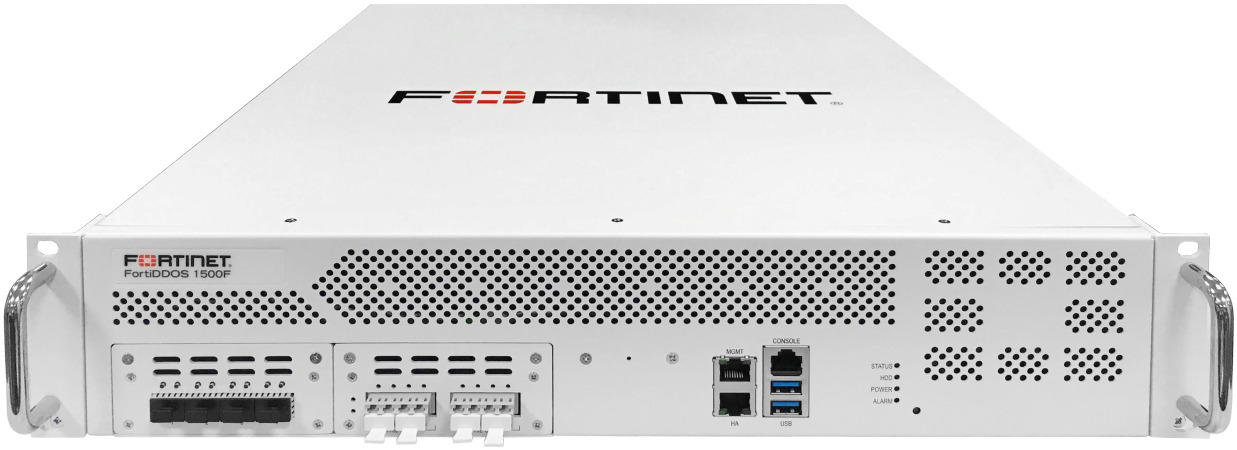
FortiDDoS



Highlights

100% packet inspection for Layer 3, 4, and 7 DDoS attack identification and mitigation, simultaneously monitoring 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 and NTP DDoS mitigation plus advanced DTLS and QUIC mitigation on F-Series

Hybrid On-premise/Cloud mitigation available with Open Attack Signaling

AI/ML Security and Deep Visibility

Distributed Denial of Service (DDoS) attacks remain a top threat to network 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, ISP link subnets, or Firewall/Proxy/WiFi Gateway public IP addresses.

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 is DDoSed?

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 create large, anonymous attacks for a few dollars.

DDoS is not an everyday occurrence for security teams and they cannot be expected to understand the thousands of attack variants that target your network.

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

Available in

Appliance

Virtual

A Different and Better Approach to DDoS Attack Mitigation

FortiDDoS massively parallel machine-learning architecture delivers the fastest and most accurate DDoS attack mitigation available.

In place of pre-defined or subscription-based signatures to identify some attack patterns, FortiDDoS uses autonomous machine learning to build an adaptive baseline of normal activity from hundreds-of-thousands of parameters and then monitors traffic patterns against those baselines. Should an attack begin, FortiDDoS sees the deviation and immediately takes action to mitigate it, often from the first packet.

FortiDDoS monitors, responds, and reports on the mitigations it has performed, not attacks where your team or the vendor ERT/NoC must intervene.

Highlights

Powerful Parallel Architecture = 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 architecture samples 100% of even the smallest packets, for over 200,000 parameters for each Protection Profile. This method allows FortiDDoS to operate completely autonomously, finding some attacks on the FIRST packet and all attacks within one second—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 Resurgence 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 routers, firewalls, and many DDoS appliances, preventing full inspection with unexpected results. FortiDDoS' 100% inspected small-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. Its Legitimate Query and DNS Allowlist features uniquely prevent your Authoritative DNS servers from becoming reflective attackers.

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 FortiOS Security Fabric Dashboards, 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 monitors only a few different attack types. Because of that, mitigations can be overly-broad, blocking all UDP traffic when an unmonitored UDP Reflection port is attacking, for example. With Google services and all conferencing services like Zoom and Teams using UDP, this situation is not conducive to business continuity.

FortiDDoS mitigates more than 150 attack events, many with depth. For example, FortiDDoS monitors more than 10 000 possible UDP Reflection ports, blocking the attacking port, not all UDP.

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 two seconds and its massively-parallel detection and mitigation ensures multi-vector, sequential and pulsed attacks are seen and stopped with no user intervention.

