



FortiGate® -1240B

多功能安全设备

攻击的多样化推动了一体化设备的发展

网络攻击的变化推动网络安全设备向着涵盖各种安全技术的发展方向发展。FortiGate 作为新一代的安全网关融合安全技术与网络功能于一体，能够有效发现和阻断各种复杂的攻击行为。业界从未有哪款产品象 FortiGate 一样集成了这么多安全功能而且性能卓越。

高密度端口与硬件加速体系

FortiGate 1240B 采用 FortiASIC 网络处理器，能够实现如交换机的线速数据处理，为网络安全行业树立了一个标杆。该系统具有 40 个接口，其中 38 个接口采用网络处理器加速的功能，可以达到基于防火墙策略的数据包线速处理。它不仅仅采用了网络层的 FortiASIC，而且还采用内容层的 FortiASIC，能够对入侵检测、防病毒等应用层的安全处理进行加速。它还支持 AMC 和 FSM(Fortinet Storage Module)标准的扩展插槽，可以增加接口数量，也可以提高存储硬盘的容量。接口数量多的好处在于，企业组织可以将用户、网络划分成多个安全域，实现多个安全域之间的安全访问。



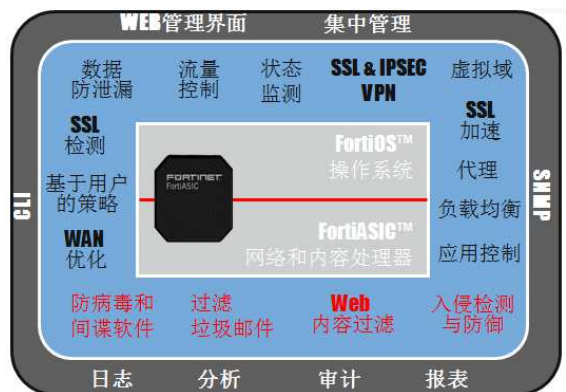
FortiOS 4.0 创造安全的新概念

FortiOS 4.0 作为 FortiGate 的核心，是以安全、性能和可靠为目标开发的。该专用系统采用了强大的 FortiASIC 芯片提高安全性和性能。FortiOS 可以实现多种安全功能，如防火墙、VPN、入侵检测与防御、反恶意软件、反垃圾邮件、web 过滤、应用控制、数据防泄漏和终端系统控制。

FortiASIC 的优势

FortiASIC 处理器使 FortiGate 更为强大，因为专用的网络处理器和内容层处理器能够加速数据的处理，它们采用了 Fortinet 独有的数字引擎。

功能	优点
● 硬件加速	支持高达 40Gbps 防火墙吞吐量和 16GbpsVPN 吞吐量，1.5Gbps 的 IPS 和 AV 吞吐量，使之不会成为网络的瓶颈
● 高密度端口	多个接口可供将网络分成多个内网安全网段
● 扩展插槽	可扩展插槽可以支持 NP 加速的接口或者用于日志和归档的硬盘
● 可扩展的模块化设计	支持 AMC 和 FSM 插槽，可以灵活地增加接口数量和本地化存储数据
● 多合一的安全体系	单一设备实现多种功能，提高了安全而降低了整体成本



