DATASHEET

FortiDDoS™

Comprehensive Protection against Distributed Denial of Service Attacks

Fast and Effective DDoS Detection and Mitigation

ASIC-based behavior analysis accurately detects and blocks anomalies, reconnaissance, and DDoS attacks.

Virtual Network Traffic Partitions

Separate traffic partitions and policies protect other segments and tenants from attack.

Comprehensive Reporting Capabilities

Real-time and historic reports provide granular visibility of each virtual network and protocol layer.

Proven DDoS Defense

Powered by the purpose-built FortiASIC-TP™ (Traffic Processors), the FortiDDoS family of purpose-built network appliances provides effective, fast protection against DDoS attacks. FortiDDoS helps you protect your internet infrastructure from threats and service disruptions by surgically removing network and application layer DDoS attacks, while letting legitimate traffic flow without being impacted.

Differentiated Technology

The FortiDDoS network behavior analysis (NBA) system provides real-time visibility into malicious activity targeting your Internet-facing network. Its hardware-based policy enforcement ensures legitimate traffic will not be affected as it detects and blocks malicious behavior.

FortiDDoS appliances inspect traffic at up to 3Gbps full-duplex line speed, even under full scale attack without having to resort to sampling traffic to reduce performance bottlenecks. It automatically learns traffic patterns and behavior, and continuously updates its set of thresholds used for policy enforcement. By dynamically setting thresholds on the broadest range of Layer 3, 4 and 7 parameters, the FortiDDoS appliance detects and blocks attacks in a matter of seconds, requiring no intervention from an administrator.

Through its unique continuous learning capability, the FortiDDoS family differentiates between gradual build-ups in legitimate traffic and attacks, thereby eliminating false positives arising from campaigns or legitimate search engines.

Unmatched Visibility

FortiDDoS gives you granular visibility into your network's behavior, accurately determining the source of an attack and allowing legitimate traffic through while blocking flood traffic. Source tracking pinpoints the address of a non-spoofed attack.

FortiDDoS immediately blocks dark address scans to prevent outbreak of worms and stealth activity. By preventing header and state anomalies, it further helps in providing a clean pipe to your network. By providing line-rate granular ACLs, FortiDDoS helps protect your infrastructure from unwanted traffic in the data center as well as at the perimeter.

By using Virtual Identification, FortiDDoS can segregate packets to eight discretely managed servers, subnets or networks into different policy domains using IP addresses/masks providing a second level of granular protection to your network.

Unmatched DDoS Protection Capabilities

- ✓ High performance ASIC-based detection and mitigation
- ✓ Virtual network partitions for multi-tenant environments
- ✓ Auto-Learning baselining reduces management overhead
- ✓ Granular visibility with comprehensive reporting of attack and traffic analysis

FROST & SULLIVAN

"FortiDDoS traffic virtual partition feature is not only beneficial in supporting multiple layers of defense but also is a cost containment and administration-friendly feature for organizations that have multiple web properties to protect, and that need unique policies for each."

Michael Suby, Stratecast vice president of research at Frost and Sullivan

FortiDDoS

- High-performance protection from custom FortiASIC-TP™ processors
- Adaptive rate-based detection adjusts policies for variable traffic patterns and seasonality
- Transparent layer 2 bridge with no MAC or IP address in the path of the packets
- Hardware-based protection eliminates need for signatures
- Self-learning baseline adapts policies based on behavior
- Multiple thresholds detect subtle changes in data flows and provide rapid mitigation

Feature	Benefit
Granular visibility and control	Detects attacking traffic utilizing patented detection algorithms; summary reports deliver clear understanding of attack source.
Inline transparent threat mitigation	Provide an automated DDoS prevention service that prevents botnet attacks, and other targeted malware threats, and is easy to deploy and manage.
Bandwidth management	Maintain policies that enable Service Providers to limit each customer or user to their predefined bandwidths.
Header and state anomaly prevention	Cleans network pipes, which improves network and infrastructure utilization.

FortiDDoS Advantages

To achieve a new threshold in security price and performance, FortiDDoS has integrated several critical technologies. No other solution combines these capabilities to give you the complete protection you need.

