DATASHEET

FortiWeb™

Combined Web Application and XML Firewall

Urge for PCI DSS Compliance

Network security threats have evolved to target web-based applications that are the interface to confidential information stored on back-end databases. In response to major security breaches, information, and identity and data theft PCI standards were formed. However, ensuring the web-application is free of vulnerabilities is complicated by the ongoing discovery of new vulnerabilities, patching challenges, code revisions, time-to-market pressures, the inherent difficulty of vulnerability identification, and even access to the application code.

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. 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 bidirectional protection against sophisticated threats like SQL injection and cross-site scripting, FortiWeb platforms help you prevent identity theft, financial fraud and corporate espionage. FortiWeb delivers the technology you need to monitor and enforce government regulations, industry best practices, and internal policies.

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 drastically reduces the time required to protect your regulated internet-facing data and eases the challenges associated with policy enforcement and regulatory compliance. Its intelligent, application-aware load-balancing engine increases application performance, improves resource utilization and application stability while reducing server response times.

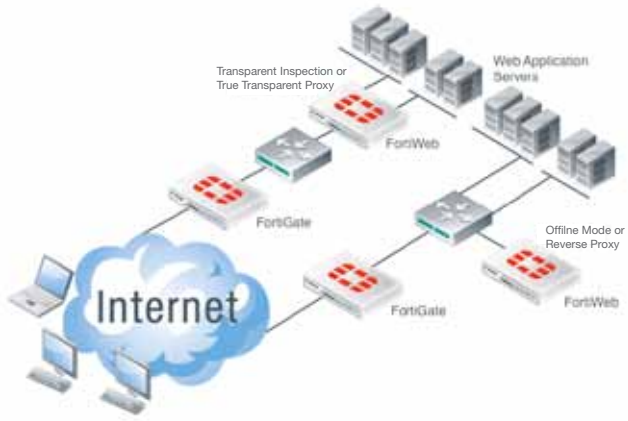
Unmatched Protection for Web Applications

- ✓ ICSA WAF certified*
- ✓ Integrates web application and XML firewalls
- ✓ Flexible deployment and simple management
- ✓ Auto-Learning base lining
- ✓ WAF and integrated scanner aid in PCI 6.6 compliance
- ✓ Periodic updates from FortiGuard

ICSA labs CERTIFIED WEB APPLICATION FIREWALL

FortiWeb Deployments

- Inline Transparent – Layer two bridge that does not require network level redesign
- True Transparent Proxy – Layer two deployment with no need for network level redesign. The traffic is internally terminated to provide more functionality than pure inspection.
- Reverse Proxy – Provides additional capabilities such as URL rewrite and advanced routing capabilities
- Offline Sniffing – Monitors environments with zero network footprint and latency



* The module under ICSA WAF testing is FortiWeb 1000B.

Flexible deployment and efficient management

- **Multiple deployment options**
  Transparent Inspection and True Transparent Proxy, Reverse Proxy and Offline Allow you to fit FortiWeb into any environment.
- **Auto-Learn Security Profiling**
  Automatically and dynamically build a security model of protected applications by continuously monitoring real time user activity. Eliminate the need for manual configuration of security profiles.
- **Authentication Offload**
  Offload your web server authentication to the FortiWeb platform while supporting different authentication schemes such as Local, LDAP and NTLM.
- **Policy wizard and pre-defined policies**
  Allows for one click deployments and greatly eases the process of policies creation.
- **High Performance**
  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.
- **High Availability**
  The high availability mode provides configuration synchronization and allows for a network-level failover in the event of unexpected outage events. Integrated bypass interfaces provide additional fail open capability for single box deployments.
- **Logging and Reporting**
  FortiWeb provides hundreds of out-of-the-box report types allowing administrators or auditors to analyze attacks, events, and traffics for regulatory compliance purposes.

Ultimate protection and monitoring

- **Data Leak Prevention**
  Extended monitoring and protection for credit card leakage and application information disclosure by tightly monitoring all outbound traffic. Allow customers to create their own granular signatures and DLP patterns together with predefined rules for any type of events.
- **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.
- **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.
- **XML Firewall**
  Provide an XML firewall with schema validation, XML Firewall, IPS and routing capabilities.
- **Application Layer Vulnerability Protection**
  Provide 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, FortiWeb is able to create rules down to the single application element.

Aides in compliance

- **PCI DSS compliance**
  FortiWeb is the only product that provides a Vulnerability Scanner module within the web application firewall that completes a comprehensive solution for PCI DSS requirement 6.6.
- **Protects against OWASP top 10**
  Incorporating a positive and a negative security module based on bidirectional traffic analysis and an embedded behavioral based anomaly detection engine FortiWeb fully protects against the OWASP TOP 10.
- **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.

