THE TOLLY GROUP

The authoritative, unbiased source for IT certification, research and testing

WHITE PAPER

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

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.

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

List of Figures

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-

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.

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

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 with out taking down the gateway.

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

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

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.

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**
Gateway		Appliance	Appliance
Perimeter FW/VPN	(SW: $6,500) (HW: $1,595)	$11,500	$7,495
IPS	Included	$9,195	$8,000
Subscription Services			
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
Support			
Perimeter FW/VPN		$1,040	$900
IPS	$975		$700
Total	**$10,070**	**$22,655**	**$17,095**

** 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.*

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

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.

# # #

Appendix: Detailed Test Results

Test 1 — Netscape NSS Library Record Parsing Buffer Overflow: Enforcement of SSLv2 Challenge Length

Description:

The vulnerability exists in the SSL version 2 parsing engine of Netscape's Network Security Server. A "Client Hello" message request with an excessive challenge length (greater than 32 Bytes) leads to a buffer overflow. In this test scenario, engineers will run Nessus script ID 14361 (NSS Library SSLv2 Challenge Overflow) and run a special exploit code using PERL command.

SmartDefense Advisory: CPAI-2004-38 TTG Ref: 1

Results & Comments:

Check Point VPN-1 NG Series	Pass	The firewall policy was configured to permit SSL traffic. The SmartDefense protection “Block SSL null-pointer assignment” was enabled. The gateway was able to block the malicious SSL traffic while permitting valid SSL traffic.

Appendix: Detailed Test Results

Cisco PIX 515E Security Appliance	Fail	The firewall policy was configured to permit SSL traffic. The Cisco PIX device was not able to validate a SSL handshake allowing malicious SSL traffic. The vulnerability is that attackers can pass a buffer overflow using a specially crafted handshake.
Juniper NetScreen-204	Fail	The firewall had a rule that allowed SSL traffic. The Juniper NetScreen gateway was not able to block the malformed "client/hello" message request. It proved that the firewall was not able to inspect SSL traffic properly.

Appendix: Detailed Test Results

Test 2 — Cisco IOS Malformed OSPF Denial of Service: Enforcement of MD5 authenticated OSPF connections.

Description:

The vulnerability exists in a Cisco device receiving a malformed OSPF packet. The device will reset and may take several minutes to become fully functional. It may be exploited repeatedly resulting in a DoS attack. In this test scenario, engineers will configure OSPF without MD5 authentication between two peers to determine if the gateway can block unauthenticated OSPF traffic.

SmartDefense Advisory: CPAI-2004-37 TTG Ref: 3

Results & Comments:

Check Point VPN-1 NG Series	Pass	The firewall policy was configured to permit OSPF traffic between the two peers. In addition, the SmartDefense setting denying non-MD5 authenticated OSPF traffic was activated. Due to the lack of MD5 authentication, OSPF traffic was blocked by the gateway.

Appendix: Detailed Test Results

Cisco PIX 515E Security Appliance	Fail	The Cisco PIX firewall cannot enforce MD5 hash authentication over OSPF packets. The firewall was configured to permit OSPF traffic between two routing peers. The test showed that the device allowed any type of OSPF traffic either authenticated or unauthenticated.
Juniper NetScreen-204	Fail	The Juniper NetScreen gateway cannot enforce MD5 hash authentication over OSPF packets. The firewall policy was configured to permit OSPF traffic between the two peers. The test showed that the gateway allowed any type of OSPF traffic either authenticated or unauthenticated.

Appendix: Detailed Test Results

Test 3 – Attacks on Dynamic Routing Protocols: Enforcement of MD5 authenticated RIP

Description:

RIP can be spoofed by making fake RIP packets and sending them to gateways and hosts to change their routes. Attacks on the RIP protocol may target either vulnerabilities in the routing software/hardware used or attack the routing information of the network. To prevent the spoofing or modification of a valid routing protocol message, message authentication has been added to all these protocols (OSPF, RIP, and BGP). These routing protocols support the MD5 digest. MD5 digest works by creating a 16-byte hash of the routing message combined with a secret key. The 16-byte value is, therefore, message-specific, and modification of the message by an attacker invalidates the 16-byte digest appended to the message. Without the secret key, which is never sent over the wire by the routing protocol, the attacker is unable to reconstruct a valid message. In this test scenario engineers will check if connectivity between client-server was successful or not using MD5 authentication over RIP.