FortiGate	FortiGate-1240B
硬件特征	
总接口数量	40
硬件加速 SFP 接口	24
硬件加速接口(10/100/1000M)	14
非硬件加速接口(10/100/1000M)	2
AMC 扩展插槽	1 个单宽
FSM 扩展插槽	6
本地存储(缺省配置)	1 FSM-064(64GB SSD)
系统性能	
防火墙吞吐量(1518 字节 UDP)	40Gbps(加 AMC 为 44Gbps)
防火墙吞吐量(512 字节 UDP)	40Gbps(加 AMC 为 44Gbps)
防火墙吞吐量(64 字节 UDP)	38Gbps(加 AMC 为 42Gbps)
防火墙 PPS	60/67Mpps
支持 AP 的数量	512
VPN 吞吐量 (AES-256+SHA-1)	16Gbps(加 AMC 为 18.5Gbps)
IPS 吞吐量	5Gbps
防病毒吞吐量(代理模式)	1.2Gbps
防病毒吞吐量(流扫描模式)	1.6Gbps
IPSec 通道(网关到网关)(系统/vdom)	10,000/5000
IPSec 通道(客户端到网关)	50,000
并发会话数	5M
新建会话数	120000
并发 SSL VPN 用户数(推荐最大)	1500
SSL VPN 吞吐量	370Mbps
策略	100000
虚拟域(最大/缺省)	100/10
不限用户数	是
MTBF	大于 5 年
热插拔冗余电源	是
尺寸	
高	8.87cm
宽	44cm
长	53cm
重	16.4kg
是否支持机架	是
环境要求	
交流电	100-240VAC, 50-60Hz, 6.3A(最大),
功率(平均)	342W
工作温度	0-40°C
存储温度	-35-70°C
湿度	5 到 95%非饱和
符合的条例	FCC class A part 15, UL/CUL, C Tick, VCCI

除了安全属性以外，还具有以下功能：

- 多种部署模式，透明和路由模式
- 二到三层的路由功能
- 流量整形和优先级
- 虚拟域
- 数据中心流量优化
- 高可用性(A/A, A/P, 集群)
- WAN 优化(需要具有本地存储)
- 基于 Web 的管理界面
- 命令行管理界面
- 存储于本地的事件日志(需要具有本地存储)
- 集中日志存储(需要部署 FortiAnalyzer)
- FortiGuard 日志分析和集中管理服务
- 支持多种认证功能



实际性能与设备的具体配置和网络环境相关。防火墙吞吐量是在 FortiGate 在 NAT 模式下，以 64、512 和 1518 字节的 UDP 数据里测出的。VPN 是以 512 字节 UDP 数据包，加密算法为 AES-256+SHA1 时测出。防病毒是根据带附件 32Kbyte HTTP 流量测试出的。IPS 是按照 NSS 的标准以 44KHTTP 文件测出。。

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 2900 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

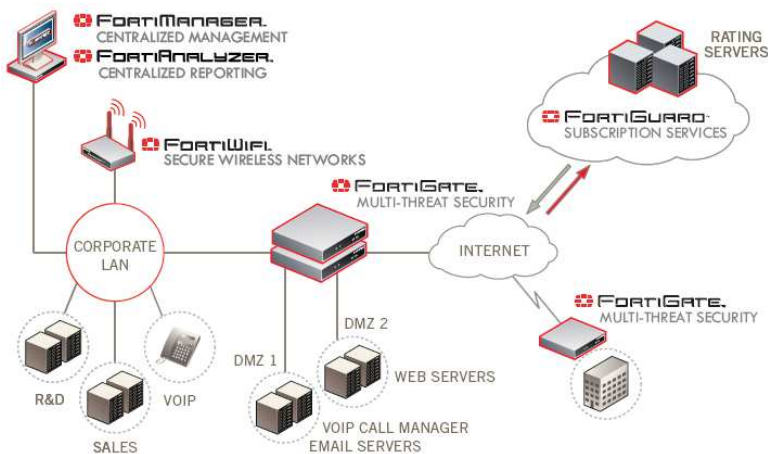
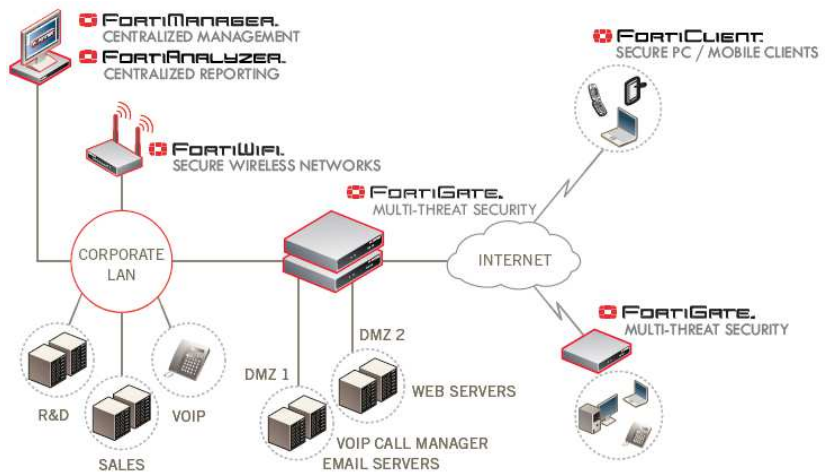
包括以下服务内容:

