WELCOME TO THE FUTURE OF CYBER SECURITY

SSL Protector
High-Performance Visibility into SSL/TLS Traffic

High Performance Visibility

Benefits

- Comprehensive inspection and mitigation solutions
- High-performance platforms
- Best price performance
- Single decryption/encryption point
- Full control over the inspected traffic flow while ensuring uninterrupted traffic
- Smooth scalability for security infrastructure

Deployment Examples

- Inbound SSL inspection (SSL Offload)
- Outbound SSL inspection
- Outbound SSL inspection (host bypass)
- Service chaining

Features

- Highly available
- Scalable SSL/TLS solution
- TLS 1.3 support
- Employs the latest QAT technology for Elliptic Curve performance

SSL/TLS INSPECTION

Check Point SSL Protector provides a simple one-box solution for high-performance visibility into enterprise SSL/TLS traffic. It removes the blind spot introduced by the rising use of SSL/TLS and allows security tools to inspect all traffic for possible breaches and leaks.

SSL Protector acts as a central switching point for Check Point perimeter network security solutions, steering the decrypted traffic before re-encrypting it on the way to its destination server. Protector also provides scalability and high availability for Check Point Next Generation Threat Prevention.

FULL VISIBILITY INTO SSL/TLS TRAFFIC

By providing visibility into SSL/TLS traffic and offloading the SSL processing from your perimeter security devices, SSL Protector greatly enhances any organizations' security and maximizes its security infrastructure.
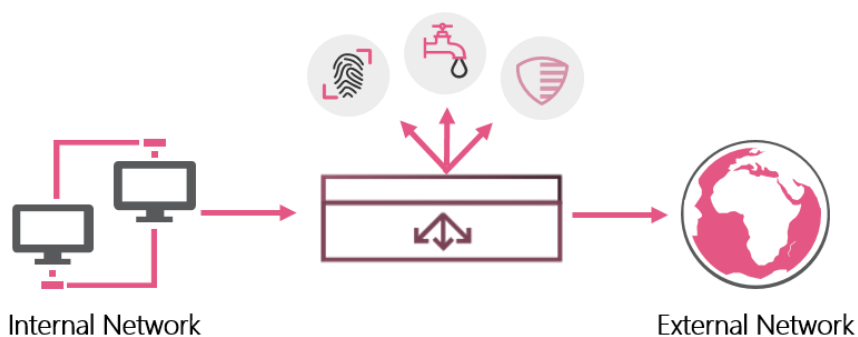

Figure 1: Single Instance SSL Inspection

As a smart centralized traffic steering solution, SSL Protector, with its high capacity SSL hardware engine, decrypts all relevant SSL traffic before forwarding it to Check Point security solutions and re-encrypts the traffic before forwarding it to the final destination. By performing the traffic decryption and re-encryption once for inspection, SSL Protector provides lower latency for all transactions and increases performance. It reduces the performance penalty up to 80% versus activating SSL traffic inspection in each of the security solutions, reducing the overall cost of the solution.

High Volume SSL Traffic Inspection

Check Point SSL Protector platforms contain hardware-based SSL engines which cost-effectively handle high capacity SSL/TLS transactions and processing of multi-gigabit per second of SSL traffic.

The need to process higher volumes of traffic with stronger encryption ciphers has placed a heavy toll on computational and memory resources and is especially critical for IoT and mobile devices. This has led the industry to introduce a stronger yet much more efficient encryption algorithm based on elliptic curve cryptography.

To provide cost effective support for the latest SSL/TLS standards, the Protector solution incorporates the latest SSL software and hardware engines, enabling high-capacity ECC-based SSL/TLS transaction processing with leading price-performance ratio across all its platform and form factor range.

Security Scalability and Availability

The unique deployment architecture of SSL Protector and its inherent load balancing capabilities enables it to monitor and load balance each security server separately and thus provide seamless scalability and ensure traffic will always flow through the most available server. Even in cases where servers are down, SSL Protector provides a simple way to define whether to bypass an unresponsive security service, ensuring continuous internet connectivity, or to block the traffic and avoid cyber threats.

Granular Traffic Inspection Policies

SSL Protector provides total control over the chaining of available security devices, enabling inspection of different traffic flows by different security device chains, based on granular filters classifying the traffic to different categories. As a result, organizations can avoid inspection of traffic they consider safe and save significant resources on their security devices, and thus optimize their utilization and their total cost of ownership. Decisions can be made on a multitude of parameters, from ports and IP addresses to hosts or web category based on third-party URL categorization feed.

Ensuring Employees Privacy

Organizations are required to maintain user privacy and need to avoid traffic inspection when their employees are browsing web services of a private nature such as their bank or healthcare provider.

SSL Protector can categorize the traffic on-the-fly and based on this information decide which traffic should be inspected and which should completely bypass decryption and inspection.

