

技术参数表

FortiWeb™

FortiWeb 100D, 400D, 600D, 1000D, 1000E, 2000E, 3000E, 3010E, 4000E, VM 和容器

FortiWeb 是一款Web应用防火墙 (WAF)，可保护托管的Web应用免受针对已知和未知漏洞的攻击。FortiWeb 使用人工智能增强的多层次和关联检测方法，为应用程序提供针对已知漏洞和零日威胁的防护。



无以伦比的防护效能

多核处理器技术与基于硬件的SSL工具相结合，提供超高的 WAF 安全过滤吞吐性能。



应用程序防护

防御 OWASP 排名前十的应用程序攻击，包括跨站点脚本攻击和 SQL 注入攻击。



基于人工智能的机器学习威胁检测

采用双层机器学习引擎来检测应用请求异常并确定它们是否构成威胁。

亮点

- 运用基于人工智能的行为扫描关联威胁检测
- WAF 安全过滤吞吐性能高达 20 Gbps
- 通过与 Fortinet Security Fabric 集成提高防护能力
- 可视化分析工具发现高级威胁
- 第三方集成和虚拟补丁技术



FortiCare 全球全天支持
support.fortinet.com



FortiGuard 安全服务
www.fortiguard.com

第三方认证



亮点

FortiWeb 提供全面的 Web 应用安全防护

FortiWeb 运用先进的多层次关联检测方法为您的外部和内部web应用提供完整的安全防护, 防御 OWASP 排名前十的应用程序攻击和许多其他威胁。FortiWeb 的核心是基于人工智能的检测引擎

使用机器学习来识别偏离正常模式的请求, 并采取措施保护应用程序免受已知和未知的零日威胁。



FortiWeb 的多层次关联威胁检测方法可针对以应用程序漏洞为攻击目标的已知和未知零日威胁提供安全防护。

由FortiGuard威胁研究与响应实验室支持的双层机器学习模型

尽管 Web 应用防火墙是针对基于Web应用的攻击的最佳防御手段, 但是为了防止 WAF 误判而进行的微调却会相当繁琐而耗时。FortiWeb 通过两个独立的检测引擎, 使用基于人工智能的机器学习方法解决了这一难题。

