FortiDDoS™

DDoS Attack Mitigation Appliances

The Ever-changing DDoS Attack

Distributed Denial of Service (DDoS) attacks continue to remain the top threat to IT security and have evolved in almost every way to do what they do best: shut down your vital online services. Never has a problem been so dynamic and broad-based without being tied to one particular technology. There is almost an unlimited array of tools that Hacktivists and Cyberterrorists can use to prevent access to your network. Sophisticated DDoS attacks target Layer 7 application services where they are much smaller in size making it nearly impossible for traditional ISP-based mitigation methods to detect them.

To combat these attacks, you need a solution that is equally dynamic and broad-based. Fortinet's FortiDDoS Attack Mitigation appliances use behavior-based attack detection methods and 100% ASIC-based processors to deliver the most advanced and fastest DDoS attack mitigation on the market today.

A Different and Better Approach to DDoS Attack Mitigation

Only Fortinet uses a 100% ASIC approach to its DDoS products without the overhead and risks of a CPU or CPU/ASIC hybrid system. The FortiASIC-TP2 transaction processors provide both detection and mitigation of DDoS attacks. The FortiASIC-TP2 processor handles all Layer 3, 4 and 7 traffic types, speeding detection and mitigation performance resulting in the lowest latency in the industry.

FortiDDoS uses a 100% heuristic/behavior-based method to identify threats compared to competitors that rely primarily on signature-based matching. Instead of using pre-defined signatures to identify attack patterns, FortiDDoS builds a baseline of normal activity and then monitors traffic against it. Should an attack begin, FortiDDoS sees this as an anomaly and then immediately takes action to mitigate it. You're protected from known attacks and from the unknown "zero-day" attacks as FortiDDoS doesn't need to wait for a signature file to be updated.

FortiDDoS also handles attack mitigation differently than other solutions. In other DDoS attack mitigation appliances, once an attack starts, it's 100% blocked until the threat is over. If an event is mistakenly matched to a signature creating a "false positive", then all traffic comes to a halt requiring intervention. FortiDDoS uses a more surgical approach by monitoring normal traffic and then using a reputation penalty scoring system, rates IP addresses that are "good" and others that are causing the problem.

Advanced DDoS Protection for Enterprise Datacenters

- 100% hardware-based Layer 3, 4 and 7 DDoS protection provides fast identification and mitigation of attacks.
- Behavior-based DDoS protection reacts to any threat without the need for signature files.
- Up to 24 Gbps full-duplex throughput with bidirectional attack mitigation.
- Combines IP reputation scoring, Geo-location ACLs, and slow attack mitigation for complete Layer 3, 4, and 7 DDoS attack protection in a single appliance.
- Industry leading ultra-low latency of less than 50 microseconds.
- Continuous threat evaluation minimizes risk of "false positive" detections.
- Advanced connectivity with up to 16x 10G SFP+ Fiber interfaces with built-in bypass capabilities.
- Easy to deploy and manage with intuitive GUI and comprehensive reporting and analysis tools.

FortiDDoS blocks the offending IP addresses then repeatedly reevaluates the attack at user defined periods (every 15 seconds by default). If the offending IP addresses continue to be a persistent threat for each of these reevaluation periods, their reputation penalty score will increase and will eventually be blacklisted once they hit a user-defined threshold.

Easy to Set up and Manage

The FortiDDoS Automated Learning tools require less than an hour to build a complete baseline of your application traffic patterns. Once complete, set your thresholds or simply use the default settings. FortiDDoS then automatically begins defending you from any DDoS attack without having to spend hours configuring option after option or worrying about signature updates.

Comprehensive reporting and dashboards give you the tools you need to review attacks and threats to your services. You can run reports as you need them or schedule them to be delivered to you on a regular basis. Dashboards allow you to view and understand attack trends in an easy-to-use single screen layout. Whether it's general status reporting or in-depth granular attack analysis, FortiDDoS provides detailed information on service level attacks and mitigation responses for specific events or over periods of time.

