DATA SHEET

FortiDDoS™

Available in:

Appliance | Virtual Machine

FortiDDoS 200F

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.

A Different and Better Approach to DDoS Attack Mitigation

FortiDDoS massively parallel machine-learning architecture delivers the most advanced and lowest-latency DDoS attack mitigation on the market today, without the performance compromises normally associated with CPU-based systems. FortiDDoS inspects 100% of both inbound and outbound Layer 3, 4, and 7 packets, to the smallest packet sizes, resulting in the fastest and most accurate detection and mitigation in the industry.

In place of pre-defined 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.

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 on selected models
- MSSP Portal for customer resale on selected models
- Central Manager for selected models
- Hybrid On-premise/Cloud mitigation available with Open Signaling

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 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 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. 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 B-/E- Series display 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.

HIGHLIGHTS

FortiDDoS also offers a wide range of static and dynamic ACLs to offload other infrastructure. For example, FortiDDoS supports BCP- 38 (select models) 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.

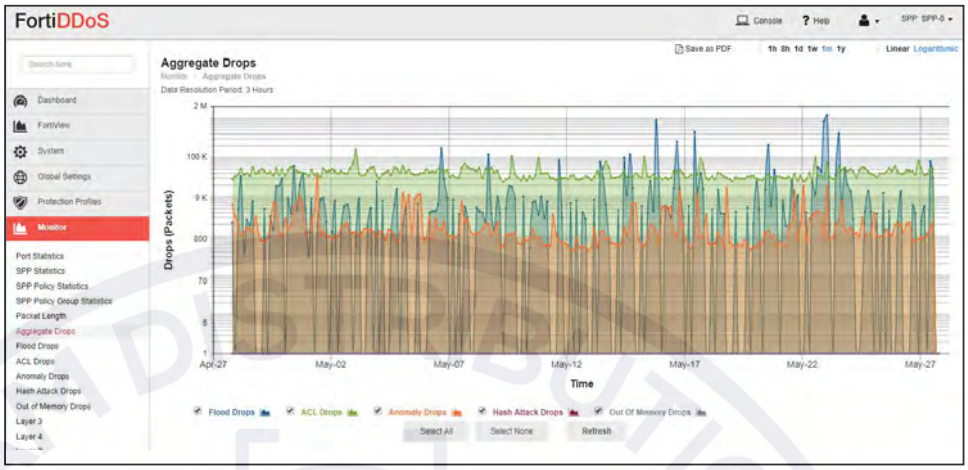
Selected FortiDDoS models offer multi-tenant real-time graphing and attack reporting for resale to customers.

FEATURES

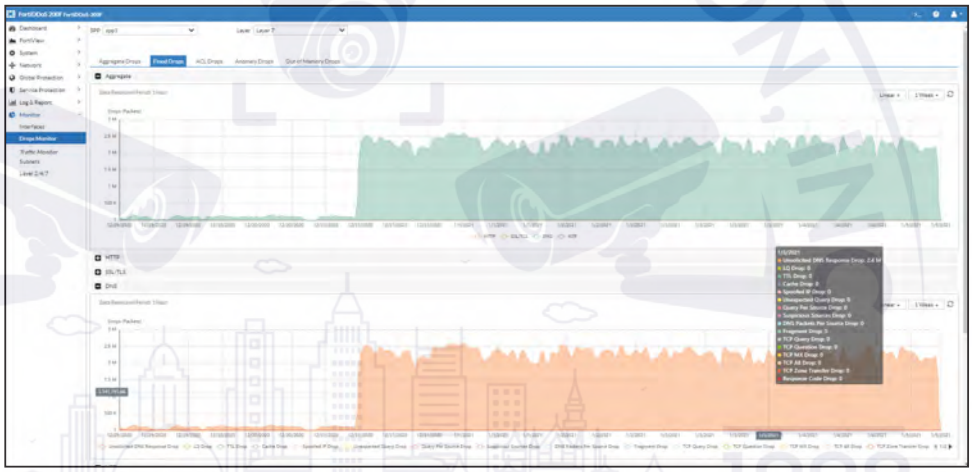
100% Machine Learning Detection	FortiDDoS doesn't rely on signature files that need to be updated with the latest threats so you're protected from both known and unknown "zero-day" attacks. No "threat-protection" subscriptions required. Saves OPEX.
Massively Parallel Architecture	Parallel architecture 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. DNS Reflection floods are stopped from the FIRST packet.
Advanced NTP Protection (selected models)	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.
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.
Fortinet Security Fabric Integration	Single-pane visibility of attack mitigation and network performance reduces management and improves response time (on selected models).
RESTful API	FortiDDoS can be integrated into almost any environment through its RESTful API.
Central Manager	FortiDDoS-CM (for B-/E-Series) is available for users with multiple geographically dispersed FortiDDoS units. One management screen for all devices with single sign-on.

