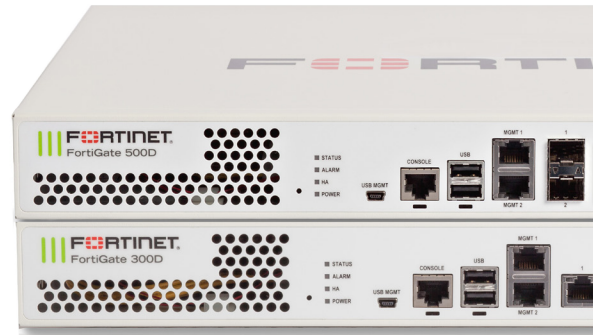


FortiGate®-300D & 500D

为中型企业和分支机构提供最佳安全保障



随着网络威胁和频繁数据泄露事件持续成为头条新闻，不论规模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，比如从传统防火墙升级到下一代防火墙，也希望包括像反恶意软件和web过滤等功能。

高速下一代防火墙

Fortinet的FortiGate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。

顶尖的防御能力

最后，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Nessus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。Fortinet公司的FortiGate NGFW产品提供了所有这一切都以实惠的价格为基础，满足您的预算。

关键特性

行业验证	提供给您在行业中屡获殊荣的下一代防火墙
高性能 硬件平台 整合安全架构	超高性能, 多功能融合, 简便管理, 降低成本
集中管理和报告	强大的管理系统, 可以快速提供和部署, 监控设备和威胁的状态, 同时提供可自定义的报告

专为如今和未来的网络安全需求而设计

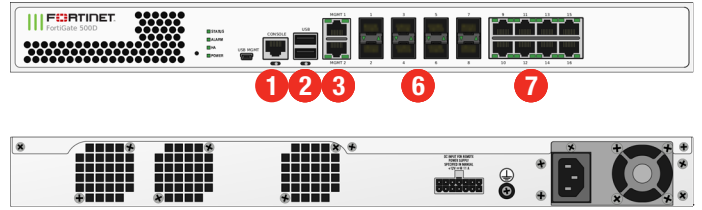
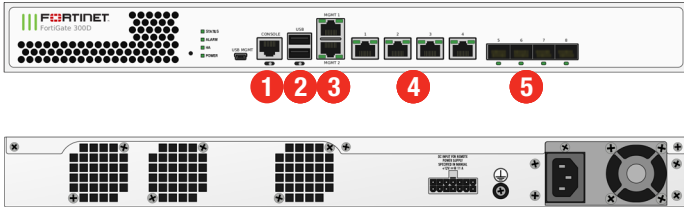
- 搭载FortiASIC专用处理芯片提供卓越的性价比
- FortiOS下一代防火墙模块可以帮助企业面对安全挑战，它提供了丰富的功能，经过验证的安全性，并且简单易用。管理员还能够获得关于网络和威胁状况的至关重要的实时可视性，使他们能够迅速采取有效的行动
- 由Fortinet的全球FortiCare技术支持与FortiGuard威胁研究团队二十四小时的保护和支为后盾



FortiCare
Worldwide 24x7 Support
support.fortinet.com




FortiGuard
Threat Research & Response
www.fortiguard.com



接口

1. Console 端口 (RJ45)
2. 2x USB 端口
3. 2x GE RJ45 管理端口
4. 4x GE RJ45 端口
5. 4x GE SFP 端口

6. 8x GE SFP 端口
7. 8x GE RJ45 端口



Powered by FortiASICs

- 定制的FortiASIC™处理器提供加速检测恶意内容，支持数千兆的性能
- 其他安全技术不能够防护当前广泛的基于内容和基于连接的威胁，因为他们依赖于通用CPU，引起严重的性能缺口
- 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

