FortiGate -600D

-企业内网防火墙

随着网络威胁和高频数据泄露事件持续成为头条新闻，不大或小的企业和组织都越来越认识到网络安全的重要性。这意味着他们希望在已有的网络基础上，提升安全在其中的地位。

FortiGate 600D 利用分布式硬件架构，提供给下一代防火墙突破性的性能，在状态防火墙上结合了入侵防御和应用程序控制，再加上Web过滤和反恶意软件等功能，让用户得到更高的安全性，从而超越了传统的状态防火墙和Web过滤器，免除让用户在网络中安装多台设备的烦恼，而且提供业界顶尖的性能表现。此外，丰富的仪表板和报告提供给用户下一代防火墙才有的可视化和控制。

最安全的网络保护解决方案

随着网络环境、使用模式和威胁的不断变化，现在的企业正面临着各种挑战。FortiGate-600D下一代防火墙可以帮助企业解决这些挑战，它提供了丰富的功能，经过验证的安全性，并且简单易用。管理员还能够获得关于网络和威胁状况的至关重要的实时可视性，使他们能够迅速采取有效的行动。

顶尖的防御能力

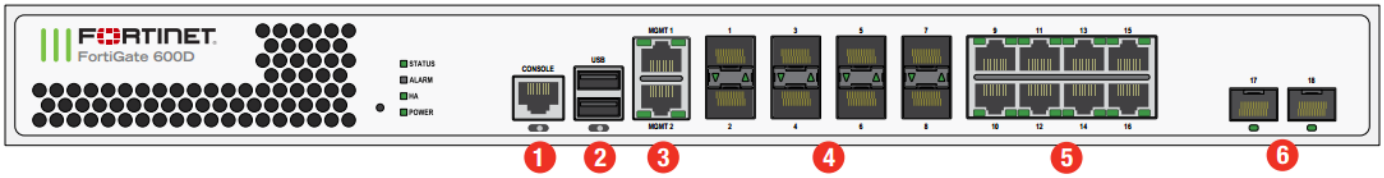
FortiGate设备的FortiOS 网络安全平台会定期提交给独立测试机构进行真实环境的测试，因此您可以确信其有效性。您还可以看到他们是如何与行业内其他产品对比的。 FortiGate参与NSS数次防火墙、数据中心防火墙、IPS、下一代防火墙测试，并且均获得“推荐”级别。证明了FortiGate产品的技术领先性以及卓越的性能表现是行业翘楚。

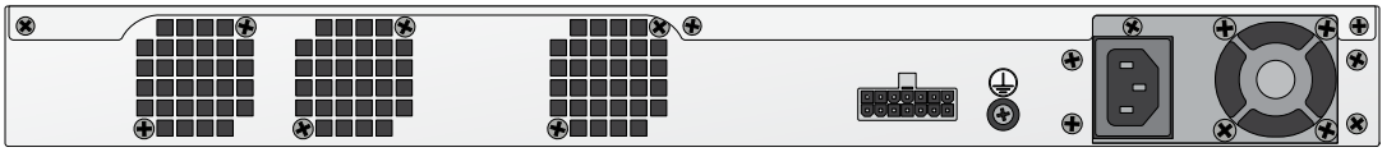
专为如今和未来的数据中心网络安全需求而设计

- 更高级的下一代防火墙，从性能、功能、易用性方面全面超越已有同水平产品。
- 搭载 FortiASIC 专用处理芯片提供卓越的性价比
- NSS Labs 推荐级 NGFW 与 NGIPS
- 屡获殊荣的反病毒引擎。
- 由 Fortinet 的全球技术支持与 FortiGuard 威胁研究团队二十四小时的保护和支持为后盾
- 更简单易用：管理员能够获得关于网络和威胁状况的至关重要的实时可视性，使他们能够迅速采取有效的行动

硬件及外观

FortiGate 600D





Interfaces

1. Console Port
2. 2x USB Ports
3. 2x GE RJ45 Management Ports
4. 8x GE SFP Slots
5. 8x GE RJ45 Ports
6. 2x 10 GE SFP+ Slots