Reporting

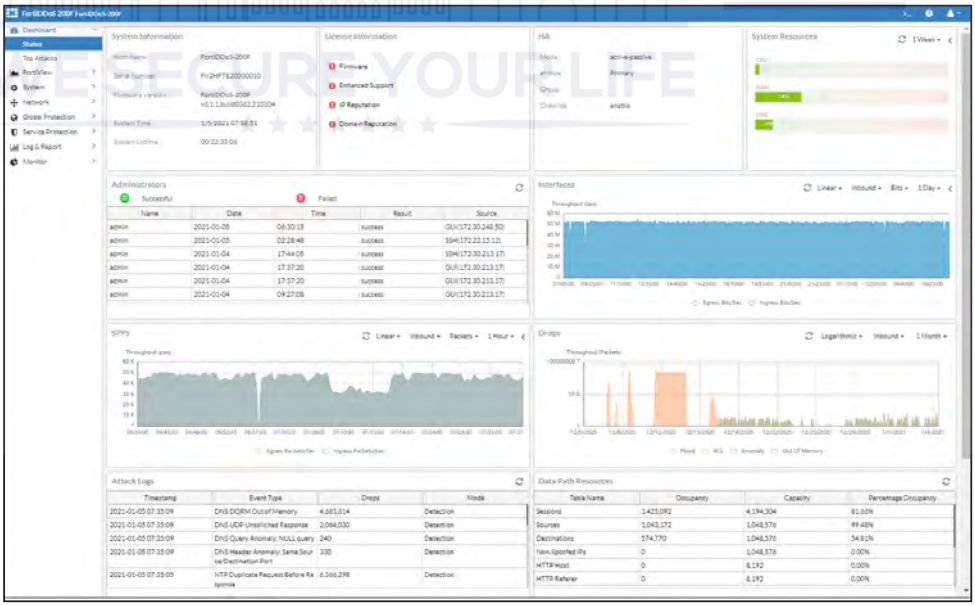
Aggregate Drops L3-L7 (E)



DNS Attacks (F)



Dashboard (F)



Sales@collsam.com
(951)282-8707

Support@collsam.com
(213)210-6744

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 (E/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 (E/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 Service Ports (>10,000)
- ICMP Type/Codes (all 65k)
- SYN, SYN/Destination with line-speed validation, SYN/Source
- **First-packet** TCP State flood mitigation
- Slow Connections
- L4 Aggressive Connection Aging

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)

Attack Mitigation

- **First-packet** DNS (B/E/F) and NTP (E/F) 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 Amplified Reflected Mode 7(monlist) and Mode 6 (varlist) Response Flood **First-packet** mitigation

* 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.

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) (B/E)
- 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)
- IPv4/v6, Protocol, TCP/UDP Port, ICMP Type-Code, TCP/UDP/Other fragment ACL
- Flowspec ACL script generation

Comprehensive 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 (B/E)

Audit Trails

- Login Audit Trail
- Configuration Audit Trail

Management

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

* 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
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	—
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	—
LAN Interfaces QSFP+ 40 GE or QSFP28 100 GE	—
WAN Interfaces QSFP+ 40 GE or QSFP28 100 GE	—
Passive Optical Bypass	—
Storage	1× 480 GB SSD
Form Factor	1U Appliance
Power Supply	Dual AC Hot-Swappable
System Performance	
Maximum Inspected Throughput (Gbps)	8
Inspected Throughput (Enterprise Mix — Gbps)	8
Inspected Packet Throughput (Mpps)	8.8
Maximum Mitigation (Gbps/Mpps)	8 / 8.8
SYN Flood Mitigation (SYN In + Cookie Out) Mpps	5.7
Simultaneous TCP Connections (M)	4.2
Simultaneous Sources (M)	1
Session Setup/Teardown (kcps)	375
Latency (µs) Maximum/Typical	<50
DDoS Attack Mitigation Response Time	1st packet to <2 seconds
Advanced DNS/NTP Mitigation	DNS/ NTP
DNS/NTP Queries per second (M)	2 / 1
DNS/NTP Response Validation under Flood (M Responses/s)	2 / 1
Open Hybrid Cloud Mitigation Support	Yes
Central Manager	No
FortiOS Security Fabric Dashboard Integration	No
Environment	
Input Voltage AC	100–240V AC, 50–60 Hz
Power Consumption (Average W / Maximum W)	117 / 152
Maximum Current AC	100V/1.5A, 240V/0.7A
Heat Dissipation (BTU/hr) / (kjoules/hr)	519 / 574
Operating Temperature	32–104°F (0–40°C)
Storage Temperature	-4–158°F (-20–70°C)
Humidity	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)	1.77 × 17 × 21.7
Height x Width x Length (mm)	44 × 438 × 550
Weight lbs (kg)	21.2 lbs (9.6 kg)