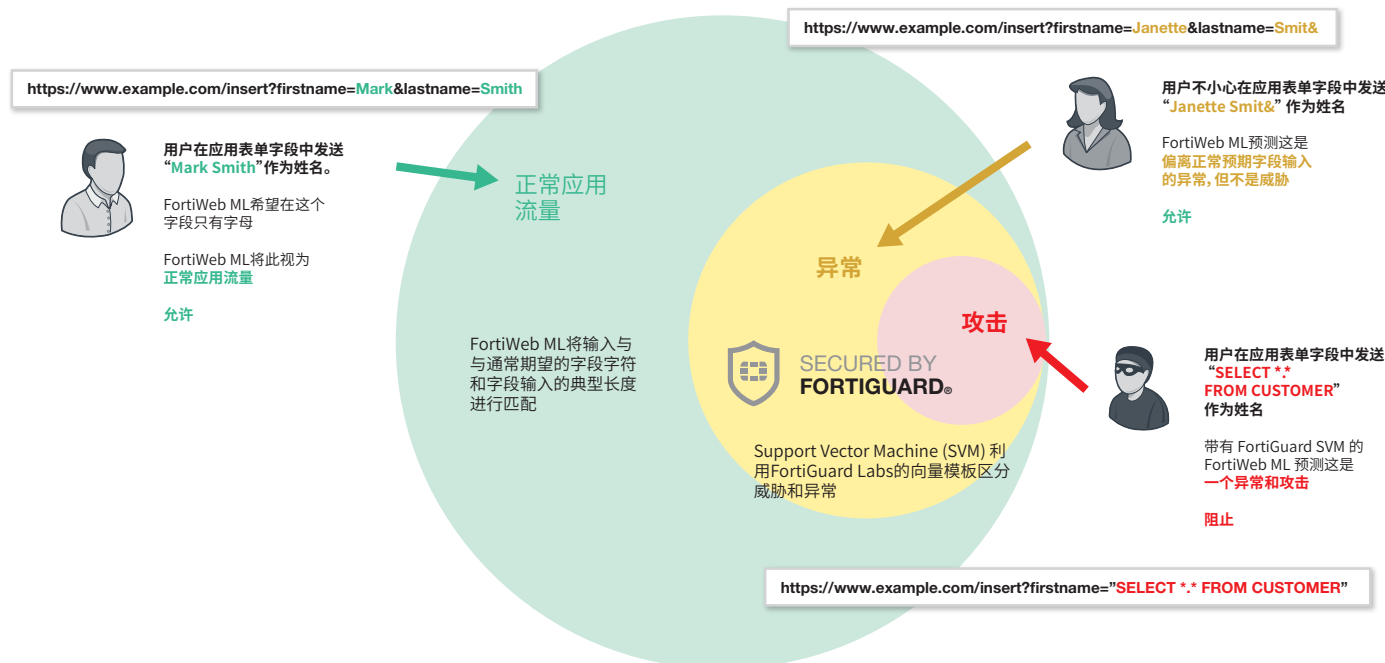
第一层自动和动态地监视所有应用程序元素的活动是否偏离了预测

的条目。如果第一个引擎标记出确定为异常的内容, 则将其发送到第二层机器学习层, 以评估它是威胁还是仅仅是一个此前未见的良性变化, 例如输入错误或新字符。如果是攻击, 那么 FortiWeb 可以采取行动, 例如记录、警报和/或阻断请求。第二个机器学习层利用包含在 FortiWeb 解决方案中的威胁模型, 并通过 FortiGuard WAF 安全服务进行更新, 以提供需要模型重新训练和测试的新威胁保护。

亮点

FortiWeb 的机器学习可以准确地检测异常,更重要的是识别出哪些是真正的威胁。与其它 WAF 供应商普遍提供的那种把所有异常都视

为威胁的自动学习检测模型不同, FortiWeb 的精度几乎消除了误判检测并捕获了其它设备无法捕获的攻击类型。

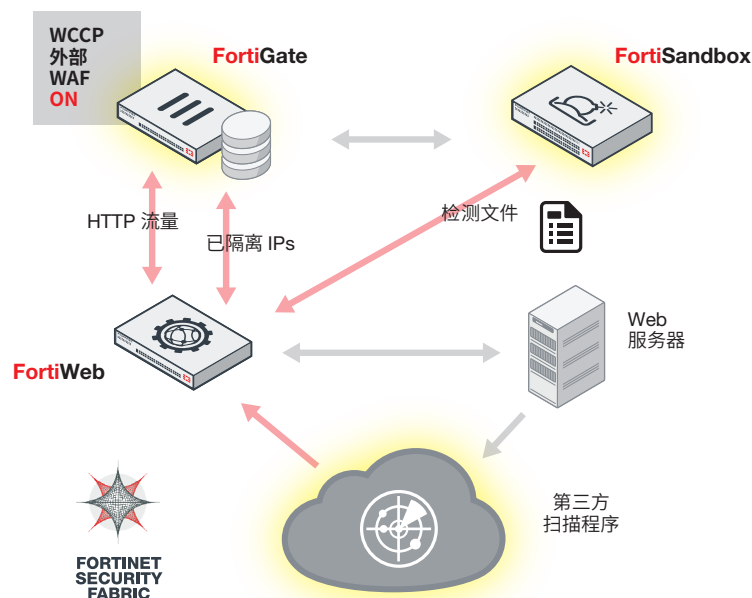


FortiWeb 基于人工智能的机器学习评估应用请求, 确定它们是正常的、良性的异常还是威胁异常。

与 Fortinet Security Fabric 和第三方扫描程序深度集成

随着威胁概况不断变化, 需要针对许多新威胁采取多管齐下的方法保护 web 应用。与传统的单一向量攻击类型相比, 针对用户的高级持续威胁可能采取多种不同形式, 并且规避仅由单个设备提供的安全防护措施。FortiWeb 与 FortiGate 和 FortiSandbox 的集成通过同步和共享威胁信息, 深度扫描可疑文件并共享已感染的内部源, 从而扩展 WAF 基础保护能力。

