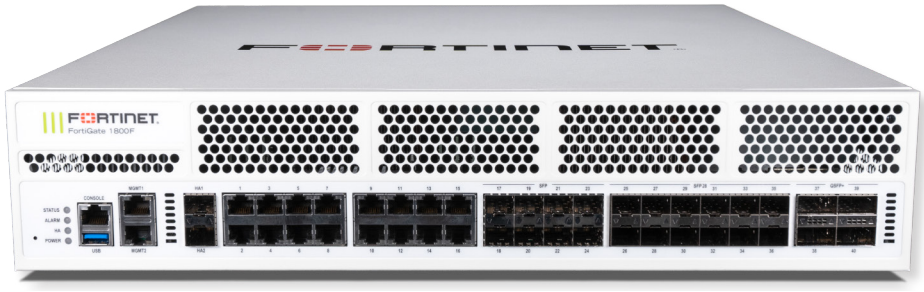
产品说明

FortiGate® 1800F 系列

FortiGate 1800F / -DC 和 1801F / -DC

下一代防火墙
网络分段
安全 Web 网关
移动安全



FortiGate 1800F 系列为大型企业和网络服务提供商提供了高性能的下一代防火墙 (NGFW) 功能。凭借多个高速接口、高端口密度和高吞吐量，该系列可灵活地部署在企业边缘、混合和超大规模数据中心以及内部网段。该系列还能够利用行业领先的 IPS、SSL 检测和高级威胁防护来优化网络性能。Fortinet 的安全驱动型网络方法可将网络与新一代安全解决方案紧密集成在一起。

安全

- 识别网络流量中的数千个应用，以进行深度检测和精细的策略执行
- 有效阻止加密以及非加密流量中的恶意软件，漏洞利用及恶意网站的攻击
- 借助 FortiGuard Labs AI 驱动型安全服务连续提供的威胁情报，防止和检测已知攻击
- 借助与 Fortinet Security Fabric 相集成的 AI 驱动型 FortiSandbox，实时主动拦截未知的复杂攻击

性能

- 使用 Fortinet专用的安全处理器 (SPU) 进行了创新设计，能够提供业界最佳的威胁防护性能和超低延迟
- 作为首家提供 TLS 1.3 深度检测的防火墙厂商，能够为 SSL 加密流量提供行业领先的性能和保护

认证

- 通过独立测试获得最佳安全性能验证
- 通过了 NSS Labs、ICSA、Virus Bulletin 和 AV Comparatives 等权威第三方机构的认证

网络

- 内置 SD-WAN 功能的应用感知路由可确保一致的应用性能和最佳的用户体验
- 内置高级路由功能可通过大规模加密 IPSEC 隧道提供出色的性能

管理

- 简单易用且有效的管理控制平台提供了全面的网络自动化及可视化
- 由 Fabric 管理中心提供支持的统一管理平台支持零接触部署
- 通过预定义合规检查清单分析部署最佳实践方案，改进整体网络安全

安全结构

- Fortinet 和 Fabric-ready 合作伙伴的产品能够密切集成和协作， 并提供更广泛的可视化、集成端到端检测、威胁情报共享和自动修复
- 自动构建网络拓扑可视化，可准确检测物联网设备并实现 Fortinet 和 Fabric-ready 合作伙伴产品的全面可视化

防火墙	IPS	NGFW	威胁防护	接口
198 Gbps	**13 Gbps**	**11 Gbps**	**9.1 Gbps**	多个 GE RJ45、25 GE SFP28 / 10 GE SFP+ / GE SFP 以及 40 个 GE QSFP+ 插槽

详情请参阅规格表

部署

下一代防火墙 (NGFW)

- 通过将威胁防护功能集成到由 Fortinet 安全处理器 (SPU) 提供支持的单个高性能网络安全设备中，降低复杂性并最大限度地提高投资回报
- 全面监控整个攻击面中的用户、设备、应用并执行一致的安全策略，无论资产位于何处
- 借助经行业验证的 IPS 安全有效性、低延迟和优化的网络性能，防止网络中可利用的漏洞
- 利用业界最高的 SSL 检测性能，包括带强制密码的最新 TLS 1.3 标准， 对流量解密并自动阻断威胁。
- 借助 AI 驱动型 FortiGuard Labs 和 Fortinet Security Fabric 中的高级威胁防护服务，实时主动拦截新发现的复杂攻击

