



FortiGate® -300C

多功能安全设备

中型企业和分布式网络的安全防护

随着网络攻击的变化和网络应用日益复杂，对于网管来说，他们亟需了解自己网络已经发生和正在发生的各种事情，也就是说提高网络的可视化和可控性。FortiGate 作为集成了多种安全功能的 UTM 产品，它能够采用各种不同的安全技术来满足这种对网络安全的需求，提高网管对网络的管理和控制能力。

FortiGate-300C 可以实现防火墙、VPN、入侵检测和防御、应用控制和 Web 内容过滤等安全功能，并且通过硬件对这些功能进行加速，使其性能领先于业界。除此之外，FortiGate-300C 还具有防病毒、垃圾邮件过滤、漏洞管理和 WAN 优化等功能。由于该设备具有多种安全功能，所以网络管理员可以充分地发挥各种安全应用的优点，以应对复杂网络环境和复杂网络攻击。

硬件加速

FortiGate300C 集成了基于网络处理器的 FortiASIC 和基于内容处理器的 FortiASIC 芯片。基于网络处理器的 FortiASIC 可以对网络层的处理进行加速，比如防火墙和 VPN，实行数据包从 64 字节到 1518 的线速吞吐。而内容处理的 FortiASIC 可以对防病毒、IPS 等内容层的网络安全功能进行加速。

随着企业网络规模的不断扩大，将其划分成多个安全区，然后分而治之成为企业一个明智的选择。FortiGate 300C 具有 8 个 ASIC 加速的 10/100/1000Mbps 接口和两个非加速的 10/100/1000Mbps 接口，可以满足企业对划分多个安全域的需求。

综合网络安全平台

FortiGate-300C 集成了多种网络安全功能，性能强大，可以灵活地部署于网络边缘和核心。除此之外，Fortinet 公司还为用户提供了 FortiGuard 升级服务，让注册的 FortiGate 可以及时地获得最新的升级特征库，以应对各种实时变化的攻击。



FortiGate 产品系列：集成多种安全功能

FortiGate 系列产品可以实现从网络层到应用层的安全防护。在不影响网络的可用性和应用的速度前提下，抵御多种复杂的攻击。

FortiGate 系统将 FortiOS 与定制开发的 ASIC 芯片集成在一起，为用户提供全面的高性能的安全功能和网络功能。

FortiGate 产品全系列覆盖了从桌面级到电信级。FortiGate 可以为用户保护其网络和资产的安全，关键业务信息，实现信息安全管理。

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。

问题	FortiGate解决方案
● 新应用和内容层变化	FortiGate-300C 提供了自动升级的应用检测功能，可以满足对应用进行管理的需求
● 某些应用对及时性要求高	FortiGate-300C 防火墙吞吐量可以达到 8Gbps，满足各种应用对高吞吐低延时的要求。
● 需要对内部划分多个安全域	FortiGate-300C 具有 8 个 ASIC 加速的 10/100/1000Mbps 接口和两个非加速的 10/100/1000Mbps 接口，可以满足企业对划分多个安全域的需求。
● 某些应用需要跨越广域网	FortiGate-300C 可以实现 WAN 优化和报表。
● 需要各种不同网络安全设备	FortiGate-300C 集成了多种安全功能，满足用户的各种安全需求。

FortiGate	FortiGate-300C
硬件特征	
10/100/1000 铜芯加速接口	8
最大接口数量	10
本地存储硬盘	32GB SSD
系统性能	
防火墙吞吐量 (1518/512/64 字节)	8Gbps
防火墙每秒处理数据包	12Mpps
IPSec VPN 吞吐量 (512 字节)	4.5Gbps
IPS 吞吐量	800Mbps
防病毒(代理模式/流扫描)	200/550Mbps
最大 FortiAP 数	256
支持 FortiToken 数	1000
网关到网关 IPSec 通道 (全局/虚拟域)	6000/3000
客户端到网关 Ipsec 通道	10000
SSL 用户数(推荐最大)	500
SSL VPN 吞吐	200Mbps
并发会话数	2,000,000
新建会话数	50,000
策略(全局/虚拟域)	40000/20000
不限用户数	是
虚拟域	10
高可用性	主备/主主/集群
防病毒是根据带附件 32KbyteHTTP 流量测试出的, IPS 是 512 字节的 UDP 基础上测试出的。实际的性能与网络的实际流量相关。	