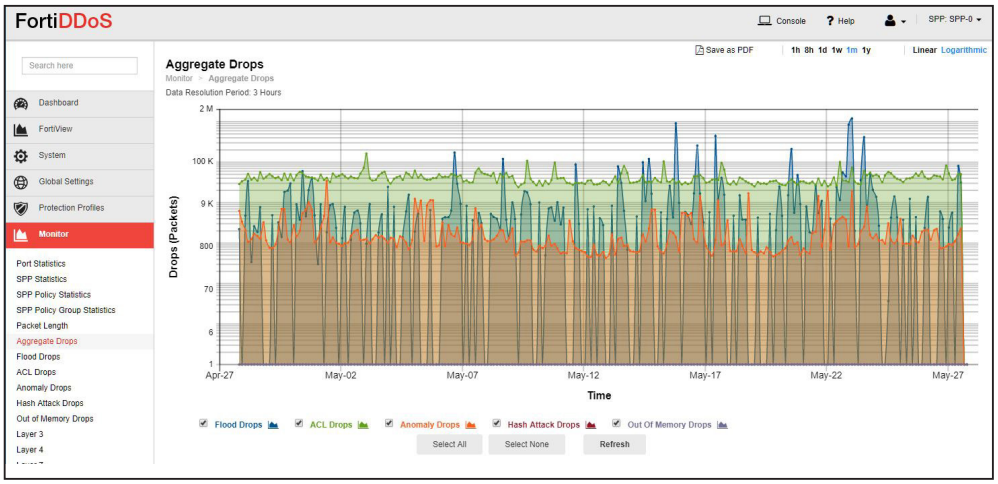
All FortiDDoS models offer High Availability and all models offer Optical Bypass (to 100 GE) to ensure network continuity in the event of system failures.

Features

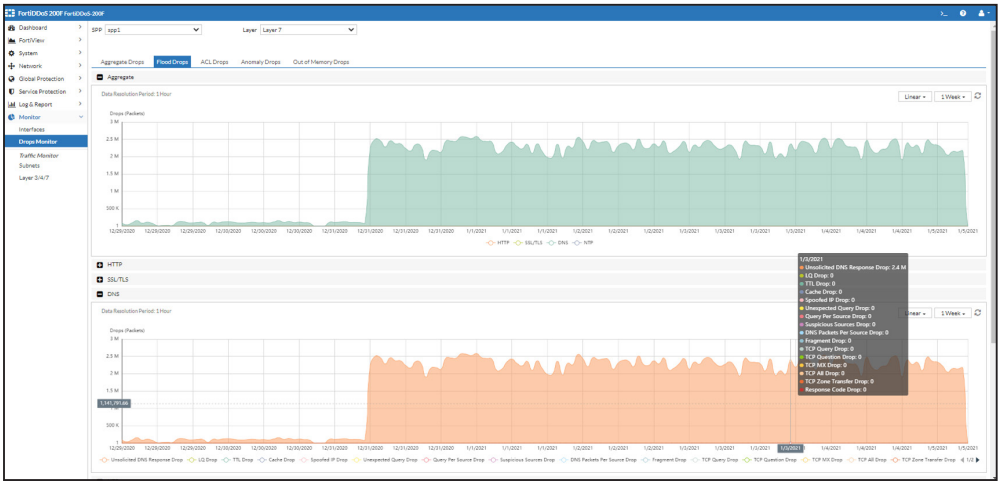
100% Machine Learning Detection	FortiDDoS doesn't rely on signature files that need to be updated with the latest threats so you're protected from both known and unknown "zero-day" attacks. No "threat-protection" subscriptions required. Saves OPEX.
Massively Parallel Architecture	Parallel architecture provides 100% packet inspection with bidirectional detection and mitigation of Layer 3, 4, and 7 DDoS attacks even at the smallest packets sizes. 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 Query and Response traffic up to 12 million QPS, for protection from a broad range of DNS-based volumetric, application, and anomaly attacks, including attacks relayed through public multicast DNS services. DNS Reflection floods are stopped from the FIRST packet.
Advanced NTP Protection	FortiDDoS provides 100% inspection of all NTP Query and Response traffic up to 6 million QPS. NTP Reflection floods are stopped from the FIRST packet.
Advanced DTLS, QUIC, and Zoom™ Protection	FortiDDoS inspects DTLS, QUIC, and Zoom™ for anomalies, reflections, and over-threshold data rates.
Continuous Learning	With continuous background learning and 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.
RESTful API	FortiDDoS can be integrated into almost any environment through its RESTful API.

Reporting

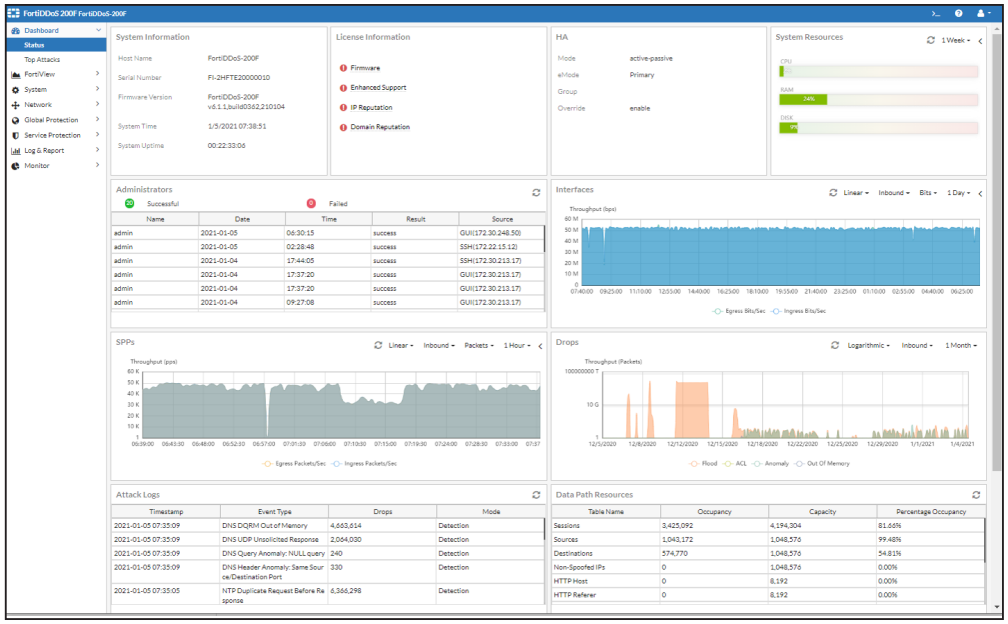
Aggregate Drops L3-L7 (E)