Flexible Defensive Mechanisms

FortiDDoS protects against every DDoS attack including Bulk Volumetric, Layer 7 Application, and SSL/HTTPS attacks. From the oldest trick in the book to the latest in advanced service-level attacks, FortiDDoS has you covered.

Bulk Volumetric Attacks were the first DDoS attack types and continue to pose significant threats today. Usually ISPs prevent most simple attacks of this type, however increasingly they are used to mask more complex application-level attack methods. The easiest way to deal with these types of threats is to simply block all traffic until the attack stops. The FortiDDoS IP Reputation scoring system continues to let "good" traffic in while mitigating IP addresses that are causing the problem. This process not only provides the protection you need, but also minimizes the effects of a "false positive" match from halting good client traffic.

Layer 7 Targeted Attacks are the fastest growing source of DDoS attacks. They attempt to exploit vulnerabilities within a service to exhaust its resources rendering it unavailable. Usually these types of attacks are embedded in Bulk Volumetric Attacks, however they can occur separately. As these types of attacks require considerably less bandwidth to deny service, they are more difficult to detect and regularly pass from ISPs directly to your network. All Layer 7 targeted attacks, large or small, will trigger changes at the service level that will be identified by the FortiDDoS behavioral analysis engine and mitigated.

SSL-Based Attacks use SSL-based encryption methods to hide the content of the attack packets. Additionally, the encryption methods employed will often mean that there are far less resources available that need to be exhausted. Most signature-based solutions require decryption of the traffic to perform matching against known attack profiles. With a behavioral system such as FortiDDoS, these attacks are detected without decryption as they will cause a change in behavior. This change can then be compared with normal behavior and an understanding of the resources available. When the relevant resources become threatened does the FortiDDoS put mitigation in place and respond to the attack.

Key Features and Benefits

100% Behavioral-based Detection	FortiDDoS doesn't rely on signature files that need to be updated with the latest threats so you're protected from both known and unknown "zero-day" attacks.
100% Hardware-based DDoS Protection	The FortiASIC-TP2 transaction processor provides bi-directional detection and mitigation of Layer 2, 3 and 7 DDoS attacks for industry-leading performance.
Continuous Attack Evaluation	Minimizes the risk of "false positive" detection by reevaluating the attack to ensure that "good" traffic isn't disrupted.
Congestion Resistant	With up to 24 Gbps of throughput, FortiDDoS won't easily be overwhelmed by high-volume DDoS attacks.
Automated Learning Process	With minimal configuration, FortiDDoS will automatically build normal traffic and resources behavior profiles saving you time and IT management resources.
Multiple Attack Protection	By understanding behaviors FortiDDoS can detect any DDoS attack from basic Bulk Volumetric to sophisticated Layer 7 SSL-based attacks without the need to decrypt traffic.

FEATURES

Packet Inspection Technology

- Granular Packet Inspection
- Stateful Monitoring
- Continuous Adaptive Rate Limiting
- Heuristic Analysis
- Predictive Behavioral Analysis

Multi-verification Process

- Dynamic Filtering
- Active Verification
- Anomaly Recognition
- Protocol Analysis
- Rate Limiting
- White List, Black List, Non-Tracked Subnets
- State Anomaly Recognition
- Stealth Attack Filtering
- Dark Address Scan Prevention
- Source Tracking
- Legitimate IP Address Matching (Anti-Spoofing)

Flood Prevention Mechanisms

- SYN Cookie, ACK Cookie, SYN Retransmission
- Connection Limiting
- Aggressive Ageing
- Legitimate IP Address Matching
- Source Rate Limiting
- Source Tracking
- Granular Rate Limiting

Layer 3 Flood Mitigation

- Protocol Floods
- Fragment Floods
- Source Floods
- Destination Floods
- Dark Address Scans
- Excessive TCP per Destination
- Geo-location Access Control Policy (ACP)