内容处理器

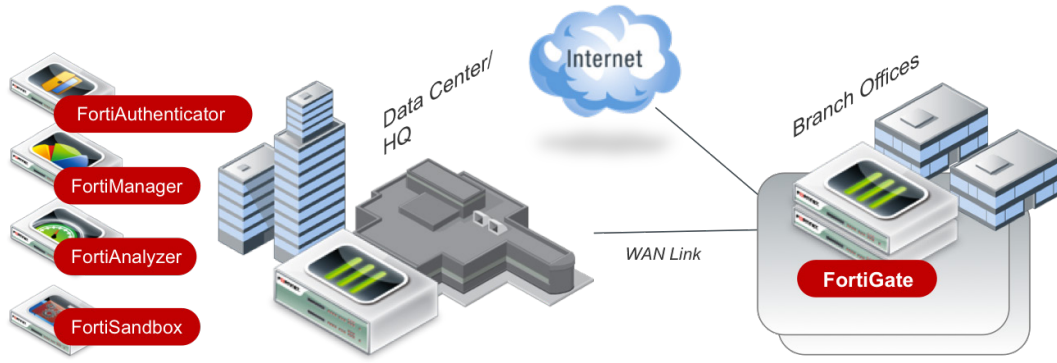
FortiASIC CP8 内容处理器主要工作于外向的流量，可提供高速的加密与内容检测服务包括：