FortiASIC NP6 与FortiASIC CP8

FortiASIC专用处理器是Fortinet 三大核心优势之一。定制的FortiASIC™处理器能够提供无与伦比的网络层处理能力以及加速检测应用层内容。FortiASIC专用芯片提供高性能的安全保护，通过众多第三方机构的严苛测试，确保您的网络安全设备不再是网络瓶颈。

FortiASIC NP6 –FortiASIC第六代网络处理器：

应用了Fortinet 最新研发的FortiASIC NP6网络处理器芯片，协同FortiOS 5，可提供的功能加速包括：

- 单颗芯片提供高达40 Gbps的IPv4与IPv6 防火墙性能
- 超级防火墙性能（IPv6与IPv4性能相同）、SCTP与多播流量，同时延迟率低于2微秒
- VPN、CAPWAP与IP通道加速
- 异常入侵防御，检验和卸载与数据包分片
- 流量控制与优先列队

FortiASIC CP8 –FortiASIC第八代内容处理器：

FortiASIC CP8 内容处理器主要工作于外向的流量，可提供高速的加密与内容检测服务包括：

- 基于签名的内容检测加速
- 加密解密卸载流量

最安全的网络保护解决方案

随着网络环境、使用模式和威胁的不断变化，现在的企业正面临着各种挑战。FortiGate-600D下一代防火墙可以帮助企业解决这些挑战，它提供了丰富的功能，经过验证的安全性，并且简单易用。管理员还能够获得关于网络和威胁状况的至关重要的实时可视性，使他们能够迅速采取有效的行动。

面向未来的安全网关

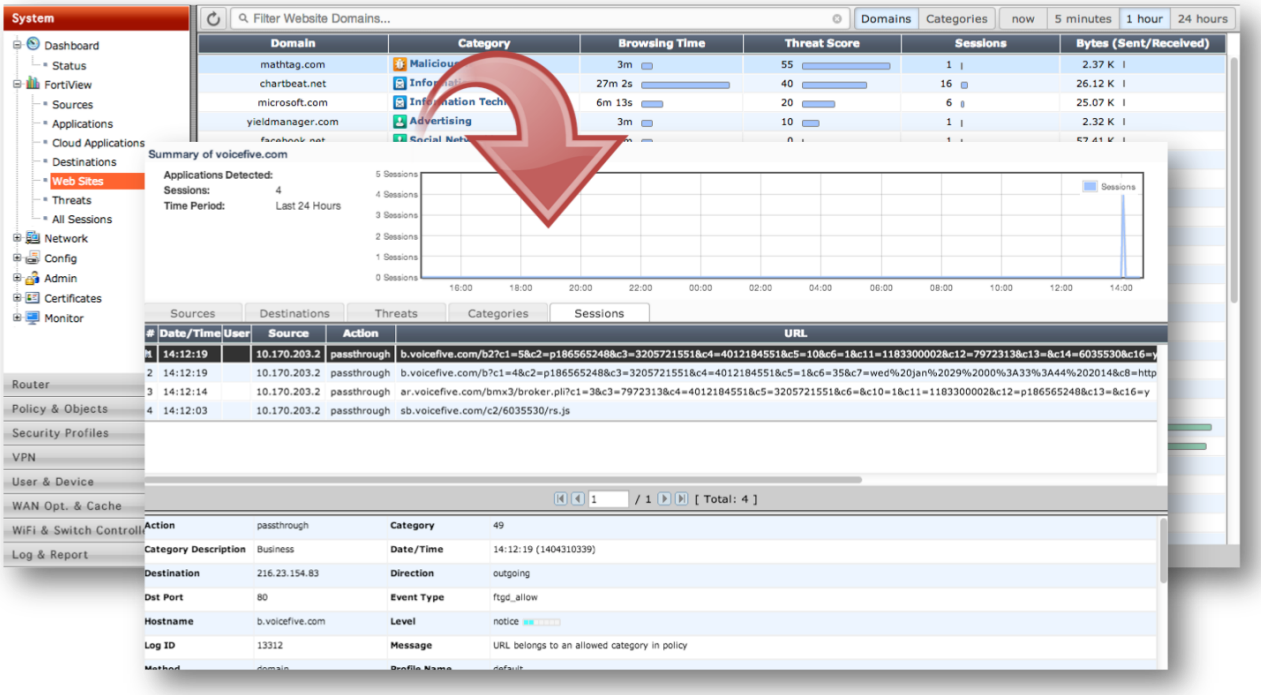
FortiOS可扩展架构让企业能够轻松地激活安全模块，而不需要复杂的授权和硬件模块。单窗格管理和关联的日志及报表还可以让管理员享受灵活平台带来的好处。通过这些功能，FortiOS让客户能够显著降低总体拥有成本和复杂性，同时实现高价值的安全保护。

