Check Point Performance Innovations with Software Blade Architecture

New enhancements to Check Point Software Blade Architecture guarantee dramatic increases in performance
## Contents

- Executive summary .......................................................... 3
- Check Point Software Blade Architecture performance enhancements 4
- SecureXL: Lightweight optimized path for known traffic .............. 4
- The Medium Path: Improving IPS, AV, and URL-filtering performance 7
- CoreXL: Using the power of multiple CPU cores ........................ 9
- Load-sharing technologies for performance .............................. 10
- Check Point appliances: Purpose-built for performance ............. 11
- Conclusion ........................................................................ 14
Executive summary

In the IT world, one thing is constant - there is an ever-growing need for more security. Several factors drive the need for greater protections, including government and industry regulations, the need to allow necessary access to resources while guaranteeing the confidentiality of customer data and intellectual property, and the imperative to keep networks available 24x7x365 for customers and users.

However, when adding greater security to the network, IT administrators must always consider the performance impacts that those protections may have on business-critical systems and networks. The Check Point Software Blade Architecture™ is uniquely positioned to provide customers with the best security functionality available in a fully featured, high-performance solution that is easy to implement and manage in any network environment.

With Software Blade Architecture, Check Point offers an integrated solution that keeps companies completely up to date with the latest security protections, without the need to compromise on performance. The Software Blade Architecture is designed from the ground up to be a modular, manageable platform with increased performance capabilities. Enhancing security protections and increasing performance can be done simply, with minimal downtime, by adding additional Software Blades when new security or management functionality is required.

The best way for customers to gain all the performance benefits of Software Blade Architecture is to base their security solution on turnkey Check Point appliances. The mature Check Point appliance portfolio includes a wide range of models that cover all market segments, starting at a price point as low as US$600. Each of these appliances is carefully engineered to take maximum advantage of the Check Point performance technologies described in this paper. Also, in keeping with the Check Point philosophy of providing extensible solutions that can grow with customers’ needs, most Check Point appliances are designed to be upgraded right in the field, by installing specialized Check Point hardware such as Accelerated Data Path (ADP) modules, encryption acceleration modules or additional network interface cards. Customers can buy a Check Point appliance today and be confident that it can be expanded to meet increased network demands as their business grows.

This paper will provide an in-depth overview into the unique performance technologies of Check Point Software Blade Architecture. It will show how they work together to provide significant performance improvements over earlier versions of Check Point software, and it will prove that through the innovative Check Point Software Blade Architecture, companies can achieve the best TCO by implementing a comprehensive security solution with Check Point appliances that can easily grow to meet their future security needs.
Check Point Software Blade Architecture

The latest Check Point Software Blade Architecture delivers the following performance enhancements:

- Improvements in SecureXL™ for better connection establishment rates and throughput acceleration
- Availability of SecureXL (accelerated path) on all Check Point appliances, including the UTM-1™ appliances, IP Appliances™ and Power-1™ for greatly enhanced firewall and IPS performance
- Dramatic enhancements to antivirus and URL filtering performance via advances in Check Point streaming technology (Medium Path)
- Newly enhanced Check Point CoreXL™ to intelligently leverage multicore CPU architecture for faster firewall, IPS, and application control processing
- Improved ClusterXL® load-sharing technology engineered to work together with CoreXL for the most scalable security gateway load balancing
- Enhanced capacity of over 5,000,000 concurrent sessions on a single gateway with Check Point SecurePlatform™ HCC

SecureXL: Lightweight optimized path for known traffic

Check Point SecureXL is a mature technology that gives customers an easy way to increase performance. With the release of R71, it is now available on the entire range of Check Point UTM-1, Power-1 and IP appliances. Through its lightweight code path and patented open API, it enables accelerated traffic throughput, lower latency, and increases in connection and transaction rates.

