42	Microsoft JPEG Processing Buffer Overflow Vulnerability: JPEG Exploits	✔	✘	✘

Testing reveals that the Check Point VPN-1 NG Series firewall was the only product tested that supported and correctly prevented more than two dozen security exploits from being passed through to the target system.

In effect, this demonstrates that in a single-box implementation, the Check Point VPN-1 NG Series firewall offers the full range of intrusion protection, while the Cisco PIX 515E and the Juniper NetScreen-204 only provide a subset of IPS functionality needed to guard against the range of threats tested.

Both of those vendors offer some intrusion prevention features in their perimeter gateway solutions, but in order to have the coverage demonstrated by the Check Point solution, users must deploy a second gateway, dedicated to intrusion protection services, that results in an overlap of services, plus users take a financial hit in the cost-of-ownership (purchase, maintenance and operation) of the two-box solution versus the Check Point offering.

There are other issues, too.

In order to provide protection on a par with Check Point, our testing would indicate that the "two-box" solution from Cisco or Juniper would be required. While this study did not examine the "two-box" solutions from Cisco or Juniper, such an approach would add significant complexity to managing the security aspect of the network. To that point, neither Cisco nor Juniper Networks offer a fully integrated management system to manage both perimeter firewall/VPN gateways and internal intrusion prevention systems gateways.

Check Point's Security Management Architecture (SMART), by contrast, can manage all Check Point perimeter and internal gateways, making for a more streamlined and easier-to-manage security environment.

Check Point also offers another advantage over the Cisco and Juniper Networks products

tested. The company bundles its SmartDefense™ Service into its firewall products. Check Point SmartDefense enables customers to configure, enforce, and update network and application attack protections. In addition, the SmartDefense service provides information on attack defenses and access to those new attack defenses, as well as related information via SmartDefense Updates and Advisories published online by Check Point. The SmartDefense console is included with VPN-1 products. SmartDefense also integrates with the Check Point SMART Management and reporting infrastructure to provide a single, centralized console for attack detection, blocking, logging, auditing and alerting.

Juniper also offers a security update service, but those services are separate for its Deep Inspection™ Firewall and IDP solutions - as they are separate boxes. Juniper offers updates for those protocols it presently supports on its firewall, yet the firewall requires an OS upgrade to implement support for new "deep inspection" protocols. For its IPS, Juniper offers a regular update service. Cisco does not offer a firewall update service, but does offer an update service for its IPS.

By contrast, defenses that are configurable in Check Point's SmartDefense can be updated and kept current with a SmartDefense Service subscription. Cisco does not offer an update service for the PIX firewall, only for the Cisco IDS. Juniper Networks offers two different update services - one for its Deep Inspection Firewall and one for the IDP.

From a TCO perspective, even a cursory analysis shows that the Check Point VPN-1 NG Series firewall costs 56% less than single-box solutions from Cisco and Juniper Networks. And those rival products offer only a subset of the intrusion protection delivered by Check Point.

In summary, the Check Point VPN-1 NG Series firewall was the only product tested that fully protected against the entire range of security exploits used in this evaluation. What that means is users gain a more robust, full-featured multifunction security solution that provides firewall, VPN and a complete complement of intrusion prevention capabilities, when compared to the Cisco and the Juniper Networks products tested.

In summary, Cisco and Juniper Networks often steer users into a two-box gateway solution should they want to support a broader range of intrusion capabilities than provided in their single-box offering.

This introduces cost-of-ownership hardships and management complexities that extend well beyond the Check Point offerings. In fact, Check Point delivers an integrated management capability so users learn one interface to manage firewall, VPN and intrusion capabilities.

## Depth of Protection via Architecture

When it comes to the architecture of the Check Point, Cisco and Juniper Networks products tested, the issue is really one of Check Point's Application Intelligence design versus the deep packet inspection approach used by Juniper Networks and the stateful packet inspection engine used by Cisco. Juniper utilizes a security architecture based upon its Deep Inspection™ Firewall technology.

