



FortiDDoS™  
DDoS Attack Mitigation Appliances



## FortiDDoS

FortiDDoS 200B, 400B, 600B, 800B, 900B, 1000B, 1000B-DC and 1200B  
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.

### Advanced DDoS Protection for Enterprise Data Centers

- 100% hardware-based Layer 3, 4 and 7 DDoS protection provides fast identification and mitigation of attacks.
- Advanced connectivity with up to 16x GE or 18x 10 GE. Built-in bypass on most models.
- Behavior-based DDoS protection reacts to any threat without the need for signature files.
- Up to 36 Gbps throughput with bidirectional attack mitigation.
- Massively parallel single-pass architecture monitors hundreds of thousands of parameters simultaneously for complete Layer 3, 4, and 7 DDoS attack protection in a single appliance.
- Advanced suite of DNS DDoS Mitigation features.
- Continuous threat evaluation minimizes risk of "false positive" detections.
- Easy to deploy and manage with intuitive GUI and comprehensive reporting and analysis tools.
- Hybrid On-premise/Cloud Mitigation Option available
- FortiDDoS Cloud Monitoring service for visualization of attack impact and services availability



## HIGHLIGHTS

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, to rate IP addresses that are "good" and others that are causing the problem.

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

FortiDDoS starts working "out-of-the-box" while its automated learning tools create a baseline of your application traffic patterns. Whether you use default or learned thresholds, FortiDDoS automatically defends you from DDoS attacks, saving your team hours configuring options, tuning profiles, analyzing reports or waiting for signature updates.

Included real-time 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. While ISPs may prevent simple attacks of this type, the attacks are increasingly 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, FortiDDoS responds to the attack with the correct mitigation.

DNS-based attacks target authoritative and recursive DNS servers. Enterprises and Carriers that host DNS servers are at risk from DDoS attacks that specifically target these resources by exploiting weaknesses in the way DNS servers handle requests and traffic. FortiDDoS is the only DDoS mitigation platform that inspects 100% of all DNS traffic to protect against the all types of DDoS attacks directed at DNS servers, including DNS reflection/Response floods, NXdomain, Query floods, and DNS header anomalies. Advanced DNS Protection is available on most FortiDDoS models. Please check the Product Specifications table for more information.

### Hybrid On-premise/Cloud DDoS Mitigation

While FortiDDoS can mitigate any DDoS attack to the limit of the incoming bandwidth available, it is possible that an attacker can overwhelm incoming link(s) or upstream resources. Using a cloud-based mitigation service in combination with FortiDDoS provides hybrid solution to mitigate most DDoS threats. When FortiDDoS detects an attack that exceeds a user-defined threshold on the Internet link(s), it will trigger an alert for the cloud-service provider to evaluate, divert the traffic and mitigate the attack upstream. Currently FortiDDoS fully supports the Verisign OpenHybrid™ DDoS Protection Service.

FortiDDoS on-premise appliances in enterprise data centers can also collaborate directly with high capacity FortiDDoS models in the service provider network using the cloud-signaling technology.

### FortiDDoS Cloud Monitoring Service

Visibility of the impact of attacks is an essential part of the DDoS mitigation strategy for IT staff. FortiDDoS Cloud Monitoring service reports on network and server health from our 10 cloud sites. Inexpensive local reporting monitors add reporting from specific customer sites or for outbound services to cloud assets, allowing single-pane-of-glass network health reporting for both inbound and outbound clients.

## Key Features & 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 3, 4 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.
Advanced DNS Protection	FortiDDoS provides 100% inspection of all DNS traffic for protection from a broad range of DNS-based volumetric, application and anomaly attacks.
Automated Learning Process	With minimal configuration, FortiDDoS will automatically build normal traffic and resources behavior profiles saving you time and IT management resources.
Hybrid On-premise/Cloud Support	Open API allows integration with third-party cloud DDoS mitigation providers for flexible deployment options and protection from large-scale DDoS attacks.
Cloud Monitoring Service	Monitor server health from 10 cloud locations and server, inbound or outbound network health from any number of private sites. Uniquely integrates cloud and private inbound and outbound service health reporting.