SecureXL provides a more efficient path through the security gateway by allowing the firewall to offload known and previously validated connections to the more efficient code on the SecureXL device (implemented either in software or in specialized hardware such as Check Point ADP modules), which then forwards the traffic.

This technique avoids the overhead of involving the firewall for a decision on every packet traversing the security gateway. Because the accelerated traffic has already been inspected and allowed by the firewall, and because the traffic is now being forwarded by the SecureXL device, the firewall itself now can devote more free resources to processing traffic which requires deeper inspection.

Throughput acceleration with SecureXL

SecureXL communicates with the firewall and other applications through its API. In order to accelerate traffic, SecureXL learns about traffic flows which have been authorized by the firewall’s security policy. The information is communicated to
SecureXL in the form of a five-tuple, composed of the source and destination IP addresses, source and destination ports and protocol.

To achieve throughput acceleration, SecureXL stores the five-tuple information in its own separate connections table. All future packets that match an entry in the SecureXL connections table can simply be forwarded by the optimized SecureXL device itself, running at the driver level in the OS kernel, or in a dedicated hardware ADP module on IP appliances. In terms of CPU utilization, this is far less demanding than sending the traffic through the firewall path, and SecureXL therefore leads to greatly increased throughput in most cases.

Connection acceleration with SecureXL

For connection rate acceleration, SecureXL uses the same five-tuple, but masks out the source port and stores the information as a template in a separate table. In contrast to the SecureXL connections table, entries in the templates table persist for a period of time after the connection which triggered it is closed. During the time that the template exists in the SecureXL table, new connections in the same direction between the same hosts using the same protocol are handled entirely by SecureXL, without the need for the firewall to validate them.

Even though SecureXL is making the decision based on its templates, administrators retain complete visibility into the traffic on the network because SecureXL sends a message to the firewall through the API, providing information about the new connection for logging and other purposes.
Overall performance gains with SecureXL

For most customers, SecureXL achieves an immediate reduction in CPU utilization by simply enabling it in software or by installing an ADP module in a Check Point IP appliance. This translates to the ability to handle more network traffic, lowering the TCO of a Check Point system by prolonging its useful service life. It is easy to see the how SecureXL changes the flow of traffic through the system, simply by using the “fwaccel” tool in the Check Point SecurePlatform CLI.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>accelerated pack</td>
<td></td>
<td>accelerated pack</td>
<td></td>
</tr>
<tr>
<td>packets</td>
<td>468550516</td>
<td>packets deleted</td>
<td>397251600975</td>
</tr>
<tr>
<td>created</td>
<td></td>
<td>deleted</td>
<td></td>
</tr>
<tr>
<td>total conns</td>
<td>356304</td>
<td>C templates</td>
<td>838</td>
</tr>
<tr>
<td>TCP conns</td>
<td>196303</td>
<td>delayed TCP conns</td>
<td>396298</td>
</tr>
<tr>
<td>non TCP conns</td>
<td>1</td>
<td>delayed nonTCP conns</td>
<td>1928</td>
</tr>
<tr>
<td>conns from templates</td>
<td>7654302</td>
<td>temporary conns</td>
<td>30</td>
</tr>
<tr>
<td>nat conns</td>
<td>0</td>
<td>dropped packets</td>
<td>7</td>
</tr>
<tr>
<td>dropped bytes</td>
<td>456</td>
<td>nat templates</td>
<td>0</td>
</tr>
<tr>
<td>port allow templates</td>
<td>0</td>
<td>conns from nat mpl</td>
<td>0</td>
</tr>
<tr>
<td>port allow conns</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example output of ‘fwaccel’ stats showing SecureXL accelerated traffic

Once traffic is flowing through SecureXL, performance is immediately enhanced. The chart below shows the throughput gains on two different Check Point appliances when SecureXL is turned on.

