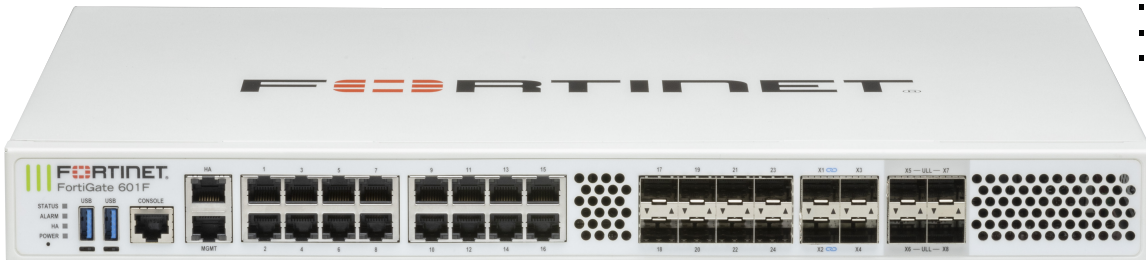


FortiGate® 600F 系列

FG-600F 和 FG-601F

下一代防火墙
安全SD-WAN
安全Web 网关



FortiGate 600F 系列可提供以应用为中心、可扩展且安全的 SD-WAN 解决方案等性能卓越的下一代防火墙优势功能，适用于大中型企业园区或分支机构的灵活部署。依托SoC加速及业内领先的安全 SD-WAN技术，为用户打造简便、性价比优越且易于部署的安全解决方案，助力企业全方位抵御网络威胁。秉承Fortinet 安全驱动网络理念，为用户打造网络与新一代安全性高效融合的新型网络架构。

安全

- 通过深度检查轻松识别网络流量中数千个应用程序，以并因此建立细粒度的防火墙策略。
- 高效检查/防御双向加密和非加密流量中的恶意软件、漏洞利用及恶意网站攻击。
- 通过AI 驱动的 FortiGuard Labs 安全服务持续共享威胁情报，全方位主动检测和预防已知和未知的网络攻击

性能

- 凭借独创的安全处理器（SPU）技术，支持超低延迟的同时，实现业内最佳的威胁防护性能
- 为企业中的 SSL 加密流量提供业内领先的检测性能和威胁防护

认证

- 经第三方独立机构测试和认证，可实现一流的性能和安全效能
- 荣获NSS Labs第三方权威机构认证

网络

- 支持 7 层高级网络功能及虚拟域（VDM）无缝集成，支持弹性灵活的部署形式，满足多租户场景需求，高效利用资源
- 提供各种高密度且支持灵活组合的高速接口，为用户的数据中心和 WAN 部署提供最优 TCO 解决方案

管理

- 简单易用且高效的管理控制平台，为用户提供全面的网络自动化及可见性
- 支持通过 Fortinet Security Fabric 统一管理平台零接触部署与集成
- 支持通过预定义的合规性检查清单，分析部署最佳实践方案，全面提升整体网络安全态势

Security Fabric

- 依托Security Fabric安全平台，支持 Fortinet 解决方案与 Fabric-ready 技术联盟合作伙伴技术紧密集成并通力协作，助力用户构建具备广泛可见性、集成式端到端检测、威胁情报共享及自动化修复的网络安全防护体系

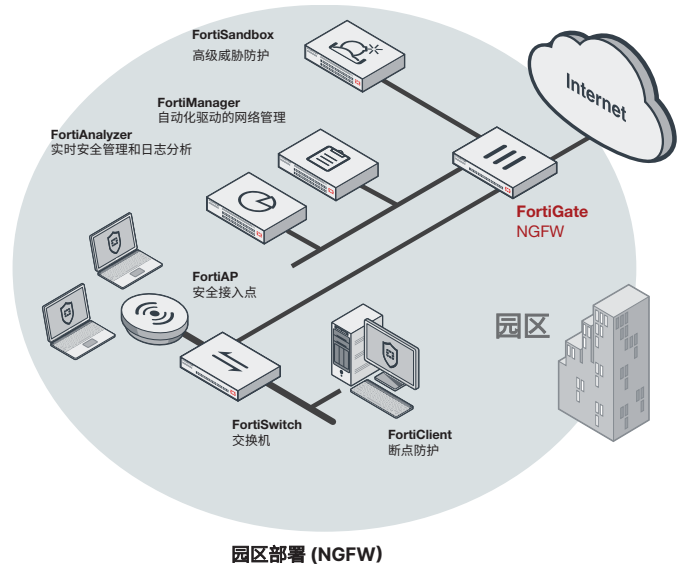
防火墙*	IPS*	NGFW*	* 威胁防护	接口
139 Gbps	14 Gbps	11.5 Gbps	10.5 Gbps	多个 25GE SFP28、10GE SFP+、GE SFP 插口与 GE RJ45接口

