Check Point DDoS Protector™

Stop Denial of Service attacks in seconds with customized, multi-layered protection that blocks a wide range of attacks.

Check Point DDoS Protector Appliances

In today's threat landscape, "Denial of Service (DoS)" attacks are increasing in number, speed and complexity. Denial of Service and Distributed Denial of Service (DDoS) attacks are relatively easy to carry out, and can cause serious damage to companies who rely on web services to operate. Multiple (more than 50) DDoS attack "toolkits" are readily available on the Internet, and an increasing number of attacks are initiated in over 230 countries. DDoS attacks are often profit-driven: in 2011, cyber criminals earned a whopping $12.5 billion dollars. 2012 shows an alarming surge of DDoS threats to the financial services industry. However hacktivisim and political motivations are fast becoming the most popular forum to launch Denial of Service attacks. Anonymous successfully spearheaded numerous attack campaigns against individuals, organizations, governments and countries in retaliation for actions or statements they didn't agree with.

Many DDoS solutions are deployed by an Internet Service Provider, offering generic protections against network layer attacks. However today's DDoS attacks have become more sophisticated, launching multiple attacks at networks and applications. Successful DDoS solutions will offer companies the ability to customize their protections to meet changing security needs, fast response time during an attack, and a choice of deployment options.

OVERVIEW

Check Point's new DDoS Protector keeps businesses running with multi-layered, customizable protections and 12Gbps performance that automatically defends against network flood and application layer attacks for fast response time against today's sophisticated denial of service attacks. DDoS Protector appliances offer flexible deployment options to easily protect any size business, and integrated security management for real-time traffic analysis and threat management intelligence for advanced protection against DDoS attacks. Check Point also provides dedicated 24/7 support and resources to ensure up-to-the-minute protections.

KEY FEATURES

- Protects against known and unknown DDoS attacks
- Defends against both network and application attacks
- Flexible filter engines detect and prevent malicious exploits
- Protects against HTTP attacks
- Protects against bandwidth flood attacks
- Fast, customized signature creation keeps businesses running

KEY BENEFITS

- Protection against evolving DDoS attacks to minimize business impacts
- Advanced techniques help maintain web services during an attack
- Turn-key appliance works right out of the box
- Integrated with Check Point security management for greater visibility and control
- High-performing DDoS solution with 14Gbps capacity and 12Gpbs throughput
- Multi-layered protection blocks multiple attack types
- Customized protections fit different business sizes and security needs
- Flexible deployment options include on-site installation or through your ISP

MULTI-LAYERED PROTECTIONS

Network and Traffic Flood Protections

Protection against DDoS attacks aimed at networks using:

Behavioral DoS—Protects against TCP, UDP, ICMP, IGMP and Fragment DDoS attacks with adaptive behavioral based detection.

DoS Shield—Protects against known DDoS attack tools with pre-defined and customized filters to block rate-limits per pattern.

Syn Protection—Blocks SYN-spoofed DoS with SYN rate thresholds per protected servers.

Black List—Blocks generic attacks with L3 and L4 source-destination classifications and expiration rules.

Connection Rate Limit—Blocks generic, non-supported protocols (non DNS, HTTP) and application level flood attacks with rate-based thresholds.

Application Based Dos/Ddos Protections

Protects against more complex DDoS attacks that misuse application resources with:

SYN Protection with Web Challenge—Protects against HTTP connection-based DoS attacks with SYN rate threshold per protected server.

Behavioral DNS Protections—Block DNS query DoS attacks with DNS adaptive behavioral based detection using DNS footprint blocking rate limits and DNS challenge and response.

Behavioral HTTP Protections (The “HTTP Mitigator”)—Blocks HTTP connection-based DoS attacks and upstream HTTP bandwidth attacks with server-based HTTP adaptive behavioral detection, HTTP footprint with web challenge response, 302 redirect and JS challenge actions.

Directed Application Dos/DDoS Protections

Repels Dos and DDoS attacks that require special filtering criteria. Flexible filtering definitions search for specific content patterns in each packet. Enables the ability to analyze and block ongoing attacks by defining on-the-fly protections.

MANAGEMENT

DDoS Appliances are integrated with Check Point Security Management, including:

SmartEvent

Unified security event and analysis solution that delivers real-time threat management information to instantly stop threats and block attacks with on-the-fly protections. Move from business view to forensics in just three clicks.

SmartLog

Advanced log analyzer that delivers proactive security intelligence with split-second search results from any log field for instant visibility into billions of log records over multiple time periods and domains.

SmartView Tracker

Comprehensive auditing solution to troubleshoot system and security issues, gather information for legal or audit purposes, and generate reports to analyze network traffic patterns. In the case of an attack or other suspicious network activity, use SmartView Tracker to temporarily or permanently terminate connections from specific IP addresses.

Alerting

SNMP V1, 2C and 3, Log File, Syslog, Email

Configuration

SNMP, V1, 2C, 3, HTTP, HTTPS, SSH, Telnet, SOAP, API, Console (user selectable).