According to Juniper Networks, the company's Deep Inspection firewall builds up stateful inspection and integrates intrusion prevention technology into the firewall to provide application-level attack protection at the network perimeter. The Juniper Networks Deep Inspection firewall can perform network security functions as well as analysis on the application message to determine whether to accept or deny traffic.

Deep Inspection technology applies a deeper level of application understanding to the traffic to make access control decisions based on the intent of that traffic. Deployed at the perimeter, a Juniper Networks Deep Inspection firewall focuses on preventing application-level attacks aimed at Internet applications such as Microsoft Windows, Peer-to-Peer (P2P) and Instant Messaging (IM). It eliminates application-level ambiguities, performing de-fragmentation, reassembly, scrubbing and normalization, to convert network packets to the application-level message transferred between the client and the server. It then looks for protocol conformance and extracts data from identified application "service fields" where attacks are perpetrated and applies attack pattern matches. It then decides to accept or deny the traffic based on high impact protocol anomalies or any given attack pattern in one of these application service fields. The Deep Inspection firewall can block application-level attacks at the Internet gateway so they never reach their destination. Additionally, users can also create their own attack protection signatures.

Cisco relies upon stateful packet inspection, but adds on its Web site that the PIX 515E utilizes "a variety of security enforcement technologies ranging from protocol conformance checking, application/protocol state tracking, Network Address Translation (NAT) services, as well as an array of attack detection/mitigation techniques such as protocol field length checking, URL length checking, and more."

Cisco's and Juniper's security architectures largely are "response-based," meaning that products based upon them cannot defend against new threats, or variants of existing threats, without first responding to an update notification from the vendor to update their signature databases. By contrast, Check Point, does not rely on signatures to defend against new threats or variants of existing threats.

Check Point has a security architecture which offers greater depth of protection for applications, as evidenced by test data. According to Check Point, the company doesn't rely solely on pattern or signature matching. Instead, it employs "class-based" detection.

Check Point's INSPECT and Application Intelligence architectures enable the company's firewalls to block not only specific attacks, but also entire categories or "classes" of attacks. Check Point provides this unique level of protection by enforcing the proper and expected usage of protocols, such as RPC, and does not rely on signatures. Traditional signature-based defenses are reactive because they require knowledge of the exact characteristics of an attack in order to create a defense signature.

Check Point's SmartDefense is based on Check Point's Stateful Inspection, Application Intelligence and Web Intelligence technologies. SmartDefense enables Check Point gateways to block not only specific attacks, but also entire categories or "classes of attacks." The core functions of Application Intelligence are:

- Validating compliance to standards
- Validating expected usage of protocols
- Blocking malicious data
- Controlling hazardous application operations

SmartDefense blocks attacks at a Check Point enforcement point. Some of the SmartDefense capabilities are enforced as an integrated part of the firewall security policy and are distributed as part of the enforcement points' security policy. In addition to the specific attack protections of SmartDefense, customers also benefit from the strict access control to network resources offered by Check Point enforcement points.

SmartDefense provides a unified security framework for various components that identify and prevent attacks. The SmartDefense tab in the company's SmartDashboard management display is divided into a tree structure that classifies the defenses provided by SmartDefense.

Each item in the tree refers to a category of functionality that includes defenses for families of attacks as well as more general attack protections and safeguards (e.g. scrambling system fingerprints). For example, SmartDefense blocks not just Blaster, but all similar variants because these attacks violate the proper connection flow as defined by the Microsoft RPC protocol. As such, SmartDefense blocks attacks in a class-based manner that is not limited to a specific set of attack signatures. For each category and subcategory in the

tree, the SmartDefense console allows administrators to configure attack protections and safeguards, as well as provides information on the attacks and vulnerabilities.