* 详细信息，请参阅规格参数表

部署

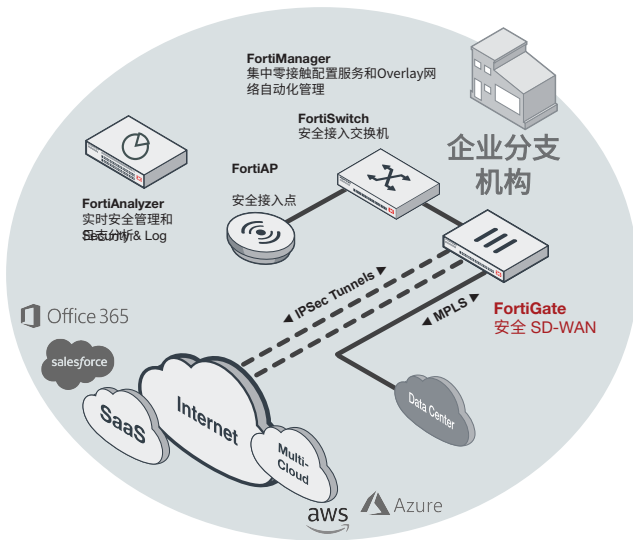
下一代防火墙 (NGFW)

- 将多种威胁防护安全功能全面集成至由 Fortinet 自研安全处理单元 (SPU) 中, 并通过 SPU 赋能给高性能网络安全设备, 简化整体的安全架构并最大限度地提高投资回报率
- 获得跨整个攻击面的用户、设备和应用程序的全面可见性 无论资产位于何处, 都能实施一致的安全策略
- 经业内验证的 IPS 高效检查与防御网络中潜在漏洞的同时 确保低延迟和优化的网络性能
- 拥有无与伦比的高效 SSL 检测性能 (包括支持 TLS 1.3), 可实时检测隐藏在加密路径中的新型威胁
- 依托人工智能 (AI) 驱动的 FortiGuard Labs 全球威胁情报共享服务及 Fortinet Security Fabric 安全平台中的高级威胁防护服务, 实时主动拦截各类新型复杂威胁攻击



