



Check Point Software Blade Architecture

Achieving the right balance between security
protection and investment

Contents

Introduction	3
Check Point Software Blade architecture overview	3
What makes Software Blade architecture different?	4
Total Security™	5
Flexibility	5
Simplicity	6
Multi-core optimized security software	6
Benefits of Software Blade architecture	7
Business Scenario 1: Consolidate security functions	7
Business Scenario 2: Open new branch office	9
Blade functions	10
Balancing security protection and investment	12

Introduction

IT professionals understand that “one-size-fits-all” security solutions are making it more difficult to adjust to changing business needs. Challenges, such as increasing pressure to reduce total cost of ownership (TCO), combating evolving threats, and keeping things simple and manageable, can be compounded when a security infrastructure is inflexible.

Complicating matters is that each organization has a different set of security requirements. For example, large organizations typically prefer best-of-breed security products for a specific problem, while small organizations favor unified security that can be managed by a single administrator. Trying to meet these different requirements with the typical ‘one-size-fits-all’ solution can lead to excessive investment in unnecessary functionality or risk exposure due to not meeting a special security need.

Security environments are growing in complexity because it is necessary to continually add more and more functions, like firewalls, intrusion prevention systems (IPS), IPsec VPN, and antivirus, just to name a few. When these functions are supported by distinct appliances, they can be difficult to integrate, test, and manage.

The Check Point Software Blade architecture provides a better alternative to deploying disparate, stand-alone security systems in order to keep up with evolving security threats. This architecture is based on independent security modules that all run on a single platform, simplifying integration and management. This revolutionary security architecture delivers a simple, flexible, and manageable total security solution. Organizations can customize security configurations to dial in the right mix of protection and investment while having the ability to easily consolidate, re-allocate, migrate, and scale up systems in the future, as needed.

Check Point Software Blade architecture overview

Check Point has developed a unique Software Blade architecture that enables IT organizations to consolidate security functions onto a single system while still maintaining network performance service level agreements (SLAs). Security functions, called Check Point Software Blades, are independent and flexible security modules that allow organizations to enable the functions they want in a custom security solution. These modules can be deployed as needed on any gateway or management system by just “turning on” functionality—no hardware, firmware, or driver upgrades required. This enables organizations to deploy security dynamically with lower total cost of ownership.

Similar to various hardware blades running in self-contained chassis, software blades are modular, interoperable security functions that share a common platform, called a “container”, as illustrated in Figure 1. The container controls software blade operations, ensuring efficiency, scalability, and central manageability and comprising the following software components:

- **Hardened operating system:** Eases security solution deployment on standard servers located anywhere in the network
- **Software blade license management:** Facilitates blade activation and migration
- **Blade update mechanism:** Keeps blades current with the latest software

- **System utilities:** Assists in backup, restore and upgrading of the operating environment
- **Web-based GUI:** Simplifies administration of the operating environment