DNS Attacks (F)



Dashboard (F)



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 Monitoring to instantly mitigate DNS Reflected attacks
- NTP Monitoring to instantly mitigate NTP reflection attacks
- DTSL and QUIC Monitoring to instantly mitigate reflection attacks (F)
- Complete invisibility with no MAC nor IP addresses in the data path
- Massively parallel processing for multiple simultaneous attack vectors

Behavioral Threshold

- 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
- NTP Header and Payload
- DTLS and QUIC header and state (F)

Layer 3 Attack Mitigation

- Protocol Floods (all 256 monitored)
- Fragment Floods (TCP/UDP/Other Protocols)
- Source Floods (up to 24M 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 Reflection Ports (>10,000)
- ICMP Type/Codes (all 65k)
- SYN, SYN/Destination with Source IP validation, SYN/Source (all three monitored for all 65k TCP ports)
- **First-packet** TCP Flag (invalid and out-of-state) flood mitigation

HTTP Attack Mitigation

- HTTP URL, Referer, Cookie, Host, User Agent
- HTTP METHOD Floods (all 8 METHODS +Total Methods/Source)
- SSL Renegotiation
- L7 Aggressive Aging
- Protocol Anomalies (F)
- Cypher Anomalies (F)
- GET/POST Client Validation (F)

Other Attack Mitigation

- **First-packet** DNS, NTP, DTLS (F), and QUIC (F) Response Flood Mitigation
- DNS, NTP, DTLS (F), and QUIC (F) Header, payload, and 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 FQDN validation
- DNS FQDN and Regex Allowlist/Blocklist, and Resource Record Blocklist (F)
- DNS Domain Reputation Subscription

* Note: Not all features are supported by all platforms. Features that are not universal will show the platform letter designation, e.g. E/F for E-Series, or F-Series.

FortiDDoS Features*

Access Control Lists

While ACLs are not very effective against current DDoS attacks using spoofed or widely-dispersed reflectors, they can be used to offload other infrastructure.

Most ACLs can be applied Globaly or per Protection Policy.

- IP Reputation – Subscription FortiGuard subset with known DDoS, Anomynous Proxies, Phishing, Spam, and/or Tor IPs per Protection Policy. Not required for DDoS mitigation
- IP/subnet Blocklist/ Allowlist
- Bulk IPv4 Blocklist Customer Upload (>1million addresses)
- IPv4 and/or IPv6 Geolocation per Protection Policy
- Enhanced BCP38 Source Address Validation/Local Address Anti-Spoofing (>2000 subnets) (E)
- Protocol, UDP, TCP, and other Protocol Fragments, DNS Fragment, L4 Port, ICMP Type/Code
- HTTP Methods, URLs, Hosts, Referrers, User Agents
- Domain Reputation – Subscription FortiGuard subset with known Malicious, Botnet, Bitcoin Mining, and/or possible DNS Tunneling Domains - per Protection Policy. Not required for DDoS mitigation
- DNS Bulk Domain Blocklist Customer Upload (up to one million Domains)
- DNS Resource Record ACLs (256 RRs) (F)
- DNS FQDN Allow/Blocklist (F)
- DNS FQDN Regex Allow/Blocklist (F)
- IPv4/IPv6: Layer 3 Protocols, TCP/UDP Port, ICMP Type-Code, TCP/UDP/Other fragment ACL
- Flowspec ACL script generation

Management

- Full TLS 1.3 Management Logging, Graphing and Reporting GUI
- Full CLI
- Open RESTful API
- RADIUS, LDAP, and TACACS+ Authentication including 2FA and Proxy
- Open Cloud Mitigation Signaling

Comprehensive Reporting

- Filterable/Exportable Attack Log
- Summary 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
- Custom, on-demand, on-schedule and/or on-Attack-Threshold reports in multiple formats
- Millions of built-in graphs with directionality and five-minute to one-year views of traffic and drop activity 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

Audit Trails

- Login Audit Trail
- Configuration Audit Trail

* Note: Not all features are supported by all platforms. Features that are not universal will show the platform letter designation, e.g. B/E/F for B-Series, E-Series, or F-Series.