Bypass decisions can be made either to ensure end-user privacy for traffic such as personal finances and health or to reduce the load on your security tools for traffic that does not need to be inspected.

Flexible Deployment Options

SSL Protector supports a wide range of deployment options that allow seamless integration in any organizations' network.

Comprehensive Traffic Inspection
- Inspection of SSL traffic from external clients to enterprise services (Inbound) and/or of SSL traffic from internal clients to the Internet (Outbound).
- SSL Protector can discover outbound SSL traffic on any TCP port, thus intercepting all SSL traffic.

Network Integration
- SSL Protector can be installed as either and inline Layer 2 device or as an inline routed Layer 3 device.
- SSL Protector can perform outbound SSL inspection as either a transparent HTTPS proxy or as an explicit HTTPS proxy.

Single or Dual Instance

SSL Protector can be implemented as a single instance solution, overseeing all of the organization's traffic to and from the Internet (Figure 1 - Single instance SSL Inspect) or as a two-instance solution with virtual/physical separation between the DMZ and the enterprise's internal network (Figure 2 - Dual-instance SSL Inspect).
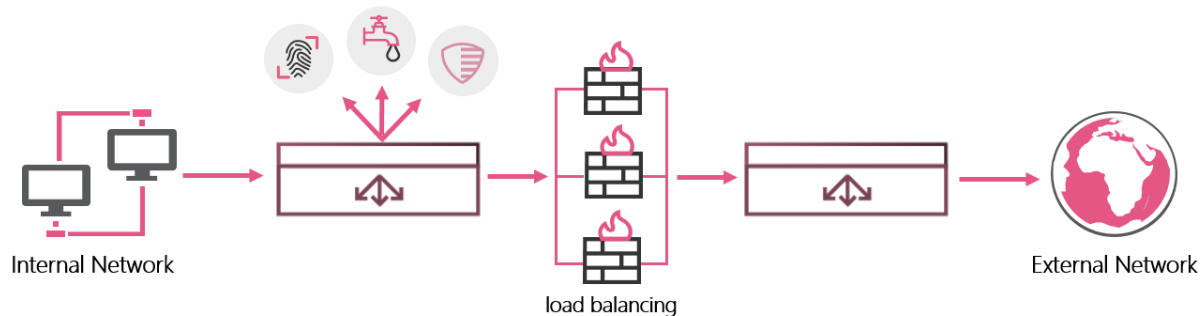
Figure 2: Dual Instance SSL Inspection with Load Balancing

Inspection Tools

SSL Protector allows combining steering traffic to active inline devices (including 1 or 2-leg solution, L2 and L3 solutions, ICAP solutions) as well as forwarding a copy of the traffic to out-of-path passive devices. It has the ability to connect to any type of value-add security service (VAS) such as firewalls, anti-malware, threat protection, DLP, Intrusion Prevention Systems, network forensics, etc.
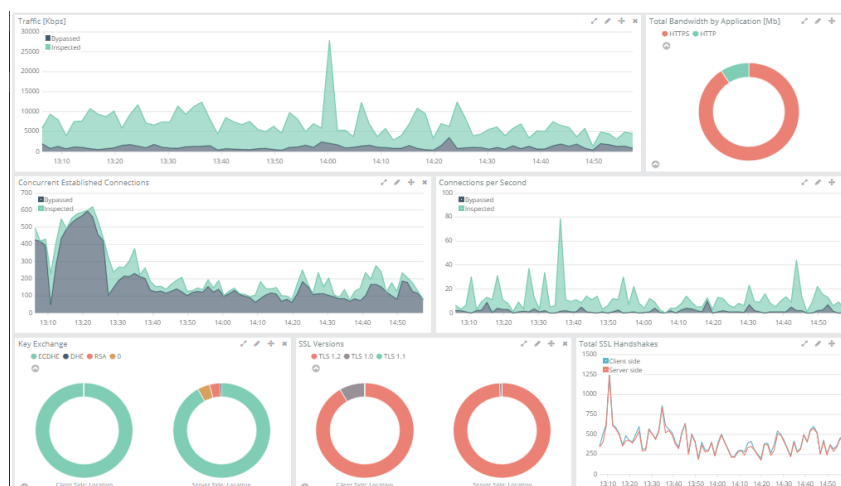
Single SSL/TLS Encryption/Decryption Point

Based on its advanced application classification capabilities, SSL Protector seamlessly intercepts and steers traffic to other Check Point security solutions for in-depth inspection before allowing it to continue to its destination. By centralizing the encryption/decryption process, you maximize performance and minimize latency and you simplify security infrastructure management.

Simplified Configuration and Monitoring

The SSL Protector dashboard provides a powerful monitoring tool and together with the configuration wizard facilitates smooth deployment and operation of SSL inspection solutions. The real-time and historical data provided allows to:

- Show the increased inspection coverage and utilization of your security infrastructure
- Visualize the SSL traffic patterns
- Quickly identify and get to the root cause of any issue.