## FORTIDDOS FEATURES

### Packet Inspection Technology

- Predictive Behavioral Analysis
- Heuristic Analysis
- Granular Deep Packet Inspection
- Continuous Adaptive Rate Limiting
- State Monitoring for specific attack vectors
- 100% Packet Inspection

### Behavior Threshold Management

- System Recommendation based on past traffic statistics
- Adaptive threshold estimation

### 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
- Local address anti-spoofing (BCP-38)
- Source Tracking
- Legitimate IP Address Matching (Anti-Spoofing)

- Elevated treatment for Proxy-IPs
  - detected based on headers and number of concurrent connections

### Layer 3 Flood Mitigation

- Layer 3 Flood Mitigation
- Protocol Floods (all)
- Fragment Floods
- Source Floods
- Destination Floods
- Local Address Anti-Spoofing ((BCP38) Geo-location Access Control Policy (ACP))
- IP Reputation

### Layer 4 Flood Mitigation

- TCP Ports (all)
- UDP Ports (all)
- ICMP Type/Codes (all)
- Connection Flood
- SYN, ACK, RST, FIN Floods
- Excessive SYN/ACK/ESTAB/FIN/RST's/second per Source or Destination
- Zombie Floods
- Excessive Connections per Source Flood
- Excessive Connections per Destination Flood
- TCP State Violation Floods

### Layer 7 Flood Mitigation

- HTTP URL
- HTTP METHOD:GET, HEAD, OPTIONS, TRACE, POST, PUT, DELETE, CONNECT Floods
- User Agent Flood
- Referrer Flood
- Cookie Flood
- Host Flood
- Mandatory HTTP Header Parameters
- Sequential HTTP Access

### Flood Prevention Mechanisms

- SYN Cookie, ACK Cookie, SYN Retransmission, DNS retransmission, DNS TC=1
- Legitimate IP Address Matching
- Source Tracking
- Source Rate Limiting
- Granular Rate Limiting
- Connection Limiting
- Aggressive Ageing

### DNS Attack Mitigation

- DNS Header anomaly prevention
- DNS Query-response matching
- DNS Query flood
- DNS Unexpected Query
- Unsolicited DNS Response flood
- DNS Response cache under flood
- DNS Query flood per source within TTL

# FORTIDDOS FEATURES

## Management

- SSL Management GUI
- CLI
- RESTful API

## Reporting Statistics

- Filterable Attack Log
- Over 80 built-in reporting graphs for each protected subnet and for each traffic direction
- Summary Graphs and Logs for:
  - Top Attacks
  - Top Attackers

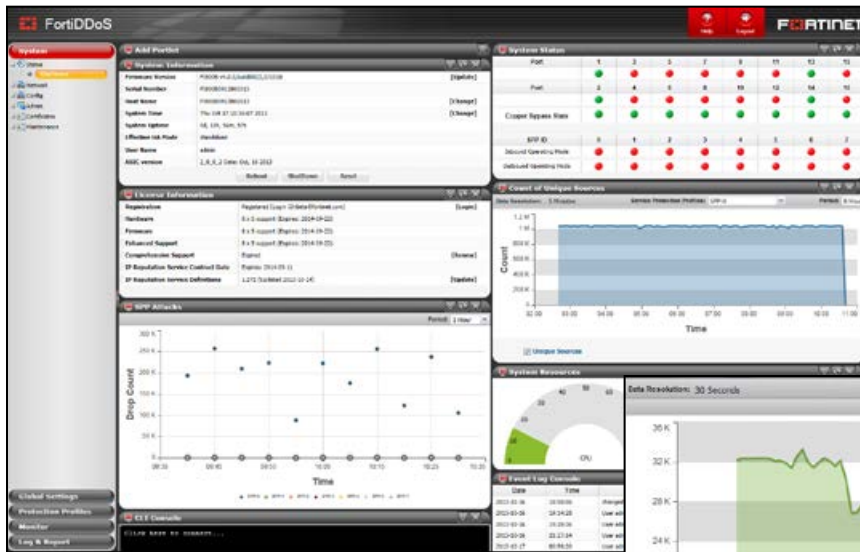
- Top ACL Drops
- Top Attacked Subnets and IP Addresses
- Top Attacked Protocols
- Top Attacked TCP and UDP Ports
- Top Attacked ICMP Types/Codes
- Top Attacked URLs
- Top Attacked HTTP Hosts, Referers, Cookies, User-Agents
- Top Attacked DNS Servers
- Top Attacked DNS Anomalies

