

# VPN-1 Power Security-Performance Solutions

*High-performance security for high-performance applications*

## YOUR CHALLENGE

Balancing the competing needs of network performance and security is harder than ever. You must provision security for real-time applications such as video and voice or transaction-based applications such as stock trading or point-of-sale (POS) terminals—without slowing them down. However, you also face increased application-layer attacks that threaten these new applications. To protect them, you must turn on advanced application-layer security protections that may slow down performance.

## OUR SOLUTION

Check Point VPN-1® security gateways enable you to deploy performance-intensive applications securely without worrying about degradation. By leveraging ongoing hardware research and development of server manufacturers, VPN-1 security gateways can provide more than 12 Gbps security throughput on an open server\*—the best price/performance available. VPN-1 Power also delivers in excess of 5 Gbps throughput of SmartDefense™ intrusion prevention when default settings are active. To ensure maximum performance in flexible deployment scenarios, VPN-1 security gateways combine four technological approaches to high-performance security:

- Security acceleration
- Multi-core CPU support
- Gateway clustering
- Coprocessor cards

VPN-1 POWER PERFORMANCE	
Maximum throughput	12 Gbps (UDP packets)
Throughput (SmartDefense default settings)	5.1 Gbps (full traffic blend)
VPN (AES 128-bit encryption)	3.1 Gbps
TCP session rate	120,000 connections/second
*Tested on IBM 3650 with two Dual Core Intel® Xeon® Processor 5100 Series at 3 GHz with 4 GB memory	

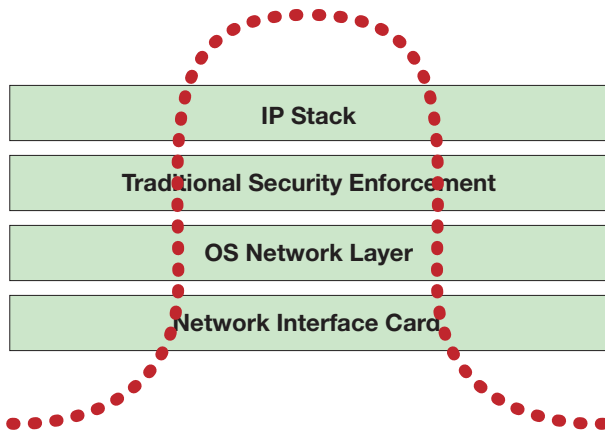
Because VPN-1 security gateways are software, it is possible to quickly take advantage of open hardware improvements such as multi-core CPUs. By avoiding closed architectures, VPN-1 enables you to maintain security against evolving threats without compromising on performance.



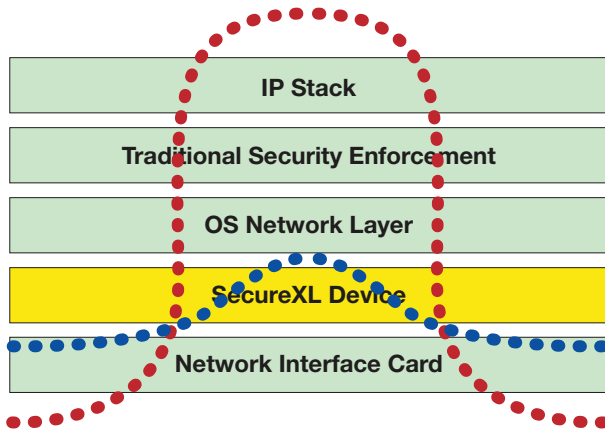
*The NGX platform delivers a unified security architecture for Check Point.*

## Security acceleration

SecureXL™, Check Point-patented security acceleration technology, removes latency associated with intense security processing (Figure 1) by creating a special device layer (Figure 2) that can make security decisions earlier. In both servers and dedicated appliances, performance is affected negatively by memory, system-bus, and CPU speed as traffic passes through a system. By creating a SecureXL device layer, VPN-1 enables security decisions to be made at a lower application level to remove roadblocks associated with poor performance. After the start of a transaction



(Figure 1) Traditional Security Inspection



(Figure 2) Accelerated Security Inspection with SecureXL

is examined using traditional security methods and is determined to be safe, the SecureXL device layer takes over responsibility for examining any remaining packets—cutting out latency caused by hardware design. SecureXL can be implemented at both a hardware layer using network processors, as is done on “Secured by Check Point” appliances from our hardware partners, or at a virtualized software layer on open servers.

## Multi-core CPU support

Multi-core CPUs, which are being used more and more in servers, enable VPN-1 gateways to share traffic among cores of a single system, providing superior price/performance in one server. The combination of multi-core CPUs and multi-threaded SecureXL security application technology is the foundation for the next generation of security acceleration—application-layer security. By joining a multi-core CPU with SecureXL security acceleration, VPN-1 Power delivers more than 5 Gbps of SmartDefense intrusion prevention.

## Gateway clustering

To provide acceleration as well as enhanced reliability, organizations can use ClusterXL® to cluster multiple VPN-1 security gateways to improve performance. ClusterXL combines stateful failover of security functions with the ability to dynamically share traffic loads among multiple gateways. This enables near-linear scalability for large deployments without the cost of separate load-balancing equipment.

## Coprocessor cards

VPN-1 security gateways can offload repetitive functions—such as regular expression matching or encryption—to an optional coprocessor card, freeing up the main CPU for more dynamic security tasks. For example, a VPN-1 Accelerator Card IV can be added to VPN-1 implementations to offload CPU-intensive encrypting from the main CPU.

## The Check Point advantage

Because VPN-1 security gateways are software-based solutions, it is possible for organizations to quickly take advantage of open-system hardware improvements such as multi-core CPUs or improved memory or bus speeds. By avoiding closed architectures—like those found in specialized security hardware that rely on ASICs, which cannot adapt to new threats for performance acceleration—VPN-1 security gateways enable you to maintain security against evolving threats without compromising on performance.

©2003–2007 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, 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, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, 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, 6,496,935, 6,873,988, and 6,850,943 and may be protected by other U.S. Patents, foreign patents, or pending applications.

February 23, 2007 P/N 502424

## Worldwide Headquarters

3A Jabotinsky Street, 24th Floor  
Ramat Gan 52520, Israel  
Tel: 972-3-753-4555  
Fax: 972-3-575-9256  
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  
www.checkpoint.com



**Check Point**  
SOFTWARE TECHNOLOGIES LTD.