Specifications

	FortiDDoS 200F	FortiDDoS 1500F / 1500F-LR	FortiDDoS 2000F
Hardware Specifications			
LAN Interfaces Copper GE with built-in bypass	4	—	—
WAN Interfaces Copper GE with built-in bypass	4	—	—
LAN Interfaces SFP GE	2	—	—
WAN interfaces SFP GE	2	—	—
LAN interfaces LC (850 nm, GE) with built-in bypass	2	—	—
WAN interfaces LC (850 nm, GE) with built-in bypass	2	—	—
LAN Interfaces SFP+ 10 GE / SFP GE	—	2	2 (10GE ONLY) See Bypass requirements below
WAN Interfaces SFP+ 10 GE / SFP GE	—	2	2 (10GE ONLY) See Bypass requirements below
LAN Interfaces 10 GE LC with built-in bypass	—	1500F - 2 (850nm) 1500F-LR - 2 (1310nm / 1550nm)	—
WAN Interfaces 10 GE LC with built-in bypass	—	1500F - 2 (850nm) 1500F-LR - 2 (1310nm / 1550nm)	—
LAN Interfaces QSFP+ 40 GE or QSFP28 100 GE	—	—	2 (40GE ONLY - LC 1310nm / 1550nm)
WAN Interfaces QSFP+ 40 GE or QSFP28 100 GE	—	—	2 (40GE ONLY - LC 1310nm / 1550nm)
Passive Optical Bypass	—	—	8 Ports (2 links) 10/40 GE 1310nm / 1550nm
Storage	1× 480 GB SSD	1× 480 GB SSD	1× 960 GB SSD
Form Factor	1RU Appliance	2RU Appliance	2RU Appliance
Dual Power Supply, redundant, hot swappable	AC	AC	AC
System Performance			
Maximum Inspected Throughput (Gbps)	8	22	39
Inspected Packet Throughput (Mpps)	9	27	52
Maximum Mitigation (Gbps/Mpps)	8/9	22/27	39/52
SYN Flood Mitigation (SYN In + Cookie Out) Mpps	5.3	19	40
Simultaneous TCP Connections (M)	4	16	32
Simultaneous Sources (M)	1	4	8
Session Setup/Teardown (kcps)	375	875	1711
Latency (µs) Maximum/Typical	<70	<70	<70
DDoS Attack Mitigation Response Time	First packet to <1 second	First packet to <1 second	First packet to <2 seconds
Advanced DNS/NTP/DTLS/QUIC Mitigation	DNS/NTP/DTLS/QUIC	DNS/NTP/DTLS/QUIC	DNS/NTP/DTLS/QUIC
DNS/NTP Queries per second (M)	2 / 1	8 / 4	8/4
DNS/NTP Response Validation under Flood (M Responses/s)	2 / 1	8 / 4	8/4
Open Hybrid Cloud Mitigation Support	Yes	Yes	Yes
Central Manager	No	No	No
Environment			
Input Voltage	100-240V AC, 50-60Hz	100-240V AC, 50-60Hz	100-240V AC, 50-60Hz
Power Consumption (Average /Maximum)	117 W / 152 W	333 W / 433 W	333 W / 433 W
Maximum Current (AC unless noted)	100V/1.5A, 240V / 0.7A	100V/4.4A, 240V/1.9A	100V/4.4A, 240V/1.9A
Heat Dissipation (BTU/hr) / (kjoules/hr)	519 / 574	1477 / 1558	1477 / 1558
Operating Temperature	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)
Storage Temperature	-4°-158°F (-20°-70°C)	-4°-158°F (-20°-70°C)	-4°-158°F (-20°-70°C)
Airflow	Front to Back	Front to Back	Front to Back
Humidity	5%–90% non-condensing	5%–90% non-condensing	5%–90% non-condensing
Compliance			
Safety Certifications	FCC Class A Part 15, UL/CB/cUL, RCM, VCCI, CE		
Dimensions			
Height x Width x Length (inches)	1RU 1.77 × 17 × 21.7	2RU 3.5 × 17.24 × 22.83	2RU 3.5 × 17.24 × 22.83
Height x Width x Length (mm)	44 × 438 × 550	88 × 438 × 580	88 × 444 × 580
Weight (lbs / kg)	21.2 lbs (9.6 kg)	43.6 lb (19.8 kg)	19.8 lbs (9.0 kg)

