



DDoS Protector

DDoS Protection and Attack Mitigation

Maintain Business Continuity Even When Under Attack

Features

- Full protection of data center applications against emerging network threats
- Maintain network performance even when under high PPS network attacks
- Maintain excellent user response time even under attack
- DDoS Protector combines intrusion prevention system (IPS), network behavioral analysis (NBA), denial-of-service (DoS) protection and SSL attack protection

Benefits

- Get the most accurate attack detection and prevention without blocking legitimate user traffic
- Reduce Total Cost of Ownership (TCO) of Security Management
- Multitude of security tools in a single box
- Single management application to manage multiple DDoS Protector units cross multiple data centers
- Full investment protection and extended platform life time with pay-as-you-grow license upgrade scalability delivering best ROI and CAPEX investment protection

DDOS ATTACKS ARE ON THE RISE

In today's info-security threat landscape, denial-of-service and distributed denial-of-service (DoS/DDoS) attacks are a major cause of network downtime. Whether executed by hacktivists to draw attention to a cause, fraudsters trying to illegally obtain data or funds, or a result of geopolitical events, DDoS attacks are a destructive cyber weapon. Governments, utilities, financial services and commercial institutions face daily attacks.

Preparing for "common" DDoS attacks is no longer enough. Thanks to the growing array of online marketplaces, it is now possible for hackers to wreak havoc with virtually no knowledge of computer programming or networks. Attack tools and services are easy to access, making the pool of possible assaults larger than ever.

With Burst attacks and Advanced Persistent DDoS campaigns, hackers launch multi-vector, blended campaigns with high volume network vectors with more sophisticated application-layer attacks. In addition, recent IoT threats spawned the largest DDoS attack in history, propelling the industry into the 1Tbps DDoS era.

With these new threats, it is critical to ensure your DDoS mitigation solution can protect your organization and customers from today and tomorrow's sophisticated attacks.

INTEGRATED ON PREMISES AND CLOUD DDOS PROTECTION

DDoS Protector is part of Check Point's Attack Mitigation Solution and is an award-winning, real-time, perimeter attack mitigation device that secures organizations against emerging network and applications threats. DDoS Protector protects the infrastructure against network and application downtime (or slow time), application vulnerability exploitation, malware spread, network anomalies, information theft and other types of attacks.

DDoS Protector provides the industry's most advanced, automated protection from fast-moving threats, including from recent IoT based attacks such as Mirai. It is uniquely built to overcome both the complexity and scale of today's sophisticated IoT-based botnets. DDoS Protector also helps organizations win the ongoing security battle against availability attacks, by detecting and mitigating known and zero-day DoS/DDoS attacks in real-time. It protects against other security threats that are usually undetected by traditional DDoS mitigation tools, such as SSL-based flood attacks, attacks on login pages and attacks behind CDNs.