SmartDefense Advisory: CPSA-2004-03 TTG Ref: 6

Results & Comments:

Appendix: Detailed Test Results

Check Point VPN-1 NG Series	Pass	The firewall policy was configured to permit RIP traffic between the two routing peers. In addition, the SmartDefense setting “Block non-MD5 authenticated RIP connections” was activated. The gateway blocked the non-authenticated traffic.
Cisco PIX 515E Security Appliance	Fail	The Cisco PIX firewall cannot enforce MD5 hash authentication over RIP packets. The firewall policy was configured to permit RIP traffic between the two routing peers. The test showed that the device allowed any type of RIP traffic either authenticated or unauthenticated.
Juniper NetScreen-204	Fail	The Juniper NetScreen gateway cannot enforce MD5 hash authentication over RIP packets. The firewall policy was configured to permit RIP traffic between the two routing peers. The test showed that the gateway allowed any type of RIP traffic either authenticated or unauthenticated.

Appendix: Detailed Test Results

Test 4 — Attacks on Dynamic Routing Protocols: Enforcement of RIPv2

Description:

In this test scenario engineers will configure RIPv2 environment in order to check if the DUT can force the version of RIP that the gateway will permit.

SmartDefense Advisory: CPSA-2004-03 TTG Ref: 7

Results & Comments:

Check Point VPN-1 NG Series	Pass	The firewall policy was configured to permit RIP traffic between the two routing peers. In addition, the SmartDefense setting “Allow RIP version 2 only” was enabled. The gateway successfully blocked non-RIPv2 packets.
Cisco PIX 515E Security Appliance	Pass	The Cisco PIX firewall was able to force RIPv2 traffic.
Juniper NetScreen-204	Pass	The Juniper NetScreen gateway was able to force RIPv2 traffic.

Appendix: Detailed Test Results

Test 5 — Attacks on Dynamic Routing Protocols: Enforcement of MD5 Authenticated BGP

Description:

BGP is highly vulnerable to a variety of attacks due to the lack of means of verifying the authenticity and authorization of BGP traffic. Any outsider can inject believable BGP messages into the communication between BGP peers and thereby inject false routing information. Since BGP uses TCP as a transport protocol, outsider sources can also disrupt communications between BGP peers by breaking their TCP connection with spoofed RST packets. To prevent the spoofing or modification of a valid routing protocol message, message authentication has been added to all these protocols (OSPF, RIP, and BGP). These routing protocols support the MD5 digest. MD5 digest works by creating a 16-byte hash of the routing message combined with a secret key. The 16-byte value is, therefore, message-specific, and modification of the message by an attacker invalidates the 16-byte digest appended to the message. Without the secret key, which is never sent over the wire by the routing protocol, the attacker is unable to reconstruct a valid message. In this test scenario engineers will check if connectivity is succesful or not using MD5 authentication over BGP protocol.

SmartDefense Advisory: CPSA-2004-03 TTG Ref: 9

Results & Comments:

Appendix: Detailed Test Results

Check Point VPN-1 NG Series	Pass	The firewall policy was configured to permit BGP traffic between the routing peers. The SmartDefense setting “Block non-MD5 authenticated BGP connections” was enabled. The gateway successfully blocked non-MD5 authenticated traffic.
Cisco PIX 515E Security Appliance	Fail	The Cisco PIX firewall cannot enforce MD5 hash authentication over BGP packets. The firewall policy was configured to permit BGP traffic between the routing peers. The test showed that the device allowed any type of BGP traffic either authenticated or unauthenticated.
Juniper NetScreen-204	Fail	The Juniper NetScreen gateway cannot enforce MD5 hash authentication over BGP packets. The firewall policy was configured to permit BGP traffic between the routing peers. The test showed that the gateway allowed any type of BGP traffic either authenticated or unauthenticated.

Appendix: Detailed Test Results

Test 6 — SOCKS-based Trojans: Block SOCKSv4

Description:

A vulnerability exists in the SOCKS protocol. The protocol has been used by worms with Trojan capabilities to gain control over systems. Some of the worms are:

* The mass-mailing Win32.Mydoom opens and listens on TCP port 1080.The worm acts as a SOCKS proxy and can be used to redirect network traffic through the infected system. (CPAI-2004-02)

* Phatbot/Agobot can run a SOCKS proxy on demand and redirect SOCKS traffic(CPAI-2004-11)

* Win32/Bagle acts as a backdoor Trojan and SOCKS proxy that allows unauthorized access to an affected machine (CPAI-2004-01)

In this test scenario, engineers will use Putty to try to connect using SOCKS 4 and they will check if the connection will be blocked or not.