简单易用

管理员的配置错误通常被认为是企业安全保护中最薄弱的环节。通过简单而创新的用户界面，FortiOS能够帮助降低运营成本，减少IT人员的工作量以及错误率。同时，直观的单窗格管理能够确保一致的政策创建和执行，并帮助最大限度地减小部署和配置挑战。

全面的可视性

FortiOS提供更好的流量可视性，并提供对用户、设备、应用程序和敏感数据的更一致、更细粒度的控制。仪表板设备还允许管理员快速查看和了解实时网络活动和威胁情况。另外，企业还可以查看全面的背景知识，例如设备类型和带宽使用情况。



FortiView - 实时查询插件和深层信息面板

广泛的网络支持

FortiOS支持多种网络设计要求，并可与其他网络设备互操作。这包括对各种路由、多播和网络弹性协议的支持。管理员还可以配置接口用于VLAN和单臂嗅探器模式，它还提供强大的高可用性和集群选项。

智能流量处理

除基本访问控制之外，FortiOS允许企业进行更多设置。例如，通过分析已允许的流量，FortiGate能够应用复杂的决策，例如策略路由和流量整形。

统一接入安全

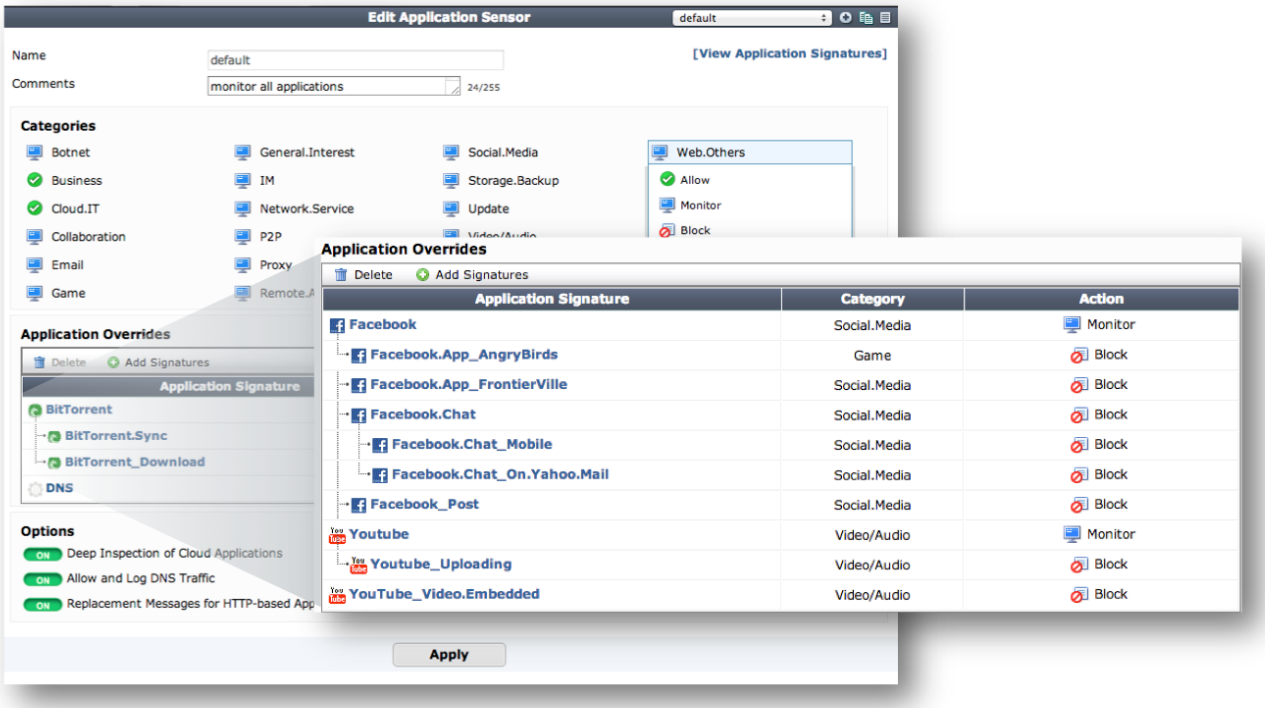
FortiOS让企业可以在不同类型的网络部署一致的政策，这帮助简化了现在复杂环境中的政策执行。而且，其无线控制器功能还将相同的保护扩展到了无线网络。同时，端点控制功能可以为移动用户配置和执行安全功能，即使他们不在办公室办公。