Specifications

	FortiDDoS 3000F	FortiDDoS 1500E	FortiDDoS 2000E / 2000E-DC
Hardware Specifications			
LAN Interfaces Copper GE w/built-in bypass	—	—	—
WAN Interfaces Copper GE w/built-in bypass	—	—	—
LAN Interfaces SFP GE	—	—	—
WAN interfaces SFP GE	—	—	—
LAN Interfaces SFP+ 10 GE / SFP GE	2 (10GE ONLY) See Bypass requirements below	8 See Bypass requirements below	8 See Bypass requirements below
WAN Interfaces SFP+ 10 GE / SFP GE	2 (10GE ONLY) See Bypass requirements below	8 See Bypass requirements below	8 See Bypass requirements below
LAN Interfaces 10 GE LC with built-in bypass	—	—	—
WAN Interfaces 10 GE LC with built-in bypass	—	—	—
LAN Interfaces QSFP+ 40 GE or QSFP28 100 GE	2 See Bypass requirements below	2 See Bypass requirements below	2 See Bypass requirements below
WAN Interfaces QSFP+ 40 GE or QSFP28 100 GE	2 See Bypass requirements below	2 See Bypass requirements below	2 See Bypass requirements below
Passive Optical Bypass	8 Ports (2 links) 10/40/100 GE 1310nm / 1550nm	8 Ports (2 links) 1/10/40/100 GE 1310nm / 1550nm	8 Ports (2 links) 1/10/40/100 GE 1310nm / 1550nm
Storage	1× 1.92 TB SSD	1× 960 GB SSD	1× 960 GB SSD
Form Factor	2U Appliance	2U Appliance	2U Appliance
Dual Power Supply, redundant, hot-swappable	AC	AC	AC / DC
System Performance			
Maximum Inspected Throughput (Gbps)	65	45	90
Inspected Packet Throughput (Mpps)	80	38	77
Maximum Mitigation (Gbps/Mpps)	65/80	280/350	280/350
SYN Flood Mitigation (SYN In + Cookie Out) Mpps	55	27	55
Simultaneous TCP Connections (M)	64	12	25
Simultaneous Sources (M)	16	12	25
Session Setup/Teardown (kcps)	2280	>1500	>3000
Latency (µs) Maximum/Typical	<70	<50/<10	<50/<10
DDoS Attack Mitigation Response Time		First packet to <2 seconds	First packet to <2 seconds
Advanced DNS/NTP/DTLS/QUIC Mitigation	DNS/NTP/DTLS/QUIC	DNS/NTP	DNS/NTP
DNS/NTP Queries per second (M)	16/8	4/3	7/6
DNS/NTP Response Validation under Flood (M Responses/s)	16/8	4/3	7/6
Open Hybrid Cloud Mitigation Support	Yes	Yes	Yes
Central Manager	No	Yes	Yes
Environment			
Input Voltage	100-240V AC, 50-60Hz	100-240V AC, 50-60Hz	100-240V AC, 50-60Hz 40-72V DC
Power Consumption (Average W / Maximum W)	400/1460	314 / 580	314 / 580
Maximum Current (AC unless noted)	127V/11A, 240V/6.1A	110V/5.3A, 220V/2.6A	110V/5.3A, 220V/2.6A 48VDC / 12A
Heat Dissipation (BTU/hr) / (kjoules/hr)	4965 / 5238	2151 / 2269	2151 / 2269
Operating Temperature	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)
Storage Temperature	-4°-167°F (-20°-75°C)	-13°–158°F (-25°–70°C)	-13°–158°F (-25°–70°C)
Airflow	Front to Back	Front to Back	Front to Back
Humidity	5%–90% non-condensing	20%–90% non-condensing	20%–90% non-condensing
Compliance			
Safety Certifications		FCC Class A Part 15, UL/CB/cUL, RCM, VCCI, CE	
Dimensions			
Height x Width x Length (inches)	2RU 3.5× 17.24 × 22.83	2RU 3.5 × 17.24 × 22.05	2RU 3.5 × 17.24 × 22.05
Height x Width x Length (mm)	88 × 438 × 580	88× 438 × 560	88× 438 × 560
Weight (lbs / kg)	75 lbs (34 kg)	44.0 lbs (20.0 kg)	44.0 lbs (20.0 kg)

Specifications

	FortiDDoS-VM04	FortiDDoS-VM08	FortiDDoS-VM16
Specifications			
Hypervisor Support	VMware ESX/ESXi from 6.x / 7.x with hardware-assisted virtualization (VT) enabled in the BIOS KVM from libvirt 6.0.0		
Throughput1	3 Gbps	5 Gbps	10 Gbps
Mitigation2,3	3 Gbps / 4 Mpps	5 Gbps / 6 Mpps	10 Gbps / 10 Mpps
Service Protection Profiles	4	8	16
vCPU Support	4	8	16
Network Interface Support	8 (4 bridged port-pairs - promiscuous mode). Interface speeds dependent on hardware.		
Management Interfaces	2	2	2
Electric/Optical Bypass	Function of the underlying NICs and not controllable from FortiDDoS		
Memory Requirements	16 GB	16 GB	32 GB
Storage Requirements	Requires at least 200 GB		

[1] 1.7KB HTTP Response

[2] Rate for 100% inspection of 64 Byte packets

[3] Actual peformance will vary depending on underlying hardware. Performance results were observed using a bare-metal appliance with Intel(R) Xeon(R) W-3245 CPU @ 3.20GHz running VMware ESXI 7.0.0. Note: Using SR-IOV NICs in VM environments is challenging but will improve performance from that stated above.

NOTE: FortiDDoS VMs are not suitable for deployment in cloud service environments such as AWS, Azure, or Google Cloud. By design, FortiDDoS VMs (and appliances) have no IP addresses on the data ports and thus cannot be addressed in cloud environments. There is no way to direct traffic to them. VMs (and appliances) must be attached to physical links.