Observed throughput increase when SecureXL is enabled
The Medium Path: Improving IPS, AV and URL-filtering performance

In the past, packets traversing the Check Point firewall had only two possible paths through the gateway. Depending on the rule base and other security protections in place, traffic was either processed by SecureXL in the accelerated path, or traffic was forwarded to the firewall when more complex and resource-intensive decisions needed to be made. Now with Check Point Security Gateway R71, there is a third option known as the Medium Path which improves performance by increasing the amount of traffic that can be handled in the accelerated path.

With the Medium Path in R71, customers can confidently activate more IPS, URLF and AV protections without suffering performance degradation. This leads to a more secure network environment and further increases the return on investment that customers can expect with a Check Point system. Since R71 is a simple software upgrade, administrators can benefit from these improvements without the need to upgrade or add additional hardware. Once R71 is installed, the Medium Path is available and fully implemented, with no additional configuration.

Medium Path architecture overview

The new Check Point Medium Path is multi-threaded and specifically designed to utilize multiple CPU cores. It improves performance by allowing many of the advanced calculations that are required for IPS, AV and URLF to take place in the accelerated path.
context of SecureXL. In R71, the SecureXL API has been extended to allow SecureXL to make direct calls into specific IPS functions within the firewall kernel, thus avoiding a time-consuming CPU context switch to the full firewall kernel.

In order to understand how this improves performance, consider the diagram below showing the R71 IPS engine.

At the bottom of the illustration is the first layer of the IPS engine, called the passive streaming library (PSL). PSL guarantees that the subsequent layers of the IPS engine receive an ordered, clean stream of packets for protocol analysis and pattern matching. Previously, the PSL layer could only receive packets that had been forwarded to the firewall. Now, with the new Medium Path in R71, PSL may receive packets directly from the SecureXL device without having to forward the packets to
the firewall. The illustration below shows a portion of the output of fwaccel stats on a Check Point R71 security gateway. In the screenshot, PXL stands for PSL acceleration, and it clearly shows how many packets were handled in the Medium Path. By comparing this information with other statistics available through the fwaccel stats command, it is easy to see the beneficial ratio of packets being handled by the firewall vs. those being accelerated by the Medium Path.

<table>
<thead>
<tr>
<th>Medium Path</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PXL packets</td>
<td>12120044</td>
</tr>
<tr>
<td>PXL bukets</td>
<td>10410001272</td>
</tr>
<tr>
<td>PXL tcmples</td>
<td>0</td>
</tr>
</tbody>
</table>

Output of ‘fwaccel stats’ showing traffic being processed in the Medium Path

For a detailed explanation of the inner workings of the IPS layers including more details about PSL, please refer to the “Check Point IPS Engine Architecture” white paper, available for download from http://www.checkpoint.com/whitepapers.

CoreXL: Using the power of multiple CPU cores

CoreXL is the first technology designed to take advantage of multiple CPU cores to improve performance when traffic must be processed by the firewall. Certain traffic is always processed by the firewall, including the first packet of flows that are eligible for SecureXL acceleration and selected IPS, AV and URL-filtering protections. With CoreXL, the firewall kernel, once limited to a single CPU core, is now able to run as multiple kernel modules, with each instance assigned to its own CPU core. This allows traffic flows to be load balanced across all available CPU cores in the Check Point appliance, so that security processing can be done in parallel.

R71 with CoreXL provides 24x IPS performance boost
Load balancing across these firewall instances is done in an intelligent way, with each instance maintaining its own state information to avoid potential performance issues resulting from resource conflicts. Performance scales as more CPU cores are added to the hardware, which allows for easy system expansion to meet growing network needs.