Time Synchronization

Based on Network Time Protocol (NTP).

Export Real-Time Signature Information

Northbound XML interface exports behavioral parameters.

SPECIFICATIONS

DDoS Protector Model	**506**	**1006**	**2006**	**3006**	**4412**	**8412**	**12412**
Network Grade	Enterprise				Datacenter		
Performance[1]							
Capacity[2]	500Mbps	1Gbps	2Gbps	3Gbps	4Gbps	8Gbps	14Gbps
Throughput[3]	500Mbps	1Gbps	2Gbps	3Gbps	4Gbps	8Gbps	12Gbps
Max Concurrent Sessions	2,000,000	2,000,000	2,000,000	2,000,000	4,000,000	4,000,000	4,000,000
Max DDoS Flood Attack prevention rate (packets per second)	1,000,000	1,000,000	1,000,000	1,000,000	10,000,000	10,000,000	10,000,000
Latency	<60 micro seconds						
Real-time Signatures	Detect and protect against attacks in less than 18 seconds						
Inspection Ports							
10/100/1000 Copper Ethernet	4	4	4	4	8	8	8
GbE (SFP)	2	2	2	2	4	4	4
10GbE (XFP)	-	-	-	-	4	4	4
Management Ports							
10/100/1000 Copper Ethernet	2	2	2	2	2	2	2
RS-232	1	1	1	1	1	1	1
Operation Mode							
Network Operation	Transparent L2 Forwarding						
Deployment Modes	In-line; span port monitoring; copy port monitoring; local out-of-path; out-of-path mitigation						
Tunneling protocols support	VLAN Tagging, L2TP, MPLS, GRE, GTP						
IPv6	Support IPv6 networks and block IPv6 attacks						
Policy Action	Block and Report; Report Only						
Block Actions	Drop packet, reset (source, destination, both), suspend (source, src port, destination, dest port or any combination); Challenge-Response for HTTP and DNS attacks						
High Availability							
Fail-open / Fail-close	Internal fail-open/fail-close for copper ports; internal fail-close for SFP ports; optional fail-open for SFP ports [4]				Internal fail-open/fail-close for copper ports; internal fail-close for SFP and XFP ports; optional fail-open for SFP and SFP ports [5]		
SKU	CPAP-DP506	CPAP-DP1006	CPAP-DP2006	CPAP-DP3006	CPAP-DP4412	CPAP-DP8412	CPAP-DP12412

[1] Actual performance figures may change per network configuration, traffic type, etc.

[2] Capacity is measured as maximum traffic forwarding when no security profiles are configured

[3] Throughput is measured with behavioral protections and signature protections using eCommerce protection profile

[4] External fiber fail-open switch with SFP ports is available at additional cost

[5] External fiber fail-open switches with SFP or XFP ports are available at additional cost

DDoS Protector Accessories	SKU
10Gbps Pluggable Optics (XFP) Singlemode LR	CPAC-DP-10LR-XFP
10Gbps Pluggable Optics (XFP) Multimode SR	CPAC-DP-10SR-XFP
1Gbps Pluggable Optics Singlemode ZX	CPAC-DP-1ZX-SFP
1Gbps Pluggable Copper 1000BASET	CPAC-DP-1C-SFP
1Gbps Pluggable Optics Singlemode LX	CPAC-DP-1LX-SFP
1Gbps Pluggable Optics Multimode SX	CPAC-DP-1SX-SFP
10GbE External Bypass unit supporting one (1) LR segment - protects against power failure and link failure - for DDoS Protector x412 series	CPAC-DP-1LR-10BP
10GbE External Bypass chassis, includes one LR interface segment, expandable up to four (4) segments - protects against power failure and link failure - for DDoS Protector x412 series	CPAC-DP-4LR-10BP
10GbE External Bypass Module, LR Interface segment - protects against power failure and link failure - for DDoS Protector x412 series	CPAC-DP-1LR-10BPM
10GbE External Bypass chassis, includes one SR interface segment, expandable up to four (4) segments - protects against power failure and link failure - for DDoS Protector x412 series	CPAC-DP-4SR-10BP
10GbE External Bypass Module, SR Interface segment - protects against power failure and link failure - for DDoS Protector x412 series	CPAC-DP-1SR-10BPM
1GbE External Bypass unit supporting one (1) SX segment - protects against power failure and link failure - for DDoS Protector x412 series	CPAC-DP-1SX-1BP
1GbE External Bypass unit supporting one (1) LX to SX segment - for DDoS Protector x412 series	CPAC-DP-1LX-1BP
Two Slot Rack Mount Frame for bypass switches	CPAC-DP-2RM
Dual DC Power Supply for DDoS Protector x412 series	CPAC-DP-2PS-DC
Single DC Power Supply for DDoS Protector x412 series	CPAC-DP-PS-DC

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
800 Bridge Parkway, Redwood City, CA 94065 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

June 7, 2012