SmartDefense Advisory: CPAI-2004-25 TTG Ref: 15

Results & Comments:

Appendix: Detailed Test Results

Check Point VPN-1 NG Series	Pass	The firewall policy was configured to permit SOCKS traffic. The SmartDefense setting “Allow SOCKS version 5 Only” was activated. The gateway blocked the connection once it determined that the client tried to use SOCKSv4 and not SOCKSv5.
Cisco PIX 515E Security Appliance	Fail	The Cisco PIX firewall was not able to blocked SOCKSv4 traffic which is vulnerable allowing any attacker to pass worms (ie. My.Doom). The firewall policy was configured to permit SOCKS traffic however the gateway was not able to enforce that only SOCKS version 5 be permitted through the gateway.
Juniper NetScreen-204	Fail	The gateway was not able to block SOCKSv4 traffic. The gateway allowed SOCKSv4 traffic which is vulnerable, allowing any attacker to pass worms (ie. MyDoom). The firewall policy was configured to permit SOCKS traffic however the gateway was not able to enforce that only SOCKS version 5 is permitted through the gateway.

Appendix: Detailed Test Results

Test 7 — SOCKS-based Trojans: Block Unauthenticated SOCKSv5

Description:

In this test scenario, engineers will use Putty to try to connect using SOCKS 5 (with no username/password) and they will check if the connection will be dropped or not.

SmartDefense Advisory: CPAI-2004-25 TTG Ref: 16

Results & Comments:

Check Point VPN-1 NG Series	Pass	The firewall policy was configured to permit SOCKS traffic. In addition, the SmartDefense protections for the SOCKS protocol were enabled. The session was dropped once the NG Series gateway determined that there was no Username and Password for the session.
Cisco PIX 515E Security Appliance	Fail	The firewall policy was set to permit SOCKS traffic. The Cisco PIX firewall allowed unauthenticated non-SOCKSv5 traffic to pass and could not block this traffic.

Appendix: Detailed Test Results

Juniper NetScreen-204	Fail	The firewall policy was set to permit SOCKS traffic. The gateway allowed SOCKSv5 traffic between client-server without requesting authentication. Neither the policy nor the Deep Inspection signatures can be configured to require authentication for SOCKSv5.

Appendix: Detailed Test Results

Test 8 — IRC-based Worms: Enforcement on Non-standard IRC Ports

Description:

IRC-based worms/Trojans target systems on which Internet Relay Chat clients are installed. An IRC worm usually spreads by dropping scripts to an IRC client directory. Some worms have backdoor and Trojan capabilities: they connect to an IRC server on TCP high ports and once they join in a channel on that server, wait for instructions from the remote attacker. A partial list of commands these worms may execute via the IRC from the attacker includes:

* Executing, uploading or downloading files
* Killing or running processes
* Retrieving system information
* Stealing product keys
* Launching attacks on other machines (DDoS)

W.32 Korgo worm

W32.Korgo is a worm that attempts to propagate by exploiting the Microsoft Windows LSASS Buffer Overrun Vulnerability (BID 10108). This worm also attempts to connect to certain IRC channels to enable remote access on the affected machine.

In this test scenario, engineers will use an IRC client (mIRC) to connect to the IRC server on a non-standard port and engineers will check if the connection was dropped or not.

SmartDefense Advisory: CPAI-2004-21 TTG Ref: 18

Appendix: Detailed Test Results

Results & Comments:

Check Point VPN-1 NG Series	Pass	In this test, engineers attempted to pass IRC traffic over the Microsoft SQL TCP port 1433. The firewall policy was set to allow traffic on TCP port 1433 and not to allow IRC standard traffic on the standard IRC port. Next, engineers activated the SmartDefense IRC protection. The gateway blocked the IRC traffic attempting to pass through the gateway on port 1433. The results showed that SmartDefense was able to block IRC traffic even though TCP port 1433 was OPEN to allow MS-SQL traffic through the gateway.
Cisco PIX 515E Security Appliance	Fail	In this test, engineers set a rule in the Cisco PIX firewall to allow TCP port 1433 to pass through the gateway and also to block the standard IRC TCP port 6667. Then, engineers ran the IRC client application through the firewall using TCP port 1433 to check whether or not the firewall will block the traffic. The Cisco PIX firewall allowed the IRC traffic. This proved that the Cisco gateway was not able to distinguish between legitimate traffic passing through on the MS-SQL port and illegitimate traffic passing through on the MS-SQL port.