## Centralized Event Reporting

- SNMP
- Email/Pager
- RESTful API
- Support for FortiAnalyzer, MRTG, Cacti

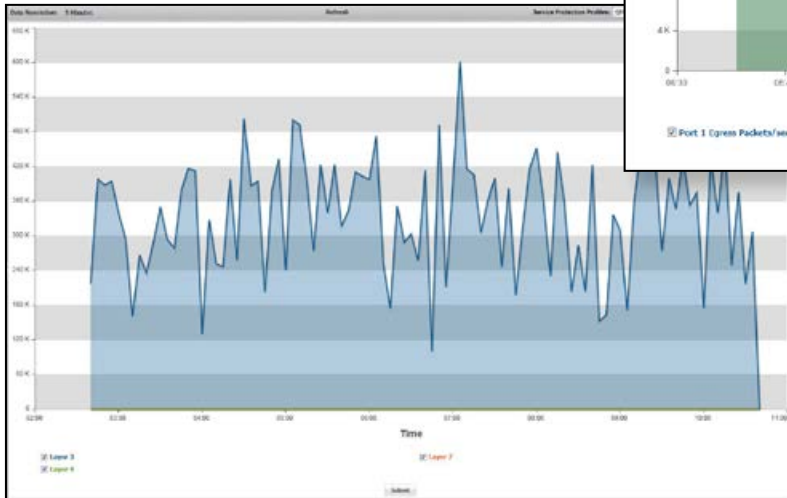
## Audit and Access Trails

- Login Audit Trail
- Configuration Audit Trail



Dashboard view of status and events

Port statistics: Packet monitoring



Aggregate drop

# SPECIFICATIONS

	FORTIDDOS 200B	FORTIDDOS 400B	FORTIDDOS 600B	FORTIDDOS 800B
<b>Hardware Specifications</b>				
LAN Interfaces Copper GE with built-in bypass	4	8	8	8
WAN Interfaces Copper GE with built-in bypass	4	8	8	8
LAN Interfaces SFP GE	4	8	8	8
WAN interfaces SFP GE	4	8	8	8
LAN Interfaces SFP+ 10 GE / SFP GE	—	—	—	—
WAN Interfaces SFP+ 10 GE / SFP GE	—	—	—	—
LAN Interfaces LC (850 nm, 10 GE) with built-in bypass	—	—	—	—
WAN Interfaces LC (850 nm, 10 GE) with built-in bypass	—	—	—	—
Storage	1x 480 GB SSD	1x 480 GB SSD	1x 480 GB SSD	1x 480 GB SSD
Form Factor	1U Appliance	1U Appliance	1U Appliance	1U Appliance
Power Supply	Single (Optional External Dual Hot-Swappable)	Single (Optional External Dual Hot-Swappable)	Single (Optional External Dual Hot-Swappable)	Single (Optional External Dual Hot-Swappable)
<b>System Performance</b>				
Throughput (Enterprise Mix — Gbps)	3	6	12	12
Packet Throughput (Mpps)	4	8	16	16
Latency (µs) Maximum/Typical	<50/<10	<50/<10	<50/<10	<50/<10
DDoS Attack Mitigation Response Time (s)	<2	<2	<2	<2
Advanced DNS Mitigation (Firmware v4.2.0)	Yes	Yes	No	Yes
DNS Queries per second (M)	1	2	NA	4
Open Hybrid Cloud Mitigation Support	Yes	Yes	Yes	Yes
<b>Environment</b>				
Input Voltage AC	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz
Input Voltage DC	—	—	—	—
Power Consumption (Average)	156 W	156 W	174 W	174 W
Power Consumption (Maximum)	260 W	260 W	285 W	285 W
Maximum Current AC	110V/5.29A, 120V/2.2A	110V/5.29A, 120V/2.2A	110V/5.29A, 220V/2.2A	110V/5.29A, 120V/2.2A
Maximum Current DC	—	—	—	—
Heat Dissipation (BTU/hr) / (kjoules/hr)	887 / 936	887 / 936	972 / 1026	972 / 1026
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
<b>Compliance</b>				
Safety Certifications	FCC Class A Part 15, UL/CB/cUL, C-Tick, VCCI, CE			
<b>Dimensions</b>				
Height x Width x Length (inches)	1.77 x 17 x 16.32	1.77 x 17 x 16.32	1.77 x 17 x 16.32	1.77 x 17 x 16.32