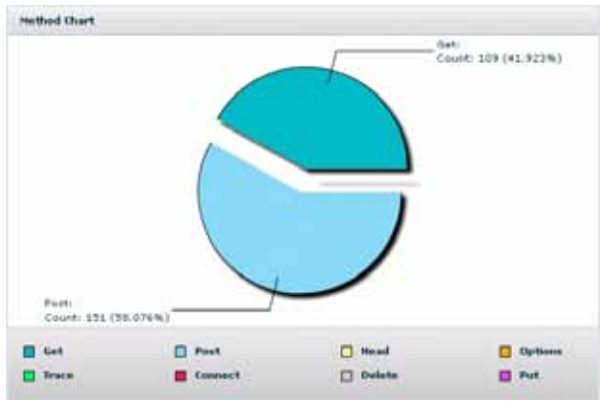
FortiWeb Protects Against a Wide Range of Attacks

Cross Site Scripting	Outbound Data Leakage	Access Rate Control
SQL Injection	HTTP Request Smuggling	Schema Poisoning
Session Hijacking	Remote File Inclusion	XML Parameter Tampering
Cookie Tampering / Poisoning	Encoding Attacks	XML Intrusion Prevention
	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	

FortiWeb Auto-Learning Profiling

The Auto-Learn profiling capability is completely transparent and does not require any changes to the application or network architecture. FortiWeb does not scan the application in order to build the profile, but rather analyzes the traffic as it monitors it flowing to the application. By creating a comprehensive security model of the application FortiWeb can now protect against any known or unknown vulnerabilities, zero day attacks.

As part of PCI 1.2 section 6.6 – deploy a web application firewall an alternative is to address new vulnerabilities by running ongoing vulnerability assessments (annually, after changes, correct vulnerabilities and rescan). FortiWeb helps organization by providing both – a web application firewall and a web application scanner.



FortiWeb Vulnerability Scanner

Provide scheduled and on-demand scan through your applications for web vulnerabilities. Complements WAF for PCI DSS 6.6

Technical Specifications	FortiWeb-400B	FortiWeb-1000B	FortiWeb-1000C	FortiWeb-3000C
Hardware Specifications				
10/100/1000 Interfaces	4	4	4 (2 from FortiModule)	6 (2 from FortiModule)
USB Interfaces	1	2	2	4
Storage	500 MB	1 TB	1 TB (standard) 2 x 1 TB slots	2 TB (standard) 6 x 1 TB slots
Form Factor	1U	1U	1U	2U
Power Supply	Standard	Standard	Standard	2U Hot Swap Redundant
System Performance				
Throughput	100 Mbps	500 Mbps	500 Mbps	1 Gbps
Max HTTP transactions per second	10,000	22,000	27,000	40,000
Latency	Sub-ms	Sub-ms	Sub-ms	Sub-ms
High Availability	Active/Passive	Active/Passive	Active/Passive	Active/Passive
User Licenses	Unlimited	Unlimited	Unlimited	Unlimited
All performance values are “up to” and vary depending on the system configuration.				
Dimensions				
Height	1.7 in (4.3 cm)	1.7 in (4.3 cm)	1.69 in (4.3 cm)	3.5 in (8.9 cm)
Width	17.5 in (43.8 cm)	16.7 in (42.6 cm)	17.09 in (43.4 cm)	17.5 in (44.5 cm)
Length	14.5 in (36.8 cm)	30.4 in (77.2 cm)	24.7 in (62.71 cm)	29 in (73.7 cm)
Weight	10 lb (4.53 kg)	36 lb (16.3 kg)	24.2 lb (11 kg)	63 lb (28.6 kg)
Rack Mountable	Yes	Yes	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	100-240 VAC, 50-60 Hz, 7 Amp max	100-240 VAC, 50-60 Hz, 9 Amp max
Power Consumption (AVG)	121W	260W	189W	200W
Operating Temperature	32 – 104 deg F (0 – 40 deg C)	50 – 95 deg F (10 – 35 deg C)	32 – 104 deg F (0 – 40 deg C)	32 – 104 deg F (0 – 40 deg C)
Storage Temperature	-13 – 158 deg F (-25 – 70 deg C)	-40 – 149 deg F (-40 – 65 deg C)	-40 – 149 deg F (-40 – 65 deg C)	-40 – 149 deg F (-40 – 65 deg C)
Humidity	5 to 95% non-condensing	5 to 95% non-condensing (twmax=38C)	5 to 95% non-condensing	5 to 95% non-condensing
Compliance				
	FCC Class A Part 15, UL/CUL, C Tick, CE, VCCI	FCC Class A Part 15, CE Mark	FCC Class A Part 15, UL/CB/CUL, C Tick, VCCI	FCC Class A Part 15, UL/CB/CUL, C Tick, VCCI

FortiWeb-400B

FortiWeb-1000B

FortiWeb-1000C

FortiWeb-3000C

Ordering Info		
Product	**SKU**	**Description**
FortiWeb-400B	FWB-400B	FortiWeb-400B, x4 10/100/1000 ports, one (1) 500 GB Hard Drive
	FC-10-V0402-137-02-DD	FortiWeb Security Service for FortiWeb-400B
FortiWeb-1000B	FWB-1000B-EMU01	FortiWeb-1000B, 4 10/100/1000 ports, one 1TB HDD
	FC-10-V1002-137-02-DD	FortiWeb Security Service for FortiWeb-1000B
FortiWeb-1000C	FWB-1000C-E07S	FortiWeb -1000C, 4 10/100/1000 ports, one 1TB HDD, rack mountable
	FC-10-V1003-137-02-DD	FortiWeb Security Service for FortiWeb-1000C
FortiWeb-3000C	FWB-3000C-E02S	FortiWeb-3000C, 6 10/100/1000 RJ45 ports, 2 1TB Hard Drive
	FC-10-V3002-137-02-DD	FortiWeb Security Service for FortiWeb-3000C

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