基于身份执行策略

FortiOS同时支持本地和远程身份验证服务（例如LDAP、Radius和TACACS+）来识别用户，以及部署相应的访问政策和安全配置文件。FortiOS简化了基于身份的部署，同时提供各种单点登录功能，确保无缝的用户授权体验。FortiOS还可以捕捉终端服务用户或无线登录凭证，并智能地部署策略和配置文件，而无需额外的用户输入。

先进的应用程序控制

在目前的Web 2.0和云环境中，识别应用程序并执行相关的政策是至关重要的功能。FortiOS提供细粒度控制，并能够识别超过3000个应用程序--即使是在加密通道的应用程序。它还可以提供安全保护，以抵御很容易规避传统防火墙的复杂的僵尸网络活动。



细粒度的设置提供强大的应用控制

高级入侵防护

Fortinet下一代IPS技术可以在应用程序层保护网络，帮助抵御可规避安全技术的高级攻击。通过分析背景信息和行为，该技术还可以阻止未知零日攻击损坏关键数字资产和服务。FortiGuard入侵防御服务拥有超过7000种已知威胁的数据库，并为用户更新了最新的威胁信息来对付网络级的威胁。

功能强大且可扩展的管理

FortiManager可以帮助企业轻松地配置和管理企业中成千上万的FortiGate，它还允许企业根据合规或操作要求部署一致的政策以及配置工作流程。该功能支持详细的配置审计跟踪，并可以放置在具有FortiAnalyzer的受保护存储的外部。并且通过我们的技术联盟，FortiOS还可以与第三方解决方案整合，例如网络管理系统和SIEM。

世界一流的技术支持和文档

Fortinet FortiCare支持产品为所有Fortinet产品和服务提供全面的全球支持。您可以放心您的Fortinet安全产品在以最佳性能运行，并保护您的用户、应用程序和数据的安全。

连续七年荣誉GartnerUTM魔力象限领导者

功能简介

网络服务与支持

内建 DHCP,NTP,DNS 服务器以及 DNS 代理

FortiGuard NTP,DDNS 和 DNS 服务

接口模式：Sniffer,loopback,VLAN（802.1Q），软件交换（vSwitch）

静态和策略路由

ECMP 的 WAN 负载均衡和冗余

动态路由协议：RIPv1 和 v2，OSPF v2 和 v3，ISIS，BGP4

多播流量：稀疏模式与密集模式，PIM 支持

内容路由：WCCP 和 ICAP

显示代理支持

IPv6 支持：基于 IPv6 的管理，IPv6 路由协议，IPv6 隧道，防火墙和 NGFW 的 IPv6 流量，NAT64，IPv6 IPSec VPN

用户和设备认证控制

本地用户数据库

远程用户认证服务支持：LDAP,Radius 和 TACACS+

单点登录：Windows AD, Novell eDirectory，FortiClient，Citrix 和终点服务器代理，Radius（账号消息），用户接入（802.1x，portal）认证