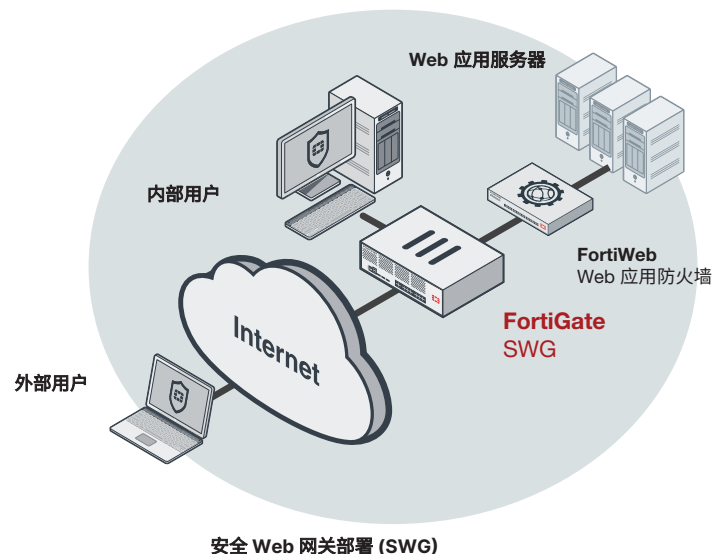
安全 SD-WAN

- 创新 SD-WAN 功能, 对流量进行精准路由, 动态选择最佳链路进行传输, 为用户提供卓越的业务应用访问体验
- 云入口加速多云访问, 助力用户快速安全访问软件即服务 (SaaS) 应用
- 自我修复型网络, 通过广域网边缘高可用性、基于亚秒级流量切换和实时带宽流量计算进行最佳流量导向
- Overlay 隧道自动化技术支持自动构建加密和基于底层物理网络抽象出的混合 WAN 架构, 使得网络摆脱物理网络的复杂性, 更易管理和编排
- FortiManger 实现简化和直观的工作流, 加速 SD-WAN 零接触部署并提高运营效率
- 强化实时分析和历史数据分析能力, 提供网络性能全面可见性, 高效识别异常事件
- 高性能下一代防火墙和实时威胁防护功能, 全面提升安全态势



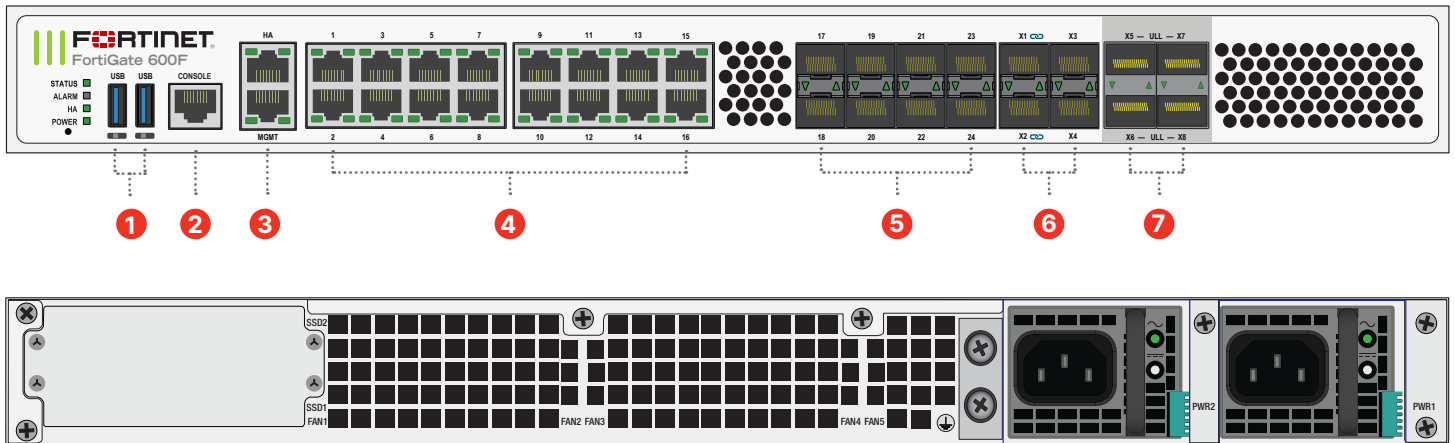
安全 Web 网关 (SWG)

- 高效检测加密流量, 不影响网络性能, 全方位保护 Web 访问 免受各种内外外部威胁侵扰
- 支持动态 Web 和视频缓存功能, 优化用户体验
- 基于跨 URL 和域的用户或用户组, 拦截并控制 Web 访问
- 防止数据丢失, 实时检测已知和未知云应用程序中的用户访问活动
- 全方位拦截针对恶意域的 DNS 请求
- 多层高级保护功能, 全面拦截通过 Web 分发的零日恶意软件威胁



硬件

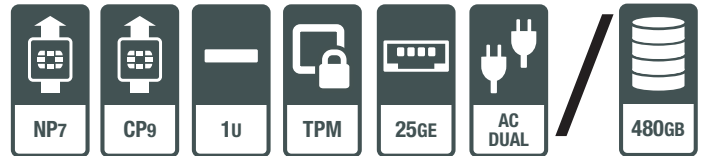
FortiGate 600F/601F



接口

1. 2x USB 接口
2. 1x 控制接口
3. 2x GE RJ45 MGMT/HA 接口
4. 16x GE RJ45 接口
5. 8x GE SFP 插口
6. 4x 10GE/GE SFP+/SFP 插口
7. 4x 25GE/10GE SFP28/SFP+ 超低时延插口

