

FortiWeb-1000B

Web Security Appliance

Datasheet

Network security threats have evolved to target web-based applications that are the interface to confidential information stored on backend databases. Because of their communication with backend databases, any exploitable vulnerability in the web application translates to a potential attack vector against the databases and the information it stores. 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. The problem is further compounded by the existence of multiple web applications and database server resources, which would require both multiple security audits and load balancing. Much like the applications and operating systems of today are inherently vulnerable, web-based applications cannot be assumed to be written or deployed securely; and therefore require independent security measures.

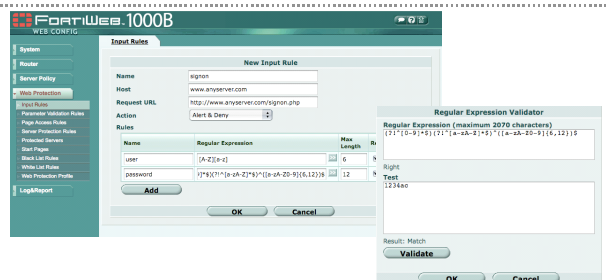
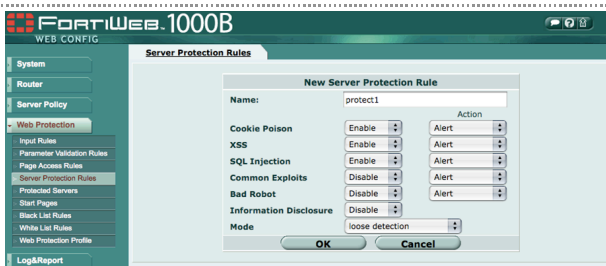
FortiWeb-1000B is a web security appliance that provides web application and XML firewalls to protect, balance, and accelerate web applications, databases, and the information exchanged between them. The FortiWeb-1000B is designed for medium and large enterprises, and can drastically reduce the deployment time and complexities of introducing web-based applications. The FortiWeb-1000B applies Fortinet's industry-leading threat research to protect web-based applications, improving the security of confidential information and aiding in legislative and PCI compliance.

In addition to security, the FortiWeb-1000B leverages an intelligent, application-aware load-balancing engine to distribute traffic and route content across multiple web servers. This load balancing increases resource utilization, application stability, and server response times. Web application traffic is further accelerated by an independent SSL and XML encryption processor, which increase transaction throughput and reduce processing requirements from web servers. In addition to industry leading web application firewall (WAF) technology, the FortiWeb-1000B goes beyond traditional web security devices to provide XML security enforcement, hardware-based application acceleration, and server load balancing to set new standards for the capabilities of a web security appliance. Finally, deployment flexibility rounds off the FortiWeb-1000B's feature set with inline reverse proxy, or offline monitoring deployment modes.

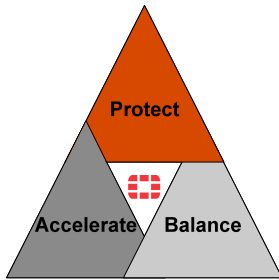


FortiWeb-1000B

Feature	Benefit
Web application firewall and XML firewall	Secures web applications Protects sensitive database content Aides PCI compliance Improves deployment times Simplifies management
SSL and XML encryption co-processing	Accelerates transaction times Offloads encryption functions Reduces server processing requirements
Server load balancing and content-based routing	Increases application speeds Improves server resource utilization Stabilizes applications
High availability support	Active/passive failover with full configuration synchronization