At the time tests were conducted, neither Cisco nor Juniper offered support for the full range of application protocols supported by Check Point. Based on our examination and understanding of the Juniper deep packet inspection, while any customer can download or upgrade signatures for existing protocols, an OS upgrade is required to implement support of new protocols.

Likewise, the Cisco PIX OS 6.3.4 tested contained minimal application-level inspection methods. PIX firewalls based upon Cisco's security architecture can not learn how to inspect new applications (protocols) without an OS upgrade. In fact, Check Point does not require an OS upgrade; the company's SmartDefense updates are incorporated into the gateway without down time. For example, Check Point can add protection for a new protocol or defense mechanism without taking down the gateway.

The test results prove that Check Point provides intelligent application security for HTTP, HTTPS, SQL, SOCKS, IPSec, BGP, OSPF, and RIP protocols. Since the other products tested are not designed to examine applications using these protocols, they allowed the protocol traffic to fall victim to a variety of security exploits.

The protocols that the Check Point firewall protected represent the most essential protocols used in enterprises today. SQL is at the heart of many mission-critical business applications. Secure Sockets Layer (SSL) is a mission-critical tool used to secure e-Commerce and other sensitive business applications. And BGP, OSPF, and RIP are core routing protocols used to ensure optimal and redundant routing conditions.

Check Point provides immediate protection against the many protocol and application-based attacks against Microsoft environments. Because Check Point solutions support intelligent inspection of such protocols as Common Internet File Sharing (CIFS), Microsoft SQL (MS SQL), and Microsoft Remote Procedure Call (RPC), it provides instant defenses as attacks appear. It also provides instant defenses against the many variants that appear.

Other products tested that are based on packet analysis provide no support for Microsoft protocols - one of the most common attack routes today. Instead, they rely on signatures. Juniper's signature-based approach does not understand the root cause of attacks, therefore it cannot recognize variants.

Customers must wait for Juniper to offer new defenses for attacks that are already crippling their network and receive no protection against

### Check Point Firewall offers three total cost advantages over rival products tested:

- Upfront capital cost for gateway/management software is lower
- Reduced operational and management costs
- Less cost for security updates

variant attacks.

## Total Cost of Security

Technology considerations, in terms of security exploits processed and the relevance of a security product's architecture, surely are factors that must be carefully weighed in any deployment of enterprise-class security products.

But technology deployment decisions are business decisions and at the heart of any business decision initial costs and ongoing expenses come into play to determine the total cost of ownership, or the total cost of security.

For the purpose of this TCO analysis, we will define TCO to include gateway costs, ongoing subscription service costs for signature updates, and support costs.

All retail prices listed (North American pricing in U.S. dollars) were gathered in November 2004. Prices pertaining to the Cisco PIX 515E

were derived from the popular Web site, CDW.com. Prices pertaining to the Juniper NetScreen-204 were taken directly from a Juniper pricelist dated November, 2004, supplied by Check Point.

TCO analysis of combined hardware, software and support costs shows that the Check Point single-box firewall/IPS solution costs 70% to 125% less than either the Juniper NetScreen-204 or the Cisco PIX 515E two-box solutions.

Even at the base functionality level, the Check Point Express 100 software bundle used in testing (perimeter firewall/VPN and integrated IPS functionality) costs from 13% to 43% less than the other single-box appliance

solutions from Cisco and Juniper. Since the Check Point solution is a software-only product, the cost of a host PC (\$1,595) brings the total solution cost to around \$8,000 - some 30% less than the Juniper Networks option and on par with the Cisco appliance. Add in the additional \$9,195 for the Juniper IDP-10 required to bring the functionality on par with the Check Point solution, and you have a sizable hardware cost difference. Cisco adds \$8,000 for an IDS 4215 on top of the PIX 515E price of \$7,495. These devices are required by both vendors to move users to the same level of protection that Check Point