Layer 4 Flood Mitigation

- TCP Ports (all)
- UDP Ports (all)
- ICMP TCP/Codes (all)
- Connection Flood
- SYN Flood
- Excessive SYN's/Source/Second
- Excessive Connection Establishments/Second
- Zombie Floods
- Excessive Connections per Source Flood
- Excessive Connections per Destination Flood
- TCP State Violation Floods

Layer 7 Flood Mitigation

- Opcode Flood
- HTTP URL Get Flood
- User Agent Flood
- Referrer Flood
- Cookie Flood
- Host Flood
- Associated URL Access
- Mandatory HTTP Header Parameters
- Sequential HTTP Access
- SIP Invites per Source
- SIP Registers per Source
- SIP Concurrent Invites per Source

IP Reputation Analysis

- Dynamic IP Reputation Analysis
- IP Reputation Database Updates

Behavioral Monitoring Metrics

- Packets/Source/Second
- SYN Packet/Second
- Connection Establishments/Second
- SYN Packets/Source/Second
- Connections/Second
- Concurrent Connections/Source
- Concurrent Connections/Destination
- Packets/Port/Second
- Fragmented Packets/Second
- Protocol Packets/Second
- Same URL/Second
- Same User-Agent/Host/Referrer/Cookie/Second
- Same User-Agent, Host, Cookie, Referrer/Second
- Anti-Spoofing Checks
- Associated URLs Heuristics

Reporting Statistics

- Top Attacks
- Top Attackers
- Top Attacked Subnets
- Top Attacked Protocols
- Top Attacked TCP Ports
- Top Attacked UDP Ports
- Top Attacked ICMP Type/Codes
- Top Attacked URLs
- Top Attacked HTTP Hosts
- Top Attacked HTTP Referrers
- Top Attacked HTTP Cookies
- Top Attacked HTTP User-Agents

Management

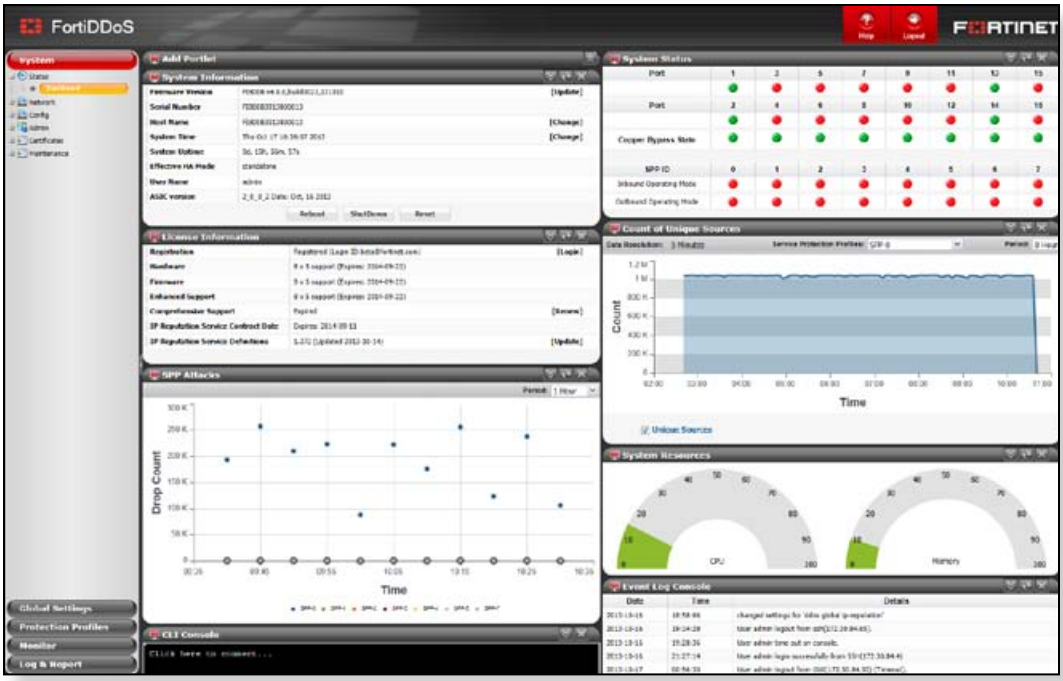
- SSL Management GUI
- CLI
- RESTful API

