FortiGate® -30-100 系列

适合中小企业和远程办公

Datasheet
技术规格

全面的网络和内容层安全解决方案

企业内的混合式攻击

网络安全攻击会造成企业商务的崩溃。知识资产、收益、客户和企业信息以及其他的重要的关键资源都是攻击的目标。随着大企业强化了网络安全，攻击的主要目标转向中小企业。SOHO类的企业往往缺乏专业的人才和强大的体系来防御这些高精尖的攻击，同样远程和分支机构(ROBO)也普遍缺乏经验处理复杂的安全问题。单一功能的安全产品不足以防御采用了多种手段的混合式攻击。Fortinet公司的FortiGate系列产品把多种安全功能集成在一个平台上，能够有效地防御应用类的基于网络的攻击。

高性价比的网络安全平台

FortiGate 安全平台是基于Fortinet公司的FortiASIC™ 内容处理器技术提供的一整套综合性实时安全解决方案。 涵盖了防火墙、IPSec和SSL VPN、入侵检测防御、Web内容过滤、反垃圾邮件、 防病毒、反间谍软件、应用控制、DLP数据泄漏防护、广域网优化以及集成的流量管理功能。FortiGate能在保证很高的网络性能情况下提供综合安全功能，为当前的企业用户和分支办公室提供了最高性价比的安全防御平台。全系列产品都可以实现HA功能。它可以支持透明模式和路由模式，部分型号硬件支持交换接口和Modem接口，集成了WiFi功能和预留了支持3G/UMTS Modem的PC卡插槽。此外，Fortinet采用的是基于设备的许可证方式，对于SOHO和ROBO企业而言， 是经济有效的。

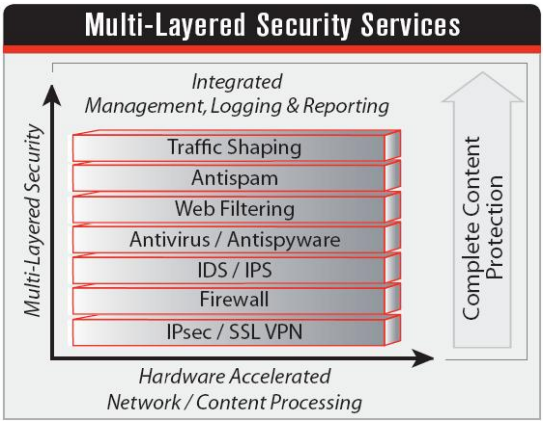
特点和益处

2	中小企业所面临着最主要的安全问题是，如何利用有限的资源处理复杂的网络和内容层的攻击。	多合一的 UTM 产品能够在更高的性价比上实现多层的防御体系。
2	不同厂家提供的单一功能的解决方案往往过于昂贵和复杂	UTM 安全解决方案提供了全套的防御体系，实现单一的管理界面
2	WiFi 技术往往带来了内部攻击的危险	内置的 WiFi 无线技术实现了在无线的层面上的安全防御
2	SOX 和 PCI 条例要求更为强大的日志和报表	UTM 能够提供多种功能，其日志和报表功能尤为丰富。

Fortinet 提供多层安全解决方案

Fortinet的解决方案经济有效地提供一整套综合的安全服务，它能支持很广范围的应用，将多项安全服务与使用方便的高性能设备结合在一起。FortiGuard Subscription Services 提供四种预订服务，即防病毒服务、入侵检测和防御服务、Web过滤服务和反垃圾邮件服务。

FortiCare Support Services 支持的服务包括Email技术支持、硬件保修制度、FortiOS(操作系统)升级等， 确保用户维持安全环境，保持企业的资源安全，防御最新的混合式威胁。

