



Solving the Performance Hurdle for Integrated IPS

New Check Point Technologies Enable a Full-Function,
Integrated Intrusion Prevention System without
Compromise to Performance or Security

Contents

Executive Summary	3
Specifying Performance for Integrated IPS	4
New Check Point Technology for Top Performance of Integrated IPS ...	5
Acceleration Technology—SecureXL™	6
Efficient Use Multiple CPU Cores—CoreXL™	7
Efficient Distribution of Network Traffic—ClusterXL®	8
Scalable	9
Focused Inspection—Accelerated Stateful Packet Inspection	9
Identification of Performance Bottlenecks	10
Protect Your Network with Integrated IPS.....	11

Executive Summary

Whenever IT performance barriers fall, there is a discovery phase as organizations learn they can solve formally unsolvable roadblocks to critical services. This white paper describes such an event for network security. For the first time, new processing technologies for a network gateway have enabled a full-function integrated intrusion prevention system (IPS) coupled with the next generation firewall—without performance limitations. These performance-enabling innovations for IPS have arrived just in time, for unpredictable, rapidly changing security threats are demanding closer integration of IPS and firewall functionality to keep networks secure.

The driver for integrated IPS is a deluge of attacks exploiting vulnerabilities in the application layer. Web applications comprised almost 55% of all vulnerability disclosures in 2008.¹ Attacks based on these vulnerabilities often evade usual port/protocol defenses established by a firewall, so detection requires deep-packet inspection with intrusion prevention. But mere inspection of packets at a deep level is not enough. The IPS must also automatically integrate its deep-packet inspections with firewall operations, and direct the firewall to block attacks that would otherwise evade defenses. Historically, integrated IPS functionality would computationally stress the typical firewall or even crash it. Network managers often turned off IPS integration with the firewall to ensure connectivity—but at the cost of weakening security.

The dilemma of connectivity or security is now moot. New performance-enabling technology from Check Point allows implementing as much integrated IPS functionality as required without system degradation. The Check Point Security Gateway R70 allows a full-function IPS integrated into the industry's leading firewall. This white paper provides background about performance issues to help you specify integrated IPS for your organization's network. It also describes how new technologies in the Security Gateway R70 will help you solve typical performance hurdles for full-function, integrated IPS without compromise to performance or security.

¹IBM ISS X-Force 2008 Trend & Risk Report.

Specifying Performance for Integrated IPS

An intrusion detection and prevention system will help your organization secure its enterprise network, and protect servers and critical data against known and unknown worms, automated malware, and blended threats—especially those exploiting application-layer vulnerabilities. The IPS system you choose should provide robust security, protecting your network and business against increasingly sophisticated attacks and attack vectors. Efficient management and compliance are also crucial; they should overcome data overload, focus on what's critical, and track compliance issues. The IPS should also provide flexible deployment to meet ever-changing security needs.

Above these considerations, your IPS must provide high performance, especially when you intend to run a full suite of in-line, integrated IPS functions that make access control decisions executed by the enterprise firewall. The following performance-related questions include business considerations that will help you specify an integrated IPS that is right for your organization.

Will the IPS meet my performance requirements? Networks are increasingly transitioning from 1G to 10G Ethernet. That's a huge jump in capacity for the growing use of multimedia applications such as Voice-over-IP and IP-based videoconferencing. More volume and faster transmission of packets, however, dramatically increases processing requirements for security in data centers and the network edge. High throughput and low latency are essential. Another common performance trouble point is the gateway connecting a branch or small office. The combination of slower wide area transmission links with multimedia applications used in remote sites demands similar high performance for the IPS and other gateway security services used to protect the network.

Does the IPS provide security at the performance level that I need?

Traditional firewall port/protocol access controls alone are no longer sufficient to protect against threats that have evolved to travel across well known ports used for normal application processing. Application-layer threats are increasingly the vector of choice of hackers and malware. These attacks, disguised as legitimate traffic, require a deeper level of inspection that needs more processing power. Your IPS must allow all required functions enabled without system degradation.

