DATA SHEET

FortiDDoS™

FortiDDoS 400B, 800B, 1000B, 1200B, 1500E, and 2000E

Distributed Denial of Service (DDoS) attacks remain a top threat to IT security and have evolved in almost every way to do what they do best: shut down access to your vital online services.

Unlike intrusion and malware attacks, DDoS attackers have learned that they don't need to attack only end-point servers to shut you down. They attack any IP address that routes to your network: unused IP addresses, Inter-router-link public IP addresses, or Firewall/Proxy/WiFi Gateway public IP addresses.

Cloud-based CDN and DNS-based cloud mitigation cannot protect you from these attacks. What is the impact to your business if your users cannot reach cloud services because your firewall or demarc router public IP is being DDoSed? Your CDN-based web servers may be up but your business is down!

Sophisticated multi-vector and multi-layer DDoS attacks use direct and reflected packets where the spoofed, randomized source IP addresses are impossible to ACL. These attacks are increasingly common as Mirai-style code has morphed into many variants and has been commercialized by providers of "stresser" sites. Anyone can call down large attacks for a few dollars.

To combat these attacks, you need a solution that dynamically protects a large attack surface.

Highlights

- 100% hardware-based Layer 3, 4, and 7 DDoS attack identification and mitigation, simultaneously monitor hundreds of thousands of parameters — a massively-parallel computing architecture
- 100% Machine Learning DDoS detection
- Completely invisible to attackers with no IP and no MAC addresses in the data path. FortiDDoS is not a routing or terminating Layer 3 device.
- Continuous threat evaluation to minimize false positive detections
- Advanced DNS DDoS mitigation on most models
- MSSP Portal for customer resale
- Central Manager
- Hybrid On-premise/Cloud mitigation available with Open Signaling

Powered by SPU — A Different and Better Approach to DDoS Attack Mitigation

Only Fortinet FortiDDoS appliances use Machine Learning detection methods in dedicated, custom-silicon Security Processing Units (SPUs) to deliver the most advanced and fastest DDoS attack mitigation on the market today, without the performance compromises of multi-CPU or CPU/ASIC hybrid systems. The TP2 and TP3 SPU Traffic Processors inspect 100% of both inbound and outbound Layer 3, 4, and 7 packets, resulting in the fastest and most accurate detection and mitigation, and the lowest latency in the industry.

FortiDDoS uses 100% machine learning, behavior-based methods to identify threats. Instead of requiring pre-defined signatures to identify attack patterns, FortiDDoS uses its massively-parallel computing architecture to build an adaptive baseline of normal activity from hundreds-of-thousands of parameters and then monitors traffic against that baseline. Should an attack begin, FortiDDoS sees this as abnormal and immediately takes action to mitigate it.

Highlights

The Power of SPUs — Flexible, Autonomous Defenses

FortiDDoS protects you from known and "zero-day" attacks without creating local or downloading subscription signatures for mitigation. Other vendors try to conserve CPU real-time by inspecting a relatively small number of parameters at a low sample rate, unless and until an explicit signature is created. FortiDDoS' massively parallel SPU Traffic Processors sample 100% of even the smallest packets, for over 230,000 parameters for each Protection Profile. This method allows FortiDDoS to operate completely autonomously, finding some attacks on the FIRST packet and all attacks within two seconds — broader and faster mitigation than any other vendor or method. There is no need to adjust settings, read pcaps, or add regex-style manual signatures or ACLs in the middle of attacks. While attacks are being mitigated, FortiDDoS continues to monitor all other parameters to instantly react to added or changed vectors.

The Resurrection of Botnets

Easily-compromised IoT devices have allowed Botnet attacks to rise again and massive IoT growth assures us they are here to stay. While individual devices have little power, large groups can generate record traffic. Attackers want to hide the real source IP addresses of botted devices so UDP, SYN, TCP Out-of-State (FIN/ACK/RST), DNS and Protocol direct and reflected floods using spoofed source IP addresses are back in vogue. Attackers can launch an unprecedented variety of simultaneous attack vectors. Small-packet floods stress both firewalls and CPU-based DDoS appliances, preventing full inspection with unexpected results. FortiDDoS' fully inspected packet rate is class-leading.