网络分段

- 可适应任何网络拓扑结构的网络分段，提供从分支机构到数据中心的端到端安全性，并扩展到多云中
- Fortinet Security Fabric 组件能够根据当前的信任级别调整访问权限，并高效实施访问控制，可通过提高网络可视化，降低安全风险
- 通过 Fortinet 的 SPU 进行高性能 7 层检测和修复，提供深度安全防护，同时提供通过第三方验证的受保护每 Mbps 总体拥有成本 (TCO)
- 保护关键业务应用并帮助实现任何合规性要求，而且无需网络重新设计

安全 Web 网关 (SWG)

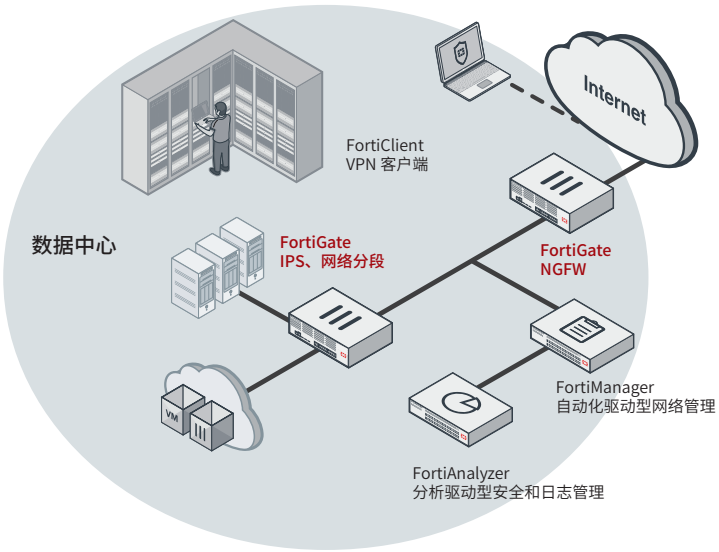
- 保护 Web 访问免遭内外部风险，甚至对高性能的加密流量也是如此
- 通过动态 Web 和视频缓存增强用户体验
- 基于跨 URL 和域的用户或用户组拦截和控制 Web 访问
- 防止数据丢失并检测已知和未知云应用上的用户活动
- 针对恶意域名拦截 DNS 请求
- 提供多层高级保护，有效抵御通过 Web 传递的零日恶意软件威胁

IPS

- 专门构建的安全处理器能够以高吞吐量和低延迟提供经行业验证的 IPS 性能
- 在网络级别部署虚拟补丁，以拦截网络可利用的漏洞并优化网络保护时间
- 线速的深度数据包检测能够提供无与伦比的网络流量（包括使用最新 TLS 1.3 加密的流量）威胁可视化
- 借助 Fortinet Security Fabric 情报服务的高级威胁防护，实时主动拦截新发现的复杂攻击

适用于 4G、5G 和物联网的移动安全性

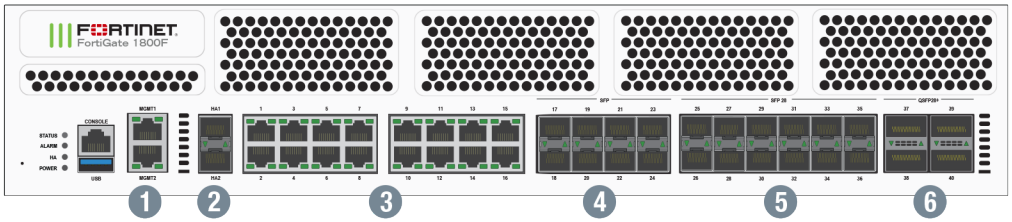
- SPU 加速的、高性能的 CGNAT 和 IPv6 迁移选项，包括 4G Gi/sGi 的 NAT44、NAT444、NAT64/DNS64、NAT46 以及 5G N6 连接和安全性
- 高度可扩展、最佳性能的 IPsec 聚合和控制安全网关 (SecGW) 可确保 RAN 访问安全性
- 全面威胁防护和 GTP-U 检测可视化可确保用户平面安全
- 适用于用户和数据平面流量（包括 SCTP、GTP-U 和 SIP）的 4G 和 5G 安全性可提供有效的攻击防护
- 高速接口支持灵活部署

