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

### DPK/TP3 ACCELERATED DEVICES AND VIRTUAL MACHINES

<table>
<thead>
<tr>
<th>VM04</th>
<th>VM08</th>
<th>VM16</th>
<th>200F</th>
<th>200F-1500F-LR</th>
<th>2000F</th>
<th>3000F</th>
<th>1500E</th>
<th>2000E-DC</th>
</tr>
</thead>
</table>

#### Recommended Connectivity for Enterprise Datacenter Environments

- **GE or 2xGE BGP**
- **2-4x GE LACP**
- **10GE or 2x 10GE BGP Capped at 4-5Gbps**
- **2x10GE LACP**
- **4x10GE LACP**
- **40GE or 2x40GE BGP**
- **100GE or 2x 100GE BGP**

#### Performance

- **Enterprise Inspected Throughput (Gbps)**
  - 9 10 10 8 22 39 74 35 70
- **SYN Validation Throughput (Mpps)**
  - 2.6 5 5 5.7 20.5 40 50 27 55

#### Other Capacities

- **Max Service Protection Profiles (SPP)**
  - 4 8 16 8 16 16 16 8
- **Max Protected Subnets**
  - 512 per SPP 512 per SPP 512 per SPP 1024 per SPP 1024 per SPP 1024 per SPP 1024 per SPP >2000 per System 1024 per SPP >2000 per System
- **Dual Power Supplies**
  - AC AC AC AC AC AC AC DC/AC
- **Form Factor**
  - 1 RU 2 RU 2 RU 2 RU 2 RU 2 RU 2 RU 2 RU

#### Interfaces

- **10/100/1000 Mbps GE SFP**
- **10GE SFP+**
- **40GE QSFP+**
- **100GE QSFP28**

#### Security Services

- Domain Reptuation: Optional and not required for DDoS mitigation.

#### Additional Services

- **24 x 7 Support**

---

To download datasheets, case studies, and other product information, visit [https://www.fortinet.com/products/ddos/fortiddos](https://www.fortinet.com/products/ddos/fortiddos)
## ORDER INFORMATION

### DPK/TP3 ACCELERATED DEVICES

<table>
<thead>
<tr>
<th>Device</th>
<th>200F</th>
<th>1500F</th>
<th>1500F-LR</th>
<th>2000F</th>
<th>3000F</th>
<th>1500E</th>
<th>2000E</th>
<th>2000E-DC</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Reputation</td>
<td>FC-10-F12HF-140-02-DD</td>
<td>FC-10-F1K5F-140-02-DD</td>
<td>FC-10-F15SF-140-02-DD</td>
<td>FC-10-FD2KF-140-02-DD</td>
<td>FC-10-F13KF-140-02-DD</td>
<td>FC-10-F1K5E-140-02-DD</td>
<td>FC-10-FD2KE-140-02-DD</td>
<td>FC-10-F2KED-140-02-DD</td>
</tr>
<tr>
<td>Domain Reputation</td>
<td>FC-10-F12HF-191-02-DD</td>
<td>FC-10-F1K5F-191-02-DD</td>
<td>FC-10-F15SF-191-02-DD</td>
<td>FC-10-FD2KF-191-02-DD</td>
<td>FC-10-F13KF-191-02-DD</td>
<td>FC-10-F1K5E-191-02-DD</td>
<td>FC-10-FD2KE-191-02-DD</td>
<td>FC-10-F2KED-191-02-DD</td>
</tr>
<tr>
<td>Support</td>
<td>FC-10-F12HF-247-02-DD</td>
<td>FC-10-F1K5F-247-02-DD</td>
<td>FC-10-F15SF-247-02-DD</td>
<td>FC-10-FD2KF-247-02-DD</td>
<td>FC-10-F13KF-247-02-DD</td>
<td>FC-10-F1K5E-247-02-DD</td>
<td>FC-10-FD2KE-247-02-DD</td>
<td>FC-10-F2KED-247-02-DD</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product</th>
<th>VM04</th>
<th>VM08</th>
<th>VM16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perpetual VM License</td>
<td>FDD-VM04</td>
<td>FDD-VM08</td>
<td>FDD-VM16</td>
</tr>
<tr>
<td>Domain Reputation</td>
<td>FC-10-FIM04-191-02-DD</td>
<td>FC-10-FIM08-191-02-DD</td>
<td>FC-10-FIM16-191-02-DD</td>
</tr>
<tr>
<td>Support</td>
<td>FC-10-FIM04-248-02-DD</td>
<td>FC-10-FIM08-248-02-DD</td>
<td>FC-10-FIM16-248-02-DD</td>
</tr>
</tbody>
</table>
## CHEAT SHEET

### The Space
State actors, professionals, and amateurs using “stresser” sites, continue to launch large, multi-vector 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 addresses 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

### Product Lineup
- Appliances from 8-70Gbps/8.8-77Mpps
- 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 seconds. 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:
- Continuous and 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

---

### Where to Find More Information
- Demo
- **What’s New:** B/E-Series and F-Series
- Landing page
- **Teams:** Files/Decks: ddoes_fdd_general and ddoes_fdd-tech
- B/E-Series Docs
- F-Series Docs

---

**Fortinet®**

Copyright © 2022 Fortinet, Inc. All rights reserved. FortiGate®, FortiGuard® and FortiCare®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet’s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet’s internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant thereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.