CHECK POINT

DDoS PROTECTOR APPLIANCE

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

KEY FEATURES

- Protects against known and unknown DDoS attacks in seconds
- Defends against both network and application attacks
- Unique real-time signature engine for continuity of legitimate traffic
- Flexible filter engines detect and prevent malicious exploits
- Protects against HTTP attacks
- Network flood attacks protection
- 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 up to 40Gbps throughput
- Multi-layered protection blocks multiple attack types
- Customized protections fit different business sizes and security needs

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 hacktivism 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 protec- tions 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 up to 40Gbps 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.

©2014 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

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).

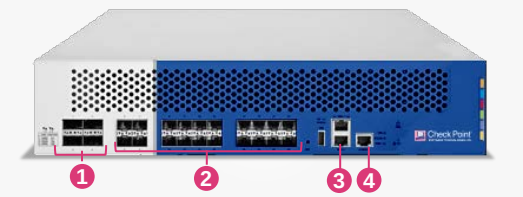
EXPORT REAL-TIME SIGNATURE INFORMATION

Northbound XML interface exports behavioral parameters.

©2014 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

X420 DDoS Protector

1. 4 x 40 Gigabit Ethernet QSFP+
2. 20 x 1/10 Gigabit Ethernet SFP+
3. 2 x Management 10/100/1000Base-T RJ45
4. Console port



TECHNICAL SPECIFICATIONS

DDoS Protector Model	10420	20420	30420	40420
Network Grade	Large Datacenter / Carrier			
Performance[1]				
Throughput [2]	10Gbps	20Gbps	30Gbps	40Gbps
Max Concurrent Sessions	6,000,000	6,000,000	6,000,000	6,000,000
Max DDoS Flood Attack prevention rate (packets per second)	25,000,000	25,000,000	25,000,000	25,000,000
Latency	<60 micro seconds			
Real-time Signatures	Detect and protect against attacks in less than 18 seconds			
Inspection Ports				
1GbE/10GbE (SFP+)	20	20	20	20
40GbE (QSFP+)	4	4	4	4
Management Ports				
10/100/1000 Copper Ethernet	2	2	2	2
RJ-45 Serial	1	1	1	1
Operation Mode				
Network Operation	Transparent L2 Forwarding / IP 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 TCP, HTTP and DNS to identify attacks			
High Availability				
Fail-open / Fail-close	Internal fail-close for SFP+ and QSFP+; optional fail-open available [3]			
Physical				
Dimensions (W x D x H) mm	426 x 537 x 88 mm (2U) EIA Rack or Standalone: 482 mm (19 in)			
Weight kg (lbs)	15.1kg (33.2 lbs)			
Power				
AC Power Supply (Auto-range)	100-120V / 200-240V, 47-63 Hz			
DC Power Supply (Auto-range)	- 36 to -72V			
Power Consumption	634W			
Thermal Output	2162 BTU / hour			
Operating Environmental Conditions				
Temperature	5-55°C (41-131°F)			
Humidity	5% to 95% (non- condensing)			
SKU (Dual AC Power)	CPAP-DP10420-D-SME	CPAP-DP20420-D-SME	CPAP-DP30420-D-SME	CPAP-DP40420-D-SME
SKU (Dual DC Power)	CPAP-DP10420DC-D-SME	CPAP-DP20420DC-D-SME	CPAP-DP30420DC-D-SME	CPAP-DP40420DC-D-SME

[1] Actual performance figures may change per network configuration, traffic type, etc.
[2] Throughput is measured with behavioral protections and signature protections using eCommerce protection profile at the egress and includes only legitimate traffic. Dropped packets are not mesured.
[3] External fiber fail-open switches with SFP ports are available at an additional cost

©2014 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

X06 DDoS Protector 

X412 DDoS Protector 

DDoS Protector Model	506	1006	2006	4412	8412	12412
Network Grade	Enterprise			Datacenter		
Performance[1]						
Throughput [2]	500Mbps	1Gbps	2Gbps	4Gbps	8Gbps	12Gbps
Max Concurrent Sessions	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	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	8	8	8
GbE (SFP)	2	2	2	4	4	4
10GbE (XFP)	-	-	-	4	4	4
Management Ports						
10/100/1000 Copper Ethernet	2	2	2	2	2	2
RS-232	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 TCP, HTTP and DNS to identify 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]		
Physical						
Dimensions (W x D x H) mm	424 x 457 x 44 mm (1U)			424 x 600 x 88 mm (2U)		
Weight kg (lbs)	Single PS:7.2kg (15.9 lbs), Dual PS:8.7kg (19.2 lbs)			18.0 kg (39.0 lbs)		
Power						
AC Power Supply (Auto-range)	100-120V / 200-240V, 47-63 Hz					
Power Consumption	Single PS: 177W, Dual PS: 147W			476W		
Thermal Output	2162 BTU / hour					
Operating Environmental Conditions						
Temperature	5-55°C (41-131°F)					
Humidity	5% to 95% (non- condensing)					
SKU	CPAP-DP506-SME	CPAP-DP1006-SME	CPAP-DP2006-SME	CPAP-DP4412-D-SME	CPAP-DP8412-D-SME	CPAP-DP12412-D-SME

[1] Actual performance figures may change per network configuration, traffic type, etc.
[2] Throughput is measured with behavioral protections and signature protections using eCommerce protection profile
[3] External fiber fail-open switch with SFP ports is available at additional cost
[4] External fiber fail-open switches with SFP or XFP ports are available at additional cost

©2014 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

			
DDoS Protector Family	**X06**	**X412**	**X420**
Network Grade	Enterprise	Datacenter	Large Datacenter / Carrier
Certifications			
Safety	EN 60950-1:2006, CB - IEC 60950-1, cTUVus	EN, IEC #60950-1, cTUVus	EN 60950-1:2006, CB - IEC 60950-1, CCC, cTUVus
Emissions	EN 55022, EN 55024, FCC Part 15B Class A	EN 55022, EN 55024, FCC Part 15B Class A	EN 55022, EN 55024, EN 61000-3-2, EN 61000-3-3
Other	CE, FCC, VCCI, CB, TUV, CCC, C-Tick, RoHS		IEC 61000 4-2 to 4-6 , IEC 61000 4-8 & IEC 61000-4-11, FCC Part 15B Class A, ICES-003, VCCI, C-Tick RoHS 6 Compliant

©2014 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

CONTACT US

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