Virtual Partitioning

To protect virtualized environments, FortiDDoS enables you to partition the traffic and create up to 8 independent profiles for up to 512 subnets. This ensures that there is no collateral damage when a partition is attacked. Each virtual partition on its own can be set to prevention or detection mode in either direction.

Country Code/IP Address Filters (Geo-Location Protection)

FortiDDoS features a unique filtering capability through its hardware logic that enables a network administrator to block a list of entire countries in a few clicks. Just click on a country using the GUI or CLI to either accept or block them in both inbound or outbound traffic. This Geo-Location feature allows you to block or to apply additional in-depth application filtering on all traffic from countries you do not do business with, or that are known originators of malicious behavior (including US State Department identified terror sponsors). This feature dramatically saves bandwidth and lowers your risk attack.

Bogon (Bogus IP) Filtering, Access Control Lists

FortiDDoS's appliances block traffic to restricted ports and limits traffic to allowed protocols. FortiDDoS can provision an extensive list of known infected hosts which are blocked at appliance's initial logic.

Packet Flood Mitigation / Protocol Verification

FortiASIC-TP based hardware filters packets by verifying Layers 3, 4 and 7 protocols are correctly formed, preventing anomaly based attacks.

Stateful Packet Inspection, Out-of-State Filtering

This layer verifies state by confirming the completion of the three way handshake. SYN Floods or other such attempts to utilize system resources are blocked at this layer.

Granular Layer 3, 4 Filtering

FortiDDoS appliances monitor traffic granularly at layers 3, 4 and 7. They can monitor up to 1 million source IP addresses, 1 million connections, 1 million destinations, as well as all IP protocols, all TCP and UDP ports, and ICMP type/codes. Any behavioral threshold that is violated is stopped within 2 seconds.

Application Layer Filtering, Get and Resource Flood Filtering

Many attackers have deployed methods to overwhelm system resources by establishing valid connections. FortiDDoS appliances work at the application layer to prevent this type of attack. Patented Source Tracking helps isolate botnets that are using the same scripted attack using information such as User-Agent, Referrer, URL, Host and Cookie accesses.

Algorithmic Filtering

FortiDDoS's patented system monitors traffic for unusual behavior. Anomalies are "red flagged" by the system. These include access to a URL without accessing images or CSS files using abnormal HTTP headers.

Heuristic Filtering

At application layer, FortiDDoS's hardware logic monitors and prevents accesses that is heuristically known to be botnet oriented. This logic is continuously updated based on current trends.

Feature	Details	
Packet Inspection Technology	• Granular Packet Inspection • Stateful Analysis Firewall	• Chip(ASIC, FORTIASIC-TP) • Continuous, Adaptive rate limiting
Multi-Verification Process	• Dynamic Filtering • Active Verification • Anomaly Recognition • Protocol Analysis • Rate Limiting	• White-list, Black-list, Non-tracked subnets • State Anomaly Recognition • Stealth Attack filtering • Dark address scan prevention • Source Tracking • Legitimate IP address Matching (for anti-spoofing)
Flood Prevention Schemes	• SYN Cookie, ACK Cookie, SYN Retransmission • Connection Limiting • Aggressive Aging • Legitimate IP Address Matching	• Source Rate Limiting • Source Tracking • Granular Rate-limiting
Layer 3 Floods Mitigated	• Protocol Flood (all 256) • Fragment Flood • Source Flood	• Destination Flood • Dark Address Scan • Excessive TCP per Destination
Layer 4 Floods Mitigated	• TCP Ports (all 64K) • UDP Ports (all 64K) • ICMP Type/Codes (all 64K) • Connection Flood • SYN Flood • Excessive SYNs/Source/Second	• Excessive Connections Establishment/second • Zombie Flood • Excessive Connection/Source flood • Excessive Connections/Destination flood • TCP state violation floods
Layer 7 Floods Mitigated	• Opcode Flood • HTTP URL GET Flood • User-agent Flood • Referrer Flood • Cookie Flood	• Host Flood • Associated URL access • Mandatory HTTP header parameters • Sequential HTTP Access.
Real-time Diagnostics	• Top 100 Servers • Top 100 Tuples • Top 100 Ports • Top 100 Currently Denied Sources • Top 100 Sources	• Top 100 URLs • Top 100 User-Agents • Top 100 Referrer • Top 100 Hosts
Visibility, ACLs, Bandwidth Controls	• Yes	
Traffic and Event Analysis	• Yes	
Reconnaissance and Header and State Anomaly Prevention	• Yes	
Dynamic Switching Features	• Dynamic switching between Detection and Prevention based on behavioral thresholds.	• Dynamic switching of policies based on behavioral thresholds.
Propagate Link State Change (PLSC)/ Link Down Synchronization	• Yes	
Management	• SSL Management • CLI	
Centralized Event Reporting	• GUI • SNMP	• Email/Pager • Support for MRTG, Cacti
Audit and Access Trails	• Login trail • GUI access trail	• Audit trail for configuration changes