PKI 和认证：X.509 认证，SCEP 支持，认证登陆请求（CSR）创建，认证到期自动更新，OCSP 支持

双因子认证：第三方支持，整合令牌服务器与物理令牌，软件令牌及短信息

设备认证：设备和 OS 指纹，自动分类，清单管理

用户和基于设备的策略

防火墙

操作模式：NAT/路由和透明（桥）

会话助手&ALG：dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323,MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle)

VoIP 流量支持：SIP/H.323 /SCCP NAT traversal, RTP pin holing

协议类型支持：SCTP, TCP, UDP, ICMP, IP

分块或全局策略管理显示

策略对象：预定义，自定义，对象分组、标签和克隆

地址对象：子网，IP，IP 范围 ，地理 IP，FQDN

NAT 配置：基于每条策略，集中 NAT 表

NAT 支持：NAT64, NAT46, 静态 NAT, 动态 NAT, PAT, Full Cone NAT, STUN

流量整形和 QoS：共享策略整形，per-IP 整形，最大带宽与带宽保证，每 IP 最大并发连接数，流量优先级，服务类型（TOS）和服务区分（DiffServ）支持

VPN

IPSec VPN：

-远程对端支持：IPSEC 兼容拨号客户端，对端支持静态 IP/动态 DNS

- 认证方式: 认证, 预共享密钥

- IPSec Phase1 模式：积极的和 Main（ID 保护）模式

- 对端接受选项：任何 ID, 特定 ID, 在拨号用户组中的 ID

- 支持 IKEv1, IKEv2 (RFC 4306)

- IKE 模式配置支持(作为服务器或客户端), DHCP over IPSEC

- Phase 1/Phase 2 建议加密: DES, 3DES, AES128. AES192, AES256

- Phase 1/Phase 2 建议认证: MD5, SHA1, SHA256, SHA384, SHA512

- Phase 1/Phase 2 Diffie-Hellman 组支持: 1, 2, 5, 14

- XAuth 支持，作为客户端和服务器模式

- XAuth 作为拨号用户: 服务器类型选项(PAP, CHAP, Auto), NAT Traversal 选项

- 可配置的 IKE 加密密钥过期时间, NAT traversal 激活频率

- 离线对端检测

- 重播检测

- 自动密钥保持激活 Phase 2 SA

IPSEC VPN 部署模式: 网关到网关, hub-and-spoke, 全网状,冗余隧道, VPN termination 在透明模式

IPSEC VPN 配置选项: 基于路由或基于策略

定制化 SSL VPN portal: 颜色主题, 布局, 书签, 连接工具, 客户端下载

SSL VPN 域支持: 允许与用户组（URL 路径，设计）相关的多个自定义的 SSL VPN 登录

单点登录书签：重用以前登录或预定义的凭据访问资源

个人书签管理：允许管理员查看和维护远程客户端书签

SSL portal 并发用户数限制

每个用户选择一个时间登录：防止并发登录使用相同的用户名

SSL VPN Web 模式: 对于只配备一个网络浏览器和支持的 Web 应用程序等等的轻远程客户端 ，如:

- HTTP/HTTPS Proxy, FTP, Telnet, SMB/CIFS, SSH. VNC, RDP, Citrix

SSL VPN 的隧道模式：对于运行各种客户端和服务器的远程计算机应用，SSL VPN 客户端支持 MAC OSX，Linux 的，Windows Vista 和 64 位 Windows 操作系统

SSL VPN 的端口转发模式：使用一个 Java applet，监听本地端口用户的计算机。当它接收到来自客户端应用程序的数据，则端口转发模块进行加密，并将数据发送到 SSL VPN 设备，然后将流量转发到应用服务器

