QUANTUM™ DDoS PROTECTOR X DATASHEET

Adaptive Protection from the Most Advanced DDoS Threats

Distributed denial-of-service (DDoS) attacks are increasing in frequency and ferocity. Powerful IoT-botnets for hire over the dark web make launching large-scale attacks accessible, effortless, and cheap. Professional hackers are continuously seeking new ways to disrupt the flow of network traffic and undermine the user experience, resulting in loss of revenue, tarnishing of the brand and increased customer churn rates.

DDoS Protector, Check Point's real-time perimeter attack mitigation device, secures organizations against emerging network multi-vector attacks, powerful DDoS campaigns, IoT botnets, application vulnerability exploitation, malware, and other types of cyberattacks.

Key Features

Automated Zero-Day Attack Defense
Behavioral-based detection and mitigation to defend against unknown zero-day attacks without impacting legitimate user experience

Keyless SSL/TLS Flood Mitigation
High-capacity keyless protection from SSL/TLS-based DDoS attacks without adding latency to customer communications and while preserving user privacy

Advanced Attack Protection
Detection and mitigation of today's most advanced attacks, including Burst attacks, Domain Name System (DNS) amplification attacks, IoT botnet floods, Layer 3–7 and other crippling DDoS attacks

Patent Protected Real-Time Attack Signature
Automated signature creation and advanced challenge escalations to achieve the highest mitigation accuracy that can automatically mitigate unknown attacks and minimize the impact on legitimate traffic

CHECK POINT™

	DDoS Protector X10 / X20	DDoS Protector X40	DDoS Protector X80	DDoS Protector X100 / X200	DDoS Protector X400 / X800
PROGRAMMABLE MITIGATION PERFORMANCE					
On-Demand Scalable Clean Throughput Licenses	DDoS Protector X10-05 - 500 Mbps DDoS Protector X10-1 - 1 Gbps DDoS Protector X10-2 - 2 Gbps DDoS Protector X10-5 - 5 Gbps DDoS Protector X20-5 - 5 Gbps DDoS Protector X20-10 - 10 Gbps	DDoS Protector X40-10 - 10 Gbps DDoS Protector X40-20 - 20 Gbps DDoS Protector X40-40 - 40 Gbps	DDoS Protector X80-10 - 10 Gbps DDoS Protector X80-20 - 20 Gbps DDoS Protector X80-40 - 40 Gbps	DDoS Protector X100-50 - 50 Gbps DDoS Protector X200-100 - 100 Gbps	DDoS Protector X400-200 - 200Gbps DDoS Protector X800-380 - 380Gbps
Max Programmable Mitigation Throughput	10 Gbps / 20 Gbps	40 Gbps	80 Gbps	100 Gbps / 200 Gbps	400 Gbps / 800 Gbps
Max Attack Concurrent Sessions	Unlimited				
DDoS Flood Attack Prevention Rate	14 Mpps	30 Mpps	30 Mpps	142 Mpps	1,119 Mpps
Latency	< 60 microseconds				
Real-Time Signatures	Detect attacks and protect in less than 18 seconds				
SSL / TLS DECRYPTION					
SSL/TLS Connections per Second	43 KCPS (RSA 2K)	90 KCPS (RSA 2K)	90 KCPS (RSA 2K)	150 KCPS (RSA 2K)	-
TLS 1.3 Perfect Forward Secrecy (PFS) HW Acceleration Support	Yes	Yes	Yes	Yes	-
BLOCKING PERFORMANCE					
Maximal DDoS Blocking Throughput	-	-	-	800 Gbps	3.4 Tbps
Maximal DDoS Blocking (PPS)	-	-	-	1.19 Billion	2.7 Billion
INSPECTION PORTS					
10/100/1000 Copper Ethernet	Up to 16 (2x8) - Modular	-	-	-	-
1 GE / 10 GE	-	12 (SFP+)	12 (SFP+)	-	-
10 GE / 25 GE	Up to 8 (2x4) (SFP+) - Modular	-	-	24 (SFP+/SFP28)	-
40 GE	-	6 (QSFP+)	6 (QSFP+)	-	-
100 GE	-	-	-	8 (QSFP+/QSFP28)	18 (QSFP28)
400 GE[1]	-	-	-	-	4 (QSFP-DD)
MANAGEMENT PORTS					
10/100/1000 Copper Ethernet	2				
Management Console	RJ-45				
HIGH AVAILABILITY					
Fail-open/fail-close[2]	Internal fail-open/fail-close for modular copper ports; Internal fail-open/fail-close for fiber ports or optical transceivers (i.e., SFP+)	Internal fail-close for optical transceivers (i.e., SFP+, QSFP+)		Internal fail-close for optical transceivers (e.g., SFP+, SFP28, QSFP+, QSFP28)	Internal fail-close for optical transceivers (e.g., QSFP28, QSFP-DD)
Dual Power Supply	Yes, hot swappable				