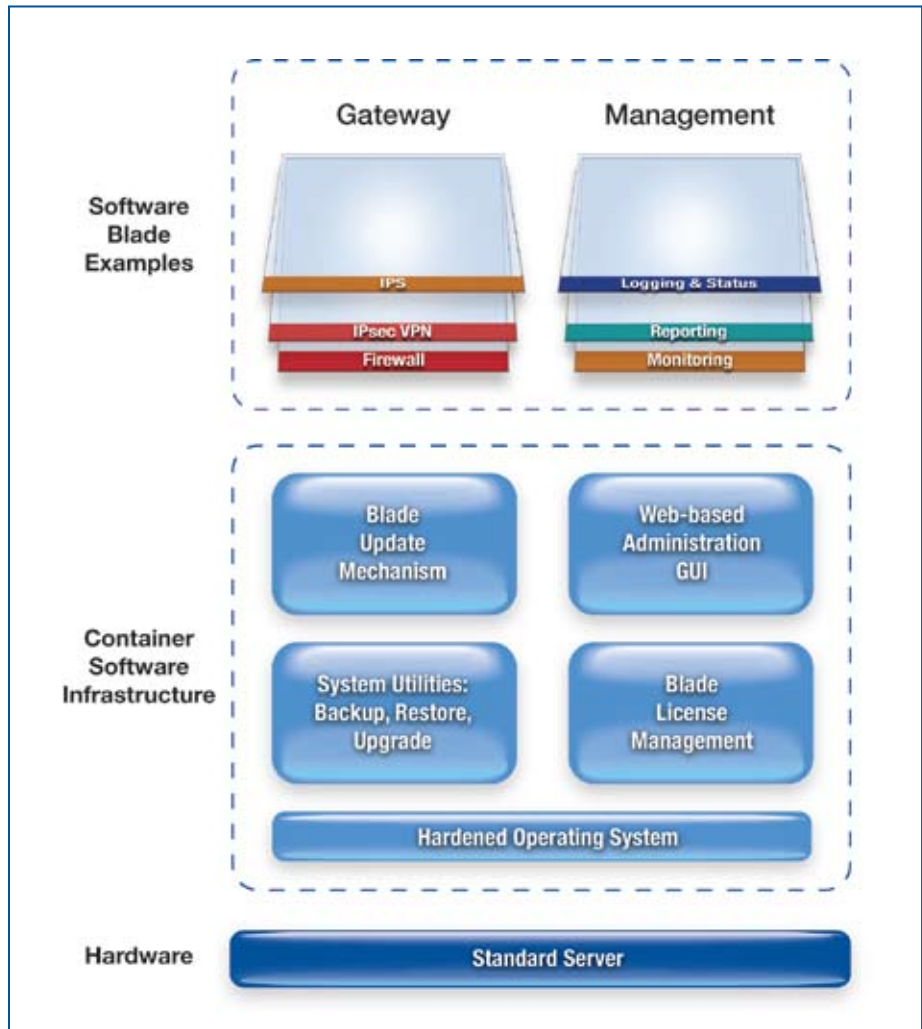


Figure 1. Software Blade container for security functions

What makes Software Blade architecture different?

Check Point Software Blade architecture is different because it allows IT to customize a modular security solution on a single, common platform that can easily be extended or modified as needs change. The architecture also delivers a high level of flexibility without sacrificing performance. Security gateway performance can be guaranteed when multiple blades are deployed by enabling performance thresholds. Thresholds, set by IT personnel, control the provisioning of system resources, such as CPU cycles and system memory, to the IPS blade as shown in Figure 2. In this example, IPS inspection can be disabled if the resource usage exceeds defined thresholds. This enables the security gateway to maintain a high level of performance even when under heavy load.