硬件特性



SPU 处理器



- Fortinet 独创的 SPU 处理器，可提供高流量带宽下检测恶意内容的强大功能
- 由于其他安全技术仍旧依赖于传统 CPU，从而导致性能无法满足用户要求，无法抵御当今基于内容和连接的各种威胁
- 荣获第三方权威认证的 SPU 处理器，提供拦截新兴威胁所需的出色性能，确保网络性能不受本地网络安全解决方案运行影响

网络处理器

Fortinet 创新突破研发的 SPU NP7 网络处理器可与 FortiOS 功能协同工作，共同提供：

- 出色的防火墙性能，适用于 IPv4 / IPv6, SCTP 和组播流量，具有超低时延功能
- VPN、CAPWAP 和 IP 隧道加速
- 基于异常行为的入侵防御，校验卸载和数据包碎片整理
- 流量整形和优先级队列

内容处理加速器

Fortinet 创新突破研发的 SPU CP9 内容处理器不受直接网络流量影响，可加速执行计算密集型安全检测：



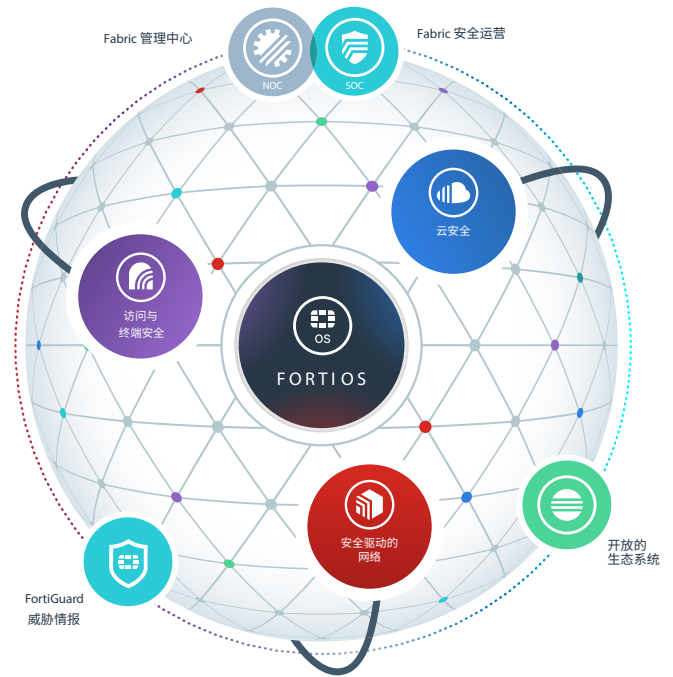
FORTINET SECURITY FABRIC

Security Fabric

作为业界性能最高的网络安全平台，Fortinet Security Fabric 由 FortiOS 提供强劲支持，拥有丰富的开放式生态系统，旨在跨越不断扩展的数字攻击面，为企业构建全面自动化、自我修复的网络安全体系。

- **全面覆盖：** 数字化攻击面的全面覆盖，提供全方位的可见性与防御能力
- **深度集成：** 多点安全产品和解决方案的深度集成，降低管理复杂性并共享威胁情报
- **动态协同：** 搭载AI驱动的安全的自修复网络，提供更快更高效的运营能力

Fabric 助力任何规模的企业组织均能在数字化创新之旅中，全方位保护和简化其混合基础设施。



FortiOS™ 操作系统

作为Fortinet 领先的操作系统，FortiOS 可跨 Fortinet Security Fabric 安全平台实现融合网络和安全的高性能服务体验，从而为企业在跨网络端点和云中交付一致且上下文感知的安全态势。有机构建的同类最佳技术功能和统一方法，助力企业组织能够享有卓越性能的同时，确保高效、安全的运营环境，支持无缝可扩展性，简化管理并降低创新成本。

FortiOS 7.2 版本的发布极大地扩展了 Fortinet Security Fabric 的能力，使其能够跨混合部署模型，包括设备、软件、SASE即服务、ZTNA策略及其他创新网络安全解决方案提供协调一致的安全性。