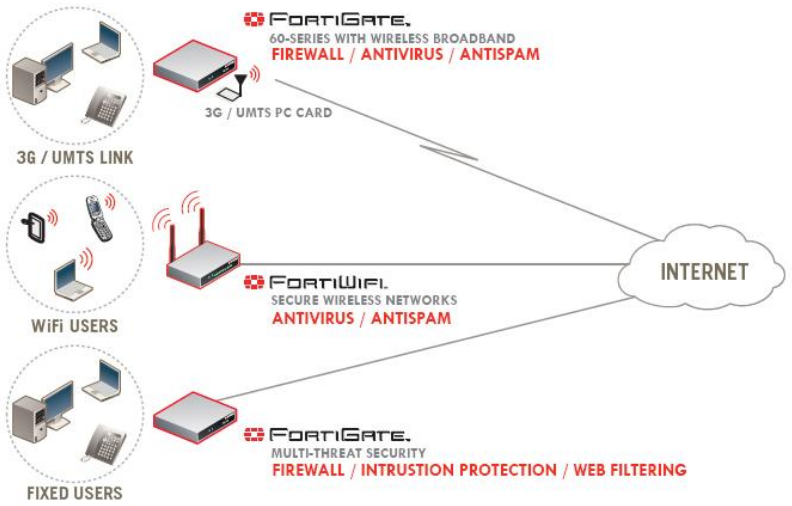


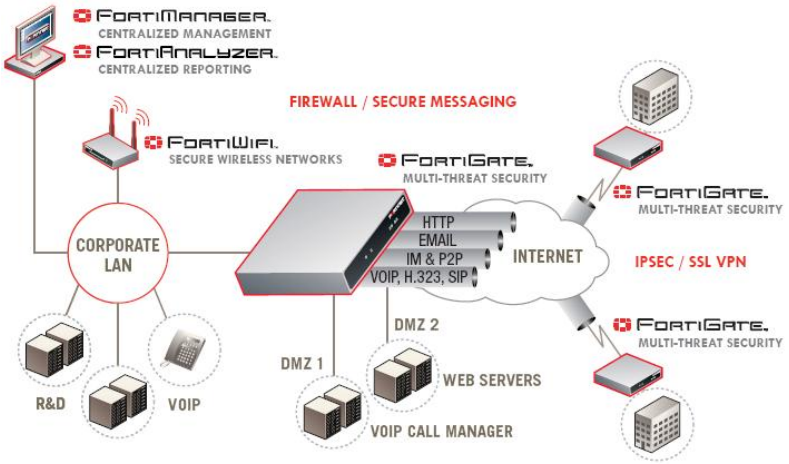
FortiGate 30-100 是为办公室和小企业设计的

小企业的有线或无线的安全网关

(防火墙+防病毒+反垃圾邮件+入侵防护+WEB过滤)

Fortinet将多种安全技术整合在一起为SOHO和ROBO用户提供全面的安全防护。它通过FortiASIC技术实现防病毒、反间谍软件、反垃圾邮件和入侵检测技术，实现对多种攻击的多层次的安全防护，从而从传播根源上解决安全的问题。FortiWiFi支持多个SSID，可以最大程度地满足复杂网络的需求。而且不同的SSID之间可以部署策略，从而提高了安全性。FortiGate-60系列还支持PC卡插槽，可以安装3G/UMTS卡来实现网络的连接。





企业 ROBO 的部署

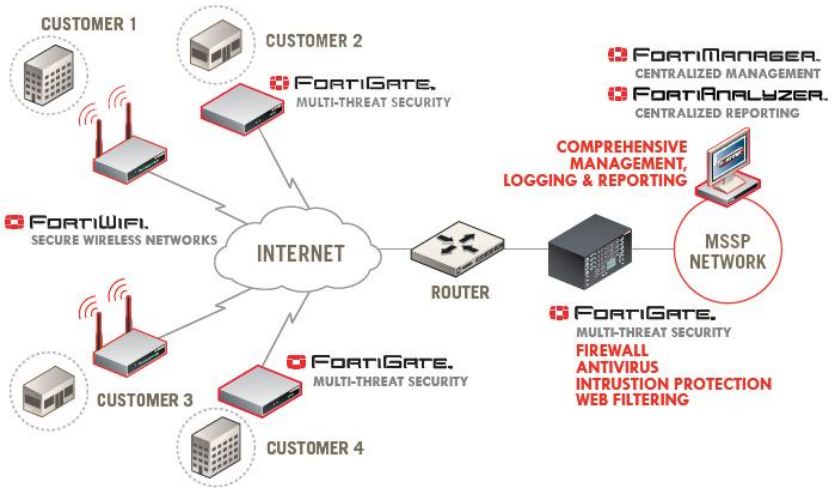
(防火墙+VPN+防病毒+邮件、应用控制)