Appendix: Detailed Test Results

Juniper NetScreen-204	Fail	In this test, engineers set a rule to permit TCP port 1433 and also to block the standard IRC TCP port 6667. Then, they ran the IRC client application through the firewall using TCP port 1433 (SQL standard port) to check whether or not the firewall will block the traffic. The Juniper gateway permitted the IRC traffic to pass through. This proved that the Juniper gateway was not able to distinguish between legitimate traffic passing through on the MS-SQL port and illegitimate traffic passing through on the MS-SQL port.

Appendix: Detailed Test Results

Test 9 — Multiple Vulnerabilities in SQL: Extended Stored Procedures (xp_cmdshell) Protections

Description:

Multiple vulnerabilities in Microsoft's SQL server and SQL monitor service have been found, which a potential attacker may exploit. These vulnerabilities give a malicious user the ability to run forbidden processes on the remote server or cause the server to reveal critical data, which may lead to the launch of other attacks. In this test scenario, engineers will run 'SQLpoke' against the SQL server and they will check if connection was blocked or not. Additionally, engineers will install Microsoft SQL client tools to connect to the server and issue a query. They will check if the connection was blocked or not.

SmartDefense Advisory: CPSA-2003-09 TTG Ref: 29

Results & Comments:

Check Point VPN-1 NG Series	Pass	The firewall policy was configured to permit SQL traffic on TCP port 1433. In addition, the SmartDefense MS-SQL protections were enabled. The Check Point gateway was able to block the use of the malicious commands.

Appendix: Detailed Test Results

Cisco PIX 515E Security Appliance	Fail	In this test, engineers set a rule to allow traffic through TCP port 1433. Then, they opened a session using the default Microsoft SQL login username and password ("sa" and no password). The session was established. As a result, engineers were able to run the "xp_cmdshell" command which can be used maliciously.
Juniper NetScreen-204	Fail	In this test scenario, engineers configure a policy permitting SQL traffic. Then, engineers were able to log into the SQL server using the default SQL administrator username and password ("sa" and no password). Next, engineers executed the "xp_cmdshell" command which can be used maliciously. The outcome proves that the Deep Inspection firewall feature was not able to inspect SQL traffic and block the malicious command.

Appendix: Detailed Test Results

Test 10 — Multiple Vulnerabilities in SQL: Public Queries (sp_start_job)

Description:

In this test scenario, engineers will use the SQL client tool to run the following: USE msdb EXEC sp_start_job @job_name = 'Nightly Backup', and engineers will check if the command was blocked or not.

SmartDefense Advisory: CPSA-2003-09 TTG Ref: 30

Results & Comments:

Check Point VPN-1 NG Series	Pass	The firewall policy was configured to permit SQL traffic on TCP port 1433. In addition, the SmartDefense MS-SQL protections were enabled. The Check Point gateway was able to block the use of the malicious commands.

Appendix: Detailed Test Results

Cisco PIX 515E Security Appliance	Fail	In this test, engineers set a rule to allow traffic through TCP port 1433. Then, they opened a session using the default Microsoft SQL login username and password ("sa" and no password). The session was established. As a result, engineers were able to run the "sp_start_job" command which can be used maliciously.
Juniper NetScreen-204	Fail	In this test scenario, engineers configure a policy permitting SQL traffic. Then, engineers were able to log into the SQL server using the default SQL administrator username and password ("sa" and no password). Next, engineers executed the "sp_start_job" command which can be used maliciously. The outcome proves that the Deep Inspection firewall feature was not able to inspect SQL traffic and block the malicious command.

Appendix: Detailed Test Results

Test 11 — Multiple Vulnerabilities in SQL: Block Admin Login without Password

Description:

In this test scenario, engineers will use the SQL client tool to try to connect to the server using 'sa' as username and no password. Then, engineers will try to connect to the server using another username with no password. Finally, engineers will run Nessus NASL script against the SQL server. All three attempts should be blocked.