服务

FortiGuard™ 安全服务

FortiGuard 威胁研究与响应实验室提供实时可操作的安全情报，在整个 Fortinet 解决方案覆盖范围内推送全方位的安全更新。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视组织联盟，及其他网络安全供应商以及执法机构通力协作，共享安全态势与威胁情报。

FortiCare™ 支持服务

Fortinet 致力于帮助我们的客户获得最大投资回报率，助力客户取得商业成功。FortiCare 支持服务每年会助力成千上万家企业部署的 Fortinet Security Fabric 解决方案以最佳状态运行。Fortinet 拥有 1,000 多名专家团队，可帮助企业加速技术实施，通过高级支持服务为企业提供可靠的帮助以及主动预防服务，以最大限度地发挥 Fortinet 产品的安全和性能



技术参数

	FG-600F	FG-601F
接口和模块		
硬件加速 GE RJ45 接口		16
硬件加速 GE SFP 插口		8
硬件加速 10 GE SFP+ 插口		4
Slots 硬件加速 25GE SFP28/ 4 10GE SFP+/ GE SFP 超低延迟插口		4
GE RJ45 MGMT/HA 接口		2
USB 接口		2
RJ45 控制接口		1
内部存储	0	2x 240 GB SSD
包含的收发器	2x SFP (SX 1 GE)	
系统性能 — 企业混合流量		
吞吐量 ²	14 Gbps	
NGFW 吞吐量 ^{2,4}	11.5 Gbps	
威胁防御吞吐量 ^{2,5}	10.5 Gbps	
系统性能		
IPv4 防火墙吞吐量 (1518 / 512 / 64 byte, UDP)	139 / 137.5 / 70 Gbps	
IPv6 防火墙吞吐量 (1518 / 512 / 64 字节, UDP)	139 / 137.5 / 70 Gbps	
防火墙延时 (64 字节, UDP)	4.12 μs	
防火墙吞吐量 (每秒包数)	105 Mpps	
并发会话(TCP)	8 百万	
新建会话/秒(TCP)	550 000	
防火墙策略	10 000	
IPsec VPN 吞吐量 (512 字节) ¹	55 Gbps	
网关到网关 IPsec VPN 隧道	2000	
客户端到网关 IPsec VPN 隧道	50 000	
SSL-VPN 吞吐量 ⁶	4.3 Gbps	
并发 SSL-VPN 用户 (建议的最大数量, 隧道模式)	10 000	
SSL 检查吞吐量 (IPS, 平均 HTTPS) ³	9 Gbps	
SSL 检查每秒连接 (IPS, 平均 HTTPS) ³	7500	
SSL 检查并发会话 (IPS, 平均 HTTPS) ³	840 000	
应用程序控制吞吐量 (HTTP 64K) ²	32 Gbps	
CAPWAP 吞吐量 (HTTP 64K)	64.5 Gbps	
虚拟域 (默认/最大)	10 / 10	
FortiSwitch 最大支持数量	96	
FortiAP 最大数量 (总计/隧道模式)	1024 / 512	
FortiToken 最大数量	5000	
高可用性配置	主动/主动、主动/被动、集群	

	FG-600F	FG-601F
尺寸和电力需求		
高度 x 宽度 x 长度(英寸)	1.75 × 17.0 × 15.0	
高度 x 宽度 x 长度(毫米)	44.45 × 432 × 380	
重量	15.6 lbs (7.1 kg)	16.2 lbs (7.35 kg)
外观	Rack Mount, 1 RU	
AC 功耗 (平均/最大)	169 W / 255 W	174 W / 260 W
AC 电源输入	100–240V AC, 50/60Hz	
最大电流	6A@100V	
散热	871 BTU/h	888 BTU/h
冗余电源 (可热插拔)	是	
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	5%–90% 无凝结	
噪声水平	55 dBA	
气流	侧面和从前到后	
工作高度	最高 7400 ft (2250 m)	
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：所有性能值均为“最高”显示，可能因系统配置而异。

1. IPsec VPN 性能测试使用 AES256-SHA256。
2. IPS (企业组合流量)、应用程序控制、NGFW 和威胁防御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密钥组合的 HTTPS 会话期间的平均值。