在 SSL 隧道模式连接之前进行主机完整性检查和操作系统检查（仅适用于 Windows 终端）

Per portal 的 MAC 主机检查

在 SSL VPN 会话结束前缓存清理选项

虚拟桌面选项，从客户端计算机的桌面环境隔离的 SSL VPN 会话

VPN 监控：查看和管理当前的 IPSEC 和 SSL VPN 连接的详细信息

其他 VPN 支持：L2TP 客户端和服务器模式，L2TP over IPSEC,

PPTP, GRE over IPEC

IPS

IPS 引擎：7,000+最新的签名，协议异常检测，自定义签名，手动，自动拉或推签名更新，整合云端威胁特征库

IPS 动作：默认，监控，阻断，重置，或检疫（攻击者 IP，攻击者 IP 和目标 IP，入向流量接口）与到期时间

过滤选项：严重程度，对象，操作系统，应用程序和/或协议

数据包日志记录选项

从指定的 IPS 特征对 IP 的豁免

IPv4 和 IPv6 的基于速率的 DoS 保护（适用于大部分机型）与阈值针对 TCP SYN 洪水的设置，TCP / UDP/ SCTP 端口扫描，ICMP 扫描，TCP / UDP/SCTP/ ICMP 会话洪水（源/目标）

IDS sniffer 模式

支持 IPS bypass

应用控制

检测超过 3000 种应用在下列 19 个分类中：

Botnet, 协作, Email, 文件共享, 游戏, 普通 internet, IM, 网络服务,P2P, 代理, 远程访问, 社交媒体，存储备份, 更新, 视频/音频, VoIP, 产业, 特殊的, Web (其他)

支持提交自定义应用签名

高级的即时通信应用于 Facebook 控制

过滤选项：类别，流行度，技术，风险，供应商和/或协议

动作：阻断，重置会话，只 监控，应用控制流量整形

威胁防护

全球 IP 信誉数据库提供僵尸网络服务器 IP 阻断

本地反病毒数据库

流扫描反病毒：支持的协议- HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S,IMAP/IMAPS, MAPI, FTP/SFTP, SMB, ICQ, YM, NNTP