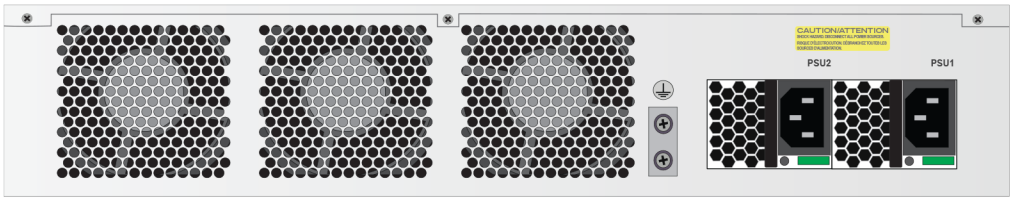


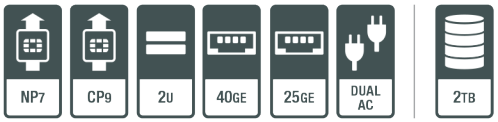
FortiGate 1800F 部署在数据中心
（NGFW、IPS 和基于意图的网络分段）

硬件

FortiGate 1800F系列







接口

1. 2 个 GE RJ45 管理端口
2. 2 个 10 GE SFP+ / GE SFP HA 插槽
3. 16 个 GE RJ45 端口
4. 8 个 GE SFP 插槽
5. 12 个 25 SFP28 / 10 GE SFP+ / GE SFP 插槽
6. 4 个 40 GE QSFP+ 插槽

由 SPU 提供支持

- 自定义 SPU 处理器支持以数千兆位速度检测恶意内容
- 由于依赖于通用 CPU 而导致性能严重不足，其他安全技术无法抵御当今广泛的基于内容和连接的威胁
- SPU 处理器可提供拦截新兴威胁所需的性能，满足严格的第三方认证，并确保网络安全解决方案不会成为网络瓶颈

网络处理器

Fortinet 的最新 SPU NP7 Hyperscale 架构是一种专用的网络处理器，可为 FortiOS 提供加速的硬件性能：

- IPv4/IPv6、SCTP、单播、多播和任播
- CAPWAP、VXLAN 和 GRE IP 隧道
- IPSec VPN (包括 Suite B)
- 针对容量耗尽攻击的硬件 DDoS 防护、分片重组、流量整形和优先级队列
- 高达 100Gbps 的大象流量

内容处理器

SPU CP9 内容处理器运行在流量路径之外，提供高速加密和内容检测服务，包括：

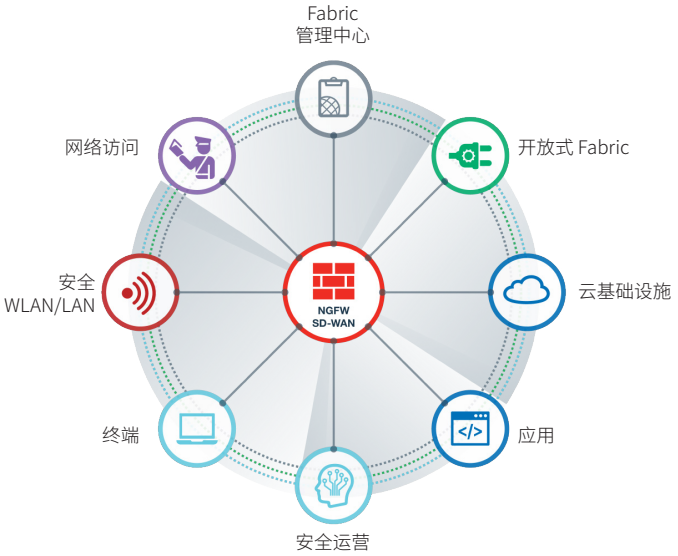
- 基于签名的内容检测加速
- 加密和解密卸载

Fortinet Security Fabric

Security Fabric

Security Fabric 网络安全平台助力数字创新。全面监控整个攻击面，从而更好地管理风险。这款统一的集成式解决方案可降低支持多点产品的复杂性，同时自动化工作流可提高整个 Fortinet 部署生态系统内的运营速度并帮助缩短响应时间。Fortinet Security Fabric 通过单个管理中心管理以下关键方面：