Centralized Event Reporting

- GUI
- SNMP
- Email/Pager
- Support for MRTG, Cacti

Audit and Access Trails

- Login Trail
- Configuration Trail Audit Trail



Dashboard view of status and events

Port statistics: Packet monitoring

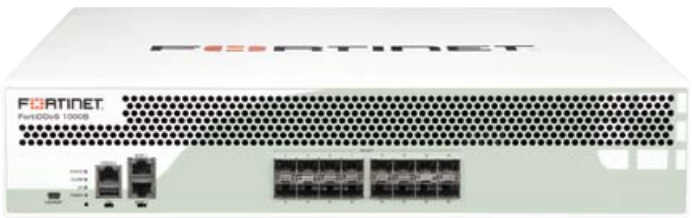
Aggregate drop

SPECIFICATIONS

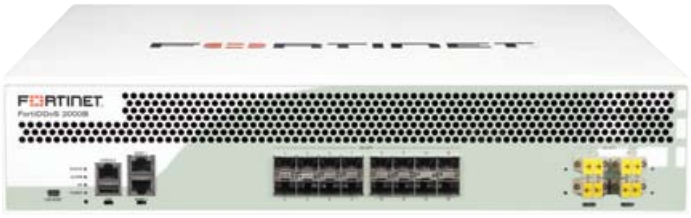
	FORTIDDOS-400B	FORTIDDOS-800B	FORTIDDOS-1000B	FORTIDDOS-2000B
Hardware Specifications				
LAN Interfaces Copper GE with built-in bypass	8	8	–	–
WAN Interfaces Copper GE with built-in bypass	8	8	–	–
LAN Interfaces (Fiber) GE	8	8	–	–
WAN Interfaces (Fiber) GE	8	8	–	–
LAN Interfaces SFP+ (10 Gbps)	–	–	8	8
WAN Interfaces SFP+ (10 Gbps)	–	–	8	8
LAN Interfaces SFP+ (10 Gbps) with built-in bypass	–	–	–	2
WAN Interfaces SFP+ (10 Gbps) with built-in bypass	–	–	–	2
Storage	1x 480 GB SSD	1x 480 GB SSD	1x 480 GB SSD	1x 480 GB SSD
Form Factor	1U Appliance	1U Appliance	2U Appliance	2U Appliance
System Performance				
Throughput (full duplex)	4 Gbps	8 Gbps	12 Gbps	24 Gbps
Simultaneous Connections	1 M	2 M	3 M	6 M
Simultaneous Sources	1 M	2 M	3 M	6 M
Session Setup/Teardown	100 K/sec	200 K/sec	300 K/sec	600 K/sec
Latency	<50 Microseconds	<50 Microseconds	<50 Microseconds	<50 Microseconds
DDoS Attack Mitigation Response Time	<2 seconds	<2 seconds	<2 seconds	<2 seconds
Dimensions				
Height x Width x Length (in)	1.77 x 17 x 16.32	1.77 x 17 x 16.32	3.5 x 17.24 x 22.05	3.5 x 17.24 x 22.05
Height x Width x Length (mm)	45 x 432 x 414.5	45 x 432 x 414.5	88 x 438 x 560	88 x 438 x 560
Weight	17.2 lbs (7.8 kg)	18.1 lbs (8.2 kg)	36.0 lbs (16.2 kg)	38.7 lbs (17.6 kg)
Environment				
Input Voltage	100-240V AC, 50–60 Hz	100-240V AC, 50–60 Hz	100-240V AC, 50–60 Hz	100-240V AC, 50–60 Hz
Power Consumption (AVG)	156 W	174 W	253 W	311 W
Power Consumption (MAX)	260 W	285 W	422 W	575 W
Maximum Current	110V/5.29A, 120V/2.2A	110V/5.29A, 120V/2.2A	110V/10.0A, 120V/5.0A	110V/10.0A, 120V/5.0A
Heat Dissipation	887 BTU/h	972 BTU/h	1,440 BTU/h	1,962 BTU/h
Operating Temperature	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)
Storage Temperature	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)
Humidity	5–95% non-condensing	5–95% non-condensing	5–95% non-condensing	5–95% non-condensing
Compliance				
Safety Certifications	FCC Class A Part 15, UL/CB/cUL, C-Tick, VCCI, CE	FCC Class A Part 15, UL/CB/cUL, C-Tick, VCCI, CE	FCC Class A Part 15, UL/CB/cUL, C-Tick, VCCI, CE	FCC Class A Part 15, UL/CB/cUL, C-Tick, VCCI, CE

