Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

IPS Software Blade
Delivers complete intrusion prevention

Check Point IPS Software Blade

The Check Point IPS Software Blade provides complete, integrated, next generation firewall intrusion prevention capabilities at multi-gigabit speeds, resulting in industry-leading total system security and performance.

The Intrusion Prevention System, IPS Blade provides complete threat coverage for clients, servers, OS and other vulnerabilities, malware/worm infections, and more. The Multi-Tier Threat Detection Engine combines signatures, protocol validation, anomaly detection, behavioral analysis, and other methods to provide the highest levels of network IPS protection. By quickly filtering 90% of incoming traffic without requiring deep inspection, the IPS engine inspects for attacks only on relevant sections of the traffic, thus reducing overhead and increasing accuracy.

OVERVIEW
Online attacks and malware have been evolving, using sophisticated and even evasive attack methods. Several recent attacks used stolen or fake certificates, marking a shift in managing and monitoring traffic to now include encrypted streams.

Check Point addresses the changing threat landscape while meeting several key operational requirements for Intrusion Prevention Systems
- Security
- Fast Performance
- Accuracy
- Reliability
- Updateability
- Resistance to Evasions
- Granular Control

Check Point was the first to exploit the performance capabilities of industry standard multi-core processors for IPS, bringing intelligent load-balancing among cores to enable fast, fully-integrated IPS functions into the industry's leading firewall. With Check Point IPS technologies, you can have confidence that your organization's network will get top performance and full functionality without compromising on security.

Accelerated IPS Performance
Check Point meets the key operational IPS requirements with proven technologies that deliver security and performance. For starters, patented technologies underpin a new level of performance for integrated IPS:
- ClusterXL
- SecureXL
- CoreXL

KEY FEATURES
- Best-in-Class Adobe and Microsoft vulnerability coverage since 2008
- Thousands of proactive, preemptive protections right out-of-the-box
- Geo-protections
- Leverages ThreatCloud and signature centers around the world
- Built-in Attack Mitigation Engine blocks up to 1 million attack packets per second
- Multi-gigabit integrated IPS performance
- Inspect SSL Traffic
- Unified management with actionable monitoring

KEY BENEFITS
- Industry leading protection verified by NSS labs
- High performance insures unimpeded business operations
- Combines with best-of-breed firewall to deliver industry leading NGFW (NSS test)
- Provides a key protective layer of threat prevention
- Automatic updates insures constant protection from latest threats
- Single pane of glass efficiency of management

NSS Labs
RECOMMEND

- **2013 Intrusion Prevention System (IPS)Test**—NSS Labs Recommended
- **2013 NGFW Highest Score**—NSS Labs

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

ClusterXL provides a method for high traffic volumes to be intelligently spread across multiple gateways.

SecureXL provides acceleration for multiple, intensive security operations by offloading the handling of those operations and acting as a director to distribute the traffic to remaining cores.

CoreXL distributes IPS inspection to run in parallel on multi-core processor systems.

Multi-threat Detection Engines

Check Point employs a high-speed 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.

Passive Streaming Library

Passive Streaming Library (PSL) technology catches packets that may arrive out of order or may be legitimate retransmissions of packets that haven't yet received an acknowledgment. The PSL layer provides applications with a coherent stream of data that is free of various network problems or attacks.

Protocol Parsers

Protocol Parsers assemble the data for further inspection by other components of the IPS engine.

In addition, the protocol parsers perform various security checks such as validating RFC compliance of protocols and checking for protocol anomalies.

Context Management Infrastructure

The Context Management Infrastructure coordinates different components, decides which protections should run on a certain packet, decides the final action to be performed on the packet and issues an event log—including a CVE reference if applicable.

Pattern Matcher

The Pattern Matcher is a key engine within the enforcement architecture, quickly identifying harmless packets, common signatures in malicious packets, and does a second level analysis to reduce false positives.

Compound Signature Identification

Compound Signature Identification technology does sophisticated signature inspections and application identification. It may match signatures from multiple parts of the traffic in order to identify a malicious activity. CSI can address signatures on multiple parts of a packet, multiple parts of the protocols such as URL and an HTTP header, multiple parts of a connection, such as CIFS request and response, or multiple connections, such as VoIP control and data connections.

INSPECTv2

The INSPECTv2 engine is used to detect complex, elusive attacks at higher performance levels. Included in INSPECT v2 is an easier protection writing system. The improved engine is also accelerated across multiple CoreXL cores.

Performance	
Integrated IPS Performance	Up to 40 Gbps
Gateway Load Threshold	Protect firewall performance under load through a configurable software bypass
Security	
Multi-Method Detection Engine	• Vulnerability and exploit signatures • Protocol validation • Anomaly detection • Behavior-based detection • Multi-element correlation
Microsoft Vulnerability Coverage	#1 for Microsoft protections
Patch Process Reinforcement	Protect your network from attack while vendor patches are being applied
Real-Time Protection	Protection updates for: • Client and server vulnerabilities • Exploits • Protocol misuse • Outbound malware communications • Tunneling attempts • Application control • Generic attack types without predefined signatures • Preemptive security functions
Open Signatures	Create your own signatures with an open signature language
DoS Mitigation Engine	Expanded protections against denial-of-service attacks

CONTACT CHECK POINT

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
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

July 15, 2013