FortiWeb™

Web Application and API Protection

FortiWeb is a web application firewall (WAF) that protects web applications and APIs from attacks that target known and unknown exploits and helps maintain compliance with regulations.

Using machine learning to model each application, FortiWeb defends applications from known vulnerabilities and from zero-day threats. High performance physical, virtual appliances, and containers deploy on-site or in the public cloud to serve any size of the organization—from small businesses to service providers, carriers, and large enterprises.

Highlights

Machine learning that detects and blocks threats while minimizing false positives

Advanced Bot Mitigation effectively protect web assets without imposing friction on legitimate users

Protection for APIs, including those used to support mobile applications

Enhanced protection with Fortinet Security Fabric integration

Simplified attack investigation with Threat Analytics

Third-party integration and virtual patching

Features

Available in

Appliance

Virtual

SaaS

Cloud

Container

FortiWeb 100E, 400E, 600E, 400F, 600F, 1000F, 2000F, 3000F, 4000F, VM, and Container

Web Application Protection

Multi layer protection against the OWASP Top 10 application attacks including machine learning to defend against known and unknown attacks.

API Protection

Protect your APIs from malicious actors by automatically enforcing positive and negative security policies. Seamlessly integrate API security into your CI/CD pipeline.

Bot Mitigation

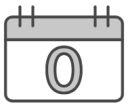
Protect websites, mobile applications, and APIs from automated attacks with advanced bot mitigation that accurately differentiates between good bot traffic and malicious bots. FortiWeb Bot Mitigation provides the visibility and control you need without slowing down your users with unnecessary captchas or challenges.

Machine Learning Improves Detection and Drives Operational Efficiency

FortiWeb's multi-layer approach provides two key benefits: superior threat detection and improved operational efficiency.

FortiWeb's ability to detect anomalous behavior relative to the specific application being protected enables the solution to block unknown, never-before-seen exploits, providing your best protection against zero-day attacks targeting your application.

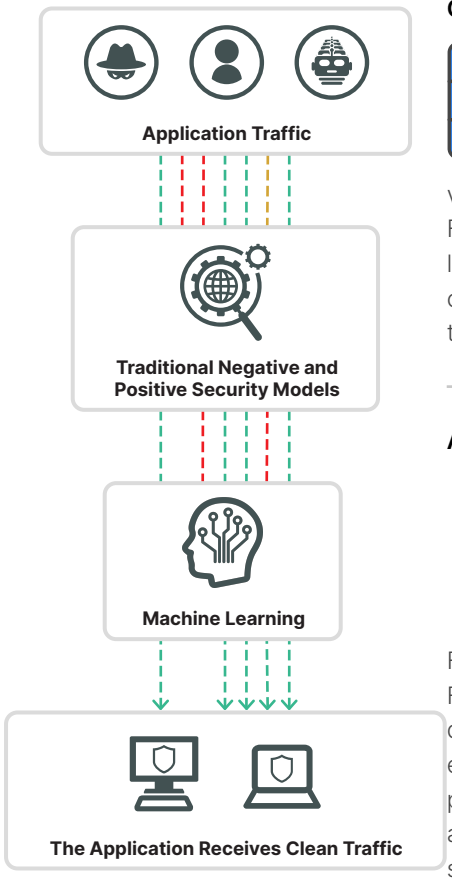
Operationally, FortiWeb machine learning relieves you of time-consuming tasks such as remediating false positives or manually tuning WAF rules. FortiWeb continually updates the model as your application evolves, so there is no need to manually update rules every time you update your application.



FortiWeb enables you to get your code into production faster, eliminating the need for time-consuming manual WAF rules tuning and troubleshooting the false positives that plague less advanced WAFs.

AI-based Threat Analytics Help Zoom In on the Most Important Threats

Without better tools, security teams risk becoming overwhelmed by the volume of events, with many of those events turning out to be of low value when seen in isolation—or even worse, turning out to be false positives after further investigation. This alert fatigue can result in critical security events being missed or overlooked. FortiWeb Threat Analytics uses machine learning algorithms to identify attack patterns across your entire application attack surface and aggregate them into comprehensible security incidents. The solution separates significant threats from informational alerts and false positives by identifying patterns and assigning a severity to help your security team focus on the threats that matter. Investigating security alerts requires context and the ability to connect the dots across multiple events over time. FortiWeb Threat Analytics removes the complexity that comes from manually evaluating alerts by evaluating thousands of alerts and grouping those alerts into incidents based on the patterns identified. With this streamlined view, SOC analysts can focus their efforts on the important threats.



FortiWeb goes beyond traditional negative and positive security models (such as attack signatures, IP address reputation, and protocol validation), and applies a second layer of machine learning-based analytics to detect and block malicious anomalies while minimizing false positives.