Is redundancy and reliability built into the IPS? Reliability of the IPS is crucial, for its failure, along with any other network component or application can trigger lost revenue for every second of down time. At the same time, security gateways must provide continuous protection against real attacks and not drop valid traffic for the wrong reasons. Specifications for an IPS should include redundancy, and reliable non-stop operations and service consistency.

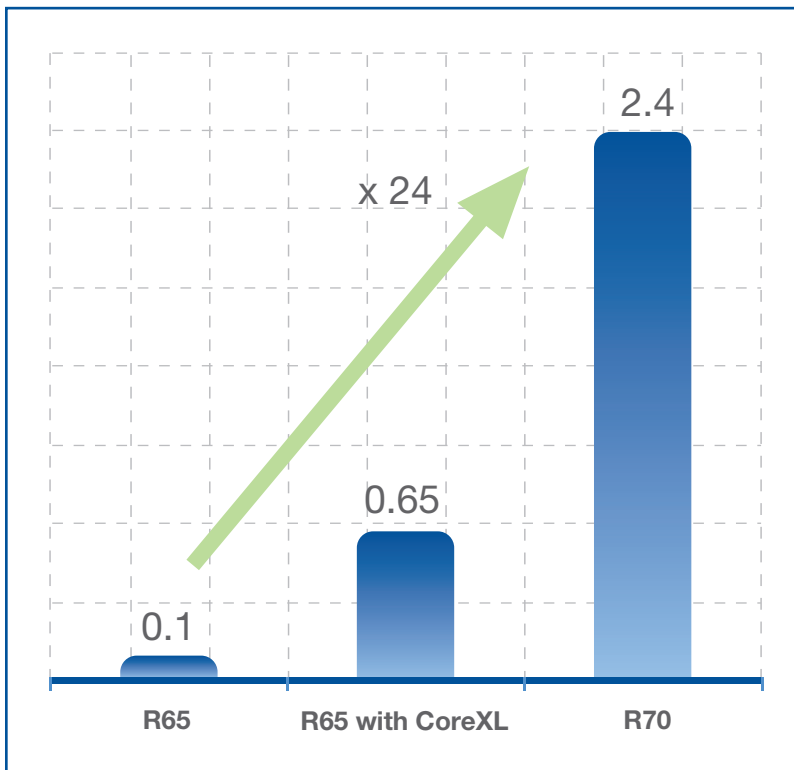
Will the IPS scale as my infrastructure needs change? All large organizations need an IPS solution that keeps pace with changes in computer processing architecture, and is flexible enough to adapt to hardware from different platform vendors. The IPS system should include the ability to scale performance for any enterprise-class security processing requirement.

Is the IPS manageable and updateable? Administrators need an easy way to see which IPS protections affect performance, and by how much. Protections must be updateable with the newest vulnerability signatures to meet evolving threats and changes to enterprise systems. The IPS should include ease of manageability of these functions for lower cost of ownership.

New Check Point Technology for Top Performance of Integrated IPS

The core architecture of an IPS will determine how well it meets specifications described above. The Check Point Open Performance Architecture is designed to provide the best intrusion prevention system available. Research and development focuses on technologies that increase the level of security within customer environments. Check Point works closely with microprocessor manufacturers, such as Intel, to ensure Check Point solutions take maximum advantage of processor platform capabilities. Technology sharing through these partnerships also helps drive the total cost of the integrated IPS solution much lower. The result is an open security ecosystem where each partner specializes in its area of expertise, for a cost-efficient integrated solution that protects networks better than a closed, proprietary IPS system.

The Check Point Open Performance Architecture underpins its integrated IPS with three performance-oriented technologies: SecureXL, CoreXL, and ClusterXL. These technologies work together to maximize IPS performance across a wide set of open servers and appliances.