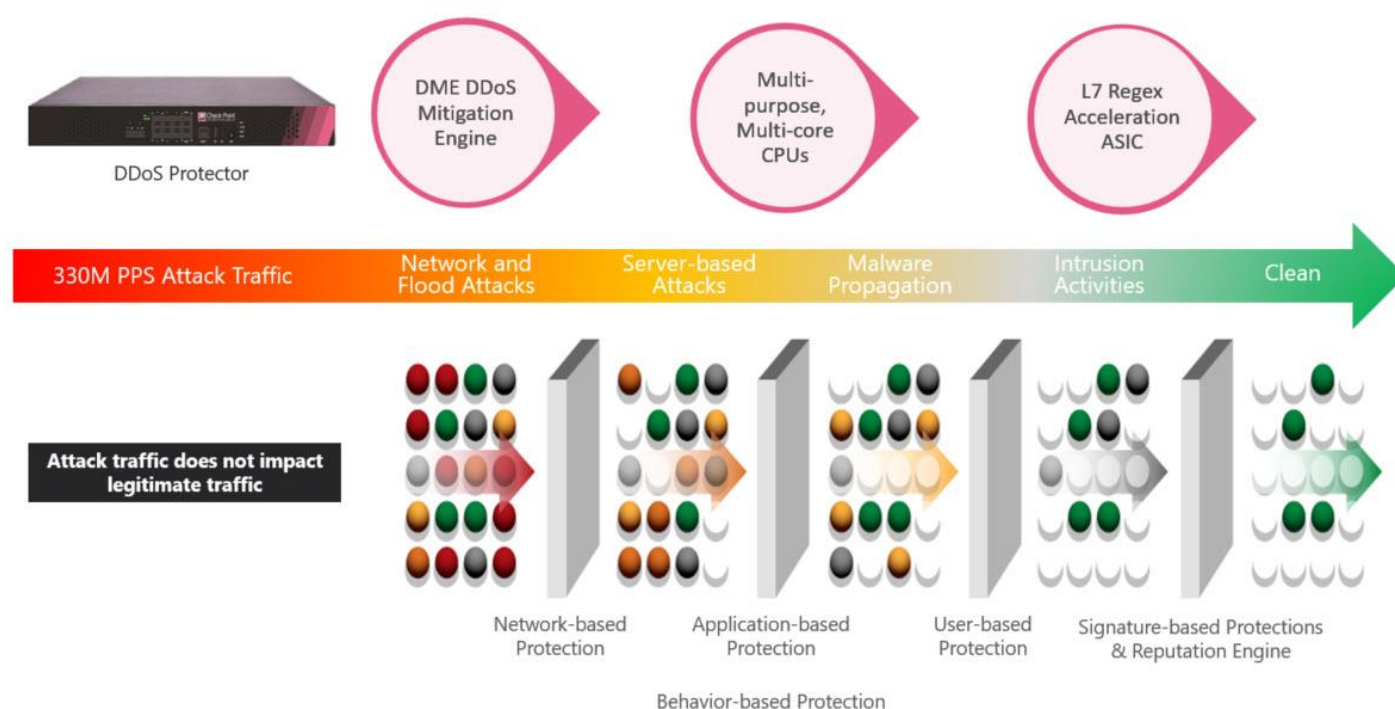
With DDoS Protector, Check Point's attack mitigation solution offers protection with the shortest mitigation time and broadest attack coverage. Check Point provides a hybrid solution combining on premise and cloud-based mitigation tools in a single integrated solution, designed to optimally block multiple attack vectors occurring in parallel.

WHY DDoS PROTECTOR?

DDoS Protector includes a comprehensive set of four essential security modules – anti-DDoS, network behavioral analysis (NBA), intrusion prevention system (IPS) and SSL-attack protection - to fully protect the application infrastructure against known and emerging network security attacks. It employs multiple detection and mitigation modules, including adaptive behavioral analysis, challenge response technologies and signature detection.

Compared to standalone solutions, the synergy of multiple security modules on a single, hardware-accelerated platform enables effective protection against attackers who seek to systematically compromise business assets while providing unified reporting, forensics and compliance.

DDoS Protector consists of adaptive, behavioral-based real-time signature technology that detects and mitigates emerging network attacks, zero-day, DoS/DDoS, application misuse attacks, network scanning and malware spread. It eliminates the need for human intervention and does not block legitimate user traffic.



A DDoS PROTECTOR SECURITY APPLIANCE TO FIT YOUR EVERY NEED

The DDoS Protector appliances offer versatile connectivity and mitigation capacities, adhering to enterprise and service provider deployments. Bandwidth mitigation capacities range from 6, all the way up to 400 Gbps. Protection can be further augmented with our Cloud DDoS Protector Services.

	DDoS Protector 6	DDoS Protector 20	DDoS Protector 60	DDoS Protector 200	DDoS Protector 400
Ports	8x RJ45, 2x 1/10 GbE	24x 1/10 GbE		20x 10, 4x 40, 4x 100 GbE	
Bandwidth (BW)	200 Mbps to 2 Gbps	2 to 12 Gbps	10 to 40 Gbps	80 Gbps	160 Gbps
Mitigation BW	6 Gbps	6 Gbps	60 Gbps	200 Gbps	400 Gbps
PPS	3 M	3 M	25 M	330 M	330 M
Enclosure	1U	2U	2U	2U	2U
SSL Option	✓	✓	✓	✗	✗

DEPLOYMENT MODES

DDoS Protector can be deployed inline, out-of-path (OoP) or in a scrubbing center to provide the highest mitigation accuracy within the shortest time. Each deployment mode offers the same performance as an inline device.