DNS-Based Attacks

Botnet-driven DNS attacks are popular because they can target any type of infrastructure or they can co-opt your DNS servers to attack others with reflected DDoS attacks. FortiDDoS is the only DDoS mitigation platform that inspects 100% of all DNS traffic in both directions, to protect against all types of DDoS attacks directed at, or from DNS servers. It validates over 30 different parameters on every DNS packet at up to 12 M Queries/second. Its built-in cache can offload the local server during floods. FortiDDoS's innovative DQRM feature stops inbound Reflected DNS attacks from the very first packet. FortiDDoS also supports FortiGuard's Domain Reputation Service for ISPs to protect clients from known malicious domains.

Security Fabric

FortiDDoS complements Fortinet's full suite of Security Fabric products, each of which uses purpose-built hardware with dedicated engineering and support resources to provide best-in-class focused protection. FortiDDoS displays system performance and mitigation activities in real-time on a FortiOS Security Fabric Dashboard, providing a single-pane-of-glass view of DDoS threats and mitigations along with other Security Fabric products and partners.

Hybrid On-premise/Cloud DDoS Mitigation

While FortiDDoS can mitigate any DDoS attack to the limit of the incoming bandwidth, large attacks can saturate incoming links, forcing ISP routers to drop good traffic. FortiDDoS's open and documented Attack Signaling API allows our Security Fabric partners to provide you a choice of best-in-class hybrid CPE/cloud DDoS mitigation when attacks threaten to congest upstream resources. FortiDDoS inspects incoming GRE clean traffic from cloud DDoS providers to ensure continuity of logging and reporting, and complete threat mitigation. FortiDDoS on-premise appliances can also provide your ISP with Flowspec scripts to support diversion and multi-parameter blocking of attack traffic.

Always-On Inline vs. Out-of-Path Mitigation

Many hosting providers, MSSPs and ISPs are moving away from out-of-path detection, diversion and scrubbing as too limited and too slow for important infrastructure. Netflow-based detection and mitigation monitor a limited number of parameters for a few different attack types. FortiDDoS mitigates more than 150 attack events, many with "depth" (all 65,000 TCP and UDP ports are monitored and mitigated, for example). 100% packet inspection and leading packet performance ensure mitigation from single-packet anomalies to link-filling small-packet, fragmented UDP floods.

Studies are showing that 75% of DDoS attacks last less than 15 minutes. Customers are also seeing multi-vector attacks, attacks that sequentially change vectors and pulsed attacks that start and stop frequently. FortiDDoS begins mitigating in less than 2 seconds and its massively-parallel detection and mitigation ensures multi-vector, sequential and pulsed attacks are seen and stopped.

All FortiDDoS models offer High Availability and select models offer Optical Bypass (to 100GE) to ensure network continuity in the event of system failures. When attacks threaten link bandwidth, Flowspec scripts can be generated to configure upstream router ACLs.

FortiDDoS also offers a wide range of static and dynamic ACLs to offload other infrastructure. For example, FortiDDoS supports BCP-38 and FortiGuard Domain Reputation blocks IoT and end-user communications to botnet controllers and malicious domains. FortiDDoS ACLs operate at line-rate with no impact on performance even with millions of blocklisted IP addresses.

FortiDDoS offers multitenant real-time graphing and attack reporting for resale to customers.

Key Features and Benefits

100% Machine Learning 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. No "threat-protection" subscriptions required. Saves OPEX.
100% Hardware-based Protection	The SPU TP2 and TP3 Traffic Processors provide 100% packet inspection with bidirectional detection and mitigation of Layer 3, 4 and 7 DDoS attacks for industry-leading performance. Get the performance you pay for.
Continuous Attack Evaluation	Minimizes the risk of "false positive" detection by reevaluating the attack to ensure that "good" traffic isn't disrupted. Less management time needed.
Advanced DNS Protection	FortiDDoS provides 100% inspection of all DNS traffic at up to 12 million QPS, for protection from a broad range of DNS-based volumetric, application and anomaly attacks. DNS Reflection floods are stopped on the FIRST packet.
Machine Learning	With minimal configuration, FortiDDoS will automatically build normal traffic and resources behavior profiles saving you time and IT management resources.
Autonomous Mitigation	No operator intervention required for any type or size of attack.
Hybrid On-premise/Cloud Support	Open, documented API allows integration with third-party cloud DDoS mitigation providers for flexible deployment options and protection from large-scale DDoS attacks.
Fortinet Security Fabric Integration	Single-pane visibility of attack mitigation and network performance reduces management and improves response time.
RESTful API	FortiDDoS can be integrated into almost any environment through its RESTful API.
Central Manager	FortiDDoS-CM is available for users with multiple geographically dispersed FortiDDoS units. One management screen for all devices with single sign-on.