Highlights

Comprehensive Web Application Security

Using an advanced multi-layered and correlated approach, FortiWeb provides complete security for your web-based applications from the OWASP Top 10 and many other threats. FortiWeb's first layer of defense uses traditional WAF detection engines (e.g. attack signatures, IP address reputation, protocol validation, and more) to identify and block malicious traffic, powered by intelligence from Fortinet's industry leading security research from FortiGuard Labs. FortiWeb's machine learning detection engine then examines traffic that passes this first layer, using a continuously updated model of your application to identify malicious anomalies and block them as well.

API Discovery and Protection

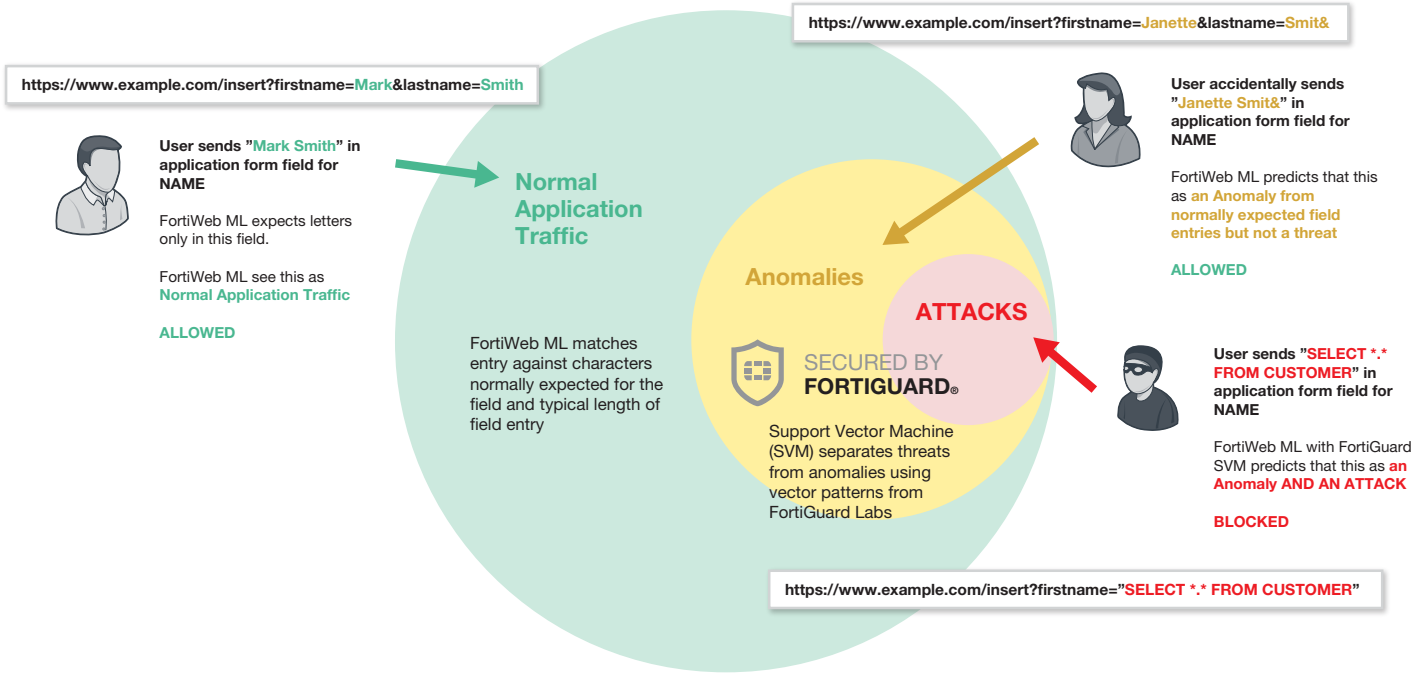
Fueling the digital transformation APIs have become increasingly popular, providing the backbone for mobile applications, automated business to business operations and ease of management across applications. However, with their popularity they also increase the attack surface with additional exposed application surfaces that organizations must secure. Fortinet's FortiWeb web application firewall provides the right tools to address threats to APIs. FortiWeb API Discovery and Protection uses machine learning algorithms to automatically discover APIs by continuously evaluating application traffic. Discovery is an integral role for establishing a positive security model and FortiWeb protects your critical APIs based on your profiled API inventory. FortiWeb can also integrate out of the box policies together with an automatically generated positive security model policy that is based on your organization's schema specification (OpenAPI, XML and generic JSON are supported schemas) to protect against API exploits. FortiWeb schema validation can be integrated into the CI/CD pipeline, automatically generating an updated positive security model policy once the API is updated.