FortiWeb 还可以与领先的第三方漏洞扫描产品集成, 包括 Acunetix, HP WebInspect, IBM AppScan, Qualys, IBM QRadar 和 WhiteHat, 针对应用程序环境中的安全问题提供动态虚拟补丁。扫描程序发现的漏洞很快就会由 FortiWeb 自动变成安全规则, 为应用程序提供防护, 直至开发人员能够在应用程序代码中解决这些问题。



与其它 Fortinet Security Fabric 架构中的其他解决方案, 包括 FortiGate 和 FortiSandbox, 的集成, 提供 APT 防护并与领先的第三方供应商合作扩展漏洞扫描范围。

亮点

解决威胁检测误报的问题

威胁检测的误报问题破坏性非常强,迫使许多管理员放松其 Web 应用防火墙中的安全规则,往往会使防火墙成为一个监控工具,而不是一个受信任的威胁防护平台。安装 WAF 可能只需要几分钟,但是配置调优可能需要几天甚至几周的时间。即使在设置完毕之后,也需要随着应用程序和环境的变化对 WAF 进行定期检查和调整。

FortiWeb 基于人工智能的机器学习解决了正确的和错误的威胁检测误报,无需繁琐地管理白名单和微调威胁检测策略。双层机器学习引擎具有接近100%的准确度,可以检测异常,然后判断它们是否真的是威胁,这一点与那些对所有异常都加以阻断而不考虑其意图的其它方法有所不同。与其它工具,包括用户跟踪、设备指纹识别和威胁权衡,结合使用时, FortiWeb 几乎可以消除所有误报场景。

API 安全

近年来,为了帮助加快应用交付并简化应用到应用的可访问性,API 的使用变得越来越流行。随着 API 成为很多应用的组成部分,它们已经成为应用层攻击和利用的一个新向量,类似于传统的基于 Web 的应用。

FortiWeb 提供了一种易于部署的解决方案,通过攻击签名,参数安全加固和其它很多工具来保护您的 API。使用 FortiWeb,在它的全面保护下可以轻松发布您的应用程序及其 API。

先进的图形分析和报告

FortiWeb 包含一套称为 FortiView 的图形分析工具。与 FortiGate 等其他 Fortinet 产品相似, FortiWeb 使管理员能够实时可见并深入了解 FortiWeb 关键要素,比如服务器/IP 配置、攻击和流量日志、攻击地图、OWASP 十大攻击类别和用户活动。FortiWeb 的 FortiView 确保管理员实时快速识别可疑活动,并及时处理关键事件,例如威胁来源、常见违规和客户端/设备风险。

FortiGuard 提供安全防护

屡获殊荣的 FortiGuard Labs 是 FortiWeb 多层架构在提供应用安全防护时的强大支柱。FortiGuard 提供 5 个独立的选项,您可以选择需要的服务保护您的网页应用程序。FortiWeb IP 信誉评级服务针对已知攻击源,比如僵尸网络、垃圾邮件发送者、匿名代理和已知感染恶意软件的来源提供安全防护。FortiWeb 安全服务专为 FortiWeb 设计,包括应用层签名、机器学习威胁模型、恶意机器人、可疑 URL 模板、和网页漏洞扫描程序更新等项目。凭证填充防御会根据 FortiGuard 的被窃取认证信息列表,检查登录尝试,并采取相应措施,从报警到阻止可疑被盗用户 ID 和密码登录。FortiSandbox Cloud 订阅使 FortiWeb 能够与 Fortinet 的云沙盒服务集成。最后, FortiWeb 提供 FortiGuard 的顶级防病毒引擎,该引擎可以扫描所有文件上传,检测可能感染服务器或其他网络要素的威胁。

