

McAfee Firewall Enterprise 设备

独具特色、可防御任意新威胁和漏洞

Web 2.0 上企业级应用的不断增多以及攻击面的不断扩大和快速变化，使得我们必须提供一种新的方法来确保防火墙安全性。第一代防火墙仅限于端口、协议和 IP 地址。今天，借助增强的新一代 McAfee® 防火墙，您可以使用可视化分析和用户标识获得高效、有效的规则，让您颇具信心地发现、控制、虚拟化和保护新的和现有的应用程序。此外，要在这些应用程序中检测出复杂的威胁，我们可以使用多个检查技术，在一个经济高效、易于管理的设备中相互传递前瞻性的威胁情报。

McAfee Firewall Enterprise 设备安全功能

AppPrism - 应用程序发现和控制，包括：

- 数据包、有状态和完全的应用程序过滤
- 完全的应用程序发现和控制
- 多个交付选项，包括多防火墙设备（一个设备可管理多达 32 个虚拟防火墙）、McAfee Firewall Enterprise for Riverbed、McAfee Firewall Enterprise for Crossbeam 和虚拟防火墙设备
- 网络地址转换 (NAT)

McAfee AppPrism™ 类别

- 匿名工具/代理
- 身份验证服务
- 业务 Web 应用程序
- 内容管理
- 商业监控
- 数据库
- 目录服务
- 电子邮件
- 机密通道
- ERP/CRM
- 文件共享
- 游戏
- 即时消息
- 基础设施服务
- IT 实用工具
- 移动软件
- 端到端 (P2P)
- 照片视频共享
- 远程管理
- 远程桌面/终端服务
- 社交网络
- 软件/系统更新
- 存储
- 流传输介质
- 工具栏和 PC 实用工具
- IP 语音 (VOIP)
- VPN
- Web 邮件
- Web 浏览
- Web 会议

传统而言，防火墙的强弱是根据您定义的策略确定的。但针对当今复杂 Web 2.0 通信的有效安全策略取决于细致的了解，而这一点很难实现。您需要对各项内容进行快速而深入的了解，不仅包含要了解用于不同 Web 应用程序和用户的端口和协议，而且还包含了解针对这些应用程序和用户的复杂威胁。

过去，您可以等待特征码，而现今威胁演化非常快，这就需要对风险进行前瞻性、可预测的诊断。应对多个属性（例如来源信誉、内容和行为）进行评估以在确认新威胁之前了解其恶意思图。

仅仅预测威胁还远远不够。还需要准确、及时地进行拦截，这就需要跨常规的产品库进行协同操作。

这些需求，再加上合规性的遵从要求，会增加网络团队的运营负担。而预算仍很紧张。因此必须做出一些改变。

15 年内最为重大的防火墙创新

借助 McAfee Firewall Enterprise 第 8 版，迈克菲重新改造了防火墙。借助三个创新，该产品以前所未闻的价格提供了前所未有的保护。我们将完全的应用程序可视性和控制、信誉感知的威胁智能以及多方位攻击保护结合起来，以提高网络安全性，同时还能节约精力和开支。

防火墙解决方案包括 McAfee Firewall Enterprise 设备系列、McAfee Firewall Enterprise Profiler、McAfee Firewall Enterprise Control Center 和 McAfee Firewall Reporter。

现在，网络安全的最弱一环是应用程序层。因此，我们采用了多个超高安全环境信任的防火墙，并增加了广泛的应用程序发现和控制。您现在可以防止新的和现有的 Web 2.0 应用程序遭受数据泄漏、网络滥用和恶意攻击的风险。借助迈克菲技术，可以确保使用您的网络的应用程序从您的业务中获益。

发现

McAfee AppPrism 技术使用创新的 Firewall Profiler 来识别所有流量，发现当前正在使用的应用程序，而且还显示有帮助的环境信息，例如来源、带宽和目标。通过检查加密的应用程序级通信，可以消除网络窃贼和攻击者所利用的漏洞。

控制

通过精确的控制，可以基于业务需求全面实施策略。与只匹配 IP 地址、端口或协议的策略不同，您现在可以将一个用户名与一个角色和一组应用程序相关联。

McAfee Firewall Enterprise 安全功能 (续)

身份验证

- 本地
- Microsoft Active Directory
- Active Directory (McAfee Logon Collector) 的透明标识
- LDAP (Sun、OpenLDAP 和 Custom LDAP)
- RADIUS
- Microsoft Windows 域身份验证
- Microsoft Windows NTLM 身份验证
- Passport (单一登录)
- 强大的身份验证 (SecurID)
- 支持 CAC 身份验证

高可用性 (HA)

- 主动/主动
- 主动/被动
- 有状态会话的故障转移
- 远程 IP 监控

Global Threat Intelligence

- McAfee Global Threat Intelligence 网络连接信誉
- 地理位置过滤
- McAfee Labs

加密应用程序过滤

- SSH
- SFTP
- SCP
- 双向 HTTPS 解密和重新加密

入侵防护系统 (IPS)