Bot Mitigation

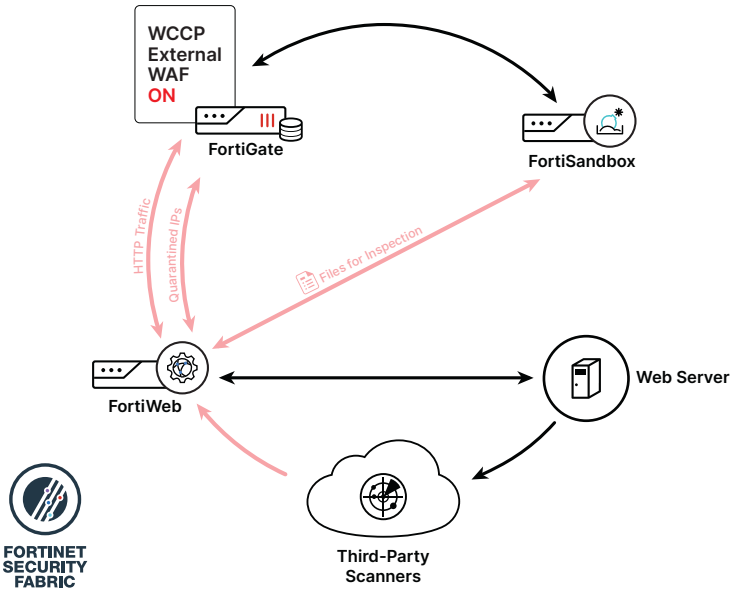
FortiWeb protects against automated bots, webs scrapers, crawlers, data harvesting, credential stuffing and other automated attacks to protect your web assets, mobile APIs, applications, users and sensitive data. Combining machine learning with policies such as threshold based detection, Bot deception and Biometrics based detection with superior good bot identification FortiWeb is able to block malicious bot attacks while reducing friction on legitimate users. With advanced tracking techniques FortiWeb can differentiate between humans, automated requests and repeat offenders, track behavior over time to better identify humans from bots and enforce CAPTCHA challenges when required. Together with FortiView, FortiWeb's graphical analysis dashboard organizations can quickly identify attacks and differentiate from good bots and legitimate users.

Highlights

FortiWeb's machine learning accurately detects anomalies and identifies which are threats. Unlike prevailing auto-learning detection models used by other WAF vendors that treat every anomaly as a threat, FortiWeb's precision nearly eliminates false positive detections and catches attack types that others cannot.



FortiWeb's AI-based machine learning evaluates application requests to determine if they are normal, benign anomalies, or anomalies that are threats.



Integration with other Fortinet Security Fabric elements, including FortiGate and FortiSandbox, delivers APT protection and extends vulnerability scanning with leading third-party providers.

Deep Integration into the Fortinet Security Fabric and Third-Party Scanners

As the threat landscape evolves, many new threats require a multi-pronged approach for protecting web-based applications. Advanced Persistent Threats that target users can take many different forms than traditional single-vector attack types and can evade protections offered only by a single device. FortiWeb's integration with FortiGate and FortiSandbox extend basic WAF protections through synchronization and sharing of threat information to both deeply scan suspicious files and share infected internal sources.

FortiWeb also provides integration with leading third-party vulnerability scanners including Acunetix, HP WebInspect, IBM AppScan, Qualys, ImmuniWeb and WhiteHat to provide dynamic virtual patches to security issues in application environments. Vulnerabilities found by the scanner are quickly and automatically turned into security rules by FortiWeb to protect the application until developers can address them in the application code.

Highlights

Solving the Challenge of False Threat Detections

False positive threat detections can be very disruptive and force many administrators to loosen security rules on their web application firewalls to the point where many often become a monitoring tool rather than a trusted threat avoidance platform. The installation of a WAF may take only minutes, however fine-tuning can take days, or even weeks. Even after setup, a WAF can require regular checkups and tweaks as applications and the environment change.

FortiWeb's AI-based machine learning addresses false positive and negative threat detections without the need to tediously manage whitelists and fine-tune threat detection policies. With near 100% accuracy, the dual layer machine learning engines detect anomalies and then determine if they are threats unlike other methods that block all anomalies regardless of their intent. When combined with other tools, including user tracking, session tracking, and threat weighting, FortiWeb virtually eliminates all false detection scenarios.

Advanced Graphical Analysis and Reporting

FortiWeb includes a suite of graphical analysis tools called FortiView. Similar to other Fortinet products such as FortiGate, FortiWeb gives administrators the ability to visualize and drill-down into key elements of FortiWeb such as server/IP configurations, attack and traffic logs, attack maps, OWASP Top 10 attack categorization, and user activity. FortiView for FortiWeb lets administrators quickly identify suspicious activity in real time and address critical use cases such as origin of threats, common violations, and client/device risks.