支持虚拟机与公有云部署形式

FortiWeb 在支持虚拟和混合云环境方面具有最大的灵活性。FortiWeb 的虚拟版本支持我们基于硬件的设备的所有相同功能,并可部署在 VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM 和 Docker 平台中。FortiWeb 也可用于 Amazon Web Services, Microsoft Azure, Google Cloud 和 Oracle Cloud。



FortiView for FortiWeb

功能

部署选项

- 反向代理
- 内联透明
- 真正透明代理
- 离线嗅探
- WCCP

网络安全

- 基于AI的机器学习
- 自动分析(白名单)
- 网络服务器和应用签名(黑名单)
- IP信誉
- IP地理信息
- HTTP RFC合规
- 支持HTTP / 2
- OpenAPI 3.0验证
- WebSocket保护和签名实施
- 浏览器中人(MiTB)保护

应用攻击防护

- OWASP Top 10
- 跨站脚本攻击
- SQL 注入攻击
- 跨站请求伪装攻击
- 会话劫持
- 内置漏洞扫描程序
- 第三方扫描程序集成(虚拟补丁)
- 使用 AV 和沙箱进行文件上传扫描

安全服务

- Web 服务签名
- XML 和 JSON协议合规
- 恶意软件检测
- 虚拟补丁
- 协议验证
- 暴力破解保护
- Cookie 签名和加密
- 威胁评分和权重
- 基于句法的 SQLi 检测
- HTTP header 安全
- 自定义错误消息和错误代码处理
- 操作系统入侵签名
- 已知的威胁和零日攻击防护
- L4状态网络防火墙
- DoS 防护
- 使用多重安全要素提供高级关联防护
- 防止数据泄漏
- 网页篡改防护

应用交付

- 7层服务器负载均衡
- URL 重写
- 内容路由
- HTTPS / SSL 卸载
- HTTP 压缩
- 缓存

认证

- 主动和被动认证
- 网站发布和 SSO
- 双因素身份验证的 RSA 访问
- LDAP, RADIUS 和 SAML 支持
- SSL 客户端证书支持
- CAPTCHA 和真实浏览器强制(RBE)

管理和报告

- Web 用户界面
- 命令行界面
- FortiView 图形分析和报告工具
- 集中管理多台 FortiWeb 设备
- 主动/主动 HA 集群
- REST API
- 集中日志记录和报告
- 用户/设备跟踪
- 实时仪表盘
- Bot 仪表盘
- OWASP 十大攻击类别
- Geo IP 分析
- SNMP, Syslog 和邮件日志/监控
- 具有全RBAC的管理域

其它

- 支持 IPv6
- HTTP / 2 到 HTTP 1.1 转换
- HSM 集成
- 无缝 PKI 集成
- 对 ActiveSync / MAPI 应用程序, OWA 和 FTP 进行附件扫描
- 具有Config-sync功能的高可用性, 用于跨多个在用应用的同步
- 自动设置和默认配置设置简化了部署
- 面向常见应用和数据库的设置向导
- 面向常见 Microsoft 应用程序; Exchange, SharePoint, OWA 预先配置
- 对 FortiWeb VM 的 OpenStack 支持
- 面向 Drupal 和 Wordpress 应用程序的预定义安全策略
- WebSockets支持