4. NGFW (下一代防火墙) 性能是在启用防火墙、IPS 和应用程序控制功能的情况下进行测量。
5. 威胁防御性能是在启用防火墙、IPS、应用程序控制和恶意软件防护功能的情况下进行测量。
6. 使用 RSA-2048 证书。



订购信息

产品	SKU	描述
FortiGate 600F	FG-600F	4x 25G SFP28 插口、4 x 10GE SFP+ 插口、18 x GE RJ45 接口 (包含1 x MGMT 接口、1 X HA 接口、16 x 交换机端口) , 8 x GE SFP 插口、SPU NP7 和CP9 硬件加速、双交流电源。
FortiGate 601F	FG-601F	4x 25G SFP28 插口、4 x 10GE SFP+ 插口、18 x GE RJ45 接口 (包含1 x MGMT 接口、1 X HA 接口、16 x 交换机端口) , 8 x GE SFP 插口、SPU NP7 和 CP9 硬件加速、480GB SSD板载存储, 双交流电源。
可选配件		
1 GE SFP LX 收发器模块	FN-TRAN-LX	1 GE SFP LX 收发器模块, 适用于所有带 SFP 和SFP/SFP+ 插口的系统。
1 GE SFP RJ45 收发器模块	FN-TRAN-GC	1 GE SFP RJ45收发器模块, 适用于所有带SFP和SFP/SFP+插口的系统。
1 GE SFP SX 收发器模块	FN-TRAN-SX	1 GE SFP SX收发器模块, 适用于所有带SFP和SFP/SFP+插口的系统。
10 GE SFP+ RJ45 收发器模块	FN-TRAN-SFP+GC	10 GE SFP+ RJ45收发器模块, 适用于所有带SFP+插口的系统。
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, 适用于所有带 SFP+和SFP/SFP+插口的系统。
10 GE SFP+ 收发器模块、远距离	FN-TRAN-SFP+LR	10 GE SFP+ 收发器模块、远距离, 适用于所有带 SFP+和SFP/SFP+插口的系统。
10 GE SFP+ 收发器模块、可扩展距离	FN-TRAN-SFP+ER	10 GE SFP+ 收发器模块、可扩展距离, 适用于所有带 SFP+和SFP/SFP+插口的系统。
25GE SFP28 收发器模块、短距离	FN-TRAN-SFP28-SR	25GE/10GE双速率SFP28 收发器模块、短距离, 适用于所有带SFP28/SFP+插口的系统。
25GE SFP28 收发器模块、远距离	FN-TRAN-SFP28-LR	25GE SFP28 收发器模块、远距离, 适用于所有带SFP28插口的系统。
AC电源	SP-FG400F-PS	适用于FG-400/401F、FG-600/601F的AC电源, 电源线 SP-FGPCOR-XX 单独出售。

服务包



FortiGuard 服务包

FortiGuard 全球威胁研究与响应实验室提供全面的安全情报服务, 以增强 FortiGate 防火墙平台的安全性能。您可选择其中一个 FortiGuard 服务包轻松优化 FortiGate 的防护性能。

服务包	企业防护	统一威胁管理	高级威胁防护
FortiCare 支持服务	24x7	24x7	24x7
FortiGuard 应用程序控制服务	•	•	•
FortiGuard IPS Service	•	•	•
FortiGuard 高级恶意软件保护 (AMP) — 防病毒 防移动恶意软件、防僵尸网络、CDR、防病毒爆发及 FortiSandbox 云服务	•	•	•
FortiGuard 网页和视频 ¹ 过滤服务	•	•	
FortiGuard 反垃圾邮件服务	•	•	
FortiGuard 安全评分服务	•		
FortiGuard IoT 威胁检测服务	•		
FortiGuard 工业保护签名服务	•		
FortiConverter 配置交换工具服务	•		

1. 运行FortiOS7.0时可用



www.fortinet.com

Copyright © 2022 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 all 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 is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA (<https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf>) and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy (https://secure.ethicspoint.com/domain/media/en/gui/19775/Whistleblower_Policy.pdf).