*IPS Recommended Profile, Traffic Blend, and Throughput (Gbps)
Check Point Power-1 9070 appliances*

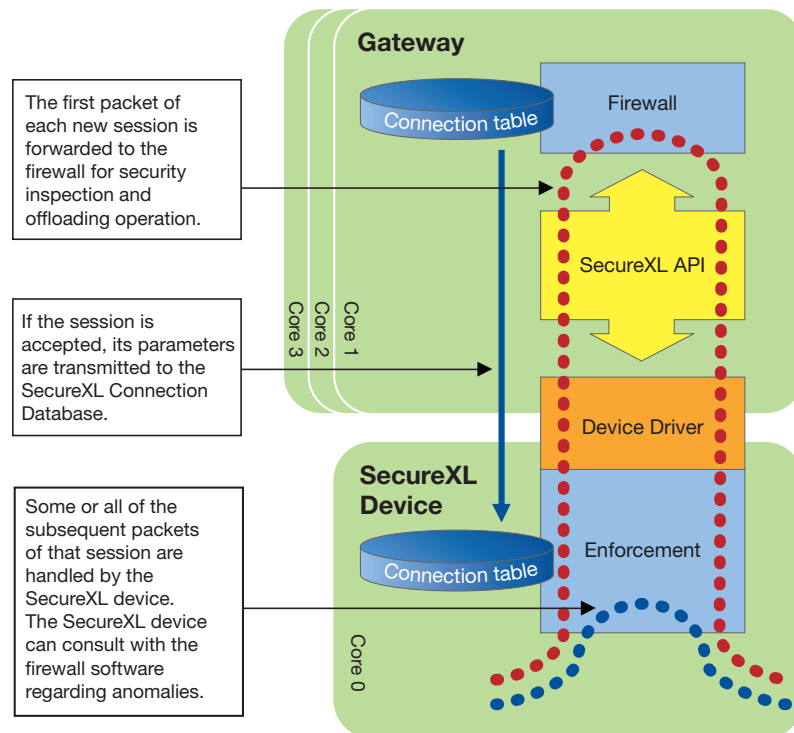
When run on a multi-core processor, the Check Point Security Gateway R70 provides near linear scalability (>70%) per additional core. Throughput performance of the IPS engine can increase an average of 600% with CoreXL activation. Testing parameters were a strict protection profile with 80% of IPS settings activated. Network traffic passed through the gateway represented a blend of protocols and applications similar to that found on the Internet.

Acceleration Technology – SecureXL

SecureXL is a patented technology consisting of a software package with an API for the acceleration for multiple, intensive security operations. In addition to the IPS, SecureXL also accelerates operations carried out by a Stateful Inspection firewall from Check Point. Through the SecureXL API, this firewall can offload the handling of those operations to a special module, the “SecureXL device,” which is a performance-optimized software module.

In a SecureXL-enabled gateway, the firewall first uses the SecureXL API to query the SecureXL device and discover its capabilities. The firewall then implements a policy that determines which parts of what sessions are to be handled by the firewall, and which should be offloaded to the SecureXL device. When new sessions attempt to get established across the gateway, the first packet of each new session is inspected by the firewall to ensure that the connection is allowed by the security policy. As the packet is inspected, the firewall determines the required behavior for the session, and based on its policy it may then offload some or all of the session handling to the SecureXL device. Thereafter, the appropriate packets belonging to that session are inspected directly by the SecureXL device. The SecureXL device implements the security logic required for further analysis and handling of the traffic. If it identifies anomalies it then consults back with the firewall software and IPS engine. In addition, SecureXL provides a mode that allows for connection setup to be done entirely in the SecureXL device, thus providing extremely high session rate.