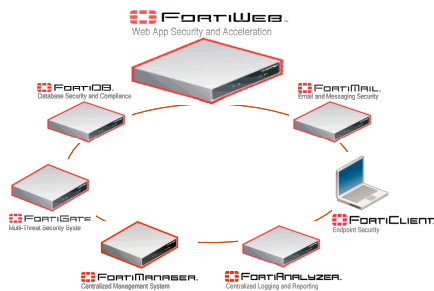


FortiWeb-1000B	
System Specifications	
Throughput (HTTP)	500 Mbps
HTTP Sessions per Second	8,000
Latency	Sub-Millisecond
Deployment Modes	Inline reverse proxy or offline monitoring
Hardware Specifications	
Security Hardened Platform	Yes
10/100/1000 Ethernet (Copper)	4
USB ports	2
Hard Drive	1 x 1 TB (2 x 1TB drive optional)
Dimensions	
Height, Width, Length	1.7 x 16.7 x 30.4 inches (4.3 x 42.6 x 77.2 cm)
Weight	36 lbs (16.3 kg)
Rack Mountable	Yes
Input Voltage	100-240 VAC
Input Current	10A
Power Consumption (AVG)	260W
Environment	
Operating temperature	32 to 104 deg F (0 - 40 deg C)
Storage temperature	13 to 158 deg F (-25 to 70 deg C)
Humidity	5 to 95% non-condensing
Compliance	FCC Class A Part 15, / CE Mark



The Fortinet Product Family

The FortiWeb-1000B web security appliance can effectively protect, balance, and accelerate web applications, and is complemented by the FortiDB database security family, the FortiGate multi-threat security family, the FortiMail email security family, the FortiClient endpoint security family, and the FortiManager and FortiAnalyzer centralized management, reporting and logging solutions.



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

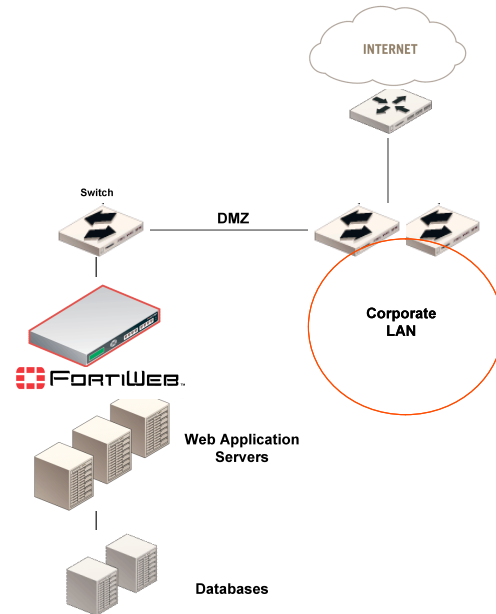
Fortinet Incorporated
120 Rue Albert Caquot
06560 Sophia Antipolis, France
Tel +33-4-8987-0510 Fax +33-4-8987-0501

APAC SALES OFFICE-SINGAPORE

Fortinet Incorporated
61 Robinson Road, #09-04 Robinson Centre
Singapore 068893
Tel: +65-6513-3730 Fax: +65-6223-6784 7259

Comprehensive WAF and XML Security

Deployed inline in front of web servers, the FortiWeb-1000B leverages signature and pattern detection engines, threshold limits, session management, flow enforcement, parameter validation, and several other technologies to identify threats such as cross-site scripting, SQL injection, buffer overflows, file inclusion, denial of service, cookie poisoning, schema poisoning, and countless other attacks.



A Sample of Technologies Leveraged and Threats Mitigated by the FortiWeb-1000B

Technologies

- Input validation and enforcement
- Predefined attack signatures
- Session Management
- Flow enforcement
- Rules-based parameter validation
- Content-based routing
- XML IPS
- SSL/XML Hardware acceleration
- XML schema validation
- WSDL verification
- XML expression limiting
- IP-based policies
- Firewall virtualization
- Server load balancing
- Inline reverse proxy deployment mode
- Offline monitoring deployment mode

Threats

- Cross site scripting
- SQL Injection
- Buffer overflows
- OS command injection
- Cross site request forgery
- Outbound data leakage
- HTTP request smuggling
- Remote file inclusion
- Encoding attacks
- Cookie tampering/poisoning
- Session hijacking
- Broken access control
- Forceful browsing / directory traversal
- Site reconnaissance
- Denial of service
- Schema poisoning
- XML parameter tampering
- WSDL scanning
- Recursive payload
- External entity attack