FortiGate	FortiGate-300C
硬件参数	
尺寸	
高	4.5cm
宽	43.2cm
长	31.9cm
重	6.36kg
是否支持机架	是
冗余电源	需要外置配件
交流电	100/5A-220/3A VAC 50-60Hz
功率(平均)	128W
功率(最大)	154W
散热	525BTU/h
环境要求	
工作温度	0-40°C
存储温度	-25-70°C
湿度	5 到 95%非饱和
符合的条例	FCC class A part 15, UL/CUL, C Tick, VCCI
认证	ICSA 认证: 防火墙, IPSec, 防病毒, IPS, SSL VPN

FortiGate 300C 前面板



FortiGate 300C 后面板



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

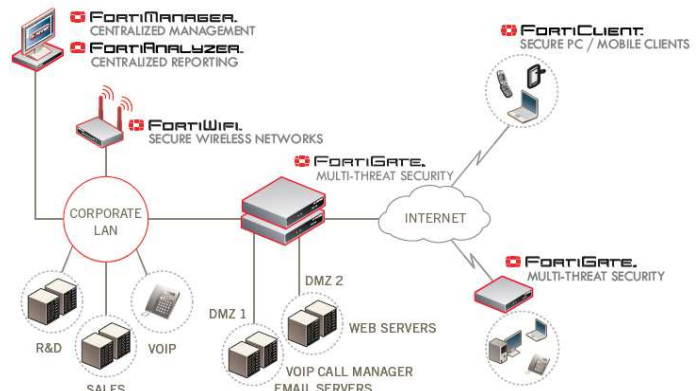
包括以下服务内容:

- 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

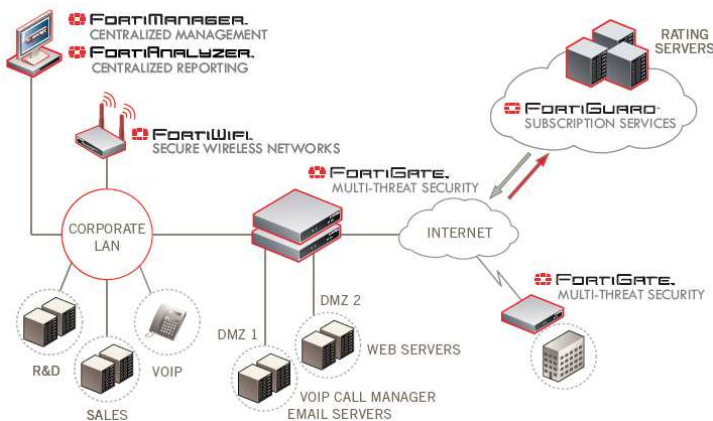
FortiGate具有强大的防火墙和VPN功能。很多大中型企业都有分公司、办事处和移动办公用户。FortiGate的IPSec VPN功能为这类企业提供了全面的、安全的互联解决方案。IPSEC VPN支持接口和通道两种类型，主和被动两种模式。它可以实现VPN通道星形或者网状结构，并且在VPN通道上部署防火墙策略、防病毒和IPS等全面的安全解决方案。OSPF over IPSEC可以实现IPSEC通道与专线，两条IPSEC通道之间互为备份，自动切换。移动用户可以使用FortiClient这样的IPSEC客户端方式连入公司，实现家庭和远程办公，也可以采用SSL VPN这样的基于浏览器的免客户端方式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

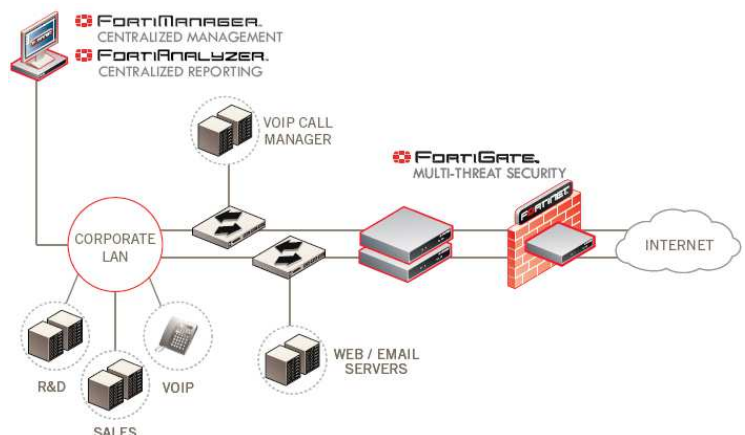
虚拟域可以将FortiGate划分出若干逻辑的虚拟设备，每个虚拟设备可以单独设置路由、防火墙策略、内容层的防病毒、IPS等功能。安全服务商可以为多个企业组织部署一个FortiGate，将其划分成若干逻辑设备分配给不同的企业组织，并且为其设置相应逻辑设备的管理权限，这样每个被服务的企业可以单独地管理安全设置，查看相应的日志信息。