远程办公往往会用到各种类型的应用，比如消息类的应用或者数据库类的应用。例如，采用了FortiGate产品的防病毒、反垃圾邮件和应用控制功能，可以有效地防止关键数据的丢失，保障邮件和IM类应用的安全。像制造类企业的用户，往往偏向于应用和数据库，能够通过FortiGate提供VPN功能来安全地访问各类的应用服务器。总而言之，Fortinet提供了集中监控、报表、日志和分析来保障远程办公室的安全运转。

安全服务运营商的最佳选择

(反垃圾邮件+防病毒+入侵防御+WEB过滤)

安全服务运营商可以采用分布式安装方式和模块化安全架构，把FortiGate低端产品作为作为CPE设备提供给客户。不同的客户可以根据他们的需求部署不同的服务。比如某些客户仅需要防火墙和入侵防御，另外一些客户需要防火墙和WEB过滤。安全服务运营商通过FortiManager和FortiAnalyzer集中监控所有设备，实现报表、日志和相关性分析。



硬件特性	FortiGate-30B FortiWiFi-30B	FortiGate-50B FortiGate-51B FortiWiFi-50B	FortiGate-60B FortiWiFi-60B	FortiGate-80C FortiGate-80CM FortiWiFi-80CM	FortiGate-110C FortiGate-111C
可配置接口	3/4(交换接口)	3(交换接口)	6	6	8
WAN 接口	1	2	2	2(千兆接口)	2(千兆接口)
DMZ 接口	无	无	1	1	0
模拟 Modem	不支持	不支持	支持	不支持/支持/支持	不支持
无线网 802.11a/b/g	不支持/ Wifi-30B 支持 802.11b/g	不支持/Wifi-50B 支持 802.11b/g	不支持/Wifi-60B 支持 802.11a/b/g	不支持/Wifi-80CM 支持 802.11b/g/n	不支持
USB 接口	不支持	2	2	2	2
PC 卡插槽	不支持	不支持	支持（PCMCIA）	支持（Express 3G）	不支持
内置硬盘	不支持	51B 支持 32G	不支持	不支持	111C 支持 64G
系统性能					
防火墙吞吐量	90Mbps	90Mbps	120Mbps	350Mbps	500Mbps
VPN 吞吐量	5Mbps	48Mbps	64Mbps	80Mbps	100Mbps
防病毒吞吐量(HTTP 32K)	15Mbps	19Mbps	20Mbps	50Mbps	65Mbps
IPS 吞吐量	10Mbps	30Mbps	60Mbps	100Mbps	200Mbps
专用的 IPSec VPN 通道数	5	20	50	200	1500
用户数限制	无	无	无	无	无
并发会话	25,000	25,000	70,000	100,000	400,000
新建会话/秒	3000	3000	3000	5000	10000
策略数	200	2000	2000	2000	4000
尺寸——高	3.175cm/3.51cm	3.51cm	4.45cm	4.45cm	4.57cm
尺寸——宽	17.14cm/21.92cm	21.92cm	27.61cm	27.61cm	33.02cm
尺寸——长	13.21cm/14.73cm	14.73cm	15.57cm	15.57cm	25.4cm
重量	0.36kg/0.68kg	0.68kg	2.48kg	1.59kg	2.7kg
供电要求	交流电源：双 100—240 VAC, 50-60 Hz, 0.8 Amp max(FortiGate 110C/111C 为 2Amp)				
功率(平均)	6W	6W	15W	32W/32W/34W	120W
电气标准	FCC Class A, Part 15, UL/CUL, C Tick, CE, VCCI				
认证	ICSA, NSS, Common Criteria, FIPS 140-2,				
环境要求	工作温度：32 — 104 º F (0 — 40 ºC) 存储温度：-13 — 158 º F (-25 — 70ºC) 湿度：5 到 95% 非凝结				