Secured by FortiGuard

Fortinet's Award-winning FortiGuard Labs is the backbone for many of FortiWeb's layers in its approach to application security. Offered as five separate options, you can choose the FortiGuard services you need to protect your web applications. FortiWeb IP address reputation service protects you from known attack sources like botnets, spammers, anonymous proxies, and sources known to be infected with malicious software.

FortiWeb Security Service is designed just for FortiWeb including items such as application layer signatures, machine learning threat models, malicious robots, suspicious URL patterns, and web vulnerability scanner updates. Credential Stuffing Defense checks login attempts against FortiGuard's list of compromised credentials and can take actions ranging from alerts to blocking logins from suspected stolen user ids and passwords. The FortiWeb Cloud Sandbox subscription enables FortiWeb to integrate with Fortinet's cloud-sandbox service. Finally, FortiWeb offers FortiGuard's top-rated antivirus engine that scans all file uploads for threats that can infect your servers or other network elements.

VM and Public Cloud Options

FortiWeb provides maximum flexibility in supporting your virtual and hybrid environments. The virtual versions of FortiWeb support all the same features as our hardware-based devices and can be deployed in VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM, and Docker platforms. FortiWeb is also available for AWS, Azure, Google Cloud, and Oracle Cloud as a VM, and as WAF as a Service. For more information, see Fortiweb-Cloud.com.

Features

Deployment Options

- Reverse Proxy
- Inline Transparent
- True Transparent Proxy
- Offline Sniffing
- WCCP

Web Security

- AI-based Machine Learning
- Automatic profiling (white list)
- Web server and application signatures (black list)
- IP address reputation
- IP address geolocation
- HTTP RFC compliance
- Native support for HTTP/2
- WebSocket protection and signature enforcement
- Man in the Browser (MiTB) protection

Application Attack Protection

- OWASP Top 10
- Cross Site Scripting
- SQL Injection
- Cross Site Request Forgery
- Session Hijacking
- Built-in Vulnerability Scanner
- Third-party scanner integration (virtual patching)
- File upload scanning with AV and sandbox

Security Services

- Malware detection
- Virtual patching
- Protocol validation
- Brute force protection
- Cookie signing and encryption
- Threat scoring and weighting
- Syntax-based SQLi and XSS detection
- HTTP Header Security
- Custom error message and error code handling
- Operating system intrusion signatures
- Known threat and zero-day attack protection
- L4 Stateful Network Firewall
- DoS prevention
- Advanced correlation protection using multiple security elements
- Data leak prevention
- Web Defacement Protection

Application Delivery

- Layer 7 server load balancing
- URL Rewriting
- Content Routing
- HTTPS/SSL Offloading
- HTTP Compression
- Caching

Authentication

- Active and passive authentication
- Site Publishing and SSO
- RSA Access for 2-factor authentication
- LDAP, RADIUS, and SAML support
- SSL client certificate support
- CAPTCHA and Real Browser Enforcement (RBE)

API Protection

- Machine Learning based API Discovery and Protection
- XML and JSON protocol conformance
- CI/CD integration
- Schema verification
- API Gateway
- Web services signatures

Bot Mitigation

- Machine Learning based Bot Mitigation
- Biometrics Based Detection
- Threshold Based Detection
- Bot Deception
- Know Bots

Management and Reporting

- Web user interface
- Command line interface
- FortiView graphical analysis and reporting tools
- Central management for multiple FortiWeb devices
- Active/Active HA Clustering
- REST API
- Centralized logging and reporting
- User/device tracking
- Real-time dashboards
- Bot dashboard
- OWASP Top 10 attack categorization
- Geo IP Analytics
- SNMP, Syslog and Email Logging/ Monitoring
- Administrative Domains with full RBAC

Other

- IPv6 Ready
- HTTP/2 to HTTP 1.1 translation
- HSM Integration
- Seamless PKI integration
- Attachment scanning for ActiveSync/MAPI applications, OWA, and FTP
- High Availability with Config-sync for syncing across multiple active appliances
- Auto setup and default configuration settings for simplified deployment
- Setup Wizards for common applications and databases
- Preconfigured for common Microsoft applications; Exchange, SharePoint, OWA
- OpenStack support for FortiWeb VMs
- Predefined security policies for Drupal and Wordpress applications
- WebSockets support