Height x Width x Length (mm)	45 x 432 x 414.5	45 x 432 x 414.5	45 x 432 x 414.5	45 x 432 x 414.5
Weight	17.2 lbs (7.8 kg)	17.2 lbs (7.8 kg)	17.2 lbs (7.8 kg)	17.2 lbs (7.8 kg)



FortiDDoS 200B



FortiDDoS 400B



FortiDDoS 600B



FortiDDoS 800B

## SPECIFICATIONS

	FORTIDDOS 900B	FORTIDDOS 1000B / FORTIDDOS 1000B-DC	FORTIDDOS 1200B
<b>Hardware Specifications</b>			
LAN Interfaces Copper GE with built-in bypass	—	—	—
WAN Interfaces Copper GE with built-in bypass	—	—	—
LAN Interfaces SFP GE	—	—	—
WAN interfaces SFP GE	—	—	—
LAN Interfaces SFP+ 10 GE / SFP GE	8	8	7
WAN Interfaces SFP+ 10 GE / SFP GE	8	8	7
LAN Interfaces LC (850 nm, 10 GE) with built-in bypass	—	—	2
WAN Interfaces LC (850 nm, 10 GE) with built-in bypass	—	—	2
Storage	1x 480 GB SSD	1x 480 GB SSD	1x 480 GB SSD
Form Factor	2U Appliance	2U Appliance	2U Appliance
Power Supply	Dual Hot-Swappable	Dual Hot-Swappable	Dual Hot-Swappable
<b>System Performance</b>			
Throughput (Enterprise Mix — Gbps)	18	18	36
Packet Throughput (Mpps)	24	24	48
Latency (µs) Max/Typical	<50/<10	<50/<10	<50/<10
DDoS Attack Mitigation Response Time (s)	<2	<2	<2
Advanced DNS Mitigation (Firmware v4.2.0)	No	Yes	Yes
DNS Queries per second (M)	NA	6	12
Open Hybrid Cloud Mitigation Support	Yes	Yes	Yes
<b>Environment</b>			
Input Voltage AC	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz
Input Voltage DC	—	40.5–57V DC	—
Power Consumption (Average)	253 W	253 W	311 W
Power Consumption (Maximum)	422 W	422 W	575 W
Maximum Current AC	110V/10.0A, 220V/5.0A	110V/10.0A, 120V/5.0A	110V/10.0A, 120V/5.0A
Maximum Current DC	—	24A	—
Heat Dissipation (BTU/hr) / (kjoules/hr)	1440 / 1420	1440 / 1420	1962 / 2070
Operating Temperature	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)
Humidity	5–95% non-condensing	5–95% non-condensing	5–95% non-condensing
<b>Compliance</b>			
Safety Certifications	FCC Class A Part 15, UL/CB/cUL, C-Tick, VCCI, CE		
<b>Dimensions</b>			
Height x Width x Length (inches)	3.5 x 17.24 x 22.05	3.5 x 17.24 x 22.05	3.5 x 17.24 x 22.05
Height x Width x Length (mm)	88 x 438 x 560	88 x 438 x 560	88 x 438 x 560
Weight	36.0 lbs (16.2 kg)	36.0 lbs (16.2 kg)	36.0 lbs (16.2 kg)