Simplified example of SecureXL process



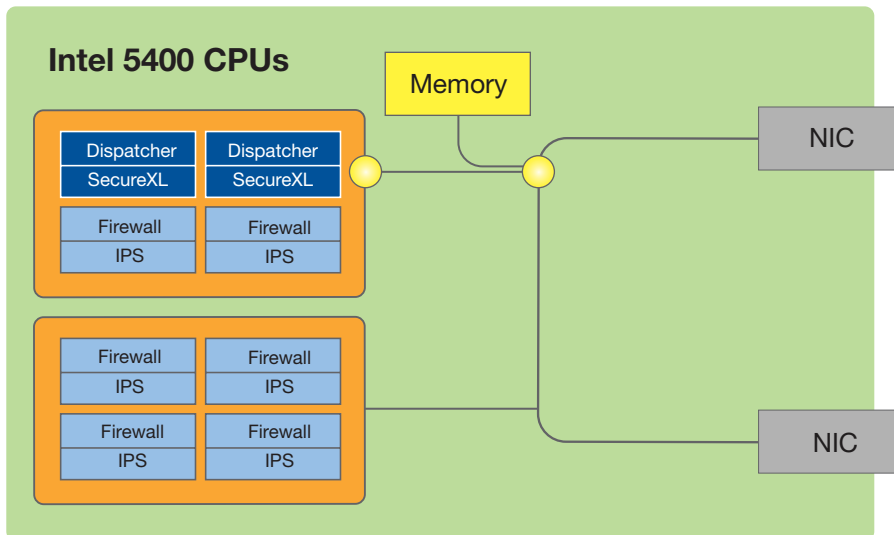
SecureXL in Multi-core CPU Minimizes Performance Hits to Integrated IPS

Performance is achieved via optimized network interface drivers and multi-threaded code in software or in hardware devices that are SecureXL-capable. Together, this combination of features increases throughput by a factor of 3X when compared to un-accelerated solutions. The end result is the best price/performance combination on the market. In a multi-core system one or more processors can be assigned to do SecureXL processing and dispatch non-accelerated packets among IPS and firewall kernel instances running on separate cores. SecureXL enables the integrated IPS and firewall to adjust and attain the optimal balance between security and performance requirements.

Efficient Use Multiple CPU Cores – CoreXL

CoreXL is the first security technology to fully leverage general-purpose multi-core processors. It introduces advanced load balancing to boost throughput for the deep inspection required to achieve integrated IPS on the firewall. The increased processing capability in multiple cores allows networks to have high performance as well as a high level of security.

When CoreXL technology is activated, it immediately assigns one or more cores that are performing SecureXL acceleration to also act as directors for traffic. The other cores are designated to run instances of IPS and Firewall on each core. For example, if an appliance contains two quad-core processors, two cores will perform SecureXL acceleration and direct traffic to the other six cores that run IPS and Firewall instances. The cores acting as directors have two main functions. First, it makes the initial security decisions whether this traffic can be accelerated by SecureXL. Second, it assigns traffic to a core to handle additional security inspection if needed.



Multi-core CPUs Enable Dedicated Processing for Integrated IPS

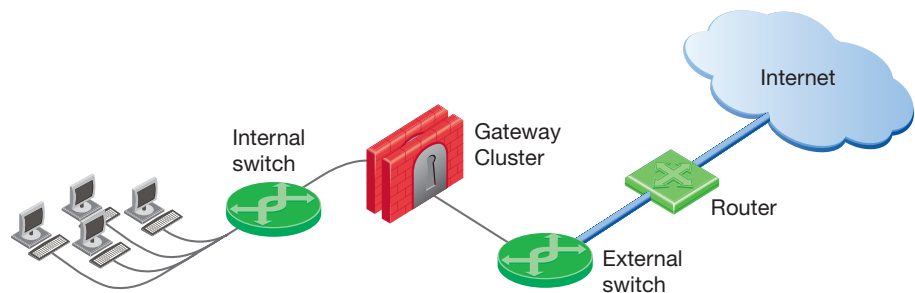
Efficient Distribution of Network Traffic—ClusterXL

ClusterXL provides a method for high traffic volumes to be intelligently spread across multiple gateways. This provides scalability and greatly increases reliability. A gateway cluster can be physically located in a single location or separated and connected via an internal backbone, further increasing the redundancy needed for business continuity.