Load-sharing technologies for performance

Check Point R71 offers flexible high-availability and load-sharing solutions in the form of Check Point ClusterXL and Check Point IP clustering. These technologies provide customers with yet another way to expand their existing Check Point installation to meet growing performance and security requirements. Check Point load sharing solutions provide customers with the following advantages:

- **Scalability and reduced TCO** — Customers can implement a Check Point load-sharing technology with as few as two cluster members, and leverage their existing investment by adding more members as traffic loads increase

- **Easy deployment** — Check Point load-sharing solutions can be deployed in unicast, multicast or forwarding modes to accommodate existing network infrastructures

- **High availability** — If a cluster member goes down, traffic will be automatically and transparently redistributed to the remaining cluster members for guaranteed uptime

- **Seamless upgrades** — When administrators wish to add new Check Point software, clusters can be upgraded one member at a time, in order to eliminate downtime

Typical Check Point clustering topology
Check Point ClusterXL smart load sharing

ClusterXL provides a method for high traffic volumes to be intelligently distributed across multiple Check Point gateways. This architecture provides near-linear scalability, as well as greatly increased reliability. This gateway cluster can be physically located in a single location or even separated and connected via an internal backbone, allowing the members of the cluster to reside in multiple physical locations for increased redundancy and guaranteed business continuity. On both the internal and external networks, the gateways will be joined together on a switched network. This enables security state information to be synchronized quickly and efficiently between cluster members. This state synchronization ensures that if a gateway becomes unavailable, other gateways can continue passing the traffic without interruption to the user.

Check Point IP Clustering

IP Clustering is a proven load-sharing and high-availability solution that is available to all Check Point customers who are running IP Appliances in their environment. It doesn’t require any additional license fees or Software Blades, except on the IP282. Communication among cluster members is done through a dedicated cluster synchronization network, isolated from production traffic networks for security and performance reasons.

Typical performance scaling benefits for Check Point ClusterXL and IP Clustering solutions can be seen in the table on the following page. The numbers indicate the performance multipliers as nodes are added to the Check Point clustering solution:

<table>
<thead>
<tr>
<th></th>
<th>2 Nodes</th>
<th>3 Nodes</th>
<th>4 Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP throughput</td>
<td>2.0x</td>
<td>2.42x</td>
<td>2.51x</td>
</tr>
<tr>
<td>IPS throughput</td>
<td>1.73x</td>
<td>2.50x</td>
<td>3.27x</td>
</tr>
<tr>
<td>IPS transaction rate</td>
<td>1.53x</td>
<td>2.17x</td>
<td>2.85x</td>
</tr>
<tr>
<td>VPN throughput</td>
<td>1.9x</td>
<td>2.7x</td>
<td>3.5x</td>
</tr>
</tbody>
</table>

For more technical details about Check Point IP clustering, please download the white paper “Clustering on Check Point IP Appliances,” available online at [http://www.checkpoint.com/whitepapers](http://www.checkpoint.com/whitepapers).

Check Point appliances: Purpose-built for performance

Check Point offers customers a complete portfolio of appliances that are specifically engineered to leverage the Check Point Software Blade Architecture and performance technologies. Except for the very low end of the appliance line, all Check Point appliances incorporate SecureXL, CoreXL, the Medium Path and load-sharing cluster
Check Point Performance Innovations with Software Blade Architecture

Check Point Power-1 and IP Appliances for the high end

For enterprise perimeter, core or large-branch security requirements, Check Point offers more than nine appliance models across the Power-1 and IP Appliance lines. The high-end line of appliances is equipped with the exceptional performance and security protections required by the most demanding enterprises, telcos, MSPs and others with high bandwidth requirements. They offer the maximum expansion capabilities provided by Check Point Software Blade Architecture, as well as a broad selection of hardware upgrades including network interface cards and acceleration modules to accommodate various connectivity and throughput requirements.

Check Point Power-1 appliances combine Check Point firewall, IPsec VPN, IPS, advanced networking and ClusterXL load-sharing technology. Power-1 appliances are field-upgradable through both the Check Point Software Blade Architecture and a wide range of add-on NICs to provide the maximum return on investment.