FortiDDoS Features

Packet Inspection Technology

- 100% Packet Inspection
- Full IPv4/IPv6 Support to single IP addresses
- Machine learning for Predictive, Heuristic, Adaptive Analysis
- Deep Packet Inspection
- TCP State knowledge to instantly mitigate out-of-state attacks
- DNS Query Monitoring to instantly mitigate DNS Reflected attacks
- Complete invisibility with no MAC nor IP addresses in the data path
- Massively parallel processing for multiple simultaneous attack vectors

Behavioral Threshold Management

- Machine-learning thresholds for millions of L3-L7 parameters
- Automatic adaptive thresholds estimation for critical L3, L4 and L7 parameters

100% Anomaly Inspection

- L3/L4/L7 HTTP Headers
- DNS Header and Payload
- TCP State and Transition Anomalies

Layer 3 Attack Mitigation

- Protocol Floods (all 256 monitored)
- Fragment Floods (TCP/UDP/Other Protocols)
- Source Floods (6M monitored)
- FortiGuard IP Reputation Subscription
- Full L3-L7 IP-inside-GRE Inspection

Layer 4 Attack Mitigation

- TCP Ports (all 65k)
- UDP Ports (all 65k)
- TCP / UDP Service / Gaming Ports
- ICMP Type/Codes (all 65k)
- SYN, SYN/Destination with line-speed validation, SYN/Source
- **First-packet** TCP State flood mitigation
- Slow Connections
- TCP Source validation
- L4 Aggressive Connection Aging

HTTP Attack Mitigation

- Top 32k HTTP URLs
- Top 500 Referers, Cookies, Hosts, User Agents
- HTTP METHOD Floods (all 8 METHODS +Total Methods/Source)
- SSL Renegotiation
- L7 Aggressive Aging

DNS (B-Series/E-Series) /NTP (E-Series) Attack Mitigation

- **First-packet** DNS / NTP Response Flood mitigation (DQRM/NRM)
- DNS / NTP Header/payload/state anomalies
- DNS Query / MX / ALL / ZT / fragment / per-Source Floods
- DNS Response Code Flood mitigation
- NTP Request / Response / Response-per-Destination Floods
- DNS Query Source validation, Unexpected Query, Legitimate Query
- DNS Query TTL validation
- DNS Response cache under flood
- DNS Resource Record ACLs
- DNS Domain Reputation Subscription
- NTP Monlist / Mode 6 ACL

FortiDDoS Features

Access Control Lists

FortiDDoS is the ONLY product in the industry that supports large ACLs in hardware with no performance degradation. While most DDoS attacks use spoofed source IP addresses, your existing Indicators of Compromise IP address and domain lists can be uploaded to FortiDDoS to offload other infrastructure.

- IP Reputation – Fortinet FortiGuard subscription
- IP/subnet Blocklist/ Allowlist
- Bulk IPv4 Blocklist Customer Upload (>1million addresses)
- Geolocation
- Enhanced BCP38 Source Address Validation/Local Address Anti-Spoofing (>2000 subnets)
- Protocol, UDP, TCP, and other Protocol Fragments, DNS Fragment, L4 Port, ICMP Type/Code
- HTTP Methods, URLs, Hosts, Referrers, User Agents
- DNS Domain Reputation – Fortinet FortiGuard subscription (>250k Malicious Domains)
- DNS Bulk Domain Blocklist Customer Upload (>500k Domains)
- DNS Resource Record ACLs (256 RRs)
- Packet Length, v4/v6, Protocol, TCP/UDP Port, ICMP Type-Code, TCP/UDP/Other fragment ACL
- Flowspec ACL script generation