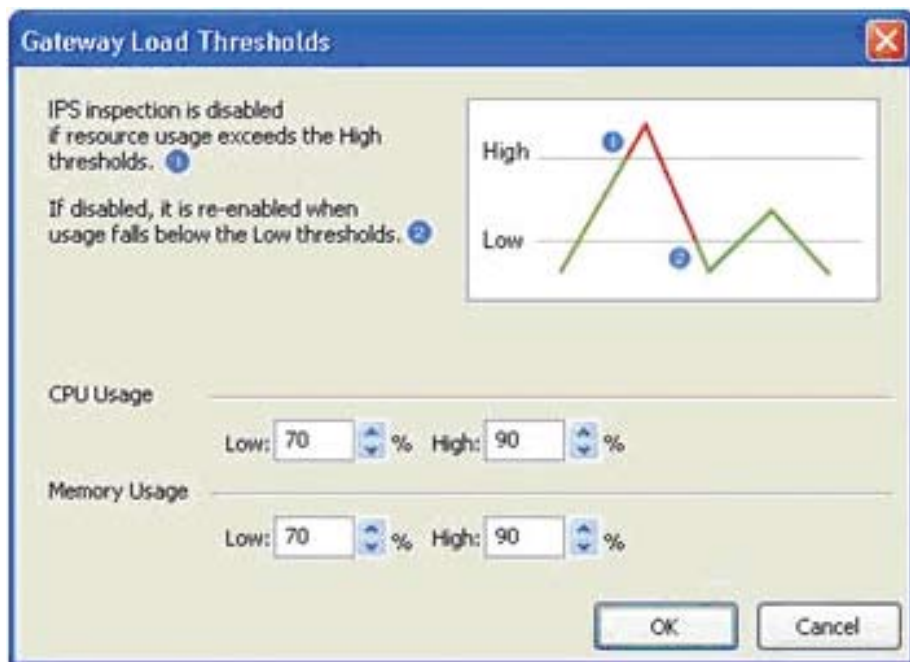


Figure 2. Setting usage thresholds to guarantee performance

This solution supports an unlimited number of system configurations, which makes it easy for organizations to customize and upgrade their security infrastructure by consolidating functions or increasing performance. For example, since all security functions are controlled by a single security management system, IT administrators don't have to master various GUIs, learn new interfaces, or figure out how different vendor solutions interact with each other.

Total Security™

There's no need to cobble together different solutions from various vendors because the Check Point Software Blade architecture is a comprehensive solution comprised of best-of-breed technologies for both security gateway and management functionality. It provides the right level of security at all enforcement points and network layers, which effectively reduces the risk of exposure to security threats.

Flexibility

When organizational needs change, Check Point offers the ultimate flexibility, as all software blades can be easily activated or transferred from one hardware platform to another. Because software blades are completely portable, organizations can easily:

- Consolidate multiple security functions on a single platform
- Change the combination of security functions on a particular gateway
- Offload some functions to a second gateway

Simplicity

It's simple to activate new security functions via the central Software Blade management system, as illustrated in Figure 3. This capability reduces the number of administrative tasks associated with updating, monitoring, event analysis, and reporting.

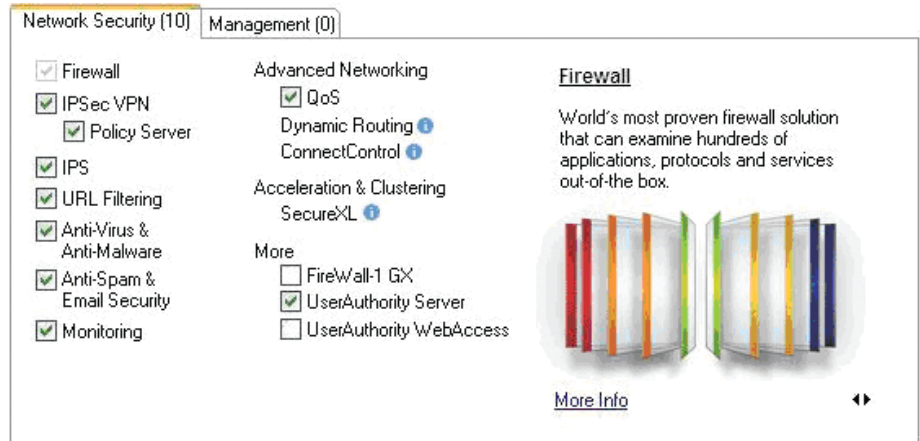


Figure 3. Software Blades can easily be activated from a single interface

Multi-core optimized security software

Designed specifically to leverage the latest multi-core processors, Check Point Software Blade architecture integrates CoreXL™ technology, which increases deep-packet inspection throughput needed for intrusion detection in an integrated security gateway. Using intelligence built into the director core, CoreXL distributes the load equally among the cores running the Check Point security gateway, as shown in Figure 4. CoreXL is designed to use as many cores as are available (4, 8, 16, and so on), enabling it to scale on higher-capacity systems without changes. The Check Point security gateway migrates easily to new systems with more cores and allows companies to increase performance without changing solutions.