Technical Specifications	FortiDDoS-100A	FortiDDoS-200A	FortiDDoS-300A
Hardware Specifications			
LAN Interfaces (copper/SFP)	2	4	6
WAN Interfaces (Copper/SFP)	2	4	6
Virtual Instances	8	8	8
Power Supply	Single AC	Dual AC	Dual AC
Storage	1x1TB HDD	2x1TB HDD	2x1TB HDD
RAID Support	No	Yes	Yes
System Performance			
Throughput (Full Duplex)	1 Gbps	2 Gbps	3 Gbps
No. of Virtual Partitions		8	
Simultaneous Connections	1,000,000	2,000,000	3,000,000
Simultaneous Sources	1,000,000	2,000,000	3,000,000
Simultaneous Legitimate IP Addresses in Cache	2,000,000	4,000,000	6,000,000
Session Setup/Teardown	100,000 / Second	200,000 / Second	300,000 / Second
Latency		Under 26 microseconds	
DDoS Attack Mitigation Response		Under 2 seconds	
Non-tracked subnets		512	
HTTP URLs/VID	64K	128K	192K
User-Agent/ Referrer/ Host/Cookie/VID	512	1024	1536
Dark address subnets		512	
Dimensions			
Height	3.5 in (88.4 mm)	7 in (177 mm)	7 in (177 mm)
Width	19 in (482 mm)	19 in (482 mm)	19 in (482 mm)
Length	17.4 (441.6 mm)	18.1 in (481 mm)	18.1 in (481 mm)
Weight	26 lb (11.78 kg)	39.2 lb (17.8 kg)	40.4 lb (18.3 kg)
Rack Mount	2U	4U	4U
Environment			
AC Power Supply	100-240 VAC 60/50 Hz, 6 - 3 Amp (PFC)	100-240 VAC 60/50 Hz, 9 - 4.5A (Redundant)	
Power Consumption (AVG)	181W	189W	200W
Operating Temperature		32 – 104 deg F (0 – 40 deg C)	
Humidity		5 to 95% non-condensing	
Compliance			
		FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	

Ordering Information		
Product	**SKU**	**Description**
FortiDDoS-100A	FortiDDoS-100A	2U appliance, 1 Gbps full duplex, 4 x 1 GbE (copper/fiber), single power supply, 1 TB HDD
FortiDDoS-200A	FortiDDoS-200A	4U appliance, 2 Gbps full duplex, 4 x 1 GbE (copper/fiber), dual power supply, 2 x 1 TB HDD (RAID 1)
FortiDDoS-300A	FortiDDoS-300A	4U appliance, 3 Gbps full duplex, 6 x 1 GbE (copper/fiber), dual power supply, 2 x 1 TB HDD (RAID 1)

GLOBAL HEADQUARTERS
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE
Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE
Fortinet Incorporated
300 Beach Road 20-01, The Concourse
Singapore 199555
Tel: +65-6513-3734
Fax: +65-6295-0015

Copyright© 2012 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance 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 the performance metrics herein. 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 guarantees. 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.

FDDoS-DAT-R2-201206