Figure 2

Total Cost of Ownership Comparison of Single-Site Hybrid Firewall/IPS Solutions			
	Check Point Express 100*	Juniper NetScreen-204/Juniper IDP-10	Cisco PIX 515E/Cisco IDS 4215
<b>Gateway</b>		Appliance	Appliance
Perimeter FW/VPN	(SW: \$6,500) (HW: \$1,595)	\$11,500	\$7,495
IPS	Included	\$9,195	\$8,000
<b>Subscription Services</b>			
Perimeter FW/VPN	(SmartDefense service \$1,000)	Deep Inspection Signature Service \$920	None available
IPS		Separate service included in IDP costs	Included in IDS costs
<b>Support</b>			
Perimeter FW/VPN		\$1,040	\$900
IPS	\$975		\$700
<b>Total</b>	<b>\$10,070</b>	<b>\$22,655</b>	<b>\$17,095</b>

\* Check Point Express 100 is the name given to the perimeter medium-business software bundle used in testing with the Check Point Internet Security Solution with Application Intelligence Firewall tested by The Tolly Group.

offers in its single-box solution and be able to stop all of the exploits used in this test.

Then there's the issue of subscription services, or updates to keep the security services abreast of new attack signatures. Check Point and Juniper charge about the same, while Cisco offers an update service only for its IDS product.

Support adds another \$975 annually for the Check Point Express 100, \$1,040 for the Juniper NetScreen-204 and \$1,600 for the two Cisco devices.

The big picture here? Users pay more than twice the cost of the Check Point Express 100 (\$10,070) for the NetScreen-204 (\$22,655) two-box solution and about 70% more for the Cisco two-box solution. (See Total Cost-of-Ownership chart, page 12) To further this analysis, one must look beyond the upfront costs of deployment.

Many attempts to quantify TCO for Internet security deployments leave out some of the most significant contributors to TCO.

Inadequate security can result in system downtime across the enterprise or loss of customers due to a public security breach. Ironically, one of the main things that buyers overlook when considering the total cost of a firewall/VPN solution is the underlying security of the solution. At heart, the primary function of a firewall is security, and the primary function of a VPN is secure connectivity.

New attacks preying on application and protocol vulnerabilities emerge every day. Security products must be agile enough to adapt and combat these threats, not in a matter of weeks, but in minutes. When a new threat is identified, defenses need to be immediately developed and distributed to devices and users around the world. This need for fast response implies a need for a software-based approach such as that offered by Check Point. The requirement for security implies a critical need for flexibility in a security system. For Check Point, that flexibility comes from tight integration between firewall and full IPS functionality in a single product.

The same cannot be said of the Juniper and Cisco solutions. Since signatures are hard-coded in ASICs, security updates must be loaded onto the system and not dynamically applied in instantaneous fashion.

On another front, the Check Point solution relies upon a single core management infrastructure, SMART (Security Management Architecture) to control firewall, VPN and IPS-like functions. That's not true with the Juniper and Cisco products. Cisco's PIX architecture lacks the capability to add new inspection capabilities dynamically, which is essential given today's dynamic threat environment.

Both Cisco and Juniper also require separate management controls for firewall/VPN and for intrusion capabilities. This adds to TCO since administrators must deal with multiple user interfaces and configuration processes.

A centralized management capability that does not require command-line interaction on a device-by-device basis can save hours of administrator time, whether that administrator is configuring an initial deployment or making a change to the configuration of an existing deployment.

In summary, the TCO analysis of the three products tested underscores a sizable advantage for Check Point.

Both Cisco and Juniper need to supplement their perimeter gateway solutions with a dedicated IPS in order to secure the same amount of applications that Check Point can with Application Intelligence. The total Juniper and Cisco solutions cost increases when users add in the cost of a separate IPS in addition to a NetScreen-204 or PIX 515E. Both the Cisco IDS and the Juniper IDP require separate management and online update systems which further increase the total cost of their solutions.