Fortinet 新一代安全网关解决方案

n 全面的高性价比的安全解决方案	Fortinet 可以实现以下所有的安全功能：防病毒、入侵防御、反间谍软件、Web 内容过滤和反垃圾邮件，其性价比非常高。
n 自动升级病毒库、间谍软件库和 IPS 特征库	可以覆盖 60,000 种攻击的 24 小时升级体系
n 高性能的专有硬件	FortiASIC 实现了超高性能和可靠性，确保安全设备不会成为网络瓶颈
n 集成的多个交换接口	减少对外置的交换机的需求，提高了可连接性
n 简化部署和管理的图形化管理	快速简便的配置界面向导可以帮助管理员完成初始化配置，性能状态和网络安全事件可以在图形界面上清楚地观察到
n 安全的坚固的操作系统	底层的 FortiOS 操作系统通过了 ICSA 认证并提供全面的图形界面

Fortinet在ASIC芯片上有强大的优势：

FortiASIC 系列包括内容层处理芯片(CP)和网络层处理器(NP)两种 ASIC 芯片技术。

FortiASIC-CP 系列是专门用来处理内容层数据，与传统的单纯采用 CPU 来处理数据相比性能更为优越。该芯片是 Fortinet 的专利技术。它的独特的算法可以实现在 VPN 通道上高速扫描病毒，以保障正常的通讯。

FortiASIC-NP 系列是用来加速网络层的数据处理的。它能够达到极高的处理性能和安全性，性价比有很强的优势。

FortiOS：专用的安全操作系统

FortiOS 是 FortiGate 多功能安全平台的操作系统。开发该系统时充分地考虑了安全、性能和可靠性。它充分地发挥了应用层加速和网络层加速的 ASIC 芯片的性能。FortiOS 集成了状态监测防火墙、IPS、防病毒、Web 过滤、反垃圾邮件、IM/P2P、虚拟系统和带宽管理等网络安全功能。FortiOS 提供了全面的 UTM 安全服务、获得了 EAL4+认证。

FortiOS 安全功能

防火墙
ICSA 认证(状态监测防火墙)
NAT/路由, 透明模式 , 混合模式
虚拟防火墙支持(虚拟域)***
标准预定义服务
（SIP,GRE,Netmeeting,h.323,OSPF 等）
自定义服务/服务组/地址/地址组
DHCP 服务器，DHCP 中继
DNS 转发（100A 以下型号）
IP/MAC 地址绑定
基于策略的 NAT
VLAN 标记(802.1Q)
IPV6 策略和路由支持
非 IP 协议透明传输
ALG 应用代理(SIP，H.323, TNS, RSTP，RAS 等 NAT 穿越)
服务器负载分担和健康检查***
策略时间表支持
单机的会话同步支持
基于用户组的认证
细粒度的每策略保护内容表

虚拟专用网(VPN)
ICSA 认证(IPSec)
PPTP, IPSec, L2TP, GRE
SSL VPN***
SSL VPN 支持通道和代理模式
SSL VPN 用户界面自定义
支持 DES, 3DES, AES 256 加密算法，
SHA-1 / MD5 认证
SCEP 简单证书登记协议
OCSP 在线证书状态协议
Hub and Spoke 星型 VPN
DPD 通道状态检测
NAT 穿越，XAUTH 认证
静态 VPN，动态拨号 VPN 支持

支持子网重叠，VPN 通道保持
基于策略和路由的 VPN
OSPF over IPSec***

反病毒
ICSA 认证(网关反病毒)
包括反间谍软件和蠕虫阻断
HTTP/SMTP/POP3//IMAP FTP/IM 协议
SMTPS/IMAPS / HTTPS/POPS 协议*
（CP6 硬件版本）
FortiGuard 网络自动"推送"升级
根据文件尺寸和类型阻断
可定义的服务端口，服务超时控制
支持病毒阻拦和监视模式
多层压缩文件扫描
支持 Tar /gzip/rar/ lzh/ cab/ arj /zip /bzip /bzip2 /msc /UPX
支持文件大小限制 文件类型限制
病毒隔离支持(需要本地硬盘或 FortiAnalyzer 日志服务器)
支持 NAC，可以隔离病毒发送者和病毒来源接口

