



DATASHEET

FortiWeb™

Combined Web Application and XML Firewall

Unmatched Protection for Web Applications

The FortiWeb family of web application firewalls provides specialized, layered application threat protection for medium and large enterprises, application service providers, and SaaS providers. Combining both web application firewall and XML firewall capabilities in a single platform, the FortiWeb solution allows enterprises to protect against application-level attacks targeted at web applications and web services infrastructure.

FortiWeb's integrated web application and XML firewalls protect your web-based applications and internet-facing data from attack and data loss. Using advanced techniques to provide bi-directional protection against sophisticated threats like SQL injection and cross-site scripting, FortiWeb platforms help you prevent identity theft, financial fraud and corporate espionage.

Measure Policy Compliance

You can measure your compliance with policies, such as the Payment Card Industry's Data Security Standard (PCI DSS) regulatory framework, with FortiWeb's customizable, preconfigured reporting tools. FortiWeb delivers the technology you need to monitor and enforce government regulations, industry best practices, and internal policies.

The FortiWeb family drastically reduces the time required to protect your regulated internet-facing data and eases the challenges associated with policy enforcement and regulatory compliance. FortiWeb appliances also leverage an intelligent, application-aware load-balancing engine to distribute traffic and route content across multiple web servers. This load balancing increases application performance, improves resource utilization and application stability while reducing server response times.

Accelerate Deployment and Lower Costs

FortiWeb significantly reduces deployment costs by consolidating Web Application Firewall, XML filtering, web traffic acceleration, and application traffic balancing into a single device with no per-user pricing. It offers an integrated, cost-effective web application security platform for any medium and large enterprise.



The Fortinet Family: Performance, Flexibility, and Scalability

Fortinet solutions offer you unparalleled security and performance, whether you're looking for a single platform to deliver unified threat management or a focused solution to protect specific content such as web, messaging, or database traffic. Fortinet provides network security solutions that address the most critical needs facing organizations of every size, including global enterprises, carriers, and service providers.

To provide strong security without performance penalties, Fortinet products leverage breakthroughs in chip design, networking, security and content pattern recognition analysis. The unique, ASIC-based architecture analyzes network content and behavior in real-time, enabling all key network services—including real-time web applications—to be screened for both network and content-level threats without impacting network performance.

Fortinet's integrated approach enables you to lower your costs and simplify your network infrastructure by consolidating stand-alone security products.

Features

Benefits

Inline Reverse Proxy, Transparent, and Offline Deployment Modes

Deploy FortiWeb into existing networks without the need for a network-level redesign or changes to web application and network infrastructure

Auto-Learning Security Profiles

Discovers the structure and usage pattern of web applications, removes the need for manual configuration of access policies and security profiles

Web Vulnerability Scanner

Scans web applications to detect existing vulnerabilities, complementing the Web Application Firewall for PCI DSS section 6.6

Data Leak Prevention

Analyzes all outbound traffic alerting/blocking any credit card leakage and information disclosure

PCI DSS

Helps organizations meet PCI compliance requirements by providing a comprehensive solution for web application protection

Ultimate Protection and Monitoring for Web Applications

FortiWeb provides flexible and reliable protection by utilizing a range of security modules

Data Leak Prevention

Extended monitoring and protection for credit card leakage and application information disclosure by tightly monitoring all outbound traffic.

Anti Web Defacement

Unique capabilities for monitoring protected applications for any defacement and ability to automatically and quickly revert to stored version.

HTTP RFC Compliance Validation

FortiWeb blocks any attacks manipulating the HTTP protocol by maintaining strict RFC standards to prevent attacks such as encoding attacks, buffer overflows and other application specific attacks.

Web Application Vulnerability Assessments

Automatically scans and analyzes the protected web applications and detects security weaknesses, potential application known and unknown vulnerabilities to complete a comprehensive solution for PCI DSS.

Auto-Learn Security Profiling

Automatically and dynamically builds a security model of protected applications by continuously monitoring real time user activity. Access outside the baseline can then be alerted or blocked.

Application Layer Vulnerability Protection

Out of the box protection for the most complex attacks such as SQL Injection, Cross Site Scripting, CSRF and many others. Together with the Auto Learn profiling system and advanced abilities to create rules down to the single application element. FortiWeb provides the ultimate protection from today's most sophisticated hackers.

FortiGuard

Utilizing Fortinet's renowned FortiGuard service FortiWeb customers get up to date dynamic protection from the Fortinet® Global Security Research Team, which researches and develops protection against known and potential application security threats.

PCI DSS

Helps organizations meet PCI compliance requirements by providing a comprehensive solution for web application protection.

XML Firewall

Provides an XML firewall capability with schema validation, XML Firewall, IPS and routing capabilities.