Order Information

Product	SKU	Description
FortiDDoS 200F	FDD-200F	DDoS Protection Appliance — 8 port-pairs DDoS Defence Ports, including 4 pairs x GE RJ45 with integral bypass protection, 2 pairs x GE LC SR MM 850nm with integral optical bypass protection, 2 pairs GE SFP (no bypass protection), 2x GE RJ45 Management Ports, dual redundant AC power supplies. Includes 480 GB SSD storage. 8 Gbps / 9 Mpps inspected Mitigation. Supports Advanced DNS and NTP, DTLS, QUIC DDoS attack Mitigation.
FortiDDoS 1500F	FDD-1500F	DDoS Protection Appliance — 4 port-pairs DDoS Defence Ports, including 2 pairs x 10 GE SFP+ (or GE SFP) (no bypass protection) and 2 pairs x 10 GE LC SR MM (850nm) ports with integral optical bypass protection, 2x GE RJ45 Management Ports, dual redundant AC power supplies. Includes 480GB SSD storage. 22 Gbps / 27Mpps inspected Mitigation. Supports Advanced DNS and NTP, DTLS, QUIC DDoS attack Mitigation.
FortiDDoS 1500F-LR	FDD-1500F-LR	DDoS Protection Appliance — 4 port-pairs DDoS Defence Ports, including 2 pairs x 10 GE SFP+ (or GE SFP) (no bypass protection) and 2 pairs x 10 GE LC LR SM 1310nm ports with integral optical bypass protection, 2x GE RJ45 Management Ports, dual redundant AC power supplies. Includes 480GB SSD storage. 22 Gbps / 27 Mpps inspected Mitigation. Supports Advanced DNS and NTP, DTLS, QUIC DDoS attack Mitigation.
FortiDDoS 2000F	FDD-2000F	DDoS Protection Appliance — 4 port-pairs DDoS Defence Ports, including 2 pairs x 10GE SFP+, 2 pairs 40GE QSFP+, with 2-link optical bypass module used with SM DR/LR/ER/ZR (1310 /1550nm) transceivers, 2x GE RJ45 Management Ports, dual redundant AC Power Supply. Includes 960GB SSD storage. 39 Gbps / 52 Mpps inspected Mitigation. Supports Advanced DNS and NTP, DTLS, QUIC DDoS attack Mitigation.
FortiDDoS 3000F	FDD-3000F	DDoS Protection Appliance — 4 port-pairs DDoS Defence Ports, including 2 pairs 100GE QSFP28 or 40 GE QSFP+, and 2 pairs x 10GE SFP+, with 2-link optical bypass module used with SM DR/LR/ER/ZR (1310 /1550nm) transceivers, 2x GE RJ45 Management Ports, dual redundant AC Power Supply. Includes 1.2TB SSD storage. 65 Gbps / 80 Mpps inspected Mitigation. Supports advanced DNS, NTP, DTLS, and QUIC DDoS mitigation.
FortiDDoS 1500E	FDD-1500E	DDoS Protection Appliance — 10 port-pairs DDoS Defence Ports, including 8 pairs x 10 GE SFP+ or GE SFP and 2 pairs x 40 GE QSFP+ or 100 GE QSFP28, with 2-link optical bypass module used with SM DR/LR/ER/ZR (1310/15550nm) transceivers, 2x GE RJ45 Management Ports, dual redundant AC Power Supply. Includes 960 GB SSD storage. 40 Gbps / 38 Mpps inspected Mitigation (280 Gbps Max Mitigation). Supports Advanced DNS and NTP DDoS attack mitigation.
FortiDDoS 2000E	FDD-2000E	DDoS Protection Appliance — 10 port-pairs DDoS Defence Ports, including 8 pairs x 10 GE SFP+ or GE SFP and 2 pairs x 40 GE QSFP+ or 100 GE QSFP28, with 2-link optical bypass module used with SM DR/LR/ER/ZR (1310/15550nm) transceivers, 2x GE RJ45 Management Ports, dual redundant AC Power Supply. Includes 960 GB SSD storage. 80 Gbps / 75 Mpps inspected Mitigation (280 Gbps Max Mitigation). Supports Advanced DNS and NTP DDoS attack mitigation.
FortiDDoS 2000E-DC	FDD-2000E-DC	DDoS Protection Appliance — 10 port-pairs DDoS Defence Ports, including 8 pairs x 10 GE SFP+ or GE SFP and 2 pairs x 40 GE QSFP+ or 100 GE QSFP28, with 2-link optical bypass module used with SM DR/LR/ER/ZR (1310/15550nm) transceivers, 2x GE RJ45 Management Ports, dual redundant DC Power Supply. Includes 960 GB SSD storage. 80 Gbps / 75 Mpps inspected Mitigation (280 Gbps Max Mitigation). Supports Advanced DNS and NTP DDoS attack mitigation.
Virtual Machine	**SKU**	**Description**
FortiDDoS-VM04	FDD-VM04	DDoS Protection System - virtual appliance for all supported platforms. Supports up to 4 x vCPU cores, 8 x NIC Ports, 2 x MGMT Ports.
FortiDDoS-VM08	FDD-VM08	DDoS Protection System - virtual appliance for all supported platforms. Supports up to 8 x vCPU cores, 8 x NIC Ports, 2 x MGMT Ports.
FortiDDoS-VM16	FDD-VM016	DDoS Protection System - virtual appliance for all supported platforms. Supports up to 16 x vCPU cores, 8 x NIC Ports, 2 x MGMT Ports.

NOTE: FortiDDoS VMs are not suitable for deployment in cloud service environments such as AWS, Azure or Google Cloud. By design, FortiDDoS VMs (and appliances) have no IP addresses on the data ports and thus cannot be addressed in cloud environments. There is no way to direct traffic to them. VMs (and appliances) must be attached to physical links.