Comprehensive Built-In Reporting

- Filterable/Exportable Attack Log
- 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, HTTP Hosts, Referers, Cookies, User-Agents
- Top Attacked DNS Servers
- Top Attacked DNS Anomalies
- Physical Port, SPP, SPP Policy (subnet) and SPP Policy Group statistics: Mbps/pps and Drops graphing
- Custom, on-demand, on-schedule and/or on-Attack-Threshold reports in multiple formats
- Millions of built-in reporting graphs for real-time and forensic analysis

Centralized Event Reporting

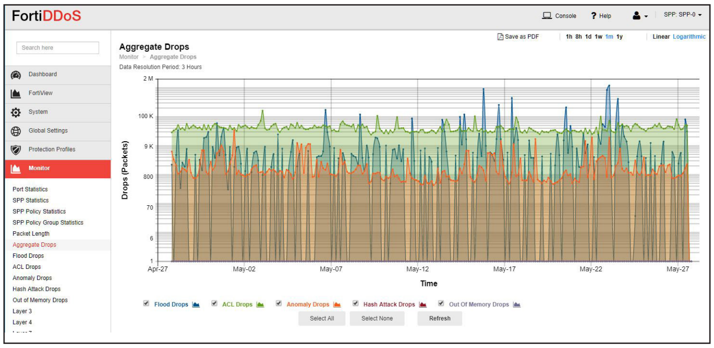
- SNMP v2/v3 MIB and Traps
- Email Alerts and Reports
- Open RESTful API
- Syslog support for FortiAnalyzer, FortiSIEM and third-party servers
- FortiDDoS Central Manager centralized attack log and executive summary

Audit Trails

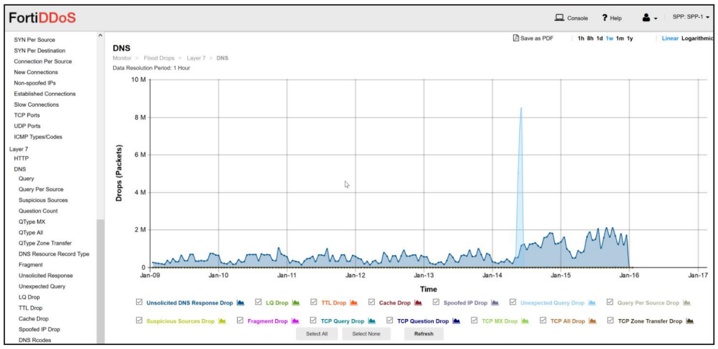
- Login Audit Trail
- Configuration Audit Trail

Management

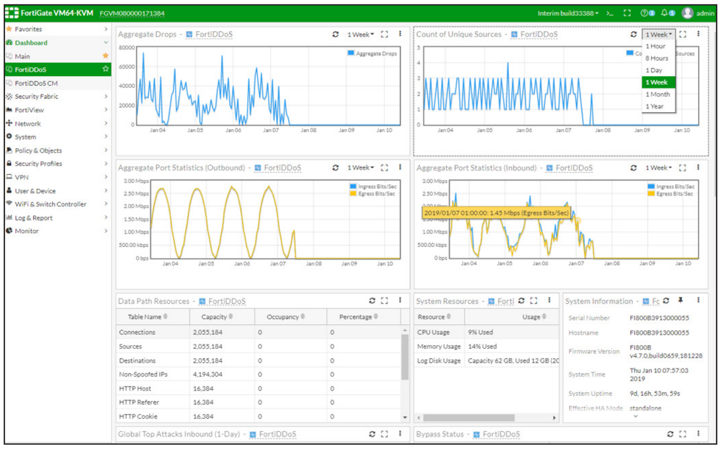
- Full TLS 1.3 Management GUI
- Full CLI
- Open RESTful API
- RADIUS, LDAP, and TACACS+ Authentication including 2FA and Proxy
- Multi-Tenant MSSP Portal
- Central Manager for multiple FortiDDoS
- Open Cloud Mitigation Signaling



Aggregate Drops L3-L7



DNS Attacks



Data Path Resources - FortiDDoS

Table Name	Capacity	Occupancy	Percentage
Connections	2,055,184	0	0
Sources	2,055,184	0	0
Destinations	2,055,184	0	0
Non-Spoofed IPs	4,194,304	0	0
HTTP Host	16,384	0	0
HTTP Referer	16,384	0	0
HTTP Cookie	16,384	0	0