- 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://support.fortinet.com.cn/support/support/support.html>

UTM 构建安全的 VPN 体系

FortiGate具有强大的防火墙和VPN功能。很多大中型企业都有分公司、办事处和移动办公用户。FortiGate的IPSec VPN功能为这类企业提供了全面的、安全的互联解决方案。IPSEC VPN支持接口和通道两种类型，主和被动两种模式。它可以实现VPN通道星形或者网状结构，并且在VPN通道上部署防火墙策略、防病毒和IPS等全面的安全解决方案。OSPF over IPSEC可以实现IPSEC通道与专线，两条IPSEC通道之间互为备份，自动切换。移动用户可以使用FortiClient这样的IPSEC客户端方式连入公司，实现家庭和远程办公，也可以采用SSL VPN这样的基于浏览器的免客户端方式连接到公司的内网。FortiGate对于企业而言，提供作为防火墙、防病毒网关、Web过滤、入侵检测和防御等功能。



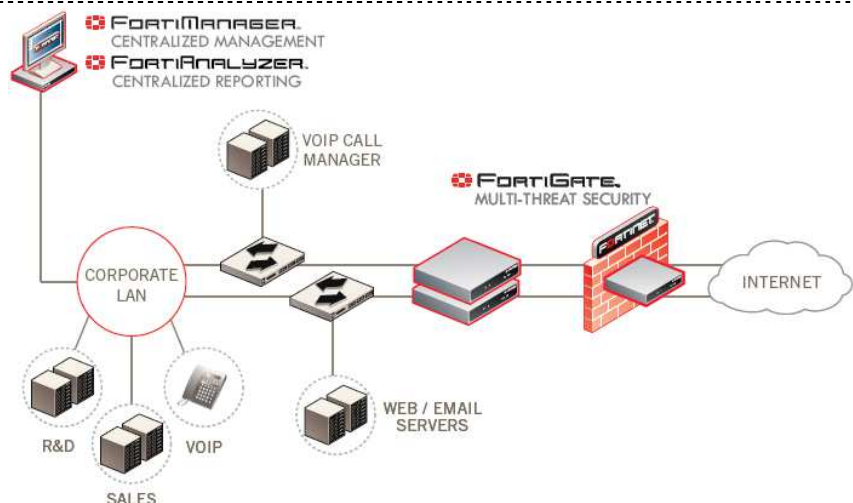
虚拟域为安全服务提供商提供解决方案

虚拟域可以将FortiGate划分出若干逻辑的虚拟设备，每个虚拟设备可以单独设置路由、防火墙策略、内容层的防病毒、IPS等功能。安全服务商可以为多个企业组织部署一个FortiGate，将其划分成若干逻辑设备分配给不同的企业组织，并且为其设置相应逻辑设备的管理权限，这样每个被服务的企业可以单独地管理安全设置，查看相应的日志信息。

所有 FortiGate 解决方案都是相同的灵活高性能架构，每个型号都有核心网络功能（比如 HA）和动态路由支持，使 FortiGate 能够安装在分布式的和全网状网络环境。