SmartDefense Advisory: CPSA-2003-09 TTG Ref: 31

Results & Comments:

Check Point VPN-1 NG Series	Pass	The firewall policy was configured to permit SQL traffic on TCP port 1433. In addition, the SmartDefense MS-SQL protections were enabled. The Check Point gateway was able to block the use of the malicious commands.

Appendix: Detailed Test Results

Cisco PIX 515E Security Appliance	Fail	In this test, engineers set a rule in the Cisco PIX firewall to permit TCP traffic on port 1433 (default SQL port). Then, engineers opened a new session using the default Microsoft SQL administrator login username and password (“sa” and no password) to check whether or not the firewall will allow the session. The Cisco PIX firewall did not block the SQL session using the login information previously described. This proved that the Cisco PIX firewall cannot inspect a SQL application stream and block the session that uses the default login.
Juniper NetScreen-204	Fail	In this test scenario, engineers configured a policy permitting SQL traffic. Then, engineers were able to logged into the SQL server using the default SQL administrator username and password ("sa" and no password). The outcome proved that the Deep Inspection firewall feature was not able to inspect SQL traffic and block the session using the default login.

Appendix: Detailed Test Results

Test 12 — Microsoft SSL Library Remote Compromise Vulnerability: Block Malformed PCT (Protected Communications Transport)

Description:

The severity of this vulnerability is compounded by the fact that SSL is most often used to secure communications involving confidential or valuable information, and it is therefore believed that hackers will aggressively target this vulnerability. An available exploit sends a malformed SSL/PCT CLIENT_HELLO message, along with sufficient code that allows it to open a remote shell on the victim's server. Once exploited, a remote shell is created on the target system on TCP port 31337. In this test scenario, engineers will run two specific exploits which will try to establish connection. Engineers will check if both trials were blocked.

SmartDefense Advisory: CPAI-2004-19 TTG Ref: 33

Results & Comments:

Appendix: Detailed Test Results

Check Point VPN-1 NG Series	Pass	The firewall policy was configured to permit SSL traffic. In addition the SmartDefense “Block SSL null-pointer assignment” was enabled. Both exploits were successfully blocked (1) Exploit from http://www.k-otik.com/exploits/04242004.iis5x_ssl_pct.pm.php and (2) Exploit: http://www.metasploit.org/projects/Framework/exploits.html#windows_ssl_pct)
Cisco PIX 515E Security Appliance	Fail	The firewall policy was set to permit SSL traffic. The Cisco device did not inspect SSL traffic properly. The outcome showed a malformed "client_hello" message been allowed through the gateway which means the device did not enforce a proper SSL handshake.
Juniper NetScreen-204	Fail	The firewall policy was set to permit SSL traffic. The Deep Inspection firewall feature did not inspect SSL traffic properly. The outcome showed a malformed "client_hello" message been allowed through the gateway which means the device did not enforce a proper SSL handshake.

Appendix: Detailed Test Results

Test 13 — IKE Aggressive Mode Vulnerabilities: Block IKE Aggressive Exchange

Description:

By design, the IKE protocol does not encrypt the identities of the initiator or responder when Aggressive Mode is used for shared secret authentication. Devices that implement this protocol as specified will leak username information while negotiating IKE sessions. In this test scenario, engineers will try to pass an 'IKE Aggressive' packet and they will check if the connection would be dropped or not.

SmartDefense Advisory: CPAI-2004-15 TTG Ref: 36

Results & Comments:

Check Point VPN-1 NG Series	Pass	The firewall policy was configured to permit VPN traffic using IKE. In addition, the SmartDefense protection “Block IKE aggressive exchange” was enabled. The client sent an IKE "Aggressive Mode" malformed packet through the gateway. The gateway blocked the traffic.

Appendix: Detailed Test Results

Cisco PIX 515E Security Appliance	Fail	In this test, the Cisco PIX device was not able to block IKE “Aggressive Mode” traffic passing through it. Engineers used a server behind the gateway such that the client attempted to establish an IKE “Aggressive Mode” session through the gateway. The outcome showed an establishment of an IKE “Aggressive Mode” session. By default, the Cisco VPN client uses “Aggressive Mode”. The gateway was not able to restrict IKE "Aggressive Mode" traffic.
Juniper NetScreen-204	Fail	In this test, the firewall policy was set to permit IKE traffic. The test showed that IKE “Aggressive Mode” traffic was allowed through the gateway. The gateway was not able to block IKE “Aggressive Mode” traffic.