System Resources - Forti

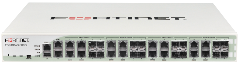
Resource	Usage
CPU Usage	9% Used
Memory Usage	14% Used
Log Disk Usage	Capacity 62 GB, Used 12 GB (20

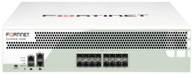
System Information - Fc

Serial Number	FI800B3913000055
Hostname	FI800B3913000055
Firmware Version	FI800B v4.7.0,build0659,181228
System Time	Thu Jan 10 07:57:03 2019
System Uptime	9d, 16h, 53m, 59s
Effective HA Mode	standalone

FortiOS Security Fabric Dashboard

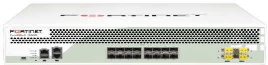
Specifications





	FORTIDDOS 400B	FORTIDDOS 800B	FORTIDDOS 1000B
Hardware Specifications			
LAN Interfaces Copper GE with built-in bypass	8	8	—
WAN Interfaces Copper GE with built-in bypass	8	8	—
LAN Interfaces SFP GE	8	8	—
WAN interfaces SFP GE	8	8	—
LAN Interfaces SFP+ 10 GE / SFP GE	—	—	8
WAN Interfaces SFP+ 10 GE / SFP GE	—	—	8
LAN Interfaces LC (850 nm, 10 GE) with built-in bypass	—	—	—
WAN Interfaces LC (850 nm, 10 GE) with built-in bypass	—	—	—
LAN Interfaces QSFP+ 40 GE or QSFP28 100 GE	—	—	—
WAN Interfaces QSFP+ 40 GE or QSFP28 100 GE	—	—	—
Passive Optical Bypass	—	—	—
Storage	1x 480 GB SSD	1x 480 GB SSD	1x 480 GB SSD
Form Factor	1U Appliance	1U Appliance	2U Appliance
Power Supply	Single (Optional 2nd External PS, Hot-Swappable)	Single (Optional 2nd External PS, Hot-Swappable)	Dual AC Hot-Swappable
System Performance			
Maximum Inspected Throughput (Gbps)	7	14	21
Inspected Throughput (Enterprise Mix — Gbps)	6	12	18
Inspected Packet Throughput (Mpps)	8	15	23
Maximum Mitigation (Gbps/Mpps)	8 / 12	12 / 18	80 / 120
SYN Flood Mitigation (SYN In + Coookie Out) Mpps	7	14	21
Simultaneous TCP Connections (M)	1	2	3
Simultaneous Sources (M)	1	2	3
Session Setup/Teardown (kcps)	100	200	300
Latency (μs) Maximum/Typical	<50/<10	<50/<10	<50/<10
DDoS Attack Mitigation Response Time	1st packet to <2 seconds	1st packet to <2 seconds	1st packet to <2 seconds
Advanced DNS/NTP Mitigation	DNS	No	DNS
DNS/NTP Queries per second (M)	2 / NA	4 / NA	6 / NA
DNS/NTP Response Validation under Flood (M Responses/s)	2 / NA	4 / NA	6 / NA
Open Hybrid Cloud Mitigation Support	Yes	Yes	Yes
Environment			
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)	156 W	174 W	253 W
Power Consumption (Maximum)	260 W	285 W	422 W
Maximum Current AC	110V/5.29A, 120V/2.2A	110V/5.29A, 120V/2.2A	110V/10.0A, 220V/5.0A
Maximum Current DC	—	—	24A
Heat Dissipation (BTU/hr) / (kjoules/hr)	887 / 936	972 /1026	1440 / 1420
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
Compliance			
Safety Certifications		FCC Class A Part 15, UL/CB/cUL, RCM, VCCI, CE	
Dimensions			
Height x Width x Length (inches)	1.77 x 17 x 16.32	1.77 x 17 x 16.32	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
Weight	17.2 lbs (7.8 kg)	17.2 lbs (7.8 kg)	36.0 lbs (16.2 kg)