With DDoS Protector deployed either inline or out-of-path as well as in a scrubbing center, the devices are able to communicate with each other in real-time to collect automatic updates of normal traffic baselines, detect behavioral patterns and obtain attack footprints. This constant real-time flow of Defense Messaging enables DDoS Protector to provide accurate and instant mitigation without the need to learn this information when an attack occurs.

Deploying DDoS Protector devices out-of-path or in a scrubbing center is the most scalable and flexible solution as it is based on the maximum attack mitigation capacity needed, without being limited by the actual network physical topology.

INTEGRATED, HYBRID SOLUTION

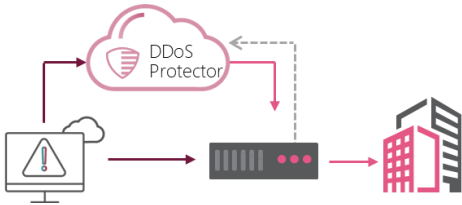
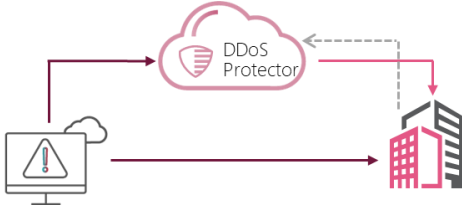
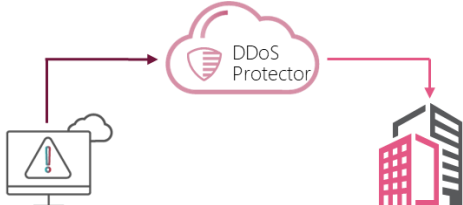
In addition to the security modules integrated in DDoS Protector, Check Point's Attack Mitigation Solution (AMS) includes an SSL decryption/encryption engine, a WebApp Protector module and Hybrid Cloud DDoS Protector Service that works in sync with the on premises solution. With no performance impact or risk, Check Point's AMS ensures business continuity even when under attack.

The solution is enhanced with a central Security Information Event Management (SIEM) to provide unified situational awareness and an Emergency Response Team (ERT). Unique messaging assures that each component provides information about traffic baselines and real-time signatures to the others, so that all system components have full visibility into all information.

Through this messaging, Check Point's AMS can detect attacks where it should and mitigate attacks where it's best. For example, the system can detect a volumetric attack at the network perimeter but mitigate it in the cloud. This automatic, real-time feature enables organizations to scale the mitigation capabilities of the solution by moving mitigation as far as possible from the application infrastructure.

CLOUD DDOS PROTECTOR SERVICES

Check Point's DDoS Protector Cloud Service can be delivered in On-demand, Always-on, or in a Hybrid configuration, and can be custom-tailored to suit any customer need, network topology or threat profile.

Choosing the Right Solution		
Hybrid	On-demand	Always-on
 <p>On premises inline or out-of-path devices backed by cloud-based scrubbing capacity Real-time protection and minimal latency Recommended security best practice Best suited for data center protection</p>	 <p>No added latency Traffic diverted only upon attack detection Allows lowest-cost, cloud-only simple deployment Best suited for latency-sensitive applications and organizations that are infrequently attacked</p>	 <p>Always-available, real-time, cloud-based DDoS protection Provides immediate protection but with small added latency Best suited for applications hosted on the cloud and for organizations that constantly come under attack</p>

WELCOME TO THE FUTURE OF CYBER SECURITY

GLOBAL COVERAGE, MASSIVE CAPACITY

Check Point's DDoS Protector Cloud Service is backed by a worldwide network of 9 global scrubbing centers, with 3.5 Tbps of mitigation capacity (and growing). Check Point's scrubbing centers are globally connected in full mesh mode, using Anycast-based routing. This ensures that DDoS attacks are mitigated closest to their point of origin, and provides truly global DDoS mitigation capable of absorbing even the largest volumetric attacks.



CHECK POINT DDOS PROTECTOR CLOUD SERVICE FEATURES

Our cloud-based service includes the same features you get in the on premises solution. This includes behavioral-based detection using advanced, patented machine-learning algorithms to protect against known and unknown threats, zero-day protection against network and application layer DDoS attacks such as Burst attacks, DNS attacks and others. Our unique protection against SSL-based attacks does not add latency or require customers provide full SSL certificates. Our extensive compliance options and certification are unparalleled by any rival and include industry-specific certifications such as PCI and HIPAA, as well as cloud security standards such as ISO 27001, ISO 27017, ISO 27018, ISO 27032 and others.