## Intelligent Approach to Security

In today's rapidly changing security environment, users need an enterprise-class security solution that delivers multiple services from a single platform. This helps to curb costs dramatically and simplifies day-to-day management of the network, and helps make the network perimeter more responsive, and even proactive, against new attacks.

All three of the vendors examined in this test offer a multifunction security platform that combines firewall, VPN and intrusion services. But that does not mean that all integrated single-box solutions are equal. In fact, testing shows that is far from the truth.

As discussed earlier, the Check Point VPN-1 NG Series firewall delivers a number of benefits that make it a far more compelling multiservice platform than with the Juniper or Cisco solutions tested.

Testing proved that Check Point provides application-level security for a greater number of protocols. Protocols like SQL, HTTP, HTTPS, SQL, SOCKS, IPSec, BGP, OSPF, and RIP either support mainstream applications or provide for transport of application data across enterprise networks. Check Point provides security for the most common and less commonly used protocols.

Due to this broad protocol support, the Check Point VPN-1 NG Series firewall delivers extensive application support and protection, including sup-

port for such strategic applications as SQL, CIFS, SOCKS, P2P, IM and major routing protocols.

Attacks are taking place not just on common protocols like HTTP but they are traversing over other mission-critical protocols such as SQL and dynamic routing protocols such as OSPF, BGP, and RIP. Check Point's Application Intelligence is well positioned to defend a broad range of application protocols.

Check Point supports all of these protocols, while Cisco and Juniper do not, relying instead on an attack signature framework to secure the network. However, in doing so, they leave application data vulnerable while Check Point does not.

Check Point also has a security architecture better tailored to supporting application data. The company's Application Intelligence technology guards against odd behavior at the protocol level, while other products tested simply look for attack signatures. Deep packet inspection for attack signatures does not guard against application-level attacks. Moreover, competitive products examined by The Tolly Group require an OS upgrade when adding new application inspection capabilities.

Check Point's SmartDefense feature set within VPN-1 NG Series provides for a shorter deployment time than traditional IPS systems that require OS upgrades.

Finally, from a TCO perspective, Check Point packs support for firewall, VPN and intrusion services in a single device, with a full complement of support for application protocols. Testing demonstrated that the Juniper and Cisco single-box solutions fall well short of the functionality offered by Check Point. In effect, these vendors coax users to a second, intrusion-dedicated box that further skews TCO lifecycle costs in Check Point's favor.

In essence, while Juniper and Cisco may convince users to deploy their single-box solutions, buyers soon learn that they must add a second intrusion appliance to come up to the enterprise-class level of protection already offered by Check Point in a single-box solution.

In the end, users will pay more than twice as much for the competitive two-box solutions as they would for the Check Point single-box deployment.

It pays, significantly, for users to look at the facts before deploying any single-box multiservice security platform to meet firewall, VPN and intrusion protection needs. By doing so, they'll learn there are both technology reasons and cost factors that drive them to the Check Point VPN-1 NG Series firewall.

In the final analysis, users will realize that seeing double is trouble, both

from a cost and a technology standpoint, when it comes to the dual-box solutions offered by Cisco and Juniper Networks.

Check Point's intelligent security solutions have the design that currently offers the broadest protection for application traffic from a variety of common security exploits. And that's not some marketing hype; it's evidence based on solid hands-on testing of all three products. It's just a fact.

###

Information technology is an area of rapid growth and constant change. The Tolly Group conducts engineering-caliber testing in an effort to provide the internet working industry with valuable information on current products and technology. While great care is taken to assure utmost accuracy, mistakes can occur. In no event shall The Tolly Group be liable for damages of any kind including direct, indirect, special, incidental, and consequential damages which may result from the use of information contained in this document. All trademarks are the property of their respective owners.



The Tolly Group, Inc.  
3701 FAU Blvd. Suite 100  
Boca Raton, FL 33431  
Phone: 561.391.5610  
Fax: 561.391.5810  
<http://www.tolly.com>  
[info@tolly.com](mailto:info@tolly.com)