Specifications



	FORTIWEB 100E	FORTIWEB 400E	FORTIWEB 600E
Hardware			
10/100/1000 Interfaces (RJ-45 ports)	4	4 GE RJ45, 4 SFP GE	4 GE RJ45 (2 bypass), 4 SFP GE
10G BASE-SR SFP+ Ports	—	—	—
SSL/TLS Processing	Software	Software	Hardware
USB Interfaces	2	2	2
Storage	32 GB SSD	480 GB SSD	480 GB SSD
Form Factor	Desktop	1U	1U
Trusted Platform Module (TPM)	No	No	No
Power Supply	Single	Single	Dual
System Performance			
Throughput	50 Mbps	250 Mbps	750 Mbps
Latency	<5ms	<5ms	<5ms
High Availability	Active/Passive, Active/Active Clustering	Active/Passive, Active/Active Clustering	Active/Passive, Active/Active Clustering
Application Licenses	Unlimited	Unlimited	Unlimited
Administrative Domains	—	32	32
All performance values are "up to" and vary depending on the system configuration.			
Dimensions			
Height x Width x Length (inches)	1.61 × 8.27 × 5.24	1.73 × 17.24 × 16.38	1.73 × 17.24 × 16.38
Height x Width x Length (mm)	41 × 210 × 133	44 × 438 × 416	44 × 438 × 416
Weight	2.3 lbs (1.1 kg)	22 lbs (9.97 kg)	22 lbs (9.97 kg)
Rack Mountable	Optional	Yes	Yes
Environment			
Power Required	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz
Maximum Current	110V/1.2A, 220V/1.2A	100V/5A, 240V/3A	100V/5A, 240V/3A
Power Consumption (Average)	18 W	109 W	109 W
Heat Dissipation	74 BTU/h	446.3 BTU/h	446.3 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Storage Temperature	-13°F to 158°F (-25°C to 70°C)	-13°F to 158°F (-25°C to 70°C)	-13°F to 158°F (-25°C to 70°C)
Forced Airflow	N/A (fanless)	Front to Back	Front to Back
Humidity	10% to 90% non-condensing	10% to 90% non-condensing	10% to 90% non-condensing
Compliance			
Safety Certifications	FCC Class A Part 15, RCM, VCCI, CE, UL/cUL, CB	FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL

Specifications


	FORTIWEB 400F	FORTIWEB 600F
Hardware		
10/100/1000 Interfaces (RJ-45 ports)	4 GE RJ45, 4 SFP GE	4 GE RJ45 (2 bypass), 4 SFP GE
10G BASE-SR SFP+ Ports	—	—
SSL/TLS Processing	Software	Hardware
USB Interfaces	2	2
Storage	480 GB SSD	480 GB SSD
Form Factor	1U	1U
Trusted Platform Module (TPM)	No	No
Power Supply	Single	Dual
System Performance		
Throughput	500 Mbps	1 Gbps
Latency	<5ms	<5ms
High Availability	Active/Passive, Active/Active Clustering	Active/Passive, Active/Active Clustering
Application Licenses	Unlimited	Unlimited
Administrative Domains	32	32
All performance values are "up to" and vary depending on the system configuration.		
Dimensions		
Height x Width x Length (inches)	1.73 × 17.24 × 16.53	1.73 × 17.24 × 16.54
Height x Width x Length (mm)	44 × 438 × 420	44 × 438 × 420
Weight	11.91 lbs (5.4 kg)	14.99 lbs (6.8 kg)
Rack Mountable	Yes	Yes
Environment		
Power Required	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz
Maximum Current	100V/1.53A, 240V/0.64A	100V/1.66A, 240V/0.69A
Power Consumption (Average)	127.33 W	138.74 W
Heat Dissipation	521.38 BTU/h	568.09 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Storage Temperature	-13°F to 158°F (-25°C to 75°C)	-13°F to 158°F (-25°C to 75°C)
Forced Airflow	Front to Back	Front to Back
Humidity	5% to 95% non-condensing	5% to 95% non-condensing
Compliance		
Safety Certifications	FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL

Specifications




	FORTIWEB 1000F	FORTIWEB 2000F	FORTIWEB 3000F	FORTIWEB 4000F
Hardware				
10/100/1000 Interfaces (RJ45 ports)	8 bypass, 4x SFP GE (non-bypass)	4GE (4 bypass), 4 SFP GE	8GE (8 bypass)	8GE (8 bypass)
10G BASE-SR SFP+ Ports	2	4	10 (2 bypass)	10 (2 bypass)
40G QSFP	-	-	-	2 bypass
SSL/TLS Processing	Hardware	Hardware	Hardware	Hardware
USB Interfaces	2	2	2	2
Storage	2× 480 GB SSD	2 × 480 GB SSD	2 × 960 GB SSD	2 × 960 GB SSD
Form Factor	2U	2U	2U	2U
Trusted Platform Module (TPM)	No	Yes	Yes	Yes
Power Supply	Dual Hot Swappable	Dual Hot Swappable	Dual Hot Swappable	Dual Hot Swappable
System Performance				
Throughput	2.5 Gbps	5 Gbps	10 Gbps	70 Gbps
Latency	<5ms	<5ms	<5ms	<5ms
High Availability	Active/Passive, Active/Active Clustering	Active/Passive, Active/Active Clustering	Active/Passive, Active/Active Clustering	Active/Passive, Active/Active Clustering
Application Licenses	Unlimited	Unlimited	Unlimited	Unlimited
Administrative Domains	64	96	96	192
All performance values are “up to” and vary depending on the system configuration.				
Dimensions				
Height x Width x Length (inches)	3.46 × 16.93 × 19.73	3.5 × 17.2 × 20.8	3.5 × 17.5 × 22.6	3.5 × 17.5 × 22.6
Height x Width x Length (mm)	88 × 430 × 501.20	88 × 438 × 530	88 × 444 × 574	88 × 444 × 574
Weight	28 lbs (12.8 kg)	33 lbs (15 kg)	56.2 lbs (22.5 kg)	56.2 lbs (22.5 kg)
Rack Mountable	Yes, with flanges	Yes	Yes	Yes
Environment				
Power Required	100–240V AC, 50–60 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz
Maximum Current	100V/5A, 240V/3A	120V/6A, 240V/3A	120V/2.6A, 240V/1.3A	120V/3A, 240V/1.5A
Power Consumption (Average)	140 W	200 W	200 W	248.5 W
Heat Dissipation	471 BTU/h	1433 BTU/h	1045.5 BTU/h	1219.8 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Storage Temperature	-4°F to 158°F (-20°C to 70°C)	-4°F to 158°F (-20°C to 70°C)	-4°F to 158°F (-20°C to 70°C)	-4°F to 158°F (-20°C to 70°C)
Forced Airflow	Front to Back	Front to Back	Front to Back	Front to Back
Humidity	5% to 90% non-condensing	5% to 90% non-condensing	5% to 90% non-condensing	5% to 90% non-condensing
Compliance				
Safety Certifications	FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL

Specifications

VIRTUAL MACHINES	FORTIWEB-VM (1 VCPU)	FORTIWEB-VM (2 VCPU)	FORTIWEB-VM (4 VCPU)	FORTIWEB-VM (8 VCPU)	FORTIWEB-VM (16 VCPU)
System Performance					
HTTP Throughput	25 Mbps	100 Mbps	500 Mbps	3 Gbps	6 Gbps
Application Licenses	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Administrative Domains	4 to 64 based on the amount of memory allocated				
Virtual Machine					
Hypervisor Support	VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud, and Oracle Cloud. Please see FortiWeb VM Installation Guide for versions supported.				
vCPU Support (Minimum / Maximum)	1	2	2 / 4	2 / 8	2 / 16
Network Interface Support (Minimum / Maximum)	1 / 10	1 / 10	1 / 10	1 / 10	1 / 10
Storage Support (Minimum / Maximum)	40 GB / 2 TB	40 GB / 2 TB	40 GB / 2 TB	40 GB / 2 TB	40 GB / 2 TB
Memory Support (Minimum / Maximum)	1024 MB / Unlimited for 64-bit	1024 MB / Unlimited for 64-bit	1024 MB / Unlimited for 64-bit	1024 MB / Unlimited for 64-bit	1024 MB / Unlimited for 64-bit
Recommended Memory	8 GB	8 GB	16 GB	32 GB	64 GB
High Availability Support	Yes	Yes	Yes	Yes	Yes

Actual performance values may vary depending on the network traffic and system configuration. Performance metrics were observed using 4 x Intel(R) Xeon(R) Gold 6242 CPU @ 2.80GHz running VMware ESXi 6.7 with 8 GB of vRAM assigned to the 1 vCPU and 2 vCPU FortiWeb Virtual Appliance, 16 GB assigned to the 4 vCPU, 32 GB assigned to the 8 vCPU and 64 GB assigned to the 16 vCPU FortiWeb Virtual Appliance.

CONTAINER APPLIANCES	FORTIWEB-VMC01	FORTIWEB-VMC02	FORTIWEB-VMC04	FORTIWEB-VMC08
System Performance				
HTTP Throughput (Maximum)	25 Mbps	100 Mbps	500 Mbps	3 Gbps
Application Licenses	Unlimited	Unlimited	Unlimited	Unlimited
Administrative Domains	4 to 64 based on the amount of memory allocated			
Virtual Appliance				
Container Manager Support	Docker			
Network Interface Support (Minimum / Maximum)	1 / 10	1 / 10	1 / 10	1 / 10
Storage Support (Minimum / Maximum)	30 GB / 500 GB	30 GB / 500 GB	30 GB / 500 GB	30 GB / 500 GB
Memory Support (Minimum)	4 GB	4 GB	4 GB	4 GB
Recommended Memory	8 GB	8 GB	8 GB	8 GB
High Availability Support	No	No	No	No

Throughputs and other metrics are maximum values permitted for each version. Actual performance values may vary depending on the network traffic and system configuration.