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

Order / Compatibility Information

SKU	Description	Fiber Mode/ Wavelength (nm)	200F Ports/Bypass	1500F/ 1500F-LR Ports/Bypass	2000F 3000F Ports/Bypass	1500E 2000E / 2000E-DC Ports/Bypass
1 GE						
FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.	Copper	Y / N	Y / N	N / N	Y / N
FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.	MM 850	Y / N	Y / N	N / N	Y / N
FR-TRAN-SX	1 GE SFP SX transceiver module, -40°–85°C, over MMF, for all systems with SFP and SFP/SFP+ slots.	MM 850	Y / N	Y / N	N / N	Y / N
FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.	SM 1310	Y / N	Y / N	N / N	Y / Y
FR-TRAN-ZX	1 GE SFP transceivers, -40°–85°C operation, 90 km range for all systems with SFP slots.	SM 1550	Y / N	Y / N	N / N	Y / Y
10 GE						
FN-CABLE-SFP+1	10 GE SFP+ passive direct attach cable, 1m for systems with SFP+ and SFP/SFP+ slots.	End-to-End	N	Y / N	Y / N	Y / N
FN-CABLE-SFP+3	10 GE SFP+ passive direct attach cable, 3m for systems with SFP+ and SFP/SFP+ slots.	End-to-End	N	Y / N	Y / N	Y / N
FN-CABLE-SFP+5	10 GE SFP+ passive direct attach cable, 5m for systems with SFP+ and SFP/SFP+ slots.	End-to-End	N	Y / N	Y / N	Y / N
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 / N	Y / N	Y / N
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 / N	Y / N	Y / N
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 / N	Y / N	Y / N
FN-TRAN-SFP+GC	10 GE copper SFP+ RJ45 Fortinet Transceiver (30m range) for systems with SFP+ slots.	Copper	N	Y / N	Y / N	Y / N
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 / N	Y / N	Y / N
FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.	MM 850	N	Y / N	Y / N	Y / N
FN-TRAN-SFP+BD27	10 GE SFP+ transceiver module, 30KM long range.	SM BiDi	N	Y / N	Y / N	Y / N
FN-TRAN-SFP+BD33	10 GE SFP+ transceiver module, 30KM long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD27, ordered separately).	SM BiDi	N	Y / N	Y / N	Y / N
FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.	SM 1310	N	Y /N	Y / Y	Y / Y
FN-TRAN-SFP+ER	10 GE base-ER SFP+ transceiver module, 1550nm Single Mode, 40km range for systems with SFP+ Slots.	SM 1550	N	Y /N	Y / Y	Y / Y
FN-TRAN-SFP+ZR	10 GE SFP+ transceiver module, 80KM extreme long range for systems with SFP+ and SFP/SFP+ slots.	SM 1550	N	Y / N	Y / Y	Y / Y

Note: If a transceiver does not appear on this list it is incompatible with all Models/Platforms