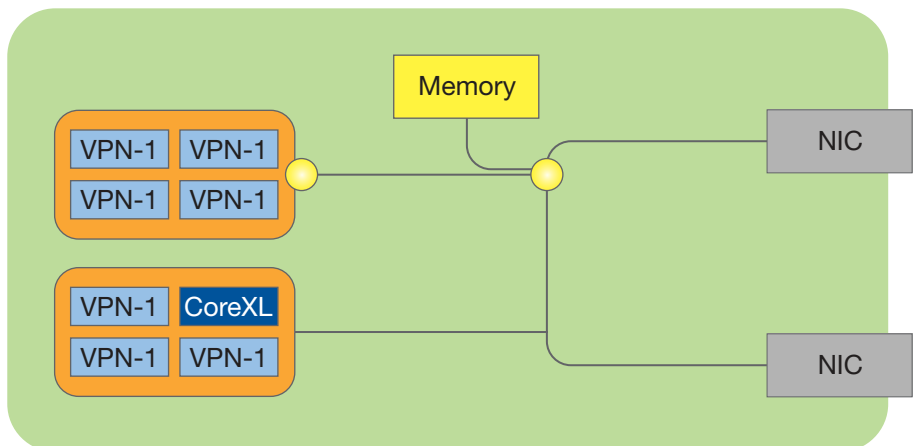


Figure 4. Check Point CoreXL intelligently balances security duties across multiple cores

Benefits of Software Blade architecture

Check Point Software Blade architecture facilitates straightforward configuration and policy changes, including the ability to add new security applications to an existing platform or migrate security functions to another platform in a seamless manner, with no downtime. Like hardware blades, software blades can be added, swapped, or removed as needed. When configuration changes are made, the software blade container (Figure 1) carries out all the necessary adjustments. This simplifies the task of consolidating and adding performance to existing Check Point security solutions and enables organizations to deploy security dynamically.

This solution offers unmatched benefits to organizations responding to changing business and security needs, as shown in Table 1. Check Point Software Blade architecture provides industry-leading security threat protection that is easy to manage and has a lower TCO than one-size-fits-all or multi-vendor solutions. These benefits are discussed in more detail in the next two business scenarios.

Table 1. Key benefits of the Check Point Software Blade architecture

Features	Benefits
Simple deployment and upgrades	Responds to business-environment changes
New security functions run on existing platforms	Reduces TCO (total cost of ownership)
Comprehensive set of security modules	Combats evolving threats
Central management via Web-based GUI	Keeps things simple and manageable

Business Scenario 1: Consolidate security functions

Situation: Business growth has resulted in sprawling security infrastructure that spans many organizations and locations, as shown in Figure 5. The current configuration increases cost and risk because IT administration must support several generations of multi-vendor equipment based on custom hardware and dedicated management software.

IT requirements:

- A standardized security platform that reduces operational expense-related change and configuration management of security systems
- The flexibility to implement global and/or local policy management
- Central visibility into security effectiveness: incident logging and tracking, system health checks, user monitoring, and compliance audits and reporting
- Common hardware that runs all security functions and maximizes the potential cost savings from reducing hardware footprint, rack space, cabling, and utility costs
- System configurations tuned for locations, which avoids the overhead and cost from unused security functions

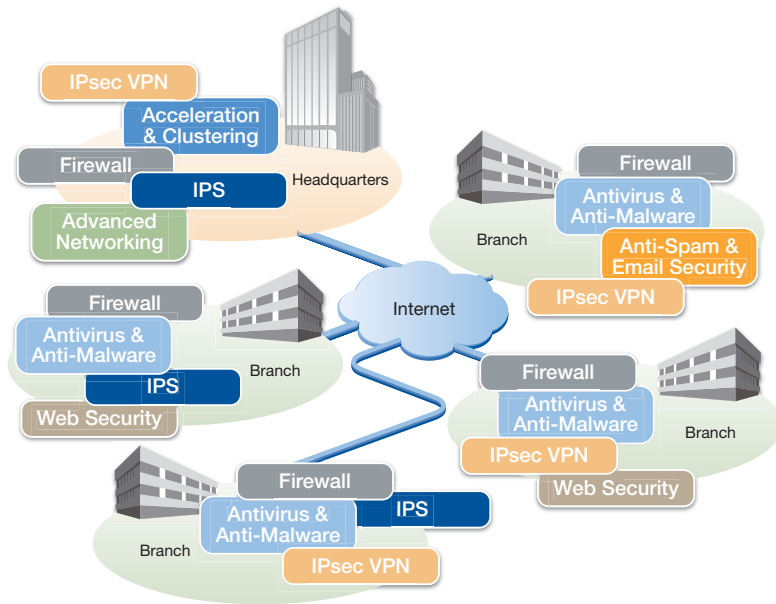


Figure 5. Organizational infrastructure before consolidation

Solution: Check Point Software Blade configurations, as shown in Figure 6 and described in Table 2, are customized for each business location. The same Check Point container software runs at every location, simplifying management and policy proliferation and cutting validation time. Employing a single hardware platform, each location runs the security function it needs, which optimizes cost/performance. IT can easily move functions around, from location to location, and leverage their existing infrastructure. The result is one deployment project, multiple configurations, and a single system-management function.