Ordering Information

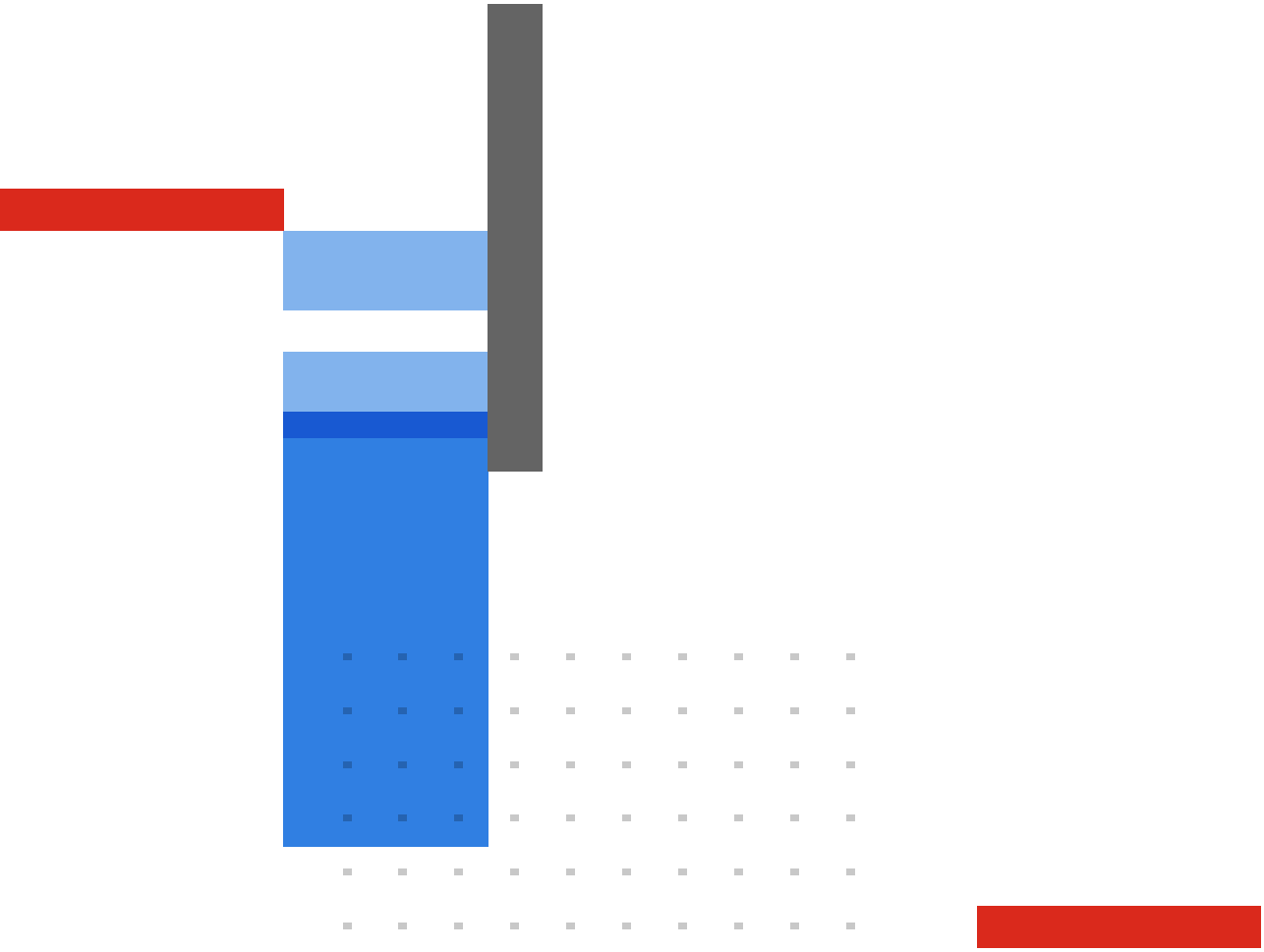
Product	SKU	Description
FortiWeb 100E	FWB-100E	Web Application Firewall — 4x GE RJ45 ports, 4 GB RAM,1× 32 GB SSD storage.
FortiWeb 400E	FWB-400E	Web Application Firewall — 4x GE RJ45 ports, 4x GE SFP ports, 480 GB SSD storage.
FortiWeb 600E	FWB-600E	Web Application Firewall — 4x GE RJ45 ports (2x bypass), 4x GE SFP ports, 480 GB SSD storage.
FortiWeb 400F	FWB-400F	Web Application Firewall — 4x GE RJ45 ports, 4x GE SFP ports, 480 GB SSD storage.
FortiWeb 600F	FWB-600F	Web Application Firewall — 4x GE RJ45 (2 bypass), 4x GE SFP ports, 480 GB SSD storage.
FortiWeb 1000F	FWB-1000F	Web Application Firewall — 2× 10 GE SFP+ ports, 8x GE RJ45 bypass ports, 4x GE SFP ports, 2 x GE management ports, dual AC power supplies, 2× 480 GB SSD storage
FortiWeb 2000F	FWB-2000F	Web Application Firewall - 4 × 10GE SFP+ ports, 4 x GE RJ45 bypass ports, 4 x GE SFP ports, 2 x GE management ports, dual AC power supplies, 2×480GB SSD storage.
FortiWeb 3000F	FWB-3000F	Web Application Firewall - 10 × 10GE SFP+ ports (2 bypass), 8 x GE RJ45 bypass ports, 2 x GE management ports, dual AC power supplies, 2×960GB SSD storage.
FortiWeb 4000F	FWB-4000F	Web Application Firewall - 2 × 40GE bypass ports, 10 × 10GE SFP+ ports (2 bypass), 8 x GE RJ45 bypass ports, 2x GE management ports, dual AC power supplies, 2×960GB SSD storage.
FortiWeb-VM01	FWB-VM01	FortiWeb-VM, up to 1 vCPU supported. 64-bit OS.
FortiWeb-VM02	FWB-VM02	FortiWeb-VM, up to 2 vCPUs supported. 64-bit OS.
FortiWeb-VM04	FWB-VM04	FortiWeb-VM, up to 4 vCPUs supported. 64-bit OS.
FortiWeb-VM08	FWB-VM08	FortiWeb-VM, up to 8 vCPUs supported. 64-bit OS.
FortiWeb-VM16	FWB-VM16	FortiWeb-VM, up to 16 vCPUs supported. 64-bit OS.
FortiWeb-VMC01	FWB-VMC01	FWB-VMC01 for container-based environments. Up to 25 Mbps throughput.
FortiWeb-VMC02	FWB-VMC02	FWB-VMC02 for container-based environments. Up to 100 Mbps throughput.
FortiWeb-VMC04	FWB-VMC04	FWB-VMC04 for container-based environments. Up to 500 Mbps throughput.
FortiWeb-VMC08	FWB-VMC08	FWB-VMC08 for container-based environments. Up to 2 Gbps throughput.
Central Manager 10	FWB-CM-BASE	FortiWeb Central Manager license key, manage up to 10 FortiWeb devices, VMware vSphere.
Central Manager Unlimited	FWB-CM-UL	FortiWeb Central Manager license key, manage unlimited number of FortiWeb devices, VMware vSphere.