In operation, each Security Gateway R70 that is a cluster member maintains its own IP address and physical MAC address. To systems that are not part of the cluster, it will appear that all cluster members have a single virtual IP address that represents the cluster. On both the internal and external networks, the gateways will be joined together.

These processes enable information to be shared quickly between cluster members. The communications exchange is used to ensure synchronization of security information and decisions between multiple Security Gateway R70s. This is necessary because network traffic may not exit a network from the same cluster member that was previously used for entry. Sharing firewall, VPN, NAT, and IPS tables is called state synchronization and ensures that if a gateway becomes unavailable, other gateways can allow traffic to continue without interruption. In the event of a failover, the cluster member uses the synchronized state tables to ensure that the security inspection continues as before on the active (non-failed) cluster members.

The actual load sharing decision is made in one of two ways: Unicast or Multicast mode. In Unicast mode, one of the Security Gateway R70s acts as a “pivot,” or coordinator for the cluster. This pivot will receive all incoming traffic and then decides which cluster member will handle the connection or traffic. In Multicast mode, physical network interface cards can be bonded, or joined together, to form a single virtual interface with a single virtual MAC address. This gives the administrator additional flexibility in handling complex deployment scenarios involving multiple network segments. In this scenario, each cluster member with a virtual interface receives all packets. Each gateway decides whether it should take the packet, with one gateway taking responsibility for it. After the initial packet, that gateway is responsible for that connection.



Scalable

Check Point is leading the security industry with changes in computer processing architecture, and is flexible by adapting to different vendor platforms.

The following points chronicle the evolution of Check Point's IPS performance:

- 2001 and earlier: Kernel mode security is performance oriented
- 2001: SecureXL (Awarded Patent # 6,496,935) Security Acceleration API to provide highly optimized security processing can be utilized both on hardware level or in software (Performance Pack)
- 2002: ClusterXL Load Sharing is released, providing multi-nodal scalability
- 2002: Multi-threaded SecureXL—Performance Pack provides kernel level multi-threading for scaling up VPN performance
- 2004: SecureXL medium-path, a SecureXL architectural enhancement enabling optimized code running from both Performance Pack (multi-threaded) and Firewall context
- 2006: ClusterXL VLSLS (Pending Patents 1893/43; 1893/46)—ClusterXL enhancements for providing multi-nodal near linear scalability—VSX NGX Scalability Pack is launched
- 2007: CoreXL - Worry free security (Pending Patent 1893/46) Architecture for scaling up kernel Firewall security processing by amount of cores
- 2008: IPS Security Engines—Fusion of CoreXL with SecureXL medium path to provide kernel level multi-threading

Focused Inspection— Accelerated Stateful Packet Inspection

In 2009, Check Point offers the latest advance in the Open Performance Architecture; a high performance IPS engine accelerated by fusing CoreXL with SecureXL Security Gateway R70 includes a new multi-tier IPS engine running as instances that are distributed among multiple CPU cores and optimized within SecureXL contexts.

Once a connection is established and registered in the SecureXL connection table, the Secure Network Dispatcher assigns a CPU core to perform additional inspections. Each core has an infrastructure layer called the Passive Streaming Library, which provides packet reordering, congestion handling, and serves as a middleman between the various security applications and the network packets.

One security application is the new multi-tiered IPS engine. The Internet Protocol Suite is composed of a set of protocols and rules specifying how data should be formatted, addressed, routed, and delivered to the right destination. One layer of the IPS inspection engine quickly identifies anomalous packets that are out of compliance with these standards.

Performance Enhances IPS Detection Engine

Check Point IPS performance technology ensures functionality of the detection engine.

- Limited false positives
- Secure
- Reliable
- Timely updates
- Application aware
- Granular control

Learn more about the Security Gateway R70 detection engine in a companion paper, [Proving Technical Confidence in Your IPS Detection Engine](#).