Specifications



	FORTIDDOS 1200B	FORTIDDOS 1500E	FORTIDDOS 2000E
Hardware Specifications			
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	8
WAN Interfaces SFP+ 10 GE / SFP GE	8	8	8
LAN Interfaces LC (850 nm, 10 GE) with built-in bypass	2	—	—
WAN Interfaces LC (850 nm, 10 GE) with built-in bypass	2	—	—
LAN Interfaces QSFP+ 40 GE or QSFP28 100 GE	—	2	2
WAN Interfaces QSFP+ 40 GE or QSFP28 100 GE	—	2	2
Passive Optical Bypass	—	8 Ports (2 links) 1/10/40/100 GE 1310nm	8 Ports (2 links) 1/10/40/100 GE 1310nm
Storage	1x 480 GB SSD	1x 960 GB SSD	1x 960 GB SSD
Form Factor	2U Appliance	2U Appliance	2U Appliance
Power Supply	Dual AC Hot-Swappable	Dual AC Hot-Swappable	Dual AC Hot-Swappable
System Performance			
Maximum Inspected Throughput (Gbps)	42	45	90
Inspected Throughput (Enterprise Mix — Gbps)	36	35	70
Inspected Packet Throughput (Mpps)	45	38	77
Maximum Mitigation (Gbps/Mpps)	100 / 150	280 / 420	280 / 420
SYN Flood Mitigation (SYN In + Coookie Out) Mpps	42	27	55
Simultaneous TCP Connections (M)	6	12	25
Simultaneous Sources (M)	6	12	25
Session Setup/Teardown (kcps)	600	>1500	>3000
Latency (µs) Maximum/Typical	<50/<10	<50/<10	<50/<10
DDoS Attack Mitigation Response Time	1st packet to <2 seconds	1st packet to <2 seconds	1st packet to <2 seconds
Advanced DNS/NTP Mitigation	DNS	DNS / NTP	DNS / NTP
DNS/NTP Queries per second (M)	12 / NA	6 / 3	12 / 6
DNS/NTP Response Validation under Flood (M Responses/s)	12 / NA	6 / 3	12 / 6
Open Hybrid Cloud Mitigation Support	Yes	Yes	Yes
Environment			
Input Voltage AC	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz
Input Voltage DC	—	—	—
Power Consumption (Average)	311 W	1320 W	1320 W
Power Consumption (Maximum)	575 W	2200 W	2200 W
Maximum Current AC	110V/10.0A, 220V/5.0A	110V/12A, 220V/9A	110V/12A, 220V/9A
Maximum Current DC	—	—	—
Heat Dissipation (BTU/hr) / (kjoules/hr)	1962 / 2070	8327 / 8785	8327 / 8785
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
Compliance			
Safety Certifications	FCC Class A Part 15, UL/CB/cUL, RCM, VCCI, CE		
Dimensions			
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)	44.0 lbs (20.0 kg)	44.0 lbs (20.0 kg)

Order Information

Product	SKU	Description
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 inspected throughput. Supports 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 inspected throughput. Supports Advanced DNS Mitigation.
FortiDDoS 1000B	FDD-1000B	DDoS Protection Appliance — 8 pairs x 10 GE SFP+ or GE SFP DDoS Defense Ports, 2x GE RJ45 Management Ports, Dual AC Power Supplies. Includes 480 GB SSD storage and 2x 10 GE SR SFP+. 18 Gbps inspected throughput. Supports Advanced DNS Mitigation.
FortiDDoS 1200B	FDD-1200B	DDoS Protection Appliance — 8 pairs x 10 GE SFP+ or GE SFP DDoS Defense Ports, plus 2 pairs x 10 GE LC Ports with optical bypass, 2x GE RJ45 Management Ports, Dual AC Power Supply. Includes 480 GB SSD storage and 2x 10 GE SR SFP+. 36 Gbps inspected throughput. Supports Advanced DNS Mitigation.
FortiDDoS 1500E	FDD-1500E	DDoS Protection Appliance — 8 pairs x 10 GE SFP+ or GE SFP and 2 pairs x 40 GE QSFP+ ports plus 2-link optical bypass module (1310nm), 2x GE RJ45 Management Ports, Dual AC Power Supply. Includes 960 GB SSD storage. >35 Gbps inspected throughput. Supports Advanced DNS Mitigation.
FortiDDoS 2000E	FDD-2000E	DDoS Protection Appliance — 8 pairs x 10 GE SFP+ or GE SFP and 2 pairs x 40 GE QSFP+ or 100 GE QSFP28 ports plus 2-link optical bypass module (1310nm), 2x GE RJ45 Management Ports, Dual AC Power Supply. Includes 960 GB SSD storage. > 70 Gbps inspected throughput. Supports Advanced DNS Mitigation.