Appendix: Detailed Test Results

Test 14 — OpenSSL Null-Pointer Assignment Vulnerability: Enforcement of SSL Length

Description:

OpenSSL contains a null-pointer assignment in the do_change_cipher_spec() function. By sending a specially crafted SSL/TLS handshake to an application that uses a vulnerable OpenSSL library, a remote, unauthenticated attacker could cause OpenSSL to crash. Repeated exploitation of this vulnerability would result in a Denial of Service (DoS) in the target application. In this test scenario, engineers will run a special PERL command exploit. Engineers will check if the attack was blocked or not.

SmartDefense Advisory: CPAI-2004-19 TTG Ref: 38

Results & Comments:

Check Point VPN-1 NG Series	Pass	The firewall policy was set to permit SSL traffic. In addition, the SmartDefense protection “Block SSL null-pointer assignment” was enabled. The exploit tried to establish a connection using a malformed SSL handshake to the server. The gateway blocked the malicious traffic.

Appendix: Detailed Test Results

Cisco PIX 515E Security Appliance	Fail	In this test, engineers set a rule to permit SSL traffic through port 443. During the testing, engineers found that both client and server were able to transmit buffer overflow. The Cisco PIX device was not able to validate a SSL handshake. The vulnerability is that attackers can pass a buffer overflow using a specially crafted handshake.
Juniper NetScreen-204	Fail	In this test, engineers set a rule to permit SSL traffic through port 443. During the testing, engineers found that both client and server were able to transmit buffer overflow. Juniper's NetScreen device was not able to validate a SSL handshake. The vulnerability is that attackers can pass a buffer overflow using a specially crafted handshake.

Appendix: Detailed Test Results

Test 15 — Microsoft ASN.1 Remote Code Execution: Enforcement over NTLM (NT LAN Manager)

Description:

A security vulnerability exists in the Microsoft ASN.1 Library that could allow code execution on an affected system. The vulnerability is caused by an unchecked buffer in the Microsoft ASN.1 Library, which could result in a buffer overflow. An attacker who successfully exploited this buffer overflow vulnerability could execute code with system privileges on an affected system. The attacker could then take any action on the system, including installing programs, viewing data, changing data, deleting data, or creating new accounts with full privileges. In this test scenario, engineers will run a special exploit and they will check if the connection was dropped or not.

SmartDefense Advisory: CPAI-2004-07 TTG Ref: 41

Results & Comments:

Appendix: Detailed Test Results

Check Point VPN-1 NG Series	Pass	The firewall policy was set to permit NTLM traffic. In addition, the SmartDefense protection “Block ASN.1 BitString encoding attack” was enabled. During the test, Client-server NTLM authentication was established; however, once the client transmitted the malicious ASN.1 bitstream code, the gateway blocked that part of the session.
Cisco PIX 515E Security Appliance	Fail	In this test, engineers set a rule to permit NetBIOS over TCP port 139 which is a core Microsoft Networking protocol. The exploit opened an NTLM session with a Windows Server delivering an attack to the ASN.1 library on the target server. The client and server machines received the buffer overflow. The Cisco PIX device was not able to block this attack.
Juniper NetScreen-204	Fail	In this test, set a rule to permit NTLM traffic. Engineers were able to pass the ASN.1 vulnerability over SMB and trigger the buffer overflow despite the activation of the relevant DI protections.

Appendix: Detailed Test Results

Test 16 — Microsoft SQL Worm (Slammer): Slammer Test

Description:

This worm attempts to exploit Microsoft SQL server vulnerable to the SQL Server Resolution service buffer overflow (CVE CAN-2002-0649), or another, unknown Microsoft SQL vulnerability. Once a vulnerable computer is compromised, the worm will infect that target, randomly select a new target, and resend the exploit and propagation code to that host. The worm resident only in memory and it is undetected by Anti Virus systems. In this test scenario, engineers will configure Microsoft SQL server protocol and Microsoft SQL Monitor protection in the SmartDefense tab; then they will run a special exploit. Finally, engineers will check the log file containing such attack.

SmartDefense Advisory: CPAI-2003-04 TTG Ref: 47

Results & Comments:

Check Point VPN-1 NG Series	Pass	The firewall was configured to permit traffic over TCP port 1433. In addition, the relevant MS-SQL SmartDefense protections were enabled. The SQL "Slammer" worm was successfully blocked by the gateway.