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大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，需要全面的安全战略，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)</p> <p>NAT/路由,透明模式,混合模式</p> <p>虚拟防火墙支持(虚拟域)***</p> <p>标准预定义服务</p> <p>(SIP,GRE,Netmeeting,h.323,OSPF 等)</p> <p>自定义服务/服务组/地址/地址组</p> <p>DHCP 服务器, DHCP 中继</p> <p>DNS 转发</p> <p>IP/MAC 地址绑定</p> <p>基于策略的 NAT</p> <p>VLAN 标记(802.1Q)</p> <p>IPv6 策略和路由支持</p> <p>非 IP 协议透明传输</p> <p>ALG 应用代理(SIP, H.323, TNS, RSTP, RAS 等 NAT 穿越)</p> <p>服务器负载均衡和健康检查**</p> <p>策略时间表支持</p> <p>单机的会话同步支持</p> <p>基于用户组的认证</p> <p>精细度的每策略保护内容表</p> <p>虚拟专用网(VPN)</p> <p>CSA 认证(IPSec)</p> <p>PPTP, IPSec, L2TP, GRE</p> <p>SSL VPN**</p> <p>SSL VPN 用户界面自定义</p> <p>支持 DES, 3DES, AES 256 加密算法, SHA-1 / MD5 认证</p> <p>SCEP 简单证书登记协议</p> <p>OCSP 在线证书状态协议</p> <p>Hub and Spoke 星型 VPN</p> <p>DPD 通道状态检测</p> <p>NAT 穿越, XAUTH 认证</p> <p>静态 VPN, 动态拨号 VPN 支持</p>	<p>支持子网重叠, VPN 通道保持</p> <p>基于策略和路由的 VPN</p> <p>OSPF over IPSec***</p> <p>反病毒</p> <p>ICSA 认证(网关反病毒)</p> <p>包括反间谍软件和蠕虫阻断</p> <p>HTTP/SMTP/POP3/IMAP FTP/IM 协议</p> <p>SMTPS/IMAPS / HTTPS/POPS 协议* (CP6 以上硬件版本)</p> <p>FortiGuard 网络自动“推送”升级</p> <p>根据文件尺寸和类型阻断</p> <p>可定义的服务端口, 服务超时控制</p> <p>支持病毒阻拦和监视模式</p> <p>多层压缩文件扫描</p> <p>支持 Tar /gzip/rar/ lzh/ cab/ arj /zip /bzip /bzp2 /msc /UPX</p> <p>支持文件大小限制 文件类型限制</p> <p>病毒隔离支持(需要本地硬盘或 FortiAnalyzer 日志服务器)</p> <p>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</p> <p>自定义 URL 地址, 域名过滤</p> <p>基于分值的网页关键词阻断规则</p> <p>自定义分类库, 基于用户认证的分类库控制</p> <p>URL 地址/域名 黑白名单</p> <p>阻断 Java Applet, Cookies, Active X</p> <p>反垃圾邮件</p> <p>支持 SMTP/POP3/IMAP 协议</p> <p>支持 SMTPS/POPS/IMAPS 协议(CP6 硬件版本)*</p> <p>RBL/ORDBL</p> <p>FortiGuard 垃圾邮件库动态更新</p> <p>MIME 头检查、关键字/短句过滤</p>	<p>IP 地址和 Email 黑名单/免屏蔽</p> <p>返回地址 DNS 检查</p> <p>支持邮件阻断或者标记</p> <p>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:</p> <p>备份软件类, 如 IBM Tivoli, CA MQ 等</p> <p>商务软件, 如指南针, 证券之星, 分析家数据库, 如 DB2, MySQL, Oracle 等</p> <p>文件传输类, 如 DuDu, 纳米盘等</p> <p>游戏, 如赤壁、劲舞团、联众、魔兽等</p> <p>即时通讯, 如 MSN、QQ、新浪 UC、飞信等</p> <p>媒体类, 如土豆、酷 6、PPS 网络电视等</p> <p>网络服务, 如 BGP、ISCSI、QUAKE 等</p> <p>P2P, 如电驴、迅雷、VeryCD</p> <p>协议命令类, 如 ftp 命令, sip 命令</p> <p>代理软件, 如无界、Tor 等</p> <p>远程控制软件, 如 VNC、Pcanywhere 等</p> <p>工具类, 如 Google、yahoo、MSN 工具类等</p> <p>升级程序, 如各种杀毒软件升级, firefox 升级</p> <p>VoIP, 如 Sip, netmeeting, net2phone 等</p> <p>网站与论坛, 如网易论坛、QQ 论坛等</p> <p>Web Mail, 如 126mail、hotmail、QQmail 等</p> <p>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</p> <p>SMTPS/IMAPS / HTTPS/POPS 协议 (CP6 以上硬件版本)</p> <p>支持对压缩文件的扫描和存档</p> <p>(Tar /gzip/rar/ lzh/ cab/ arj /zip /bzip /bzp2 /msc /UPX)</p> <p>支持 TXT、PDF 和 Word 