- 基于签名的内容检测加速
- 加密解密卸载流量

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：

- 超级防火墙性能 (IPv4/IPv6)、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



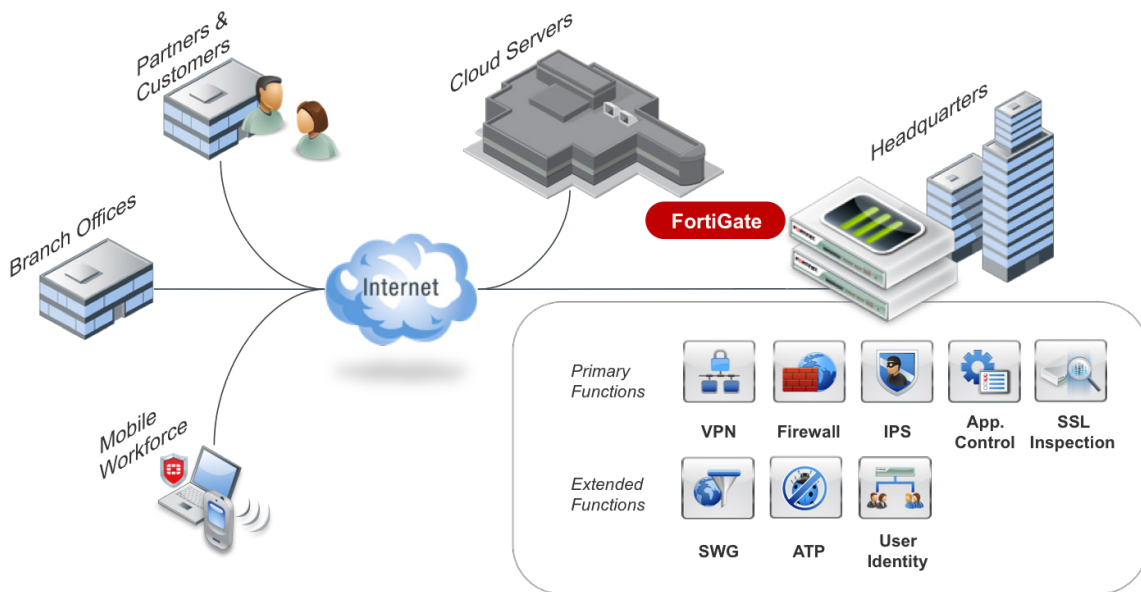
FortiGate 作为分支机构防火墙部署

分支机构防火墙

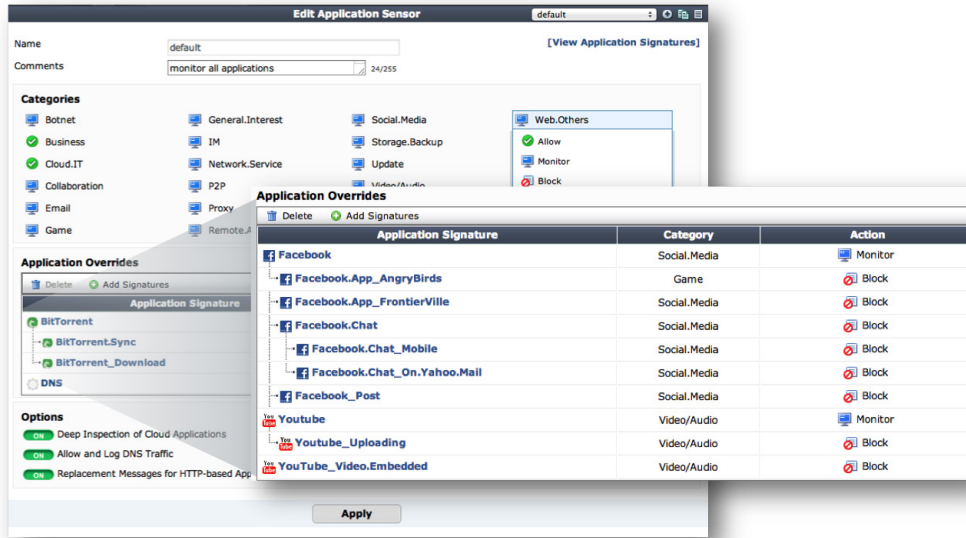
今天的分支机构的安全网关已经不再只是一个基本的防火墙和站点到站点的VPN网关。很多的应用程序都是基于云的，不论是公共应用还是私人应用，网关要能够提供两种接入的可用性和安全性的相关要求。安全网关将需要强大的网络和高可用性功能，包括智能广域网链路转发和灵活的网络部署选项。从安全的角度来看，一个分公司的防火墙应该具备识别用户，位置，设备和应用程序的能力，从而提供控制力与更精细的粒度和基于信誉的访问。随着企业的发展，Fortinet的解决方案也在发展，分支机构可以使用FortiSandbox进行文件分析以识别未知威胁，使用FortiAuthenticator进行用户接入管理与身份认证。从而达到端到端的安全保障。

中型企业边界防火墙

Fortinet的中端防火墙是成长型企业的完美选择，因为能够提供给他们足够的敏捷性和高性能的网络安全。FortiGate300D和500D不但提供超出预期的良好保护能力，它们还适用于整合其他安全组件。这使组织能够显著降低的TCO，简化了网络。不像其他NGFW（下一代防火墙），FortiGate由FortiASIC提供安全无妥协的性能动力。它们运行在世界上众多的知名企业，能够满足每个组织的独特需求，全都依赖FortiOS这款最先进的安全操作系统。更多先进的功能，如集成的端点控制和令牌服务器可以帮助企业快速部署增强安全性和管理移动办公的员工，同时基于设备的策略部署，以实现安全BYOD。



FortiGate 作为中型企业边界防火墙部署



细粒度的设置提供强大的应用控制

经过行业验证的安全性

与其它竞争产品相比，运行FortiOS的FortiGate拥有更多的第三方行业评测机构的证书，这保证该产品的功能质量，并为您提供一流的保护

与FortiManager设备集成时，可以设置复杂的政策实施和配置工作流程，以满足合规性和操作要求的能力。该FortiManager设备还提供了日志记录，并且简化并降低总体拥有成本报告模块。

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

基于身份执行策略

FortiOS支持本地和远程认证服务，如LDAP，RADIUS和TACACS+来识别用户并应用相应的访问策略和安全配置文件。它可以简化基于身份的实现，并提供单点登录功能的无缝用户授权体验。FortiOS具有较强的PKI和基于证书的认证服务，同时还集成了内部双因素身份认证服务器进行额外的安全性。

全面的可视性

FortiView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。仪表盘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

