ORDERING GUIDE

FortiDDoS

Available in

Appliance Virtual Hybrid

FortiDDoS is an advanced inline DDoS mitigation system that ensures network, resource, and application availability and security, protecting from known and zero-day Layer 3 to Layer 7 DDoS attacks.

FortiDDoS's massively parallel architecture delivers the most advanced and lowest-latency DDoS attack mitigation on the market today without the packet-rate performance compromises of other vendors.

FortiDDoS's 100% packet inspection for more than 200 000 parameters, inbound and outbound, at the highest packet rates, results in the fastest and most accurate detection and mitigation in the industry with extensive forensics visibility.

In place of predefined or subscription-based signatures to identify 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 with no operator intervention.

FortiDDoS uses unmatched "state awareness" of TCP, DNS, NTP (E/F-Series); plus DTLS and QUIC (F-Series) to stop the most frequent and largest attack types (DNS and NTP reflection floods and SYN-ACK floods) from the first packet, while competitive options are forced to create overly broad "signatures" after many seconds or minutes.

You can deploy FortiDDoS as a physical or virtual machine (VM):

- Inline on-premise appliance (E-/F-Series)
- Inline on-premise VM on bare-metal servers (F-Series only)
- Hybrid on-premise/Cloud DDoS mitigation through our Cloud DDoS partners (E-/F-Series)

Major customer verticals include:

- Enterprise
- Education
- Government
- Hosting providers
- MSSPs/smaller ISPs who can use inline and do not require DDoS resale/multitenancy

PRODUCT OFFERINGS

	DPDK/TP3 ACCELERATED DEVICES AND VIRTUAL MACHINES								
	VM04	VM08	VM16	200F	1500F 1500F-LR	2000F	3000F	1500E	2000E 2000E-DC
Recommended Connectivity for Enterprise Datacenter Environments									
GE or 2xGE BGP	✓	✓	✓	✓					
2-4x GE LACP		✓ (2x GE)	✓	✓					
10GE or 2× 10GE BGP Capped at 4-5Gbps		✓	✓		✓				
10GE or 2× 10GE BGP			✓		✓	✓	✓	✓	✓
2×10GE LACP					✓	✓	✓	✓	✓
2×10GE + 2×10GE BGP						✓	✓	✓	✓
4×10GE LACP								✓	✓
40GE or 2×40GE BGP						✓	✓	✓	✓
100GE or 2× 100GE BGP							✓		✓
Performance									
Enterprise Inspected Throughput (Gbps)	3	5	10	8	22	39	65	45	90
Small UDP Inspected Throughput (Mpps)	4	6	10	9	27	52	80	38	77
SYN Validation Throughput (Mpps)	2.6	5	5	5.3	19	40	55	27	55
Other Capacities									
Max Service Protection Profiles (SPP)	4	8	16	8	16	16	16	8	8
Max Protected Subnets	512 per SPP	512 per SPP	512 per SPP	512 per SPP	1024 per SPP	1024 per SPP	1024 per SPP	> 2 000 per System	> 2 000 per System
Dual Power Supplies				AC	AC	AC	AC	AC	AC/DC
Form Factor				1 RU	2 RU	2 RU	2RU	2 RU	2 RU
Interfaces									
10/100/1000 Mbps	**Maximum 8 ports with native data rates based on the Recommended Connectivity above.**			8					
GE SFP				4					
GE LC SR with Optical Bypass				4					
10GE SFP+					4	4	4	16	16
10GE LC SR with Optical Bypass					4				
40GE QSFP+						4	4	4	4
100GE QSFP28									
Optical Bypass for 10GE/40GE LC 1310/1550nm						4			
Optical Bypass for 10GE/40GE/100GE LC 1310/1550nm							4	4	4
Security Services									
Domain Reputation	Optional and not required for DDoS mitigation.								
Additional Services									
24 × 7 Support	✓	✓	✓	✓	✓	✓	✓	✓	✓

To download datasheets, case studies, and other product information, visit https://www.fortinet.com/products/ddos/fortiddos