1. Requires 400G connectivity, available at additional cost.

QUANTUM DDOS PROTECTOR X

	DDoS Protector X10 / X20	DDoS Protector X40	DDoS Protector X80	DDoS Protector X100 / X200	DDoS Protector X400 / X800
OPERATION MODE					
Network Operation	Transparent L2 Forwarding, IP Forwarding				
Deployment Modes	Inline, SPAN port monitoring, Copy port monitoring, Out-of-path mitigation (scrubbing center solution)				
Tunneling Protocols	VLAN Tagging, L2TP, MPLS, GRE, GTP, IPinIP				
IPv6	Yes				
Jumbo Frame	-	Supported			
Block Actions	Drop packet, reset (source, destination, both), suspend (source IP address, source port, destination IP address, destination port or any combination), challenge-response for TCP, HTTP and DNS suspicious traffic				
PHYSICAL					
Dimensions (W x D x H) mm	436 x 406 x 44 mm (1U)	438 x 530 x 88 mm (2U) EIA rack or standalone: 530 mm (20.86 in)	438 x 530 x 88 mm (2U) EIA rack or standalone: 530 mm (20.86 in)	482 x 550 x 87 mm (2U) EIA rack or standalone: 482 mm (19 in)	424 x 600 x 88 mm (2U) EIA rack or standalone: 482 mm (19 in)
Weight	Single power supply: 6 kg (13.2 lbs.) Dual power supply: 6.5 kg (14 lbs.)	Single power supply: 11 kg (24.2 lbs.) Dual power supply: 12 kg (26.4 lbs.)	Single power supply: 11 kg (24.2 lbs.) Dual power supply: 12 kg (26.4 lbs.)	Dual power supply: 14.5 Kg (31.9 lbs)	Dual power supply: 27.5 kg (60.6 lbs.)
Power Supply (Auto-range)	80 plus certified AC:100–120V/200–240V, 47–63 Hz DC: -36 to -72V	80 plus certified AC:100–120V/200–240V, 47–63 Hz DC: -44 to -72V	80 plus certified AC:100–120V/200–240V, 47–63 Hz DC: -44 to -72V	80 plus certified AC:100-120V/200-240V, 47-63 Hz DC: -36 to -72V	80 plus certified AC:100–120V/200–240V, 47–63 Hz DC: -41 to -72V
Power Consumption	Single and dual power supply: 140W	Dual power supply: 400W	Dual power supply: 400W	Dual power supply: 550W	Dual power supply: 970W
Heat Dissipation	Single and dual power supply: 480 BTU/h	Dual power supply: 1,364 BTU/h	Dual power supply: 1,364 BTU/h	Dual power supply: 1880 BTU/h	Dual power supply: 3,300 BTU/h
Operating Temperature	0°–40°C (32°–104°F)				
Humidity	5% to 95% non-condensing				
COMPLIANCE & CERTIFICATIONS					
Compliance					
RoHS	Compliant (EU directive 2011/65/EU, 2015/863/EU)				
ECCN	5A002.a.2				
Safety/EMC/EMI & Certifications	UL/TUV, FCC (USA), IC (Canada), CE (Europe), UKCA (UK), RCM (Australia/ NZ) , VCCI (Japan), KCC (Korea), EAC (Russia), BSMI (Taiwan), Anatel (Brazil), NOM (Mexico)				
Warranty	1-year hardware and software maintenance				
Support	Certainty Support Program				

External fiber fail-open switch is available at additional cost.