规格

	FORTIWEB 100D	FORTIWEB 400D	FORTIWEB 600D	FORTIWEB 1000D	FORTIWEB 1000E
硬件					
10/100/1000 接口 (RJ-45)	4	4 GE RJ45, 4 SFP GE	4 GE RJ45 (2 bypass), 4 SFP GE	6 (4 bypass), 2x SFP GE (non-bypass)	6 (4 bypass), 4x SFP GE (non-bypass)
10G BASE-SR SFP+ 接口	0	0	0	0	2
SSL / TLS 处理	软件	软件	软件	软件	硬件
USB 接口	2	2	2	2	2
存储	16 GB	240 GB 固态硬盘	240 GB 固态硬盘	2x 2 TB	2x 1 TB
外观	桌面	1U	1U	2U	2U
电源	单电源	单电源	双电源	双热插拔电源	双热插拔电源
系统性能					
吞吐量	25 Mbps	100 Mbps	250 Mbps	1 Gbps	1.3 Gbps
延时	亚毫秒	亚毫秒	亚毫秒	亚毫秒	亚毫秒
高可用性	主动/被动, 主动/主动群集	主动/被动, 主动/主动群集	主动/被动, 主动/主动群集	主动/被动, 主动/主动群集	主动/被动, 主动/主动群集
应用程序许可	无限制	无限制	无限制	无限制	无限制
管理域	0	32	32	64	64
所有性能值均为“高达”，并取决于系统配置。					
尺寸					
高x宽x长 (英寸)	1.61 x 8.27 x 5.24	1.73 x 17.24 x 16.38	1.73 x 17.24 x 16.38	3.50 x 17.24 x 14.49	3.46 x 16.93 x 19.73
高x宽x长 (毫米)	41 x 210 x 133	44 x 438 x 416	44 x 438 x 416	88 x 438 x 368	88 x 430 x 501.20
重量	2.3 lbs (1.1 千克)	22 lbs (9.97 千克)	22 lbs (9.97 千克)	27.6 lbs (12.5 千克)	28 lbs (12.8 千克)
机架安装	可选	是	是	是, 带配件	是, 带配件
环境					
所需电源	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz
最大电流	110V/1.2A, 220V/1.2A	100V/5A, 240V/3A	100V/5A, 240V/3A	100V/5A, 240V/3A	100V/5A, 240V/3A
功耗 (平均)	18 W	109 W	109 W	115 W	140 W
散热	74 BTU/h	446.3 BTU/h	446.3 BTU/h	471 BTU/h	471 BTU/h
工作温度	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)
存储温度	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-4–158°F (-20–70°C)
湿度	10% 至 90% (无凝结)	10% 至 90% (无凝结)	10% 至 90% (无凝结)	5% 至 95% (无凝结)	5% 至 90% (无凝结)
合规					
安全认证	FCC Class A Part 15, C-Tick, VCCI, CE, UL/cUL, CB	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL



FortiWeb 100D



FortiWeb 400D



FortiWeb 600D



FortiWeb 1000D



FortiWeb 1000E

规格

	FORTIWEB 2000E	FORTIWEB 3000E	FORTIWEB 3010E	FORTIWEB 4000E
硬件				
10/100/1000 接口 (RJ-45)	4 bypass, 4 SFP GE (non-bypass)	8 bypass, 4 SFP GE (non-bypass)	8 bypass, 4 SFP GE (non-bypass)	8 bypass, 4 SFP GE (non-bypass)
10G BASE-SR SFP+ 接口	2	4	4 (2 bypass)	4 (2 bypass)
SSL / TLS 处理	硬件	硬件	硬件	硬件
USB 接口	2	2	2	2
存储	2x 1 TB	2x 2 TB	2x 2 TB	2x 2 TB
外观	2U	2U	2U	2U
电源	双热插拔电源	双热插拔电源	双热插拔电源	双热插拔电源
系统性能				
吞吐量	2.5 Gbps	5 Gbps	5 Gbps	20 Gbps
延时	亚毫秒	亚毫秒	亚毫秒	亚毫秒
高可用性	主动/被动, 主动/主动群集	主动/被动, 主动/主动群集	主动/被动, 主动/主动群集	主动/被动, 主动/主动群集
应用程序许可	无限制	无限制	无限制	无限制
管理域	64	64	64	64
所有性能值均为“高达”，并取决于系统配置。				
尺寸				
高x宽x长 (英寸)	3.5 x 17.2 x 20.8	3.5 x 17.5 x 22.6	3.5 x 17.5 x 22.6	3.5 x 17.5 x 22.6
高x宽x长 (毫米)	88 x 438 x 530	88 x 444 x 574	88 x 444 x 574	88 x 444 x 574
重量	33 lbs (15 千克)	56.2 lbs (22.5 千克)	56.2 lbs (22.5 千克)	56.2 lbs (22.5 kg)
机架安装	是	是	是	是
环境				
所需电源	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz
最大电流	120V/6A, 240V/3A	120V/2.6A, 240V/1.3A	120V/2.6A, 240V/1.3A	120V/3A, 240V/1.5A
功耗 (平均)	200 W	200 W	200 W	248.5 W
散热	1433 BTU/h	1045.5 BTU/h	1045.5 BTU/h	1219.8 BTU/h
工作温度	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)
存储温度	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)
湿度	5% 至 95% (无凝结)	5% 至 95% (无凝结)	5% 至 95% (无凝结)	5% 至 95% (无凝结)
合规				
安全认证	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, C-Tick, VCCI, CE, UL/CB/cUL



FortiWeb 2000E



FortiWeb 3000E



FortiWeb 3010E



FortiWeb 4000E

规格

	FORTIWEB-VM (1 vCPU)	FORTIWEB-VM (2 vCPU)	FORTIWEB-VM (4 vCPU)	FORTIWEB-VM (8 vCPU)
系统性能				
HTTP 吞吐速率	25 Mbps	100 Mbps	500 Mbps	2 Gbps
应用程序许可	无限制	无限制	无限制	无限制
管理域	4 到 64 (基于分配的内存数量)			
虚拟机				
支持虚拟控制程序	VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud, and Oracle Cloud. 关于版本支持信息, 请参阅 FortiWeb VM 安装指南。			
vCPU支持(最少/最多)	1	2	2 / 4	2 / 8
网络接口支持(最少/最多)	1 / 10	1 / 10	1 / 10	1 / 10
硬盘存储支持(最少/最多)	40 GB / 2 TB	40 GB / 2 TB	40 GB / 2 TB	40 GB / 2 TB
内存支持(最少/最多)	1,024 MB / 64-bit 无限制	1,024 MB / 64-bit 无限制	1,024 MB / 64-bit 无限制	1,024 MB / 64-bit 无限制
推荐内存	4 GB	4 GB	4 GB	4 GB
高可用性支持	是	是	是	是

实际性能值取决于网络流量和系统配置。测试性能指标使用 Dell PowerEdge R710服务器 (2个 Intel Xeon E5504 处理器, 主频为2.0 GHz, 4 MB 缓存) 运行VMware ESXi 5.5 (4 GB 的 vRAM 分配给 4 vCPU 和 8 vCPU FortiWeb 虚拟设备, 4 GB 的 vRAM 分配给 2 vCPU FortiWeb 虚拟设备)。

	FORTIWEB-VMC01	FORTIWEB-VMC02	FORTIWEB-VMC04	FORTIWEB-VMC08
容器设备				
系统性能				
HTTP吞吐速率	25 Mbps	100 Mbps	500 Mbps	2 Gbps
应用程序许可	无限制	无限制	无限制	无限制
管理域	4 到 64 (基于分配的内存数量)			
虚拟机				
容器管理员支持	Docker			
网络接口支持(最少/最多)	1 / 10	1 / 10	1 / 10	1 / 10
硬盘存储支持(最少/最多)	30 GB / 500 GB	30 GB / 500 GB	30 GB / 500 GB	30 GB / 500 GB
内存支持(最少/最多)	4 GB	4 GB	4 GB	4 GB
推荐内存	4 GB	4 GB	4 GB	4 GB
高可用性支持	否	否	否	否