Appendix: Detailed Test Results

Cisco PIX 515E Security Appliance	Fail	The firewall policy was set to permit TCP port 1433. The Cisco PIX device did not restrict engineers from using the Microsoft SQL default login username and password ("sa" and no password). As a result, engineers were able to attack the SQL server using the "Slammer" worm.
Juniper NetScreen-204	Fail	The firewall policy was set to permit TCP port 1433. Juniper's NetScreen device did not restrict engineers from using the Microsoft SQL default login username and password ("sa" and no password). As a result, engineers were able to attack the SQL server using the "Slammer" worm.

Appendix: Detailed Test Results

Test 17 — Microsoft JPEG Processing Buffer Overflow Vulnerability: JPEG Exploits

Description:

Component included in several Microsoft products. Systems affected are those that provide an operating system version of the GDI component that is vulnerable to this issue. This vulnerability is triggered by a malformed JPEG image file. An attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs, viewing, changing or deleting data; or creating new accounts with full privileges. The vulnerability has been publicly exploited. In this test scenario, engineers will try to download two files: a malicious JPEG image, and a valid JPEG image. Engineers will check if both downloads were successful or not.

SmartDefense Advisory: CPAI-2004-42 TTG Ref: 49

Results & Comments:

Appendix: Detailed Test Results

Check Point VPN-1 NG Series	Pass	The firewall policy was set to permit HTTP traffic. In addition, the SmartDefense protection “Malformed JPEG” was enabled. Two files were used for this test: "evil.jpg" and "test4.jpg". The first file contains malicious code and the second file was a valid JPEG image. The gateway successfully blocked the attempt to download "evil.jpg" and only allowed "test4.jpg".
Cisco PIX 515E Security Appliance	Fail	In this test, engineers set a rule to permit TCP traffic on port 80 with the HTTP protocol fix-up enabled. Then, they attempted to download both files ("evil.jpg" and "test4.jpg") to check whether or not both files can be downloaded. The Cisco PIX device allowed both files to be downloaded, including "evil.jpg" (malicious JPEG code), which shows that the device was not able to block this exploit.
Juniper NetScreen-204	Fail	In this test, engineers set a rule permitting TCP traffic on port 80. Then, they attempted to download both image files ("evil.jpg" and "test4.jpg"). Both files were successfully downloaded, including the "evil.jpg" (malicious JPEG code), which means the Deep Inspection feature was not able to stop it, despite the fact its signatures were enabled.

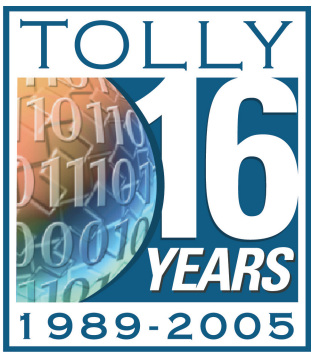
The Tolly Group
Devices Under Test Information

Vendor:	Check Point Software Technologies Ltd.
Product Name:	Check Point VPN-1 NG Series
Software/Firmware Rev Level:	Early Availability 1 R60
Description:	Software-based firewall and VPN system with "inline" intrusion prevention capabilities. SmartDefense service option provides real-time, dynamic updates to protect against new vulnerabilities.
Details:	Platform: Dell PowerEdge 1750, Intel Dual Xeon 3.06GHz, 1GB DRAM

Vendor:	Cisco Systems, Inc.
Product Name:	Cisco PIX 515E Security Appliance
Software/Firmware Rev Level:	PIX OS 6.3.4
Description:	Purpose-built firewall/VPN device with application security
Details:	Processor: 433-MHz Intel Celeron Processor - Advanced application and protocol inspection.

Vendor:	Juniper Networks, Inc.
Product Name:	Juniper NetScreen-204
Software/Firmware Rev Level:	ScreenOS 5.1 with latest available DI signature database at time of test.
Description:	Purpose built firewall/VPN device with "Deep Inspection(tm)" (in-line IPS) capability outfitted with 4 10/100 interfaces.
Details:	- Supports up to four 10/100 Mbps interfaces. - Delivers up to 400 Mbps Forward and 200 Mbps 3-DES VPN. - Supports up to 128,000 sessions. - Supports up to 4,000 policies.

Information technology is an area of rapid growth and constant change. The Tolly Group conducts engineering-caliber testing in an effort to provide the internetworking 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

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