FortiDDoS-400B

FortiDDoS-800B



FortiDDoS-1000B



FortiDDoS-2000B

ORDER INFORMATION

Product	SKU	Description
FortiDDoS-400B	FDD-400B	DDOS Protection Appliance — 8x Shared Media pairs (including 8x GE RJ45 with bypass protection, 8x GE SFP slots). 2x GE RJ45 Management Ports. Includes 480 GB SSD default storage. Up to 4 Gbps throughput.
	FC-10-04H00-140-02-DD	IP Reputation Service for FortiDDoS-400B
	FC-10-04H00-311-02-DD	8x5 FortiCare Contract
	FC-10-04H00-247-02-DD	24x7 FortiCare Contract
FortiDDoS-800B	FDD-800B	DDOS Protection Appliance — 8x Shared Media pairs (including 8x GE RJ45 with bypass protection, 8x GE SFP slots). 2x GE RJ45 Management Ports. Includes 512 GB SSD default storage. Up to 8 Gbps throughput.
	FC-10-08H00-140-02-DD	IP Reputation Service for FortiDDoS-800B
	FC-10-08H00-311-02-DD	8x5 FortiCare Contract
	FC-10-08H00-247-02-DD	24x7 FortiCare Contract
FortiDDoS-1000B	FDD-1000B	DDoS Protection Appliance — 8x 10 Gigabit Ethernet SFP+ DDoS Defense Ports, 2x Gigabit RJ45 Management Ports, Dual Power Supply option. Up to 12 Gbps throughput.
	FC-10-01K00-140-02-DD	IP Reputation Service for FortiDDoS-1000B
	FC-10-01K00-311-02-DD	8x5 FortiCare Contract
	FC-10-01K00-247-02-DD	24x7 FortiCare Contract
FortiDDoS-2000B	FDD-2000B	DDoS Protection Appliance — 8x 10 Gigabit Ethernet SFP+ DDoS Defense Ports, 2 pairs with optical bypass, 2x Gigabit RJ45 Management Ports, Dual Power Supply. Up to 24 Gbps throughput.
	FC-10-02K00-140-02-DD	IP Reputation Service for FortiDDoS-2000B
	FC-10-02K00-311-02-DD	8x5 FortiCare Contract
	FC-10-02K00-247-02-DD	24x7 FortiCare Contract

FortiDDoS Compatible Transceivers	SKU	Description
FortiDDoS Transceivers	FG-TRAN-LX	Transceiver LX module for all FortiDDoS models with SFP interfaces with LC connector
	FG-TRAN-GC	Transceiver Base-T (Copper) module for all FortiDDoS models with SFP interfaces, supports 1000Base-T only
	FG-TRAN-SX	Transceiver SX module for all FortiDDoS models with SFP interfaces
	FG-TRAN-SFP+SR	10-Gig transceiver, short range SFP+ module for all FortiDDoS models with SFP+ interfaces with LC connector
	FG-TRAN-SFP+LR	10-Gig transceiver, SFP+, long range

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road #20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480