Robust, Efficient Implementation and Management

FortiWeb accelerates and simplifies the process of protecting your critical web applications

Multiple Deployment Options

FortiWeb provides a flexible solution that you can easily introduce into any environment or existing network implementations:

- Inline Transparent Mode – Layer two bridge that does not require network level redesign
- Inline Reverse Proxy – Provides additional capabilities such as URL rewrite and advanced routing capabilities
- Non-Inline Sniffing – Monitors environments with zero network footprint and latency

Authentication Offload

FortiWeb introduces a simple integration with any environment allowing you to offload your web server authentication to the FortiWeb platform while supporting different authentication schemes such as Local, LDAP and NTLM.

High Performance and Availability

With the integration of award winning FortiASIC™ technology, FortiWeb is able to process tens of thousands of web transactions and provide hardware accelerated SSL offload and advanced load balancing capabilities. The high availability mode provides configuration synchronization and allows for a network-level failover in the event of unexpected outage events.

Logging and Reporting

FortiWeb's extensive and accurate logging capabilities provide you with the specific attack details you need to pinpoint the threat as it happens. Hundreds of out-of-the-box report types allow administrators or auditors to analyze attacks, events, and traffics for regulatory compliance purposes.

FortiWeb Protects Against A Wide Range of Attacks

- | | | |
|------------------------------|------------------------|--------------------------|
| Cross Site Scripting | HTTP Request Smuggling | Schema Poisoning |
| SQL Injection | Remote File Inclusion | XML Parameter Tampering |
| Session Hijacking | Encoding Attacks | XML Intrusion Prevention |
| Cookie Tampering / Poisoning | Broken Access Control | WSDL Scanning |
| Cross Site Request Forgery | Forceful Browsing | Recursive Payload |
| Command injection | Directory Traversal | External Entity Attack |
| Remote File Inclusion | Site Reconnaissance | Buffer Overflows |
| Forms Tampering | Search Engine Hacking | Denial of Service |
| Hidden Field Manipulation | Brute Force Login | |
| Outbound Data Leakage | Access Rate Control | |



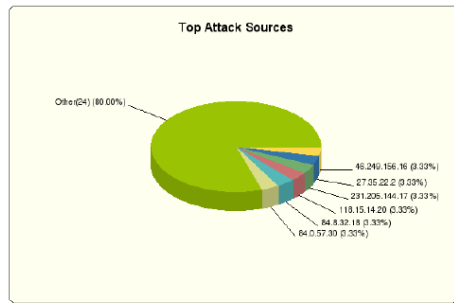
Dashboard

High-level view of your environment with real time traffic and attack statistic graphs to provide 'at a glance' view of status of web application security

Top Attack Sources

The most frequent sources of attacks over the reporting period.

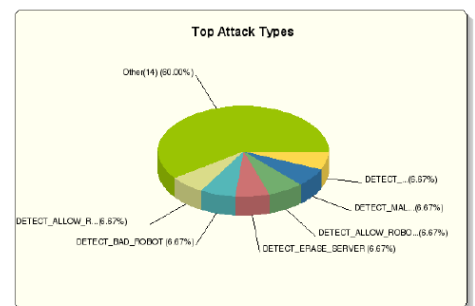
Source	Events	% of Total
46.249.156.16	1	3.33
27.35.22.2	1	3.33
231.205.144.17	1	3.33
118.15.14.20	1	3.33
84.8.32.18	1	3.33
84.0.57.30	1	3.33
Other(24)	24	80.00
Total(30)	30	100.00



Top Attack Types

The most frequently detected attack types over the reporting period.

Attack Type	Events	% of Total
DETECT_BRUTE_FORCE_LOGIN	2	6.67
DETECT_MALICIOUS_ROBOT	2	6.67
DETECT_ALLOW_ROBOT_MSN	2	6.67
DETECT_ERASE_SERVER	2	6.67
DETECT_BAD_ROBOT	2	6.67
DETECT_ALLOW_ROBOT_YAHOO	2	6.67
Other(14)	18	60.00
Total(20)	30	100.00



Management Reports

FortiWeb management reports contain the information you need to measure your policy compliance and risk profile, as well as understand the threats you face