Check Point Power-1 appliance specifications

<table>
<thead>
<tr>
<th>Expansion options</th>
<th>Power-1 11085</th>
<th>Power-1 11075</th>
<th>Power-1 11065</th>
<th>Power-1 9075</th>
<th>Power-1 5075</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 GbE ports</td>
<td>Up to four</td>
<td>Up to four</td>
<td>Up to four</td>
<td>Up to four</td>
<td>Up to two</td>
</tr>
<tr>
<td>10/100/1000 ports</td>
<td>Up to 18</td>
<td>Up to 18</td>
<td>Up to 18</td>
<td>Up to 18</td>
<td>Up to 18</td>
</tr>
<tr>
<td>Firewall throughput</td>
<td>30 Gbps</td>
<td>20 Gbps</td>
<td>15 Gbps</td>
<td>16 Gbps</td>
<td>9 Gbps</td>
</tr>
<tr>
<td>IPS throughput</td>
<td>15 Gbps</td>
<td>12 Gbps</td>
<td>10 Gbps</td>
<td>10 Gbps</td>
<td>7.5 Gbps</td>
</tr>
<tr>
<td>VPN throughput</td>
<td>4.5 Gbps</td>
<td>4 Gbps</td>
<td>3.7 Gbps</td>
<td>3.7 Gbps</td>
<td>2.4 Gbps</td>
</tr>
<tr>
<td>Concurrent sessions</td>
<td>1.2 million</td>
<td>1.2 million</td>
<td>1.2 million</td>
<td>1.2 million</td>
<td>1.2 million</td>
</tr>
</tbody>
</table>

The Check Point line of IP appliances includes four models aimed at the enterprise. One important differentiator between the Power-1 line and the IP Appliance line is that the IP2455, IP1285, and IP695 can accept optional Accelerated Data Path (ADP) hardware acceleration modules which are designed to handle offloaded SecureXL traffic for substantial boosts in performance in most enterprise environments. In addition to increased throughput, the ADP modules also significantly reduce packet latency in both unicast and multicast network environments.
Check Point Performance Innovations with Software Blade Architecture

Check Point high-end IP Appliance specifications

<table>
<thead>
<tr>
<th></th>
<th>IP2455</th>
<th>IP1285</th>
<th>IP695</th>
<th>IP565</th>
<th>IP395</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 GbE ports</td>
<td>Up to ten</td>
<td>Up to ten</td>
<td>Up to six</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>10/100/1000 ports</td>
<td>Up to 32</td>
<td>Up to 28</td>
<td>Up to 16</td>
<td>Up to 12</td>
<td>Up to 8</td>
</tr>
<tr>
<td>Firewall throughput (no ADP/ADP)</td>
<td>11/30 Gbps</td>
<td>10.3/17.5 Gbps</td>
<td>7.2/11.7 Gbps</td>
<td>7 Gbps*</td>
<td>3 Gbps*</td>
</tr>
<tr>
<td>IPS throughput</td>
<td>9 Gbps</td>
<td>7 Gbps</td>
<td>4 Gbps</td>
<td>2.9 Gbps</td>
<td>2.9 Gbps</td>
</tr>
<tr>
<td>VPN throughput (no ADP/ADP)</td>
<td>8.3/1.9 Gbps</td>
<td>8.3/1.9 Gbps</td>
<td>3.3/1.9 Gbps</td>
<td>1.7 Gbps*</td>
<td>677 Mbps*</td>
</tr>
<tr>
<td>Concurrent sessions</td>
<td>1 million</td>
<td>1 million</td>
<td>1 million</td>
<td>1 million</td>
<td>1 million</td>
</tr>
<tr>
<td>Expansion options</td>
<td>Software Blades, ADP, NICs, IP Clustering</td>
<td>Software Blades, ADP, NICs, IP Clustering</td>
<td>Software Blades, ADP, NICs, IP Clustering</td>
<td>Software Blades, ADP, NICs, IP Clustering</td>
<td>Software Blades, ADP, NICs, IP Clustering</td>
</tr>
</tbody>
</table>

Check Point UTM-1 and IP Appliances for the mid-range

For the mid-range security market, Check Point offers four models in the UTM-1 product line as well as two models in the IP Appliance line. With the release of Check Point R71 with Software Blade Architecture, all of the UTM-1 models now include SecureXL in the base price for the Firewall Software Blade.