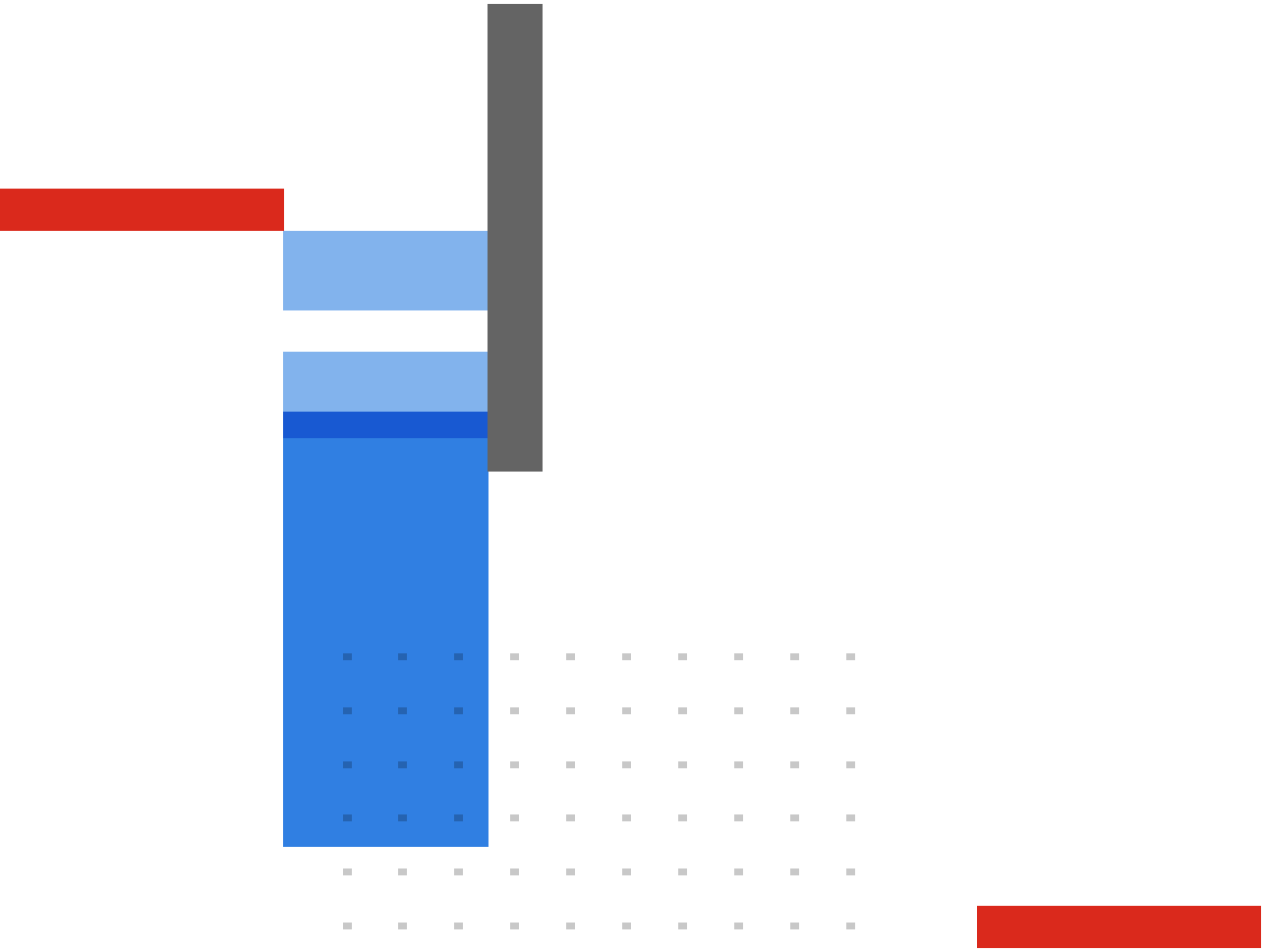
Order / Compatibility Information

SKU	Description	Fiber Mode/ Wavelength (nm)	200F Ports/Bypass	1500F/ 1500F-LR Ports/Bypass	2000F 3000F Ports/Bypass	1500E 2000E / 2000E-DC Ports/Bypass
40 GE						
FN-CABLE-QSFP+1	40 GE QSFP+ passive direct attach cable, 1m for systems with QSFP+/ QSFP28 slots.	End-to-end	N	N	Y / N	Y / N
FN-CABLE-QSFP+3	40 GE QSFP+ passive direct attach cable, 3m for systems with QSFP+/ QSFP28 slots.	End-to-end	N	N	Y / N	Y / N
FN-CABLE-QSFP+5	40 GE QSFP+ passive direct attach cable, 5m for systems with QSFP+/ QSFP28 slots.	End-to-end	N	N	Y / N	Y / N
SP-CABLE-FS-QSFP+1	40 GE QSFP+ passive direct attach cable, 1 m for systems with QSFP+ slots.	End-to-End	N	N	Y / N	Y / N
SP-CABLE-FS-QSFP+3	40 GE QSFP+ passive direct attach cable, 3 m for systems with QSFP+ slots.	End-to-End	N	N	Y / N	Y / N
SP-CABLE-FS-QSFP+5	40 GE QSFP+ passive direct attach cable, 5 m for systems with QSFP+ slots.	End-to-End	N	N	Y / N	Y / N
FG-TRAN-QSFP+SR-BIDI	40 GE QSFP+ transceiver, short range BiDi for systems with QSFP+ slots.	MM 850	N	N	Y / N	Y / N
FN-TRAN-QSFP+SR	40 GE QSFP+ transceivers, short range for all systems with QSFP+ slots.	MM 850	N	N	Y / N	Y / N
FN-TRAN-QSFP+LR	40 GE QSFP+ transceivers, long range for all systems with QSFP+ slots.	SM 1310	N	N	Y / Y	Y / Y
FN-TRAN-QSFP+ER	40 GE QSFP+ transceiver module, 40km extended range for systems with QSFP+/QSFP28 slots.	SM 1550	N	N	Y / Y	Y / Y
100 GE						
FN-CABLE-QSFP28-1	100 GE QSFP28 Passive Direct Attach Cable, 1 m for Systems with QSFP28 slots.	End-to-End	N	N	Y / N	Y / N
FN-CABLE-QSFP28-2	100 GE QSFP28 Passive Direct Attach Cable, 2 m for Systems with QSFP28 slots.	End-to-End	N	N	Y / N	Y / N
FN-CABLE-QSFP28-3	100 GE QSFP28 Passive Direct Attach Cable, 3 m for Systems with QSFP28 slots.	End-to-End	N	N	Y / N	Y / N
FN-CABLE-QSFP28-5	100 GE QSFP28 Passive Direct Attach Cable, 5 m for Systems with QSFP28 slots.	End-to-End	N	N	Y / N	Y / N
FN-TRAN-QSFP28-SR	100 GE QSFP28 transceivers, 4 channel parallel fiber, short range for all systems with QSFP28 slots.	MM 850	N	N	Y / N	Y / N
FN-TRAN-QSFP28-BIDI-I	100 GE QSFP28 BIDI transceiver module, short range, for systems with QSFP28 slots.	BiDi	N	N	Y / N	Y / N
FN-TRAN-QSFP28-DR	100 GE QSFP28 transceiver module, single channel single-mode fiber, 100GBase-DR for systems with QSFP28 slots.	SM 1310 500M	N	N	Y / Y	Y / Y
FN-TRAN-QSFP28-CWDM4	100 GE QSFP28 transceivers, LC connectors, 2KM for all systems with QSFP28 Slots.	SM CWDM ~1310	N	N	Y / Y	Y / Y
FN-TRAN-QSFP28-LR	100 GE QSFP28 transceivers, long range for all systems with QSFP28 slots.	SM 1310	N	N	Y / Y	Y / Y
FN-TRAN-QSFP28-ER	100 GE QSFP28 transceivers, extended long range 20KM for all systems with QSFP28 Slots.	SM 1550	N	N	Y / Y	Y / Y

Note: If a transceiver does not appear on this list it is incompatible with all Models/Platforms

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

November 14, 2024

FDDoS-DAT-R46-20241114