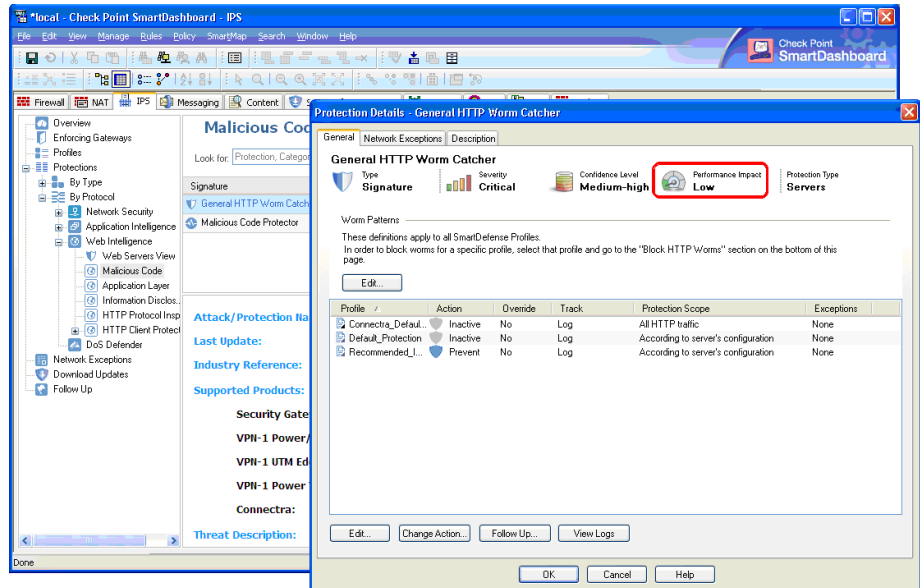
Other attacks occur within packets that comply with the standards and target specific application or host vulnerabilities. Some of these attacks inject commands that exploit known and unknown vulnerabilities. One method of identifying these attacks is to identify the commands used and block them. Other attacks take advantage of the lack of adequate protections in applications and operating systems to specify buffer limits. In this case, an attacker can craft a packet that includes commands for running outside of the context of the normal application processing yet with the same operating system privileges.

Security Gateway R70 employs a fast pattern-matching engine to identify attacks that are known and unknown by looking at the specific contexts where the attack occurs in the packet stream. This is done in a two-tiered inspection. The first tier quickly filters out about 90% of the malicious traffic. Adding additional signatures on the same protocol has minimal impact on performance.

Identification of Performance Bottlenecks

Administrators need an easy way to see which protections affect performance. Protections must be updateable and open to keep up to date as threats evolve and systems change from being hardened to vulnerable as threats evolve. At the same time updating and adding more protections should not create a management nightmare.

The Security Gateway R70 provides the ability to apply granular protections based on their performance impact. A management console clearly marks each protection with a performance impact setting; Low, Medium, High, or Critical (see screen shot, next page).



SmartDashboard shows exact performance impact of any security setting.

Protect Your Network with Integrated IPS

The Check Point Security Gateway R70 provides the foundation for integrated IPS required by large organizations to gain high performance while maintaining a high level of security—all at an affordable price per Gbps of throughput. The Open Performance Architecture of the Security Gateway R70 will help your organization protect its network from evolving application-layer threats, without sacrificing performance or connectivity. Patented technologies underpin performance: ClusterXL, SecureXL, CoreXL, and a new turbocharged IPS engine will deliver the performance you need to meet all integrated IPS requirements. Check Point, the worldwide leader in securing the Internet, invites you to contact us for more information about Security Gateway R70. To learn more, please contact a Check Point sales representative at www.checkpoint.com.



About Check Point Software Technologies Ltd.

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

CHECK POINT OFFICES

Worldwide Headquarters

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

U.S. Headquarters

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

©2009 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMSecure, INSPECT, INSPECTXL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpec, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, SmartSecurity, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, the totalsecurity logo, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.