代理模式反病毒：

-协议支持：HTTP/HTTPS，STMP/SMTPS，POP3/POP3S，IMAP/IMAPS, MAPI,

FTP/SFTP, ICQ, YM, NNTP

-外部云沙盒（文件分析）支持

-文件提交黑名单和 白名单

-文件检查

-启发式扫描选项

Web 过滤检查模式支持：基于代理，基于流 和 DNS

基于 URL、Web 内容和 MIME 头的 手动定义 Web 过滤

基于云的实时分类数据库进行动态 Web 过滤：超过 2 亿 5 千万 URL，被分为 78 个类别，70 种语言

安全搜索增强：透明插入安全搜索参数查询，支持 Google，Yahoo！，Bing&Yandex，可定义的 YouTube 教育过滤

基于代理的 Web 过滤还支持如下附加功能：

-过滤 Java Applet, ActiveX 和/或 cookie

-阻断 HTTP post

-记录搜索关键词

-基于 URL 的图片速率

-基于速率阻断 HTTP 重定向

-对某些类别可由于隐私原因豁免扫描加密连接

-基于类别的 Web 浏览配额

Web 过滤本地分类和分类打分重写

Web过滤配置重写：允许管理员 暂时分配不同的配置给用户/用户组/IP

代理规避预防：代理网站类别拦截，速度由域名和 IP 网址地址块从高速缓存和翻译网站重定向，代理规避应用阻塞（应用控制），代理行为阻断（IPS）

DLP 信息过滤 ：

-协议支持：HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP

-动作：只记录，阻断，检查用户/IP/接口

-预定义过滤器：信用卡号，社交安全 ID

DLP 文件过滤：

-协议支持：HTTP-POST，HTTP=-GET,SMTP，POP3，IMAP，MAPI, FTP, NNTP

-文件选项：大小，文件类型，水印，内容，是否被加密

DLP 水印：允许通过 FortiGate 设备和过滤器，包含一个文件

企业标识（文本字符串）和灵敏度等级（严重，私人和警告）

隐藏水印。支持 Windows 和 Linux 的免费水印工具。

DLP 指纹：从截获的文件生成一个校验和指纹，并在指纹数据库中进行对比

DLP 归档：记录 email, FTP, IM, NNTP, 和 web 流量中的全部内容

终端控制

通过客户端软件管理网络设备：

-状态检查：强制客户端软件安装和所需的设置

-客户端配置监控：根据设备类型/组和/或用户/用户组推送并更新如 VPN 和 Web 过滤配置

-“离线”安全强化 ：当不受网关安全保护时，自动激活安全配置

-允许客户端激活日志部署

客户端软件支持：Windows，OS X，iOS，Android

高可靠性

HA 模式：主被，双主，虚拟集群，VRRP

冗余心跳接口

HA 保留管理接口

故障转移：

-端口，本地和远程链路监控

-状态故障切换

-亚秒级故障切换

-故障检测通知

部署选项：

-全网状 HA

-地理分布式 HA

独立模式会话同步

管理、监控和诊断

管理接入：通过 Web 浏览器的 HTTPS，SSH，telnet，console

Web UI 管理语言支持：英语，西班牙语，法语，葡萄牙语，

日语，简体中文，繁体中文，韩语

集中管理支持：FortiManager, FortiCloud 服务, web 服务 API

系统集成：SNMP, sFlow, syslog, 合作伙伴

快速部署：USB 自动安装，本地和远程脚本执行

动态，实时面板状态显示和监控插件

日志和报告

日志支持：多 syslog 服务器，多 FortiAnalyzer，WebTrends 服务器，FortiCloud 托管服务

日志记录，使用 TCP 选项（RFC3195）

加密日志记录，日志整合到 FortiAnalyzer

批量日志上传

流量细节日志：转发，违规会话，本地流量，无效包

整合事件记录：系统和管理员行为审计，路由和网络，VPN，用户认证，WiFi 相关事件

流量摘要日志格式化选项

IP 和服务端口名决定选项

认证

ICSA 防火墙, SSL VPN, IPSEc VPN, AV 和 IPS 认证

IPv6 Ready

FortiGate-600D			
硬件规格		**外观和环境**	
GE SFP+ 接口槽	2	重量	11.46 lbs (5.2 kg)
GE SFP 接口槽	8	高x宽x长(inch)	1.73 x 17 x 12.68
GbE RJ45 接口	8	高x宽x长(mm)	44 x 432 x 322
Console 接口	1	外观	机架 1U
GE RJ45 管理接口/HA 接口	2	耗电量（平均/最大）	113 W / 202 W
内部存储	120 GB	散热	690 (BTU/h)
设备性能		冗余电源	外置，支持 FRPS-100
IPv4 防火墙吞吐量 (1518 / 512 / 64 Bytes UDP)	36 / 36 / 24 Gbps	电源	100–240V AC, 60–50 Hz
防火墙延迟 (64 Bytes)	3 us	湿度	20 to 90% 无冷凝
包转发率	36 Mpps	运行温度	32–104°F (0–40°C)
最大并发会话	550 万	存储温度	-31–158°F (-35–70°C)
每秒新建会话	27 万	运行高度（最高）	2250m
最大防火墙策略数	10000		
IPSec吞吐量	20 Gbps	**合规与认证**	
网关到网关IPSec VPN隧道 客户端到网关IPSec VPN隧道	2,000 10,000	合规	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB
SSL VPN吞吐量	2.2 Gbps	认证	ICSA Labs: Firewall, IPSec, IPS, Antivirus, SSL VPN
SSL VPN隧道模式最大用户数	5000		
IPS吞吐量	7 Gbps		
虚拟防火墙（最多）	10		
最多支持FortiAP	1024		
最多支持FortiToken	1000		
最多支持FortiClient	2000		
HA	主备，主主，集群		

注意：所有性能指标都是“最大”值，并且根据设备配置会有变化。反病毒性能是在 44K 字节 HTTP 文件情况下测得的结果。IPS 性能是在使用 1M 字节 HTTP 文件情况下测得的结果

GLOBAL HEADQUARTERS
Fortinet Inc.
1090 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737

飞塔信息科技（北京）有限公司
北京市海淀区北四环西路 52 号方正国际大厦 12 层, 100080
Tel:010-62690376
Fax: 010-62690239

上海销售办公室
上海市普陀区中山北路 3323 号春之声大厦 1605 室, 200062
Tel:021-52049325
Fax: 021-5204 9326

广州销售办公室
广州市天河区体育西路 101 号维多利广场 B 座 1205 室,510620
Tel: 020-38105509
Fax:020-38105507