为了解决如今普遍使用个人设备带来的安全问题，FortiOS提供状态监控，即让用户设置更智能的安全策略最先进的设备识别能力。

详细的日志提供了深刻的网络洞见，通过FortiGate设备产生的全面报告有助于企业准确地把握网络情况的趋势

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。

强大的策略管理

可根据自己的喜好选择两种类型的策略管理方式：全局和局部视图。策略对象可以很容易地在策略表中编辑，复制或移动。强大的管理功能包括策略对象的搜索，标记，排序和过滤。

高级入侵防护

FortiGuard入侵防御服务拥有超过8000个IPS签名，并持续为

特点

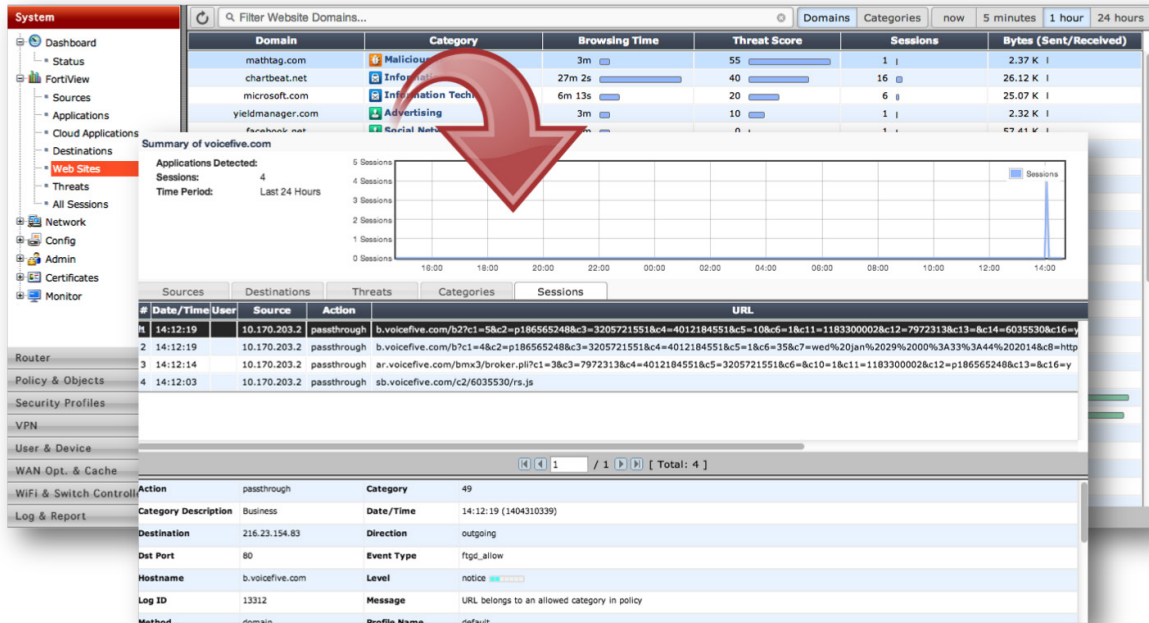
用户更新最新的威胁信息来对付网络级的威胁。Fortinet下一代IPS技术可以在应用程序层保护网络，帮助抵御可规避安全技术的高级攻击。通过分析背景信息和行为，该技术还可以阻止未知零日攻击损坏关键数字资产和服务，哪怕这些攻击还没有签名特征存在。

不只是下一代防火墙

我们的Web安全网关功能允许您阻止最终用户在不知情的访问恶意网站，保护公司隐私信息不被暴露在互联网上，并维持一个安全和高效的工作环境。实时仪表板为管理员提供可视化的最终用户活动，同时丰富的报告不断执行最新的更新。高级

策略引擎为您提供所需的高级工具，例如基于时间的配额，用户策略重写等等。

认识到尽管所有最新的安全控制都部署了，有针对性的高级威胁仍可能成为漏网之鱼，因此企业有必要增加额外层面的检查，在补充建立的威胁防御应该专注于先进的威胁检测。通常被称为“沙盒”或违规检测，Fortinet提供内部部署和基于云的选项来扩展你的下一代防火墙。



FortiView - 实时查询插件和下钻信息面板

FortiGuard 安全服务 & FortiCare 支持

- 顶尖的安全专家
我们拥有200余位安全研究人员，以及庞大的数据收集系统，在世界范围内多个国家部署最先进的分析系统检查最新的网络违法犯罪活动和技术，提供适合您的组织的实时保护。通过第三方评估，我们的产品和服务得到了很高的评价，通过我们不断进行的安全更新，您可以放心应对不断变化的复杂的或有针对性的威胁。
- 世界级支持团队
让您的网络正常运行，并能够快速解决问题是至关重要的。我们团队拥有快速响应的资深技术支持工程师，再加上全面的资源，随时准备满足您的关键需求。另外，Fortinet公司还提供各种支持服务的，满足您的组织和项目需求。