吞吐量和其它指标是每个版本允许的最大值。实际性能值可能因网络流量和系统配置而异。

订购信息

产品	SKU	描述
FortiWeb 100D	FWB-100D	Web应用防火墙 — 4个GE RJ45接口, 16 GB硬盘。
FortiWeb 400D	FWB-400D	Web应用防火墙 — 4个GE RJ45接口, 4个GE SFP接口, 240 GB SSD硬盘。
FortiWeb 600D	FWB-600D	Web应用防火墙 — 4个GE RJ45接口 (2个旁路接口), 4个GE SFP接口, 240 GB SSD硬盘。
FortiWeb 1000D	FWB-1000D	Web应用防火墙 — 2个GE SFP插槽, 6个GE RJ45接口 (包括4个旁路接口), 双交流电源, 2 TB硬盘。
FortiWeb 1000E	FWB-1000E	Web应用防火墙 — 2个10 GE SFP +接口, 2个GE RJ45接口, 4个GE RJ45旁路接口, 4个GE SFP接口, 双交流电源, 2 TB硬盘。
FortiWeb 2000E	FWB-2000E	Web应用防火墙 — 2个10 GE SFP +接口, 4个GE RJ45旁路接口, 4个GE SFP接口, 双交流电源, 2 TB硬盘。
FortiWeb 3000E	FWB-3000E	Web应用防火墙 — 4个10 GE SFP +接口, 8个GE RJ45旁路接口, 4个GE SFP接口, 双交流电源, 2个2 TB硬盘。
FortiWeb 3010E	FWB-3010E	Web应用防火墙 — 8个GE RJ45旁路接口, 4个GE SFP接口, 2个10G SFP +旁路接口, 2个10G SFP +接口, 双交流电源, 2个2 TB HDD硬盘。
FortiWeb 4000E	FWB-4000E	Web应用防火墙 — 8个GE RJ45旁路接口, 4个GE SFP接口, 2个10G SFP +旁路接口, 2个10G SFP +接口, 双交流电源, 2个2 TB HDD硬盘。
FortiWeb-VM01	FWB-VM01	FortiWeb-VM, 最多支持1个vCPU。64位操作系统。
FortiWeb-VM02	FWB-VM02	FortiWeb-VM, 最多支持2个vCPU。64位操作系统。
FortiWeb-VM04	FWB-VM04	FortiWeb-VM, 最多支持4个vCPU。64位操作系统。
FortiWeb-VM08	FWB-VM08	FortiWeb-VM, 最多支持8个vCPU。64位操作系统。
FortiWeb-VMC01	FWB-VMC01	FWB-VMC01, 用于基于容器的环境。吞吐量高达25 Mbps。
FortiWeb-VMC02	FWB-VMC02	FWB-VMC02, 用于基于容器的环境。吞吐量高达100 Mbps。
FortiWeb-VMC04	FWB-VMC04	FWB-VMC04, 用于基于容器的环境。吞吐量高达500 Mbps。
FortiWeb-VMC08	FWB-VMC08	FWB-VMC08, 用于基于容器的环境。吞吐量高达2 Gbps。

订购信息

产品	SKU	描述
Central Manager 10	FWB-CM-BASE	FortiWeb Central Manager 许可证密钥, 最多可管理10个 FortiWeb 设备, VMware vSphere。
Central Manager Unlimited	FWB-CM-UL	FortiWeb Central Manager 许可证密钥, 可管理无限数量的 FortiWeb 设备, VMware vSphere。



www.fortinet.com

Copyright © 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results 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 certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. 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 covenants, representations, and guarantees pursuant hereto, whether express or implied. 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. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. 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.