EXPERT SUPPORT

The Emergency Response Team (ERT) is a group of security experts that provides 24x7 support and mitigation services for customers facing a broad array of application and network layer DDoS attacks. The ERT complements an organization's ability to deal with cyber-attacks by leveraging both security expertise and real-time threat intelligence services. The team engages in mitigating a broad array of security events, including malware outbreaks, application exploits, DDoS attacks and DoS attacks. The ERT provides the required expertise and service during prolonged, complex attacks and helps to quickly restore the operation by mitigating DDoS attacks fast.

EASY MANAGEMENT AND CONTROL

Absolute Vision is a unified management and monitoring system. It provides advanced element management capabilities through a unique plug-and-play device support mechanism, including initial device setup, on-going maintenance, SSL certificate management, real-time reporting, capacity utilization measurement, forensics, task scheduling and more. It provides automation of monitoring and maintenance processes across all the devices it manages and includes a central repository of vital device information for IT managers to easily find hardware platform details, upgrade and software version management, and installed licenses. As a result, continuous service delivery through the entire device's operational life cycle is ensured. A REST API is available for SIEM integrations.

DDOS PROTECTOR SPECIFICATIONS

Enterprise Grade				Ultra High End	
Appliances	6	20	60	200	400
<div></div>					
Performance					
Max Mitigation Capacity/Throughput (Gbps)	6	20	60	200	400
Max Legit Concurrent Sessions	3,000,000	12,000,000	12,000,000	18,000,000	18,000,000
Max Attack Concurrent Sessions	Unlimited				
Max DDoS Flood Attack Prevention Rate (PPS)	5,800,000	25,000,000	25,000,000	330,000,000	330,000,000
SSL/TLS Connections per Second	20,000 (RSA 2K)	95,000 (RSA 2K)			
Latency	< 60 micro seconds				
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 (scrubbing center solution)				
Tunneling Protocol	VLAN Tagging, L2TP, MPLS, GRE, GTP, IPinIP				
IPv6	Yes				
Jumbo Frame	Supported				
Inspection Ports					
10/100/1000 Copper	6	-	-	-	-
1/10 GbE SFP+	2	24	24	20	20
40 GbE QSFP+	-	-	-	4	4
100 GbE QSFP28	-	--	-	4	4
Physical					
Enclosure	1U	2U	2U	2U	2U
Standard (W x D x H)	17.2 x 16 x 1.73 in.	17.2 x 18.9 x 3.46 in.		16.7 x 23.6 x 3.46 in.	
Metric (W x D x H)	436 x 406 x 44 mm	436 X 480 X 88 mm		424 x 600 x 88 mm	
Weight	7 Kg (15.4 lbs.)	11.2 kg (24.7 lbs.)		18.7 kg (41.2 lbs.)	
Power					
Dual, Hot-Swappable PSU	Optional	Included	Included	Included	Included
Power Input	AC 100 ~ 120V, AC 200 ~ 240V @ 47 ~ 63Hz, DC: -36 - -72V				
Power Consumption	140W	320W		890W	
Heat Dissipation	480 BTU/h	1088 BTU/h		2930 BTU/h	
Environment Conditions					
Operating Environment	32° to 104° F / 0° to 40° C, 5~95% Humidity (non-condensing)				
Certifications					
Safety	cTUVus, EN/IEC 60950-1 (CB), CCC, IEC 60950-1, GB4943, CNS 14336				
Emissions	USA Title 47 Part 15; EMC 2014/30/EU; LVD 2014/35/EU; FCC Part 15B (Class A); CS03; ETSI EN 300 386 V2.1.1 (2016-07); EN 61000–3–2, EN 61000–3–3, AS/NZS CISPR 32, Brazil ANNEX TO RES N° 442, Japan V-2/2015.04 & V-3/2015.04, China GB 9254-2008, Russia CU TR 020 2011, Korea KN 32/35, Taiwan CNS 13438				
Environment	RoHS II (EU directive 2011/65/EU)				