Figure 3: SSL Inspection Dashboard

SPECIFICATIONS

	5208S	6024SL	8420SL
Performance			
Max processed throughput	26 Gbps	80 Gbps	160 Gbps
Inspected SSL throughput	4 Gbps	9 Gbps	14 Gbps
Full SSL handshakes per second (RSA 2k)	6,600	14,500	30,600
Full SSL handshakes per second (ECC p-256)	5,200	11,000	25,000
Hardware Specifications			
Processor	1 x Intel quad-core CPU	1 x Intel 6-core CPU	2 x Intel 10-core CPU
Memory	32 GB	64 up to 256 GB	128 up to 256 GB
Traffic Ports	2 x 10 GbE SFP+ 8 x 1 GbE RJ45	24 x 10 GbE SFP+	4 x 40 GbE QSFP+ 20 x 10 GbE SFP+
USB Port	Yes	Yes	Yes
RS-232C Console	RJ-45 Serial Connection	RJ-45 Serial Connection	RJ-45 Serial Connection
Environmental Specifications			
Power Supply	100-240V, 47-63 Hz, Dual and DC Options		
Power consumption	140W	250W	670W
Heat dissipation	478 BTU/h	853 BTU/h	2286 BTU/h
Dimensions			
Enclosure	1U	2U	2U
Metric (W x D x H)	436 x 406 x 44 mm	436 x 480 x 88 mm	426 x 600 x 88 mm
Standard (W x D x H)	17.1 x 16 x 1.7 in.	17.1 x 18.9 x 3.4 in.	16.7 x 23.6 x 3.4 in.
Weight	6 kg (13.2 lbs.)	10.5 kg (23.1 lbs.)	16.15 kg (35.53 lbs.)
Operating environment	Temperature: 0-40 °C (32-104 °F)		
Humidity	10% to 95% non- condensing		
Airflow Direction	Front-Right/Front-Left – To-Back	Front-To-Back	Front-To-Back
Min CFM	50	200	200
Certifications			
ROHS	Compliant (EU directive 2011/65/EU)		
Safety	CE LVD (EN 60950-1), CB – IEC 60950-1, CCC, cTUVus		
EMC	CE EMC (EU directive 2004/108/EC), FCC Part 15B Class A, ICES-003, VCCI, C-Tick		

WELCOME TO THE FUTURE OF CYBER SECURITY

ORDERING SSL PROTECTOR

PROTECTOR SECURITY APPLIANCES [1]	SKU
Protector AL5208 Security Appliance	CPAP-AL5208-S
Protector AL5208 Security Appliance with a DC power supply	CPAP-AL5208-D-S
Protector AL6024 Security Appliance	CPAP-AL6024
Protector AL6024 Security Appliance with a DC power supply	CPAP-AL6024-D
Protector AL8420 Security Appliance with a DC power supply	CPAP-AL8420-D-S
SOFTWARE UPGRADES	
SSL Protector AL6024S - Upgrade S to SL SSL Acceleration	CPSB-AL6024S-UPG-SL
SSL Protector AL8240 S - Upgrade S to SL SSL Acceleration	CPSB-AL8420-S-UPG-SL
SSL INSPECTION and WAF UPGRADE	
License upgrade For Protector AL5208 to include WAF and SSL Inspection	CPSB-AL5208-WAF-SSL
License upgrade For Protector AL6024 to include WAF and SSL Inspection	CPSB-AL6024-WAF-SSL
License upgrade For Protector AL8420 to include WAF and SSL Inspection	CPSB-AL8420-WAF-SSL
HARDWARE ACCESSORIES	
SSL Protector AL6024 - Upgrade to S SSL Acceleration - Factory installed	CPAC-AL6024-UPG-S
SSL Protector AL6024 Memory Upgrade to 64 GB - Factory installed	CPAC-AL6024-UPG-64G
Single AC Power Supply - SSL Protector AL5208	CPAC-PSU-AC-AL5208
Single AC Power Supply - SSL Protector AL6024	CPAC-PSU-AC-AL6024
SERVICES	
SecURL Gateway for SSL Protector AL8420 for 1 year	CPSB-AL-8K-SECURE- 1Y
SecURL Gateway for SSL Protector AL6024/AL6420 for 1 year	CPSB-AL-6K-SECURE-1Y
SecURL Gateway for SSL Protector AL5208 for 1 year	CPSB-AL-5K-SECURE-1Y
Application Performance Monitoring (APM) for SSL Protector AL6024/AL6420 for 1 year	CPSB-AL-APM-MID-1Y
APM for SSL Protector AL5280 for 1 year	CPSB-AL-APM-ENTRY-1Y

[1] GBICs must be purchased separately

CONTACT US

Worldwide Headquarters | 5 Shlomo Kaplan 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: 650-628-2117 | www.checkpoint.com