Check Point mid-range UTM-1 and IP Appliance specifications

<table>
<thead>
<tr>
<th></th>
<th>UTM-1 3076</th>
<th>UTM-1 2076</th>
<th>UTM-1 1076</th>
<th>UTM-1 576</th>
<th>IP295</th>
<th>IP282</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/100/1000 ports</td>
<td>10</td>
<td>8</td>
<td>6</td>
<td>6</td>
<td>Up to 8</td>
<td>6</td>
</tr>
<tr>
<td>Firewall throughput</td>
<td>4.5 Gbps</td>
<td>3.5 Gbps</td>
<td>3 Gbps</td>
<td>2.5 Gbps</td>
<td>1.5 Gbps</td>
<td>1.5 Gbps</td>
</tr>
<tr>
<td>IPS throughput</td>
<td>4 Gbps</td>
<td>2.7 Gbps</td>
<td>2.2 Gbps</td>
<td>1.7 Gbps</td>
<td>1.4 Gbps</td>
<td>1.4 Gbps</td>
</tr>
<tr>
<td>VPN throughput</td>
<td>1.1 Gbps</td>
<td>450 Mbps</td>
<td>350 Mbps</td>
<td>300 Mbps</td>
<td>1.0 Gbps</td>
<td>1.0 Gbps</td>
</tr>
<tr>
<td>Concurrent sessions</td>
<td>1.1 million</td>
<td>1.1 million</td>
<td>1.1 million</td>
<td>640,000</td>
<td>900,000</td>
<td>900,000</td>
</tr>
<tr>
<td>Expansion options</td>
<td>Software Blades, ClusterXL</td>
<td>Software Blades, ClusterXL</td>
<td>Software Blades, ClusterXL</td>
<td>Software Blades, ClusterXL</td>
<td>Software Blades, NICs, IP Clustering</td>
<td>Software Blades, NICs, IP Clustering</td>
</tr>
</tbody>
</table>

*IP565 and IP395 cannot accommodate an ADP module. Throughput is quoted for non-ADP only on these models.
Check Point Performance Innovations with Software Blade Architecture

Check Point appliances for the small or branch office

In addition to the high-end and mid-range appliances shown above, Check Point includes a complete line of appliances for small or branch offices. These models range from the Safe@ and UTM-1 Edge appliances starting at US$600 for 190 Mbps of firewall throughput, to the UTM-1 276 at US$6,300 for 1,500 Mbps firewall throughput with six Software Blades, including the capability to manage up to two Check Point gateways.

Also included in this line of Check Point appliances is the all-new Series 80 security gateway, running an embedded version of the Software Blade Architecture. The SG82 model starts at US$2,500 and delivers 1,500 Mbps of firewall throughput. It offers easy deployment and provisioning options, and is managed by an external Check Point SmartCenter or Provider-1 management server.

For detailed information on all Check Point security and management appliances, see the latest Appliance Comparison Chart at http://www.checkpoint.com/products/downloads/appliances/appliance-comparison-chart.pdf.

Conclusion

The Software Blade Architecture allows Check Point to provide the most flexible and high-performance security solution on the market today. Because Check Point Software Blade systems are engineered with the capability to expand in both performance and functionality as network security demands increase, they provide the maximum return on investment and the lowest possible total cost of ownership to all types of businesses. The Software Blade Architecture provides ever-increasing security protections through easy software-based addition of new Software Blades. In addition, through the proven technologies outlined in this paper, Check Point provides the most effective performance enhancement solutions, so that administrators are no longer faced with the dilemma of security vs. performance.