FORTIDDOS COMPATIBLE TRANSCEIVERS

SKU	Description	Wavelength	FDD-200B–FDD-800B	FDD-1000B–FDD-1200B /FDD-2000B	FDD-1500E–FDD-2000E
FG-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.	SM 1310nm	Y	Y	Y
FR-TRAN-LX	1 GE SFP LX transceiver module, -40–85°C, over SMF, for all systems with SFP and SFP/SFP+ slots.	SM 1310nm	Y	Y	Y
FR-TRAN-ZX	1 G SFP transceivers, -40–85°C operation, 90 km range for all systems with SFP slots.	SM 1550nm	Y	Y	Partial (Note 1)
FG-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.	MM 850nm	Y	Y	Partial (Note 1)
FR-TRAN-SX	1 GE SFP SX transceiver module, -40–85°C, over MMF, for all systems with SFP and SFP/SFP+ slots.	MM 850nm	Y	Y	Partial (Note 1)
FG-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.	Copper	Y	N	N
FG-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.	SM 1310nm	N	Y	Y
SP-CABLE-FS-SFP+1	10 GE SFP+ passive direct attach cable, 1 m for systems with SFP+ and SFP/SFP+ slots.	End-to-End	N	Y	Partial (Note 1)
SP-CABLE-FS-SFP+3	10 GE SFP+ passive direct attach cable, 3 m for systems with SFP+ and SFP/SFP+ slots.	End-to-End	N	Y	Partial (Note 1)
SP-CABLE-FS-SFP+5	10 GE SFP+ passive direct attach cable, 5 m for systems with SFP+ and SFP/SFP+ slots.	End-to-End	N	Y	Partial (Note 1)
SP-CABLE-FS-SFP+7	10 GE SFP+ passive direct attach cable, 7 m for systems with SFP+ and SFP/SFP+ slots.	End-to-End	N	Y	Partial (Note 1)
SP-CABLE-ADASFP+	10 GE SFP+ active direct attach cable, 10 m/32.8 ft for all systems with SFP+ and SFP/SFP+ slots.	End-to-End	N	Y	Partial (Note 1)
FG-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.	MM 850nm	N	Y	Partial (Note 1)
FS-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.	MM 850nm	N	Y	Partial (Note 1)
FS-TRAN-SFP+ER	10Gbase-ER SFP+ transceivers for FortiSwitch and FortiGate, 1550nm. Single Mode. 40 km range for systems with SFP+ slots.	SM 1550nm	N	Y	Partial (Note 1)
FG-TRAN-QSFP+LR	40 GE QSFP+ transceivers, long range for all systems with QSFP+ slots.	SM 1310nm	N	N	Y
FG-TRAN-QSFP+SR	40 GE QSFP+ transceivers, short range for all systems with QSFP+ slots.	MM 850nm	N	N	Partial (Note 1)
FG-TRAN-QSFP+SR-BIDI	40 GE QSFP+ transceiver, short range BiDi for systems with QSFP+ slots.	MM 850nm	N	N	Partial (Note 1)
SP-CABLE-FS-QSFP+1	40 GE QSFP+ passive direct attach cable, 1 m for systems with QSFP+ slots.	End-to-End	N	N	Partial (Note 1)
SP-CABLE-FS-QSFP+3	40 GE QSFP+ passive direct attach cable, 3 m for systems with QSFP+ slots.	End-to-End	N	N	Partial (Note 1)
SP-CABLE-FS-QSFP+5	40 GE QSFP+ passive direct attach cable, 5 m for systems with QSFP+ slots.	End-to-End	N	N	Partial (Note 1)
FG-TRAN-QSFP28-LR4	100 GE QSFP28 transceivers, long range for all systems with QSFP28 slots.	SM 1310nm	N	N	Y
FG-TRAN-QSFP28-SR4	100 GE QSFP28 transceivers, 4 channel parallel fiber, short range for all systems with QSFP28 slots.	MM 850nm	N	N	Partial (Note 1)

Note 1: Can be used in E-Series pluggable optical ports. NOT compatible with E-Series optical bypass module.

OPTIONAL ACCESSORY

Product	SKU	Description
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 and FDD-800B. Not supported for: FG-200D-POE/240D-POE.

www.fortinet.com