DDoS Protector VA for Private Clouds			DDoS Protector VA for Public Clouds	
Hypervisor	KVM kernel 3.19, QEMU 2.0, VMware (ESX server versions: 6.0, 6.5, 6.7), OpenStack 16.1		Native Public Cloud support	AWS, Azure
Minimum VM requirements	2 vCPUs, 16GB RAM, 10GB storage		Minimum VM requirements	2 vCPUs, 16GB RAM, 10GB storage
PERFORMANCE[1]			**PERFORMANCE**	
OnDemand Scalable Throughput Licenses	DDoS Protector VA 200 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps, 20 Gbps[2], 40 Gbps		Max Mitigation Capacity/ Throughput	Up to 25 Gbps per DDoS Protector VA instance
Max Mitigation Capacity/ Throughput	Up to 50 Gbps per DDoS Protector VA instance		Max Legit Concurrent Sessions	1,000,000 sessions per vCPU
Max Legit Concurrent Sessions	1,000,000 sessions per vCPU		Max Attack Concurrent Sessions	Unlimited
Max Attack Concurrent Sessions	Unlimited		Max DDoS Flood Attack Prevention Rate	Up to 500,000 pps per vCPU
Max DDoS Flood Attack Prevention Rate	Up to 950,000 pps per vCPU		**INSPECTION PORTS**	
Latency	< 60 microseconds		Ethernet	1 or 2 inspection ports for typical deployments. Additional inspection ports up to a limit supported by the instance type.
Real-Time Signatures	Detect attacks and protect in less than 18 seconds		**MANAGEMENT PORTS**	
INSPECTION PORTS			Ethernet	1 port
10 GE, 25 GE, 40 GE, 100 GE	2 (Intel® Ethernet Server Adapter X520, 10 GE; Intel® Ethernet Controller XL710, 40 GE), PCI Passthrough		**OPERATION MODE**	
	4 (Intel® Ethernet Network Adapter XXV710, 10 GE, 25 GE), SRIOV		Network Operation	AWS: Symmetric inspection, IP Forwarding Mode Azure: Asymmetric inspection, Destination NAT Forwarding Mode
	2 (Intel® Ethernet Network Controller E810 10GE, 25GE, 50GE, 100GE), SRIOV		Deployment Mode	AWS: In-VPC or Security VPC Azure: In-VPC
MANAGEMENT PORTS			**HIGH AVAILABILITY**	
Ethernet	Via virtual interface (virtio)		Active:Active	AWS and Azure: integration with AWS Gateway Load Balancer and Azure Load Balancer
Management Console	KVM Virsh; VMware Serial Port		Fail-open/fail-close	AWS: with Check Point-provided Lambda function
OPERATION MODE			Support	Certainty Support Program
Network Operation	Transparent L2 Forwarding/IP Forwarding			
Deployment Modes	In-line			
Tunneling Protocols	VLAN Tagging, L2TP, MPLS, GRE, GTP, IPinIP			
IPv6	Yes			
Jumbo Frame	Up to 2KB			
Block Actions	Drop packet, reset (source, destination, both), suspend (source IP address, source port, destination IP address, destination port or any combination), challenge-response for TCP, HTTP and DNS suspicious traffic			
SUPPORT				
Support	Certainty Support Program			

1. Performance figures assume Intel® server-grade processor with 3 GHz

2. 20 Gbps, 40 Gbps Throughput License supported on KVM

Widest Attack Coverage

- Complete Layer 3–7 protection against known and zero-day DoS/DDoS attacks that misuse network bandwidth, server, and application resources.

- Bidirectional visibility to defend against even the most complicated attacks that require looking at both ingress and egress traffic.

- Burst attack protection provides immediate behavioral-based detection and mitigation from one of today's top threats with signature creation and instant enforcement for the fastest remediation.

- Advanced DNS attack coverage that leverages first-in-class behavioral-based algorithms to protect from known and unknown DNS Flood attacks, including DNS Water Torture attacks, in the most cost-effective way.

- A patent-protected stateless and keyless SSL/TLS attack mitigation solution that protects from all types of encrypted attacks with reduced latency and no packet decryption for high protection capacity.

Multiple Deployment Options to Fit Your Needs

- Supports both in-line or out-of-path (Smart Tap) implementations or a scrubbing center deployment.

- Integrates with Check Point's Hybrid Cloud DDoS Protection Service to offer a single vendor hybrid solution that provides zero time to mitigate.

- Enables service providers to offer market-leading DDoS mitigation services to hosted applications and network tenants with multitenant and multipolicy support.

- Virtual appliance enables DDoS mitigation for software-defined data centers (SDDC).

- Range of protection devices offers mitigation capacity from 6 Gbps to 800 Gbps.