To review, Check Point Software Blade Architecture solutions provide the following key benefits:

- SecureXL on software or IP Appliance ADP modules for throughput and connection acceleration
- CoreXL for maximizing firewall processing on multicore hardware
- The Medium Path for breakthrough IPS, AV, and URL-filtering performance
- Check Point active-active load-sharing solutions such as ClusterXL and IP Clustering for high availability and easy expansion of system capacity

The elegance of the Check Point solution becomes even more apparent as administrators combine these advanced features, and build on them as their network...
traffic grows. Performance gains are largely cumulative as the different performance solutions are combined.

- When combining SecureXL with CoreXL, the accelerated path provided by SecureXL frees up the remaining firewall kernel instances for deeper packet inspection
- When adding ADP to an IP Appliance, SecureXL functionality is offloaded to a purpose-built hardware module, freeing the main system CPU cores to process more traffic
- The Medium Path greatly accelerates IPS, AV, URLF and other advanced security functionality through a powerful new SecureXL API
- Systems running R71 features such as SecureXL, CoreXL and the Medium Path can handle even greater traffic loads when they are used in a load-sharing cluster topology
- Check Point advanced technologies for performance, combined with Software Blade Architecture, offer customers the most flexible and extensible security solution on the market today
About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com), worldwide leader in securing the Internet, is the only vendor to deliver Total Security for networks, data and endpoints, unified under a single management framework. Check Point provides customers uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented Stateful Inspection technology. Today, Check Point continues to innovate with the development of the software blade architecture. The dynamic software blade architecture delivers secure, flexible and simple solutions that can be fully customized to meet the exact security needs of any organization or environment. Check Point customers include tens of thousands of businesses and organizations of all sizes including all Fortune 100 companies. Check Point award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

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

©2003–2010 Check Point Software Technologies Ltd. All rights reserved. Check Point, Abra, AlertAdvisor, Application Intelligence, Check Point DLP, Check Point Endpoint Security, Check Point Endpoint Security On Demand, the Check Point logo, Check Point Full Disk Encryption, Check Point Horizon Manager, Check Point Media Encryption, Check Point NAC, Check Point Network Voyager, Check Point OneCheck, Check Point R70, Check Point Security Gateway, Check Point Update Service, Check Point WebCheck, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, DefensiveNet, DLP-1, DynamicID, Endpoint Connect VPN Client, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IPS Software Blade, IPSO, Software Blade, IQ Engine, MailSafe, the More, Better, Simpler Security logo, MultiSpect, NG, NGX, Open Security Extension, OPSEC, QSG, FireWall-1, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, Secure Virtual Workspace, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecureRemote, SecureServer, SecureUpdate, SecuBlade, SecuXL, TurboCard, Security Management Portal, SiteManager-1, Smart-1, SmartCenter, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefence, SmartDefence Advanced, SmartDefend, SmartSecurity, SmartSM, SmartMap, SmartPortal, SmartProvisioning, SmartReporter, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SmartWorkflow, SBF, SBF On-Demand, ScoWare, Software Blade Architecture, the softwareblades logo, SSL Network Extender, Stateful Clustering, Total Security, the totalsecurity logo, TrueVector, UseCheck, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Edge, VPN-1 MASS, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VXS, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VE, VPN-1 VXS, VXS-1, Web Intelligence, ZoneAlarm, ZoneAlarm Antivirus, ZoneAlarm DataLock, ZoneAlarm Extreme Security, ZoneAlarm ForceField, ZoneAlarm Free Firewall, ZoneAlarm Pro, ZoneAlarm Internet Security Suite, ZoneAlarm Security Toolbar, 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. 5,668,668, 5,835,725, 5,987,611, 6,498,930, 6,873,986, 6,850,943, 7,165,076, 7,540,013 and 7,725,737 and may be protected by other U.S. Patents, foreign patents, or pending applications.

November 17, 2010