数据中心和关键应用的高性能解决方案

在数据中心这样吞吐量并且对实时性要求很高的环境中，新一代基于应用的攻击目标web2.0、VoIP甚至IPTV等应用，需要全面的安全策略，包括多层网络防御。不幸得是许多新型应用是需要实时的，迫使管理员在性能和安全性之间做出选择。FortiGate系列多个千兆性能解决方案提供实时的多层安全威胁防御，这些威胁主要目标是应用服务器。另外还提供新攻击类型的防御，先进的反垃圾邮件功能过滤间谍软件和安全策略不允许访问的内容。



FortiOS 安全功能

<p>防火墙</p> <p>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/服务器组/地址/地址组 DHCP 服务器, DHCP 中继 DNS 转发 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) 服务器负载均衡和健康检查*** 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</p> <p>虚拟专用网(VPN)</p> <p>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 OCSP 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</p>	<p>支持子网重叠, VPN 通道保持 基于策略和路由的 VPN OSPF over IPSec***</p> <p>反病毒</p> <p>ICSA 认证(网关反病毒) 包括反向间谍软件和蠕虫阻断 HTTP/SMTP/POP3/IMAP FTP/IM 协议 SMTPS/IMAPS / HTTPS/POPS 协议* (CP6 以上硬件版本) 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 /bzp /bzp2 /msc /J/PX 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</p> <p>WEB过滤</p> <p>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</p> <p>反垃圾邮件</p> <p>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</p>	<p>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</p> <p>应用控制</p> <p>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</p> <p>数据泄露防护(DLP)</p> <p>HTTP/SMTP/POP3/FTP/NNTP/IM 协议支持 SMTPS/IMAPS / HTTPS/POPS 协议 (CP6 以上硬件版本) 支持对压缩文件的扫描和存档 (Tar /gzip/rar/ lzh/ cab/ arj /zip /bzp /bzp2 /msc /J/PX) 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</p>	<p>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 NTP 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)</p> <p>终端控制(NAC)</p> <p>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</p> <p>入侵防御系统(IPS)</p> <p>ICSA 认证(NIPS) DOS 和 DDOS 攻击控制 4000+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。</p>
--	--	--	---

FortiOS 网络功能

<p>网络/路由</p> <p>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</p>	<p>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***</p> <p>广域网优化**</p> <p>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</p>	<p>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</p> <p>流量整形 ***</p> <p>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</p>	<p>高可靠性(HA) ***</p> <p>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</p>
--	---	--	--

FortiOS 管理功能

<p>配置与管理</p> <p>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</p>	<p>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</p> <p>日志与监控</p> <p>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</p>	<p>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</p> <p>防火墙用户认证</p> <p>本地数据库 Windows AD 认证</p>	<p>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</p> <p>UTM 管理界面定义</p> <p>自定义基于 WEB 的管理菜单</p>
--	--	---	--

*采用了 CP6 以上芯片的产品支持该功能
**只有具有硬盘的特定型号才支持
*** FG (FWF) 20C/30B/40C 不支持



飞塔信息科技(北京)有限公司
地址: 北京市海淀区北四环西路52号方正国际大厦12层 邮编: 100080
电话: (010) 62960376
传真: (010) 62960239
售后: support_cn@fortinet.com

飞塔信息科技(北京)有限公司
上海分公司
地址: 上海市黄浦区南京西路338号天安中心
1404室 邮编: 200021
电话: (021) 6120 2836
传真: (021) 6120 2856
http://www.fortinet.com.cn

飞塔信息科技(北京)有限公司
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塔1205室 邮编: 510620
电话: (020) 2885 8303
传真: (020) 2885 8378

GLOBAL HEADQUARTERS
Fortinet Incorporated
1090 Kifer Road, Sunnyvale,
CA 94086 USA
Tel: +1-408-235-7700
Fax: +1-408-235-7737