The following SKUs adopt the annual subscription licensing scheme:

Product	SKU	Description
FortiWeb-VM01-S Standard	FC1-10-WBVMS-916-02-DD	Subscription license for FortiWeb-VM (1 CPU) with Standard bundle included.
FortiWeb-VM01-S Advanced	FC1-10-WBVMS-633-02-DD	Subscription license for FortiWeb-VM (1 CPU) with Advanced bundle included.
FortiWeb-VM02-S Standard	FC2-10-WBVMS-916-02-DD	Subscription license for FortiWeb-VM (2 CPU) with Standard bundle included.
FortiWeb-VM02-S Advanced	FC2-10-WBVMS-633-02-DD	Subscription license for FortiWeb-VM (2 CPU) with Advanced bundle included.
FortiWeb-VM04-S Standard	FC3-10-WBVMS-916-02-DD	Subscription license for FortiWeb-VM (4 CPU) with Standard bundle included.
FortiWeb-VM04-S Advanced	FC3-10-WBVMS-633-02-DD	Subscription license for FortiWeb-VM (4 CPU) with Advanced bundle included.
FortiWeb-VM08-S Standard	FC4-10-WBVMS-916-02-DD	Subscription license for FortiWeb-VM (8 CPU) with Standard bundle included.
FortiWeb-VM08-S Advanced	FC4-10-WBVMS-633-02-DD	Subscription license for FortiWeb-VM (8 CPU) with Advanced bundle included.
FortiWeb-VM16-S Standard	FC5-10-WBVMS-916-02-DD	Subscription license for FortiWeb-VM (16 CPU) with Standard bundle included.
FortiWeb-VM16-S Advanced	FC5-10-WBVMS-633-02-DD	Subscription license for FortiWeb-VM (16 CPU) with Advanced bundle included.

FortiCare Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare Services help thousands of organizations get the most from our Fortinet Security Fabric solution. Our lifecycle portfolio offers Design, Deploy, Operate, Optimize, and Evolve services. Operate services offer device-level FortiCare Elite service with enhanced SLAs to meet our customer's operational and availability needs. In addition, our customized account-level services provide rapid incident resolution and offer proactive care to maximize the security and performance of Fortinet deployments.



FORTINET

www.fortinet.com

January 10, 2024

FWEB-DAT-R70-20240110