WEB过滤
82 种 Web 过滤类别，超过 20 亿个 Web 页面
自定义 URL 地址，域名过滤
基本于分值的网页关键词阻断规则
自定义分类库，基于用户认证的分类库控制
URL 地址/域名 黑白名单
阻断 Java Applet, Cookies, Active X

反垃圾邮件
支持 SMTP/POP3/IMAP 协议
支持 SMTPS/POPS/IMAPS 协议(CP6 硬件版本)*
RBL/ORDBL
FortiGuard 垃圾邮件库动态更新
MIME 头检查、关键字/短句过滤

IP 地址和 Email 黑名单/免屏蔽
返回地址 DNS 检查
支持邮件阻断或者标记
支持用户自定义反垃圾邮件阈值

应用控制
超过 1000 种应用程序，分成以下类别：
备份软件类，如 IBM Tivoli, CA MQ 等
商务软件，如指南针，证券之星，分析家
数据库，如 DB2, MySQL, Oracle 等
文件传输类，如 DuDu，纳米盘等
游戏，如赤壁、劲舞团、联众、魔兽等
即时通讯，如 MSN、QQ、新浪 UC、飞信等
媒体类，如土豆、酷 6、PPS 网络电视等
网络服务，如 BGP、ISCSI、QUAKE 等
P2P，如电驴、迅雷、VeryCD
协议命令类，如 ftp 命令，sip 命令
代理软件，如无界、Tor 等
远程控制软件，如 VNC、Pcanywhere 等
工具条，如 Google、yahoo、MSN 工具条等
升级程序，如各种杀毒软件升级，firefox 升级
VoIP，如 Sip，netmeeting, net2phone 等
网站与论坛，如网易论坛、QQ 论坛等
Web Mail，如 126mail、hotmail、QQmail 等
可以对以上应用进行日志和阻断

数据泄露防护 (DLP)
HTTP/SMTP/POP3/FTP/NNTP/IM 协议支持
SMTPS/IMAPS / HTTPS/POPS 协议
（CP6 硬件版本）
支持对压缩文件的扫描和存档
(Tar /gzip/rar/ lzh/ cab/ arj /zip /bzip /bzip2 /msc /UPX)
支持 TXT、PDF 和 Word 类型文档
以动机确认和控制敏感信息
内建模式匹配库
正则表达式匹配引擎

SMTP/POP3/IMAP 可检测邮件头、主题、内容、附件和用户名等
FTP 可检测 GET/PUT 的文件、服务器、用户名等
HTTP 可检测 GET/POST、html 头、URL、CGI、Cookie、内容和用户等
IM 可检测传输文件、内容、发送者、用户等
NTTP 可检测传输文件、内容、用户等
可配置的行为方式(阻断/记录日志)

终端控制（NAC）
监控运行 FortiClient 终端安全的主机
检查 PC 主机是否安装如下安全软件：
防火墙、防病毒、web 过滤
可定制强制分发 FortiClient 安全软件
检查 PC 主机的操作系统和补丁
可定制监控 PC 主机安装软件

入侵防御系统(IPS)
ICSA 认证 (NIPS)
DOS 和 DDOS 攻击控制
3000+多种攻击特征
自定义攻击特征
自动升级攻击特征库
源地址/目的地址 TCP/UDP 会话控制
自定义攻击传感器，
支持基于策略的攻击防御
基于系统，协议，威胁等级的特征库管理
支持 NAC 攻击源自动隔离
可以按时间自动隔离攻击者的 Ip，攻击者和被攻击者的 IP，攻击者的接口。

FortiOS 网络功能

网络/路由
支持多 WAN 链路，多链路负载均衡***
网关健康检测
静态地址/ DHCP / PPPOE/ DDNS 域名
DHCP 服务器/中继
静态路由，策略路由
基于 TOS 的路由
基于用户认证的路由
动态路由 RIP v1 & v2, OSPF, BGP***
Multicast 组播(PIM parse, PIM Dense)***
支持多区域
安全区域间路由

VDOM 虚拟域间路由***
多链路聚合（802.3ad）
支持 IPv6 路由和策略控制
多个二级地址支持
USB 3G modem 支持
VLAN 子接口支持***

