



FortiGate/FortiWiFi® -20C

多功能安全设备

FortiGate-20C 和 FortiWiFi-20C 在一台设备里集成了多种安全功能，可以防护各种网络层、内容和应用层的攻击。很多企业都需要为远程办公、零售店和分支机构提供安全接入。而 FortiGate-20C 和 FortiWiFi-20C 集成了企业级的安全功能和性能，为小企业提供了入门级别产品。FortiGate-20C 和 FortiWiFi-20C 也非常适合作为安全服务运营商的 CPE 设备。

多种安全功能

FortiGate-20C 和 FortiWiFi-20C 以低廉的价格为用户提供了多种安全功能，比如防火墙、IPS、应用控制、VPN 和 Web 过滤。它采用了 Fortinet 公司的 SoC 技术，集成了多种安全功能到专有的处理芯片中，从而满足小企业对高性价比的安全产品需求。

FortiGuard 安全服务为用户提供了实时的、动态的、自动的升级，使之能够抵御最新的复杂的各种攻击。而且该设备支持基于浏览器的管理界面，该界面可以轻而易举地管理各种安全功能，和提供实时的日志和丰富的报表。

FortiGate-20C 和 FortiWiFi-20C 集成了多种安全功能，用户需要再单独购买各种安全软件和硬件，简化了网络部署和减少了成本投入。FortiGate 可以轻松实现只允许经过授权的终端访问公司资源，禁止未经授权使用的应用。比如，网络管理员可以部署策略允许访问社交网站，而限制其下载和聊天功能。

全面的安全解决方案

Fortinet 的解决方案覆盖了从小企业到网络核心，FortiGate 支持各种网络协议，适用范围广泛，易于管理，性能卓越。FortiWiFi-20C 比起 FortiGate 多增加了无线 AP，适用于无线用户的安全。这种组合有利于降低无线网络的构建成本。

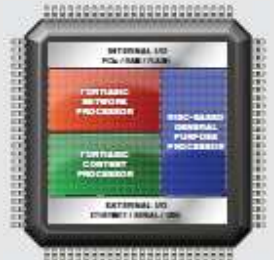


FortiOS 4.3 创造安全的新概念

FortiOS 4.3 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。

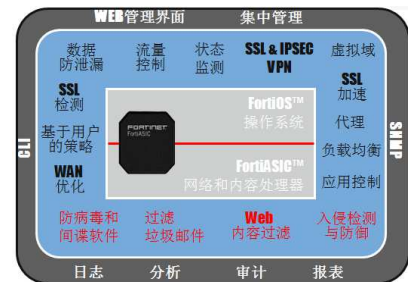
Fortinet FS1 片上系统(SoC)

Fortinet 公司开发了自有知识产权的第一款 SoC(FS1)，将其集成到 FortiGate/FortiWiFi 20C 上。FS1 将 RISC 处理器与 FortiASIC 处理逻辑结合在一起，从而简化了安全设备的系统设计，满足小企业网络爆发流量的压力需求。FS1 和它构成的 FortiGate/FortiWiFi-20C 系列能够满足小企业和大型企业的分支机构的网络安全需求，而不会带来网络的瓶颈。



优点	详细说明
----	------

- 立体防御体系 可以支持多种安全功能，提高整体性价比。
- 简化购买许可 不限用户，不限软件功能，按硬件销售
- 同时支持有线和无线 多个网络接口，并且支持 WiFi，部署简便
- 小尺寸机箱 简洁、紧凑，适合于小企业



技术指标	FortiGate-20C	FortiWiFi-20C
硬件参数		
10/100/1000 LAN(交换接口)		4
10/100/1000 WA		1
无线接口	无	802.11abgn
USB(客户端/服务器)		1/1
本地存储		2GB
系统性能		
防火墙吞吐量(1518 字节 UDP)		20Mbps
防火墙吞吐量(512 字节 UDP)		20Mbps
防火墙吞吐量(66 字节 UDP)		20Mbps
IPSec VPN 吞吐量		20Mbps
防病毒吞吐量(流扫描模式)		20Mbps
防病毒吞吐量(代理模式)		12Mbps
网关到网关的 IPSec VPN 通道数(全局/虚拟域)		5/5
客户端到网关 IPSec VPN 通道数		5
IPS 吞吐量		20Mbps
并发会话数		10k
新建会话数		1k
防火墙策略数		200
不限用户数		是
MTBF		超过 5 年
物理参数		
高		35mm
宽		215mm
长		180mm
重量		0.5kg
是否支持机架		是
电源		100-240VAC, 60-50Hz
平均功率		暂缺
最大功率		暂缺
冗余电源		否
散热		49BTU/h
环境要求		
工作温度		0~40°C
存储温度		-25~70°C
湿度		20~90% (非凝露)
电气标准		FCC Class A Part 15, UL/CUL, C Tick, VCCI
认证		ICSA Labs: Firewall, IPSec, Antivirus, IPS, Antispyware

FortiGate20C 和 FortiWiFi20C 可以支持所有 UTM 的功能, 比如防火墙、IPS、应用控制、Web 过滤、防病毒、反间谍软件和反垃圾邮件。但是与其他 FortiGate 相比, 高级配置和路由协议有所减少。详细内容请参照下表。