FortiDDoS 900B



FortiDDoS 1000B



FortiDDoS 1200B

## ORDER INFORMATION

Product	SKU	Description
FortiDDoS 200B	FDD-200B	DDoS Protection Appliance — 4 pairs x Shared Media DDoS Defense Ports (including 4 pairs x GE RJ45 with bypass protection, 4 pairs x GE SFP slots), 2x GE RJ45 Management Ports, AC Power Supply with Redundant Power Option. Includes 480 GB SSD storage. 3 Gbps throughput. Supports Advanced DNS Mitigation.
FortiDDoS 400B	FDD-400B	DDoS Protection Appliance — 8 pairs x Shared Media DDoS Defense Ports (including 8 pairs x GE RJ45 with bypass protection, 8 pairs x GE SFP slots), 2x GE RJ45 Management Ports, AC Power Supply with Redundant Power Option. Includes 480 GB SSD storage. 6 Gbps throughput. Supports Advanced DNS Mitigation.
FortiDDoS 600B	FDD-600B	DDoS Protection Appliance — 8 pairs x Shared Media DDoS Defense Ports (including 8 pairs x GE RJ45 with bypass protection, 8 pairs x GE SFP slots), 2x GE RJ45 Management Ports, AC Power Supply with Redundant Power Option. Includes 480 GB SSD storage. 12 Gbps throughput. Does NOT support Advanced DNS Mitigation.
FortiDDoS 800B	FDD-800B	DDoS Protection Appliance — 8 pairs x Shared Media DDoS Defense Ports (including 8 pairs x GE RJ45 with bypass protection, 8 pairs x GE SFP slots), 2x GE RJ45 Management Ports, AC Power Supply with Redundant Power Option. Includes 480 GB SSD storage. 12 Gbps throughput. Supports Advanced DNS Mitigation.
FortiDDoS 900B	FDD-900B	DDoS Protection Appliance — 8 pairs x 10 GE SFP+ DDoS Defense Ports (can also support GE SFPs), 2x GE RJ45 Management Ports, Dual AC Power Supplies. Includes 480 GB SSD storage and 2x 10 GE SR SFP+. 18 Gbps throughput. Does NOT support Advanced DNS Mitigation.
FortiDDoS 1000B	FDD-1000B	DDoS Protection Appliance — 8 pairs x 10 GE SFP+ DDoS Defense Ports (can also support GE SFPs), 2x GE RJ45 Management Ports, Dual AC Power Supplies. Includes 480 GB SSD storage and 2x 10 GE SR SFP+. 18 Gbps throughput. Supports Advanced DNS Mitigation.
FortiDDoS 1000B-DC	FDD-1000B-DC	DDoS Protection Appliance — 8 pairs x 10 GE SFP+ DDoS Defense Ports (can also support GE SFPs), 2x GE RJ45 Management Ports, Dual DC Power Supplies. Includes 480 GB SSD storage and 2x 10 GE SR SFP+. 18 Gbps throughput. Supports Advanced DNS Mitigation.
FortiDDoS 1200B	FDD-1200B	DDoS Protection Appliance — 8 pairs x 10 GE SFP+ DDoS Defense Ports (can also support GE SFPs), 2 pairs x 10 GE LC Ports with optical bypass, 2x GE RJ45 Management Ports, Dual AC Power Supplies. Includes 480 GB SSD storage and 2x 10 GE SR SFP+. 36 Gbps throughput. Supports Advanced DNS Mitigation.
<b>FortiDDoS Cloud Monitoring</b>		
FortiDDoS Cloud Monitoring	FC1-10-FMD01-148-02-12	1-year FortiDDoS Cloud Monitoring Service with up to 10 Health Check configurations. Includes 10 cloud agents for monitoring.
	FC2-10-FMD01-148-02-12	1-year FortiDDoS Cloud Monitoring Service with up to 50 Health Check configurations. Includes 10 cloud agents for monitoring and up to 4 user-deployed VM-based cloud agents.