ORDERING DDOS PROTECTION

DDoS APPLIANCE ¹	SKU
DDoS Protector 6-3 Appliance providing 6Gbps attack mitigation and 3Gbps legitimate throughput	CPAP-DP6-3-SME
DDoS Protector 6-2 Appliance providing 6Gbps attack mitigation and 2Gbps legitimate throughput	CPAP-DP6-2-SME
DDoS Protector 6-1 Appliance providing 6Gbps attack mitigation and 1Gbps legitimate throughput	CPAP-DP6-1-SME
DDoS Protector 6-05 Appliance providing 6Gbps attack mitigation and 500Mbps legitimate throughput	CPAP-DP6-05-SME
DDoS Protector 20-12 Appliance providing 20Gbps attack mitigation and 12Gbps legitimate throughput	CPAP-DP20-12-SME
DDoS Protector 20-8 Appliance providing 20Gbps attack mitigation and 8Gbps legitimate throughput	CPAP-DP20-8-SME
DDoS Protector 20-4 Appliance providing 20Gbps attack mitigation and 4Gbps legitimate throughput	CPAP-DP20-4-SME
DDoS Protector 60-40 Appliance providing 60Gbps attack mitigation and 40Gbps legitimate throughput	CPAP-DP60-40-SME
DDoS Protector 60-20 Appliance providing 60Gbps attack mitigation and 20Gbps legitimate throughput	CPAP-DP60-20-SME
DDoS Protector 60-10 Appliance providing 60Gbps attack mitigation and 10Gbps legitimate throughput	CPAP-DP60-10-SME
DDoS Protector 200-80 Appliance providing 200Gbps attack mitigation and 80Gbps legitimate throughput	CPAP-DP200-80-SME
DDoS Protector 400-160 Appliance providing 400Gbps attack mitigation and 160Gbps legitimate	CPAP-DP400-160-SME

¹ SSL option available for the DDoS Protector 6, 20 and 60. GBICs must be purchased separately.

Hybrid Cloud, DDoS Services

HYBRID CLOUD DDOS SERVICE ¹	
Hybrid Cloud DDoS Protection Service Up to Legitimate 12, 8, 4, 2, 1 0.5, 0.2, or 0.1 Gbps for 1 year	CPSB-DPL-xxGB-1Y
UPDATE SERVICE ¹	SKU
DDoS Behavioral Protection and IPS Updates for DDoS Protector 6-3, 6-2, 6-1, 6-05	CPSB-DP6-xx-SUS-1Y
DDoS Behavioral Protection and IPS Updates for DDoS Protector 20-12, 20-8, 20-4q	CPSB-DP20-xx-SUS-1Y
DDoS Behavioral Protection and IPS Updates for DDoS Protector 60-40	CPSB-DP60-xx-SUS-1Y
DDoS Behavioral Protection and IPS Updates for DDoS Protector 200-80	CPSB-DP200-80-SUS-1Y
DDoS Behavioral Protection and IPS Updates for DDoS Protector 400-160	CPSB-DP400-160-SUS-1Y
ADDITIONAL SERVICE ¹	SKU
Active Attackers Feed Subscription for DDoS Protector 6-5, 6-3, 6-2, 6-1, 6-05	CPSB-DP6-xx-AAF-1Y
Active Attackers Feed Subscription for DDoS Protector 20-12, 20-8, 20-4	CPSB-DP20-xx-AAF-1Y
Active Attackers Feed Subscription for DDoS Protector 60-40, 60-20, 60-10	CPSB-DP60-xx-AAF-1Y
Active Attackers Feed Subscription for DDoS Protector 200-80	CPSB-DP200-80-AAF-1Y
Active Attackers Feed Subscription for DDoS Protector 400-160	CPSB-DP400-160-AAF-1Y

¹ SSL option available DDoS Protector 6, 20 and 60

On-demand, Always-on DDoS Protection

ON-DEMAND CLOUD DDOS SERVICE ¹	
On-Demand Cloud DDoS Protection Service for 1 year Up to Legitimate 12, 8, 4, 2, 1 Gbps or 500, 200, 100, 50, 20, 10 Mbps	CP-CG-DP-OND-12GB-1Y
ALWAYS-ON CLOUD DDOS SERVICE ¹	
Always-On Cloud DDoS Protection Service for 1 year Up to Legitimate 12, 8, 4, 2, 1 Gbps or 500, 200, 100, 20, 10 Mbps	CP-CG-DP-AON-12GB-1Y

¹ Additional annual diversions and protected networks available in the online product catalog

CONTACT US

Worldwide Headquarters | 5 Shlomo Kaplan, 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