技术指标	FortiGate20C FortiWiFi20C	FortiGate-40C 以上
UTM 功能(防火墙、IPS、防病毒和 Web 过滤)	●	●
自动升级	●	●
Web 管理界面	●	●
集中管理和日志	●	●
IPsecVPN	●	●
应用控制	●	●
DLP	●	●
SSL 内容检测		●
WAN 优化		●
SSL VPN		●
动态路由协议 (RIP, OSPF, BGP, PIM)		●
虚拟域		●
服务器负载均衡		●
流量整形		●
FortiWiFi 20C 的技术参数		
射频的数量	1-8 个 SSID(1 个用于扫描)	
频段	2.4 和 5GHz 可自动切换	
无线标准	802.11a/b/g/n	
标准	IEEE 802.11a,b,e,g,l,j,n, 802.1x,TKIP, AES,WPA2,EAP	
支持无线集中控制器	否	
天线	2(内置)	
发送功率和接受敏感度	19dBm/-91dBm	
DDNS	是	
IP 分配方式	静态, DHCP 客户端, DHCP 服务器, DHCP 中继	

*防病毒性能的测试结果是基于 32K 字节文件附件的 HTTP 流量, IPS 的测试结果性能是基于 44 字节数据包的 HTTP 流量(NSS 测试标准)。实际性能可能会根据网络流量和环境会发生改变。



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

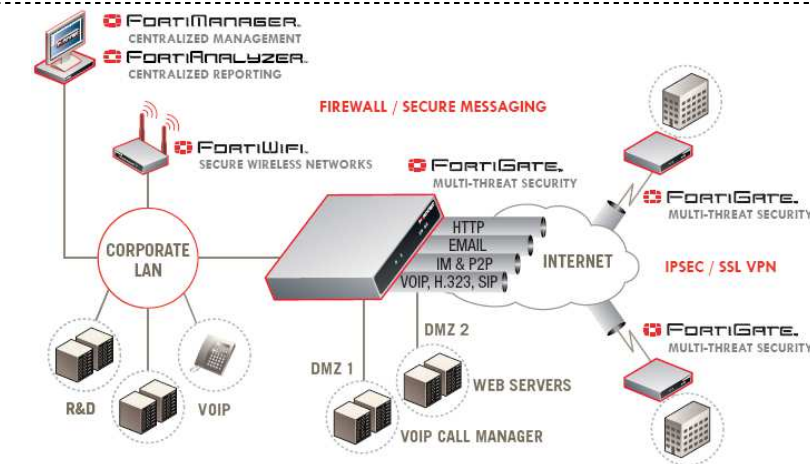
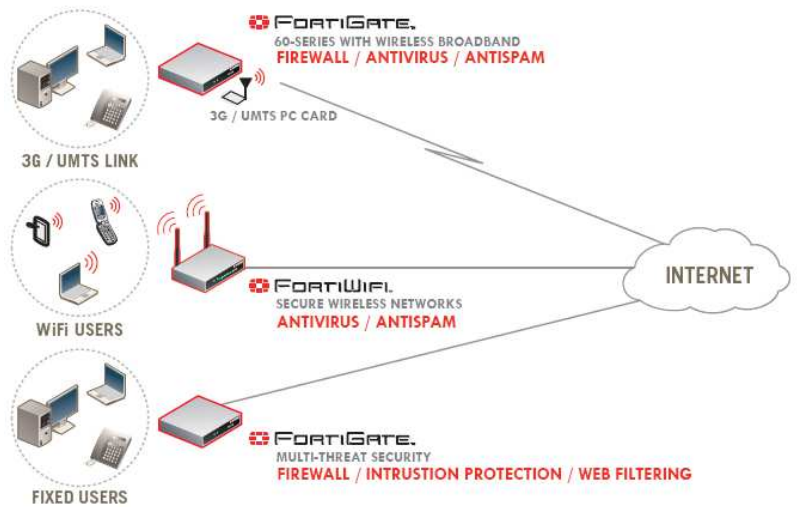
售后支持指南请参阅 <http://support.fortinet.com.cn/support/support/support.html>

FortiGate/FortiWiFi 20C 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

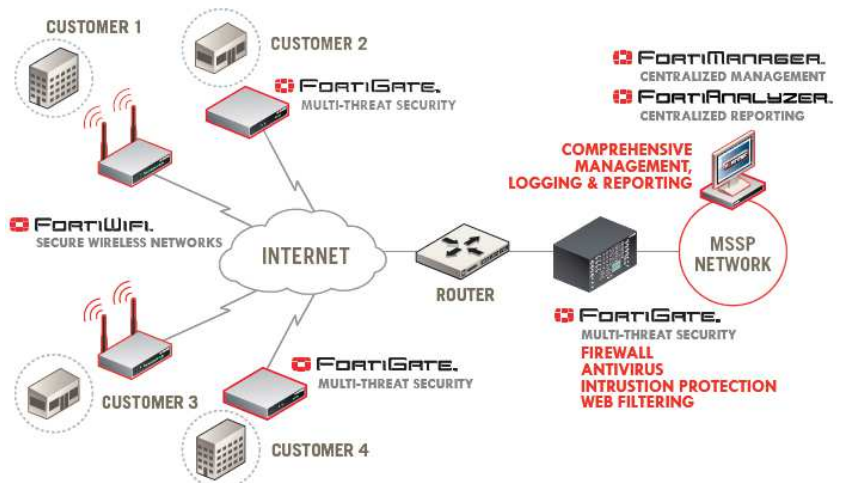
(防火墙+VPN+防病毒+邮件、应用控制)

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。



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>细粒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 支持通道和代理模式</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 /gz/zip/rar/ lzh/ cab/ arj /zip /bz/zip2 /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 /gz/zip/rar/ lzh/ cab/ arj /zip /bz/zip2 /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>可定义攻击特征</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

**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) 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