ORDER INFORMATION

DPDK/TP3 ACCELERATED DEVICES								
Product	**200F**	**1500F**	**1500F-LR**	**2000F**	**3000F**	**1500E**	**2000E**	**2000E-DC**
Device	FDD-200F	FDD-1500F	FDD-1500F-LR	FDD-2000F	FDD-3000F	FDD-1500E	FDD-2000E	FDD-2000E-DC
IP Reputation	FC-10-FI2HF-140-02-DD	FC-10-F1K5F-140-02-DD	FC-10-F15SF-140- 02-DD	FC-10-FD2KF-140-02-DD	FC-10-FI3KF-140- 02-DD	FC-10-F1K5E-140-02-DD	FC-10-FD2KE-140-02-DD	FC-10-F2KED-140-02-DD
Domain Reputation	FC-10-FI2HF-191-02-DD	FC-10-F1K5F-191-02-DD	FC-10-F15SF--191- 02-DD	FC-10-FD2KF-191-02-DD	FC-10-FI3KF-191- 02-DD	FC-10-F1K5E-191-02-DD	FC-10-FD2KE-191-02-DD	FC-10-F2KED-191- 02-DD
Support								
1/3/5-year 24×7 Support	FC-10-FI2HF-247-02-DD	FC-10-F1K5F-247-02-DD	FC-10-F15SF-247- 02-DD	FC-10-FD2KF-247-02-DD	FC-10-FI3KF-247- 02-DD	FC-10-F1K5E-247-02-DD	FC-10-FD2KE-247-02-DD	FC-10-F2KED-247-02-DD

VIRTUAL MACHINES			
Product	**VM04**	**VM08**	**VM16**
Perpetual VM License	FDD-VM04	FDD-VM08	FDD-VM16
IP Reputation	FC-10-FIM04- 140-02-DD	FC-10-FIM08-140- 02-DD	FC-10-FIM16-140- 02-DD
Domain Reputation	FC-10-FIM04- 191-02-DD	FC-10-FIM08-191- 02-DD	FC-10-FIM16-191- 02-DD
Support			
1/3/5-year 24×7 Support	FC-10-FIM04- 248-02-DD	FC-10-FIM08-248- 02-DD	FC-10-FIM16-248- 02-DD

FORTINET TRAINING AND CERTIFICATION

FortiDDoS-F Series Training

Learn how to form network baseline data and to recognize and mitigate individual and distributed denial of service attacks while preserving service and network performance.

Ordering Information

SKU	DESCRIPTION
FT-FDD	Instructor-led training: two full days or three half days
FT-FDD-LAB	On-demand self-paced labs

Course Description

For more information about prerequisites, agenda topics and learning objectives, please refer to the course description at https://training.fortinet.com/local/staticpage/view.php?page=library_fortiddos

CHEAT SHEET

THE SPACE

State actors, professionals, and amateurs using “stresser” sites, continue to launch large, multivector DDoS attacks, disrupting operations. Even if servers are in the cloud, disrupting firewalls blocks employees from reaching services. The number of DDoS attacks is growing 30% per year.

ORDERING GUIDE

CAPEX: two options available:

- **HW appliances** selected via Internet link bandwidth (GE to 2× 100GE) and throughput
- **VMs (VMware, KVM)** for bare-metal servers selected via link bandwidth (GE to 2× 10GE) and throughput
  NOTE: FortiDDoS VMs are unsuitable for deployment in cloud environments such as AWS, Azure, and Google Cloud. FortiDDoS VMs have no IP addressses in the data path and thus cannot be addressed. You must install them on physical links like FortiDDoS appliances.

HYBRID:

- **Cloud DDoS** mitigation available via partners

WHERE TO FIND MORE INFORMATION

- Demo
- Landing page
- B/E-Series Docs
- F-Series Docs

PRODUCT LINEUP

- Appliances from 8-70Gbps/8.8-75Mpps
- VMs to 10Gbps/8Mpps

MAJOR HIGHLIGHTS

FortiDDoS is the only product that stops these major attack types FROM THE FIRST PACKET, without disrupting any other traffic:

- DNS/NTP reflection floods
- SYN-ACK floods as well as all other 14 TCP out-of-state flag floods like ACK, FIN, RST and all 48 illegal flag combinations like Null (no flags) and Xmas (all flags)
- DTLS floods (F-Series)
- QUIC Floods (F-Series)

FortiDDoS mitigates all floods within one second. No multi-10s-of-seconds wait while competitor systems try to create signatures and no five-minute wait for ISP mitigation. UDP floods can take firewalls down in seconds – rapid mitigation of the attack while allowing good traffic is critical to retain services. Blocking all UDP is no longer acceptable since that not only blocks DNS but all Google (QUIC), Zoom, Teams, Webex, and other conferencing apps, among other services.

The only vendor that can stop reflection floods from the 45+ known UDP reflection flood ports as well as almost 10 000 potential reflection ports, without disrupting all UDP traffic.

Autonomous operation:

- 200000 monitored thresholds automatically learned in each of up to 16 Service Protection Profiles
- Real-time adaptive machine learning thresholds for 38 major parameters
- No requirement for manual intervention during attacks
- No requirement for regex or other manual threshold setting

No “threat signature” subscriptions required

Best reporting and forensics

Simple bill of materials

Visit www.fortinet.com for more details