类型文档</p> <p>以动机确认和控制敏感信息</p> <p>内建模式匹配引擎</p> <p>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</p> <p>FTP 可检测 GET/PUT 的文件、服务器、用户名等</p> <p>HTTP 可检测 GET/POST、html 头、URL、CGI、Cookie、内容和用户等</p> <p>IM 可检测传输文件、内容、发送者、用户等</p> <p>NTTP 可检测传输文件、内容、用户等</p> <p>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</p> <p>检查 PC 主机是否安装如下安全软件:</p> <p>防火墙、防病毒、web 过滤</p> <p>可定制强制分发 FortiClient 安全软件</p> <p>检查 PC 主机的操作系统和补丁</p> <p>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)</p> <p>DOS 和 DDOS 攻击控制</p> <p>4000+多种攻击特征</p> <p>自定义攻击特征</p> <p>自动升级攻击特征库</p> <p>源地址/目的地址 TCP/UDP 会话控制</p> <p>自定义攻击传感器,</p> <p>支持基于策略的攻击防御</p> <p>基于系统, 协议, 威胁等级的特征库管理</p> <p>支持 NAC 攻击源自动隔离</p> <p>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</p> <p>关健康检测</p> <p>静态地址/DHCP / PPPOE/ DDNS 域名</p> <p>DHCP 服务器/中继</p> <p>静态路由, 策略路由</p> <p>基于 TOS 的路由</p> <p>基于用户认证的路由</p> <p>动态路由 RIP v1 & v2, OSPF, BGP***</p> <p>Multicast 组播(PIM parse, PIM Dense) ***</p> <p>支持多区域</p> <p>安全区域间路由</p>	<p>VDOM 虚拟域间路由***</p> <p>多链路聚合 (802.3ad)</p> <p>支持 IPv6 路由和策略控制</p> <p>多个二级地址支持</p> <p>USB 3G modem 支持</p> <p>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</p> <p>支持 A-P 和 P-P 模式</p> <p>支持透明或代理方式的 Web Cache</p> <p>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*</p> <p>集成缓存和协议优化技术</p> <p>加速 CIFS/FTP/MAPI/HTTP/HTTPS/TCP</p> <p>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</p> <p>Diffserv 服务等级设置</p> <p>最大/最小/优先 带宽控制</p> <p>DSCP 服务级别设置</p> <p>上行下行双向流量控制</p>	<p>高可靠性(HA) ***</p> <p>主-主, 主-备</p> <p>状态失败恢复(FW 和 VPN)</p> <p>支持全网状 HA</p> <p>设备失败检测和通告</p> <p>链路状态监控</p> <p>链路失败恢复</p> <p>服务器负载均衡</p> <p>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)</p> <p>支持多种语言 Web 管理</p> <p>支持 Telnet, SSH, HTTP,HTTPS 管理</p> <p>多级管理员基于角色的权限配置</p> <p>可信主机控制</p> <p>基于 Radius 的管理员认证</p> <p>PKI 证书管理员认证</p>	<p>分区系统软件存储, 支持版本回退</p> <p>USB 系统软件升级, 配置文件自动上载</p> <p>集中管理、策略下发、集中管理平台</p> <p>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</p> <p>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</p> <p>自定义报表</p> <p>本地显示远程 FortiAnalyzer 日志系统管理</p> <p>SNMPv1/v2/ 支持 Email 事件告警</p> <p>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</p> <p>Windows AD 认证</p>	<p>RADIUS/LDAP 认证</p> <p>TACACS+/PKI</p> <p>IP/MAC 地址绑定</p> <p>IPSEC VPN Xauth 扩展认证</p> <p>RSA SecurID 认证</p> <p>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, 如 FG110C/FG300C/FG310B/FG620B/FG1240B/FG3016B FG3600A/FG 3810A/FG3950B/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 FG1240B FG3016B FG3600A FG3810A FG3950B FG3951B FG5001A-SW

*** FG30B 和 FW30B 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) 6296 0376
传真: (010) 6296 0239
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