- 安全驱动型网络，用于保护、加速并统一网络和用户体验
- 零信任网络访问，用于实时识别并保护联网和未联网的用户和设备
- 动态云安全性，用于保护和控制云基础设施和应用
- AI 驱动型安全运营，用于自动阻止、检测、隔离和响应网络威胁。



FortiOS

FortiGate 是 Fortinet Security Fabric 的基础，而其核心是 FortiOS。整个 FortiGate 平台的所有安全和网络功能均由一个直观的操作系统控制。FortiOS 通过将下一代安全产品和服务真正整合到一个平台中，降低了复杂性、削减了成本并缩短了响应时间。

- 这个真正的整合平台通过单个操作系统和统一管理平台管理整个数字攻击面。
- 行业领先的保护：获得 NSS Labs Recommended、VB100、AV Comparatives 和 ICSA 等机构的安全和性能验证。
- 能够利用最新技术，例如基于欺骗的安全防护。
- 真正支持 TLS 1.3，而且还可以基于数百万个实时 URL 评级过滤 web 流量、控制数千个应用、阻止最新漏洞利用并过滤 Web 流量
- 借助集成的 AI 驱动型安全防护和高级威胁防护，在数分钟内自动阻止、检测和规避高级攻击。
- 借助创新的 SD-WAN 功能以及通过自动化网络分段检测、遏制和隔离威胁的能力，改善并统一用户体验。
- 利用 SPU 硬件加速提升网络安全性能。

服务

FortiGuard™ 安全服务

FortiGuard Labs 提供有关威胁态势的实时情报，为 Fortinet 全系列解决方案推送全面的安全更新。我们的专家团队由安全威胁研究分析师、工程师和电子取证专家组成，与世界领先的威胁监控组织、其他网络安全厂商以及执法机构通力协作。

FortiCare™ 支持服务

我们的 FortiCare 客户支持团队为所有 Fortinet 产品提供全球技术支持。FortiCare 支持人员遍布美洲、欧洲、中东和亚洲地区，可满足各种规模企业的服务需求。

详情请访问 forti.net/fortiguard 和 forti.net/forticare

规格

	FG-1800F/-DC	FG-1801F/-DC
硬件规格		
硬件加速 GE RJ45 接口	16	
硬件加速 GE SFP 插槽	8	
硬件加速 25 GE SFP28 / 10 GE SFP+ / GE SFP 插槽	12	
硬件加速 40GE QSFP+ 插槽	4	
GE RJ45 管理接口	2	
10 GE SFP+ / GE SFP HA 插槽	2	
USB 3.0 接口	1	
控制台 RJ45 接口	1	
内置存储	-	2 块 1TB NVMe SSD
包含的收发器	2 个 SFP+ (SR 10GE)	
系统性能 — 企业混合流量		
IPS 吞吐量 [2]	13 Gbps	
NGFW 吞吐量 [2,4]	11 Gbps	
威胁防护吞吐量 [2,5]	9.1 Gbps	
系统性能和容量		
IPv4 防火墙吞吐量（1518 / 512 / 64 字节，UDP）	198 / 197 / 140 Gbps	
IPv6 防火墙吞吐量（1518 / 512 / 86 字节，UDP）	198 / 197 / 140 Gbps	
防火墙延迟（64 字节，UDP）	3.22 微秒	
防火墙吞吐量（每秒数据包数）	210 Mpps	
并发会话 (TCP)	1,200 万	
新建会话 / 秒 (TCP)	750,000	
防火墙策略	100,000	
IPsec VPN 吞吐量（512 字节）1	55 Gbps	
网关到网关 IPsec VPN 隧道	20,000	
客户端到网关 IPsec VPN 隧道	100,000	
SSL-VPN 吞吐量	11 Gbps	
并发 SSL-VPN 用户（建议最大数量，隧道模式）	10,000	
SSL 检测吞吐量（IPS，平均 HTTPS）[3]	17 Gbps	
SSL 检测新建会话 / 秒（IPS，平均 HTTPS）[3]	9,500	
SSL 检测并发会话（IPS，平均 HTTPS）[3]	130 万	
应用控制吞吐量 (HTTP 64K)2	34 Gbps	
CAPWAP 吞吐量 (HTTP 64K)	26.5 Gbps	
虚拟域（默认 / 最大数量）	10/250	
支持的 FortiSwitch 最大数量	196	
FortiAP 最大数量（总计 / 隧道模式）	4,096/2,048	
FortiToken 最大数量	20,000	
高可用性配置	主动 - 主动、主动 - 被动、集群	