	FC3-10-FMD01-148-02-12	1-year FortiDDoS Cloud Monitoring Service with up to 100 Health Check configurations. Includes 10 cloud agents for monitoring and up to 12 user-deployed VM-based cloud agents.
	FC4-10-FMD01-148-02-12	1-year FortiDDoS Cloud Monitoring Service with up to 500 Health Check configurations. Includes 10 cloud agents for monitoring and up to 22 user-deployed VM-based cloud agents.
<b>FortiDDoS Compatible Transceivers</b>		
FortiDDoS Transceivers	FG-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
	FG-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
	FG-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
	FG-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
	FG-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
	SP-CABLE-ADASFP+	10 GE SFP+ active direct attach cable, 10 m / 32.8 ft for all systems with SFP+ and SFP/SFP+ slots.
<b>Compatible Fiber Bypass Units</b>		
FortiBridge 2001F	FBG-2001F	1 G fiber failure bypass unit for one network segment. Includes 2x 1 G SR SFPs.
FortiBridge 2002F	FBG-2002F	1 G fiber failure bypass unit for two network segments. Includes 4x 1 G SR SFPs.
FortiBridge 2002X	FBG-2002X	10 G fiber failure bypass unit for two network segments. Includes 4x 10 G SR SFP+s.
FortiBridge 3002S	FBG-3002S	FortiBridge 3002S (Short Range), power failure bypass functionality for two network segments. 4x 10 G SFP+, 4x LC, 1x console port, dual power supply.
FortiBridge 3002L	FBG-3002L	FortiBridge 3002L (Long Range), power failure bypass functionality for two network segments. 4x 10 G SFP+, 4x LC, 1x console port, dual power supply.
FortiBridge 3004S	FBG-3004S	FortiBridge 3004S (Short Range), power failure bypass functionality for four network segments. 8x 10 G SFP+, 8x LC, 1x console port, dual power supply.
FortiBridge 3004L	FBG-3004L	FortiBridge 3004SL (Short Range + Long Range), power failure bypass functionality for two network segments for short range and two network segments for long range. 4x 10 G SFP+ (short range), 4x 10 G SFP+ (long range), 4x LC (short range), 4x LC (long range), 1x console port, dual power supply.
<b>Optional Accessory</b>		
External redundant AC power supply	FRPS-100	External redundant AC power supply for up to 4 units: FG-300C, FG-310B, FS-348B and FS-448B. Up to 2 units: FG-200B, FG-200D, FG-240D and FG-300D, FG-500D, FDD-200B, FDD-400B, FDD-600B and FDD-800B. Not supported for: FG-200D-POE/240D-POE



GLOBAL HEADQUARTERS  
Fortinet Inc.  
899 Kifer Road  
Sunnyvale, CA 94086  
United States  
Tel: +1.408.235.7700  
www.fortinet.com/sales

EMEA SALES OFFICE  
905 rue Albert Einstein  
Valbonne 06560  
Alpes-Maritimes, France  
Tel: +33.4.8987.0500

APAC SALES OFFICE  
300 Beach Road 20-01  
The Concourse  
Singapore 199555  
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE  
Sawgrass Lakes Center  
13450 W. Sunrise Blvd., Suite 430  
Sunrise, FL 33323  
United States  
Tel: +1.954.368.9990