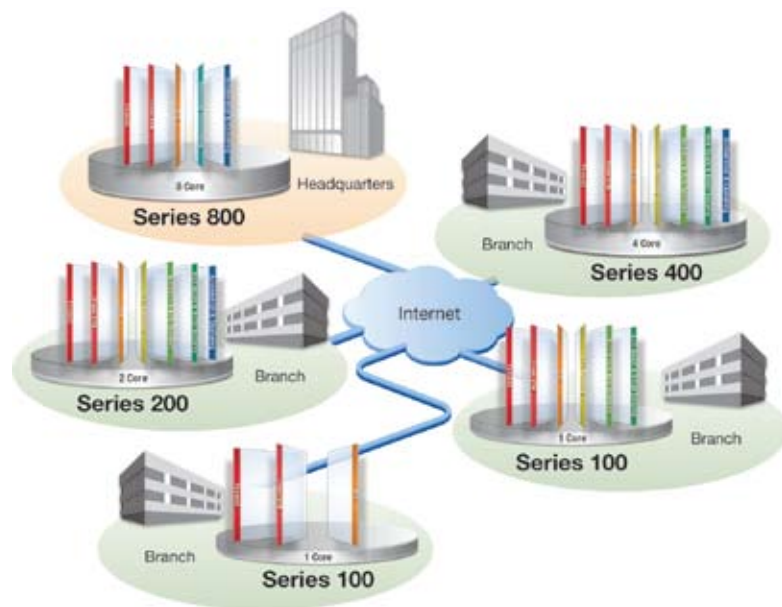


Figure 6. Organizational infrastructure after consolidation

Table 2. Check Point Security Gateway Systems

Series	Software Blades	Description
100	Firewall, VPN, IPS, Anti-Spam & Email Security, URL Filtering, Antivirus & Anti-Malware	<ul style="list-style-type: none"> • Entry-level security gateway for small or branch offices • Limited to 50 users and recommended for up to 8 ports
200	Firewall, VPN, IPS, Anti-Spam & Email Security, URL Filtering, Antivirus & Anti-Malware, Acceleration & Clustering	<ul style="list-style-type: none"> • Limited to 500 users and recommended for up to 12 ports • Comprehensive XTM (eXtensible Threat Management) security gateway with high performance capabilities for mid-sized companies and offices
400	Firewall, VPN, IPS, Anti-Spam & Email Security, URL Filtering, Antivirus & Anti-Malware, Acceleration & Clustering	<ul style="list-style-type: none"> • High-performance security gateway for offices of any size • Unlimited number of users and recommended for up to 16 ports
800	Firewall, VPN, IPS, Advanced Networking, Acceleration & Clustering	<ul style="list-style-type: none"> • The highest-performance security gateway designed for the most demanding performance environments • Ideal for large campuses and data centers

Business Scenario 2: Open new branch office

Situation: Business is expanding and additional branch offices must be supported. Today, existing branch offices are outfitted with inflexible solutions that can't scale and don't protect infrastructure investment. Security solutions at branch offices look nothing like what's deployed at headquarters, but they need the same level of protection as the corporate network since they are subjected to the same Internet threats.

IT requirements:

- One-stop shopping for all branch office connectivity and security functions to reduce cost and complexity
- All security policies provisioned from and managed at a central Security Operations Center, which minimizes deployment effort and enforces consistency with enforcement of security policy
- The ability to scale as needs change, such as adding more security, performance, or features (e.g., IPS, acceleration, clustering, VoIP security)

Solution: Check Point Software Blades are deployed in branch offices and central headquarters. The turnkey Check Point solution includes everything branch offices need to provide immediate connectivity and security for all branch office IT assets (e.g., network, servers, PCs, laptops). Organizations can manage policy centrally from headquarters—no local expertise required—or management responsibilities can be delegated to local administrators if desired.