	FG-1800F/-DC	FG-1801F/-DC
尺寸和电源		
高度 x 宽度 x 长度（英寸）	3.5 x 17.25 x 21.1	
高度 x 宽度 x 长度（厘米）	88.4 x 438 x 536	
重量	30.2 磅（13.7 公斤）	30.4 磅（13.8 公斤）
外形（支持 EIA/ 非 EIA 评估标准）	机架式，2RU	
交流输入电源	100–240VAC，50-60 Hz	
最大交流电流	7A@100VAC，3A@240VAC	
直流输入电源	-48V 至 -60V DC	
最大直流电流	20A	
最大功耗	543.6W	558.8W
平均功耗	388.3W	399.1W
散热	1,854.84 BTU/hr	1,906.70 BTU/hr
冗余电源	是，可热插拔	
工作环境和认证		
工作温度	32-104° F (0–40° C)	
存储温度	-31-158° F (-35–70° C)	
湿度	10-90%（无冷凝）	
噪声水平	62.74 dBA	
工作高度	最高 7,400 英尺（2,250 米）	
合规性	FCC Part 15 Class A、RCM、VCCI、CE、UL/cUL、CB	
认证	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6	

注意: 所有性能值均为“最高可达”，并且根据系统配置而变化。

1. IPsec VPN 性能测试使用 AES256-SHA256。
2. IPS（企业混合流量）、应用控制、NGFW 和威胁防护均在启用日志记录的情况下进行测量。
3. SSL 检测性能值使用不同密码组合的 HTTPS 会话的平均值。
4. NGFW 性能在启用防火墙、IPS 和应用控制功能的情况下进行测量。
5. 威胁防护性能在启用防火墙、IPS、应用控制和恶意软件防护功能的情况下进行测量。