广域网优化**
双向优化支持： 网关与客户端之间/网关之间
支持 A-P 和 P-P 模式
支持透明或代理方式的 Web Cache
支持通道模式和 SSL 加密通道

支持对 SSL 加密流量的优化*
集成缓存和协议优化技术
加速 CIFS/FTP/MAPI/HTTP/HTTPS/TCP
需要带硬盘的 FortiGate 设备

流量整形 ***
基于策略的流量管理
Diffserv 服务等级设置
最大/最小/优先 带宽控制
DSCP 服务级别设置
上行下行双向流量控制

高可靠性（HA）***
主-主，主-备
状态失败恢复（FW 和 VPN）
支持全网状 HA
设备失败检测和通告
链路状态监控
链路失败恢复
服务器负载均衡
透明/NAT/路由模式支持

FortiOS管理功能

配置与管理
Console 接口（RS-232）
支持多种语言 Web 管理
支持 Telnet, SSH, HTTP,HTTPS 管理
多级管理员基于角色的权限配置
可信主机控制
基于 Radius 的管理员认证
PKI 证书管理员认证

分区系统软件存储，支持版本回退
USB 系统软件升级，配置文件自动上载
集中管理、策略下发、集中管理平台
FortiManager

日志与监控
分类日志事件，流量，攻击，病毒，网页过滤，垃圾邮件，VOIP，IM、内容存档等
内部日志， 远程 Syslog/WELF 服务器日志

可选的 FortiAnalyzer 日志平台，支持丰富的图形实时和历史数据显示、查询， 300 种以上自定义报表
本地显示远程 FortiAnalyzer 日志系统管理
SNMPv1/v2/ 支持 Email 事件告警
可选的 FortiGuard 分析与管理服务

防火墙用户认证
本地数据库
Windows AD 认证

RADIUS/LDAP 认证
TACACS+PKI
IP/MAC 地址绑定
IPSEC VPN Xauth 扩展认证
RSA SecurID 认证
FSAE 一次性认证支持

UTM管理界面定义
自定义基于WEB的管理菜单

*采用了 CP6 芯片的产品支持该功能，如 FG110/ FG310B/FG620B/FG3016B FG3600A /FG 3810A/FG 5001A
**只有具有硬盘的特定型号才支持，如 FG51B/FG111C/ 配置 AMC 存储的 FG310B FG620B FG3016B FG3600A FG3810A FG5001A-SW
*** FG30B 和 FW30B 不支持

标准FortiGuard升级服务
包含以下内容(一个月)：
- 病毒库升级
- IPS 入侵库升级
- Web 分类过滤升级，包括 82 个 Web 类别，涵盖了 4000 万个域名和 20 亿个网页
- 反垃圾邮件(AntiSpam)库升级，提供实时的垃圾邮件库查询，确保准确过滤垃圾邮件

Fortinet 的全球威胁科研团队负责更新 FortiGuard 服务，专家团队 24X7 的在世界各地保障用户的安全。提供了完整的多重威胁保护，包括零日攻击等最新威胁响应。 针对用户对于可疑恶意软件威胁保证响应时间的需求， Fortinet 还可以提供 FortiGuard 防病毒安全订阅服务的 "高级响应" 服务级别。与用户购买的服务保证协议(SLA)一起，这种高级服务合同可为用户提供一个直接联系 Fortinet 全球威胁科研团队的渠道。

标准FortiCare支持服务
包括以下服务内容：
- 1 年的硬件保修
- 90 天的 FortiCare Web 技术支持
- 90 天的软件升级

售后支持指南请参阅 http://www.fortinet.com.cn/support/reg-guide.html

Copyright 2006 Fortinet, Inc. All rights reserved. Fortinet, FortiGate, FortiOS, FortiAnalyzer, FortiGuard, FortiCare, FortiASIC, FortiManager, FortiWiFi, FortiClient, FortiLog and FortiReporter are trademarks of the Fortinet Corporation in the United States and/or other s. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. Licensed under U.S. Patent No. 5,623,600, DAT140-0906-R2