The Check Point Provisioning Management Software Blade enables easy deployment and provisioning of security services for branch offices. This capability provides centralized administration and provisioning of Check Point security

devices via a single management console. Using profiles, a network administrator can easily deploy security policy or configuration settings (e.g., DNS, hosts, domain, routing and interface settings) to multiple, geographically distributed devices.

The Provisioning Software Blade also provides centralized backup management and a repository of device configurations, so administrators can easily apply existing configurations to new devices. Managed devices fetch their assigned profiles from a centralized management server, enabling one profile change to update hundreds of devices, each acquiring the new common properties, while maintaining its own local settings. By automating device configuration, the Provisioning Software Blade reduces administrative overhead, reduces errors, and ensures security consistency across the network.

Blade functions

Software Blades, shown in Figure 7, enable organizations to efficiently and quickly tailor security gateway and management functionality to specific and changing security needs. New blades are quickly licensed as needed without the addition of new hardware. Security Gateway and Security Management Software Blades available today are listed in Tables 2 and 3.



Figure 7. Security Gateway and Security Management Software Blades

Table 3. Security Gateway Software Blades

Security Gateway Software Blades	Capability
Firewall	Secures more than 200 applications, protocols, and services by employing the most adaptive and intelligent inspection technology
IPsec VPN	Safeguards the connectivity for offices and end users via a sophisticated, but easy-to-manage, site-to-site VPN and flexible remote access
IPS	Delivers the industry's best threat coverage
Web Security	Incorporates advanced protection for the entire Web environment and features the strongest protection against buffer-overflow attacks
URL Filtering	Covers more than 20 million URLs, which protects users and enterprises by restricting access to dangerous Web sites
Antivirus & Anti-Malware	Stops viruses, worms, and other malware at the gateway through heuristic virus analysis
Anti-Spam & Email Security	Blocks SPAM, protects servers, and eliminates attacks through email
Advanced Networking	Adds dynamic routing, multicast support, and Quality of Service (QOS) to security gateways
Acceleration & Clustering	Provides wire-speed packet inspection, high availability, and load sharing using the patented SecureXL™ and ClusterXL® technologies
Voice over Internet Protocol (VoIP)	Employs more than 60 VoIP application defenses, such as denial of service, to protect the VoIP infrastructure while delivering high voice quality

Table 4. Security Management Software Blades

Security Management Software Blades	Capability
Network Policy Management	Delivers comprehensive network security policy management for Check Point gateways and software blades via SmartDashboard, a single unified console
Endpoint Policy Management	Enables IT to centrally deploy, manage, monitor, and enforce security policy for all endpoint devices across any-sized organization
Logging and Status	Offers a complete visual picture of the changes to gateways, tunnels, and security activities
Monitoring	Facilitates fast response to changes in traffic patterns and security events by providing a complete view of network and security performance
Management Portal	Extends a browser-based view of security policies to outside groups such as support staff while maintaining central policy control
User Directory	Allows Check Point gateways to leverage LDAP-based user information stores, eliminating the risks associated with manually maintaining and synchronizing redundant data stores
IPS Event Analysis	Implements a complete IPS event management system, providing situational visibility, easy to use forensic tools, and reporting
Provisioning	Provides centralized administration and provisioning of Check Point security devices via a single management console
Reporting	Turns vast amounts of security and network data into graphical, easy-to-understand reports
Event Correlation	Supports centralized, real-time security event correlation and management for Check Point and third-party devices

Balancing security protection and investment

The continued evolution of security software and general-purpose servers delivers more flexibility for better security function consolidation and reuse. With Check Point Software Blade architecture, enterprises can buy the right amount of protection at the right price. Software Blades compliment existing Check Point firewall protection solutions, further securing networks without degrading gateway performance.

To learn more about Check Point Software Blade architecture, please visit <http://www.checkpoint.com/products/softwareblades/architecture/>





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>

©2003–2009 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, Full Disk Encryption, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, 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, Smart-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartProvisioning, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, Total Security, 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, VSX-1, 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.