订购信息

产品	SKU	描述
FortiGate 1800F	FG-1800F	4 个 40 GE QSFP+ 插槽、12 个 25 GE SFP28 /10GE SFP+ 插槽、2 个 10GE SFP+ HA 插槽、8 个 GE SFP 插槽、18 个 GE RJ45 端口、SPU NP7 和 CP9 硬件加速。
FortiGate 1801F	FG-1801F	4 个 40 GE QSFP+ 插槽、12 个 25 GE SFP28 /10GE SFP+ 插槽、2 个 10GE SFP+ HA 插槽、8 个 GE SFP 插槽、18 个 GE RJ45 端口、SPU NP7 和 CP9 硬件加速、2 个 1TB 板载 SSD 存储。
FortiGate-1800F-DC	FG-1800F-DC	4 个 40GE QSFP+ 插槽、12 个 25GE SFP28 /10GE SFP+ 插槽、2 个 10GE SFP+ HA 插槽、8 个 GE SFP 插槽、18 个 GE RJ45 端口。SPU NP7 和 CP9 加速，双直流电源
FortiGate-1801F-DC	FG-1801F-DC	4 个 40GE QSFP+ 插槽、12 个 25GE SFP28 /10GE SFP+ 插槽、2 个 10GE SFP+ HA 插槽、8 个 GE SFP 插槽、18 个 GE RJ45 端口、2 个 1TB 板载 SSD 存储。SPU NP7 和 CP9 加速，双直流电源
1 GE SFP LX 收发器模块	FN-TRAN-LX	1 GE SFP LX 收发器模块，可用于所有带 SFP 和 SFP/SFP+ 插槽的系统。
1 GE SFP RJ45 收发器模块	FN-TRAN-GC	1 GE SFP RJ45 收发器模块，可用于所有带 SFP 和 SFP/SFP+ 插槽的系统。
1 GE SFP SX 收发器模块	FN-TRAN-SX	1 GE SFP SX 收发器模块，可用于所有带 SFP 和 SFP/SFP+ 插槽的系统。
10 GE SFP+ 收发器模块，短距离	FN-TRAN-SFP+SR	10 GE SFP+ 收发器模块，短距离，可用于所有带 SFP 和 SFP/SFP+ 插槽的系统。
10 GE SFP+ 收发器模块，长距离	FN-TRAN-SFP+LR	10 GE SFP+ 收发器模块，长距离，可用于所有带 SFP 和 SFP/SFP+ 插槽的系统。
10 GE SFP+ 有源直连电缆，10 米 / 32.8 英尺	SP-CABLE-ADASFP+	10 GE SFP+ 有源直连电缆，10 米 / 32.8 英尺，可用于所有带 SFP+ 和 SFP/SFP+ 插槽的系统。
10GE 铜口 SFP+ RJ45 收发器（30 米距离）	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 收发器模块。
10Gbase-ER SFP+ 收发器	FN-TRAN-SFP+ER	10 GE SFP+ 收发器模块，扩展范围。
25 GE SFP28 收发器模块，长距离	FN-TRAN-SFP28-LR	25 GE SFP28 收发器模块，长距离，可用于所有带 SFP28 插槽的系统。
25 GE/10 GE 双速率 SFP28 收发器模块，短距离	FN-TRAN-SFP28-SR	25 GE/10 GE 双速率 SFP28 收发器模块，短距离，可用于所有带 SFP28/SFP+ 插槽的系统。
40 GE QSFP+ 收发器模块，短距离	FN-TRAN-QSFP+SR	40 GE QSFP+ 收发器模块，短距离，可用于所有带 QSFP+ 插槽的系统。
40 GE QSFP+ 收发器模块，短距离，BiDi	FG-TRAN-QSFP+SR-BIDI	40 GE QSFP+ 收发器模块，短距离，BiDi，可用于所有带 QSFP+ 插槽的系统。
40 GE QSFP+ 收发器，长距离	FN-TRAN-QSFP+LR	40 GE QSFP+ 40 GE QSFP+ 收发器，长距离，可用于所有带 QSFP+ 插槽的系统。
机架安装滑轨	SP-FG3040B-RAIL	机架安装滑轨，可用于 FG-1000C/-DC、FG-1100/1101E、FG-1200D、FG-1500D/-DC、FG-1800F、FG-2000E、FG-2500E、FG-3040B/-DC、FG-3140B/-DC、FG-3240C/-DC、FG-3000D/-DC、FG-3100D/-DC、FG-3200D/-DC、FG-3400/3401E、FG-3600/3601E、FG-3700D/-DC、FG-3700DX、FG-3810D/-DC 和 FG-3950B/-DC。
交流电源	SP-FG1800F-PS	FG-1800/1801F 使用交流电源。
直流电源	SP-FG1800F-DC-PS	FG-1800/1801F 和 FG-2600/2601 使用直流电源。

服务包

FortiGuard 服务包

FortiGuard Labs 提供多种安全情报服务以增强 FortiGate 防火墙平台。您可以使用其中一种 FortiGuard 服务包轻松地优化 FortiGate 的保护功能。

服务包	全面防护	企业防护	UTM	威胁防护
FortiCare	ASE[1]	24x7 全天候	24x7 全天候	24x7 全天候
FortiGuard 应用控制服务	•	•	•	•
FortiGuard IPS 服务	•	•	•	•
FortiGuard 高级恶意软件保护 (AMP) — 防病毒、移动恶意软件、僵尸网络、CDR、病毒爆发保护和 FortiSandbox 云服务	•	•	•	•
FortiGuard Web 过滤服务	•	•	•	
FortiGuard 反垃圾邮件服务	•	•	•	
FortiGuard 安全评级服务	•	•		
FortiGuard 工业安全服务	•	•		
FortiCASB SaaS 服务	•	•		
FortiConverter 服务	•	•		
SD-WAN 云辅助监控 [2]	•			
SD-WAN Overlay 控制器 VPN 服务 [2]	•			
FortiAnalyzer 云服务 [2]	•			
FortiManager 云服务 [2]	•			
FortiAnalyzer 云服务	•			
FortiManager 云服务	•			

1.24x7 全天候以及高级问题处理服务 2. 适用于 FortiOS 6.2

FORTINET

www.fortinet.com