规格参数

	FORTIGATE-300D	FORTIGATE-500D
接口 & 模块		
GE RJ45 接口	6	10
GE SFP 插槽	4	8
USB (客户端 / 服务器)	1/2	1/2
RJ-45 Console 接口	1	1
本地存储	120 GB SSD	120 GB SSD
系统性能和功能		
IPv4 防火墙吞吐量 (1518 / 512 / 64 byte, UDP)	8 / 8 / 8 Gbps	16 / 16 / 16 Gbps
防火墙延迟 (64 byte, UDP)	3 µs	3 µs
防火墙吞吐量 (包每秒)	12 Mpps	24 Mpps
并发会话数 (TCP)	6 Mil	6 Mil
每秒新建连接数 (TCP)	200,000	250,000
防火墙策略	10,000	10,000
IPSec VPN 吞吐量 (512 byte)	7 Gbps	14 Gbps
网关到网关 IPSec VPN 隧道	2,000	2,000
客户端到网关 IPSec VPN 隧道	10,000	10,000
SSL VPN 吞吐量	350 Mbps	400 Mbps
并发 SSL-VPN 用户 (建议最大)	500	500
IPS 吞吐量	2.8 Gbps	5.7 Gbps
虚拟防火墙 (默认 / 最大)	10 / 10	10 / 10
最多支持 FortiAP (全部 / 隧道)	512 / 256	512 / 256
最大支持 FortiTokens	1,000	1,000
最多注册终端	600	2,000
HA配置模式	双主、主被、集群	

	FORTIGATE-300D	FORTIGATE-500D
外形和电源		
高 x 宽 x 长	1.73 x 17 x 12.68 in (44 x 432 x 322mm)	1.73 x 17 x 12.68 in (44 x 432 x 322mm)
重量	10.5 lbs / 4.8 kg	10.8 lbs / 4.9 kg
外型	1 RU	1 RU
耗电量 (平均/最大)	106 W / 194 W	113 W / 202 W
电流 (最大)	110V/4A, 220V/2A	110V/4A, 220V/2A
散热	660 BTU/h	690 BTU/h
运行环境和认证		
运行温度	32 - 104 °F (0 - 40 °C)	
存储温度	-31 - 158 °F (-35 - 70 °C)	
湿度	20% to 90% non-condensing	
合规性	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	
认证	ICSA Labs: Firewall, IPSec, IPS, Antivirus, SSL VPN	

Note: All performance values are "up to" and vary depending on system configuration. Antivirus performance is measured using 44 Kbyte HTTP files. IPS performance is measured using 1 Mbyte HTTP files. IPSec VPN performance is based on 512 byte UDP packets using AES-256+SHA1.

For complete, up-to-date and detailed feature set, please refer to the Administration Handbook and FortiOS Datasheet

订购信息

产品	SKU	描述
FortiGate-300D	FG-300D	6 x GE RJ45 接口, 4 x GE SFP 插槽, 120GB 机载存储
FortiGate-500D	FG-500D	10 x GE RJ45 接口, 8 x GE SFP 插槽, 120GB 机载存储
可选配件		
冗余 AC 电源	FRPS-100	外部冗余AC 电源最大支持 4 台设备: FG-200B, FG-300C, FG-310B, FG-200D/240D and FG-300D. 最多两台设备: FG-500D, FDD-400B and FDD-800B
1GE SFP LX 收发器模块	FG-TRAN-LX	1GE SFP LX 收发器模块 适合全部 SFP 和 SFP/SFP+ 插槽
1GE SFP RJ45 收发器模块	FG-TRAN-GC	1GE SFP RJ45 收发器模块 适合全部 SFP 和 SFP/SFP+ 插槽
1GE SFP SX 收发器模块	FG-TRAN-SX	1GE SFP SX 收发器模块 适合全部 SFP 和 SFP/SFP+ 插槽



GLOBAL HEADQUARTERS

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

EMEA SALES OFFICE

120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE

300 Beach Road #20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE

Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480

Copyright© 2014 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.