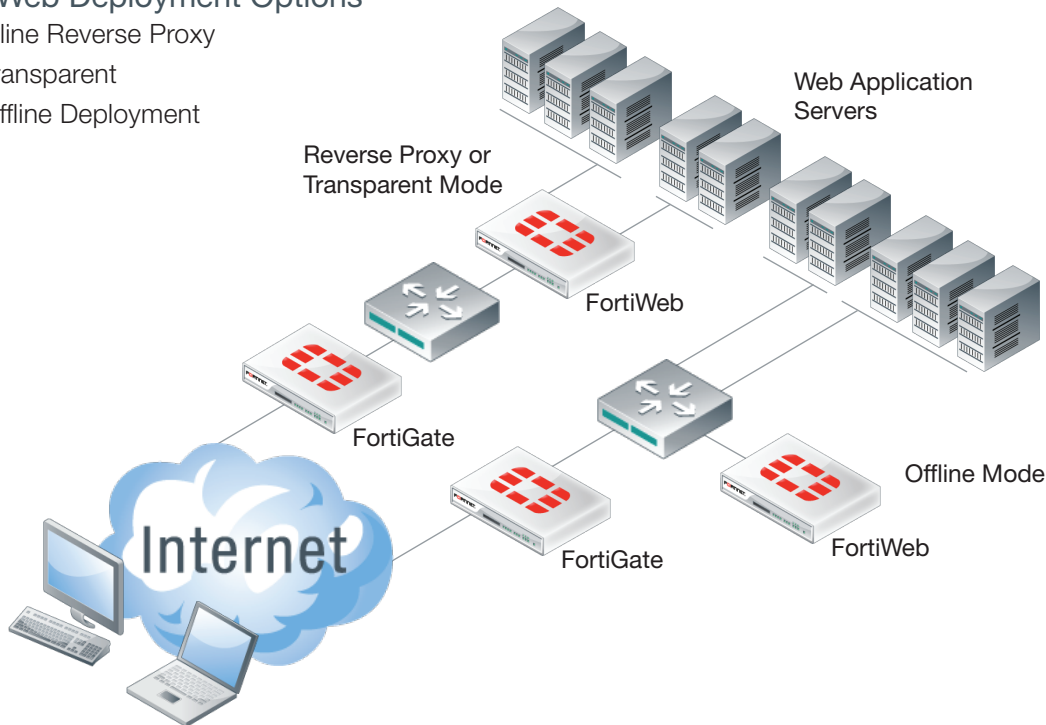


Technical Specifications	FortiWeb-400B	FortiWeb-1000B
Hardware Specifications		
10/100/1000 Interfaces (Copper, RJ-45)	4	4
USB Interfaces	1	2
Internal Storage	500 GB	1 TB
System Performance		
Throughput	100 Mbps	500 Mbps
MAX HTTP trans/sec	10,000	22,000
Latency	Sub-millisecond	Sub-millisecond
Deployment Modes	Reverse Proxy, Transparent Inline, Offline Sniffing	Reverse Proxy, Transparent Inline, Offline Sniffing
High Availability Configuration	Active / Passive	Active / Passive
Unlimited User Licenses	Yes	Yes
Dimensions		
Height x Width x Length (in)	1.7 x 17.5 x 14.5 in	1.7 x 16.7 x 30.4 in
Height x Width x Length (cm)	4.3 x 43.8 x 36.8 cm	4.3 x 42.6 x 77.2 cm
All performance values are "up to" and vary depending on system configuration		

Technical Specifications (continued)	FortiWeb-400B	FortiWeb-1000B
Dimensions (continued)		
Weight	10 lbs (4.53 kg)	36 lb (16.3 kg)
Rack Mountable	Yes	Yes
Environment		
Power Required	100-240 VAC, 50-60 Hz, 4.0 Amp (max)	100-240 VAC, 50-60 Hz, 4.8 Amp (max)
Power Consumption (AVG)	121 W	260 W
Operating Temperature	32 – 104 deg F (0 – 40 deg C)	50 to 95 deg F (10 - 35 deg C)
Storage Temperature	-13 to 158 deg F (-25 to 70 deg C)	-40 to 149 deg F (-40 to 65 deg C)
Humidity	5 to 95% non-condensing	5 to 95% non-condensing (twmax=38C)
Compliance		
	FCC Class A Part 15, CE Mark	FCC Class A Part 15, CE Mark

FortiWeb Deployment Options

- Inline Reverse Proxy
- Transparent
- Offline Deployment



FortiGuard® Security Subscription Services deliver dynamic, automated updates for Fortinet products. The Fortinet Global Security Research Team creates these updates to ensure up-to-date protection against sophisticated threats. Subscriptions include antivirus, intrusion prevention, web filtering, antispam, vulnerability and compliance management, application control, and database security services.

FortiCare™ Support Services provide global support for all Fortinet products and services. FortiCare support enables your Fortinet products to perform optimally. Support plans start with 8x5 Enhanced Support with "return and replace" hardware replacement or 24x7 Comprehensive Support with advanced replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and 90-day limited software warranty.

FORTINET®

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
61 Robinson Road, #09-04 Robinson Centre
Singapore 068893
Tel +65-6513-3730
Fax +65-6223-6784

Copyright© 2010 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. Network variables, different network environments and other conditions may affect performance results, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding contract 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. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.