- 10000 多个特征码
- 自动特征码更新
- 自定义特征码
- 预配置的特征码组

防病毒和防间谍软件

- 防范间谍软件、特洛伊木马和蠕虫
- 启发式扫描
- 自动特征码更新

Web 过滤

- 集成了 McAfee SmartFilter® 过滤和管理
- 阻止 Java、Active-X、JavaScript 和 SOAP

反垃圾邮件

- McAfee Global Threat Intelligence 网络连接信誉

VPN

- IKEv1 和 IKEv2
- DES、3DES、AES-128 和 AES-256 加密
- SHA-1 和 MD5 身份验证
- Diffie-Hellmann 组 1、2 和 5
- 策略限制的通道
- NAT-T
- Xauth

构建结合诸如以下属性的应用程序使用规则：

- 业务或娱乐用途
- 用户标识
- 嵌入式应用程序控制
- 白名单
- 地理位置

用户标识

如果不能了解用户及其使用环境并施加控制，防火墙便无法抵御不断增长的端口敏捷性应用程序、难以捉摸的应用程序和有针对性的应用程序。McAfee Firewall Enterprise 可应用用户感知的规则并对应用程序加以控制。

当用户连接时，系统会从现有用户目录中实时验证权利。防火墙会快速应用映射到授予应用程序显式使用的用户标识的策略。

通过跟踪用户，规则的精细程度足以适合现代业务运营的要求。借助基于标识的规则，可以很好地了解运营情况。越来越多的企业严重依赖联合使用用户目录和标识管理来支持访问控制。用户只需更改一次，更改即可传播出去。安全策略会随着用户社区的变化而保持最新状态。

嵌入式应用程序控制

借助嵌入式应用程序控制，您可以在应用程序内定制权限。例如，您可能会允许 Yahoo，但阻止 Yahoo IM，或者仅允许特定的用户组（可能是客户支持或销售人员）或位置（如总部）使用 IM。

您还可以指定何时可以或不可以使用应用程序，支持适合公司的使用和中断策略。例如，对于客户服务团队，规则可以允许在午餐时间使用 MySpace，而任何人无法在周末通过 VPN 使用财务应用程序。

许多漏洞利用都会尝试在常用小程序中隐藏其负载来从社交网络站点松散的安全管理中受益。借助迈克菲产品，您可以允许访问站点中的有益元素（例如 Facebook），这样仍可最大限度降低每个站点内遭损坏应用程序的风险。

白名单

要获得高级控制，应用程序白名单使您明确可以仅允许来自已批准为必需或适当的应用程序的通信。与冗长的黑名单相比，白名单减少了需要编写和维护的规则数。

地理位置

随着僵尸网络通过常用的社交网络应用程序泛滥成灾，能够锁定尝试与某些位置通信的恶意应用程序便越来越重要。您可以通过地理位置切断此联系，以防止数据泄漏和使用系统制造破坏。

我们不仅可为您提供这种精细控制，同时还能降低规则开发的复杂性。事实上，一个视图只有一个策略。使用一个简洁的控制台即可提供有效管理所有规则和添加防御能力所需的选项。由于我们也突出了规则的交互和重叠，因此这种联合模型的优势会随着时间的推移和团队的增多越来越明显。借助突出显示了潜在冲突的各种领域，可以避免错误的发生，并能增强性能。

虚拟化

现在是管理规则转为管理风险的时候了。McAfee Firewall Enterprise Profiler 可以简化网络通信的评估，因此您可以快速添加新应用程序。我们直观的可视分析能让您即时衡量每个规则更改的有效性，以便可以优化策略来实现最大收益。

丰富的图形工具会基于用户标识、地理位置和使用级别实时关联应用程序活动。您可以轻松查看什么人在使用什么应用程序。借助这种集成式视图，您只需单击几次，效果便相当于您数小时兢兢业业的调查、试验和排除故障。对于某些用户，最大的优势是可立即了解问题是否是由防火墙引发的，而且可以调查问题发生的根本原因。

McAfee SecureOS® 操作系统

功能

- McAfee Type Enforcement® 技术
- 预配置的操作系统 (OS) 安全策略
- 操作系统划分
- 网络堆栈分隔

McAfee Firewall Enterprise Control Center

- Windows 图形用户界面
- 本地控制台
- 完整命令行
- USB 灾难恢复配置备份和恢复
- 使用 McAfee Firewall Enterprise Profiler (单独销售) 快速进行故障排除和防火墙规则影响分析

日志记录、监控和报告

- 本地日志记录
- 计划日志归档和导出
- Firewall Enterprise 日志软件解压缩格式 (SEF)
- 导出格式 (XML、SEF、W3C 和 WebTrends)
- Syslog
- SNMP v1、v2c 和 v3
- 包括 McAfee Firewall Reporter SEM

网络和路由

- 与 IPv6 兼容
- 动态路由 (RIP v1 和 v2、OSPF、BGP 和 PIM-SM)
- 静态路由
- 802.1Q VLAN 标记
- DHCP 客户端
- 默认路由故障转移
- QoS

安全服务器

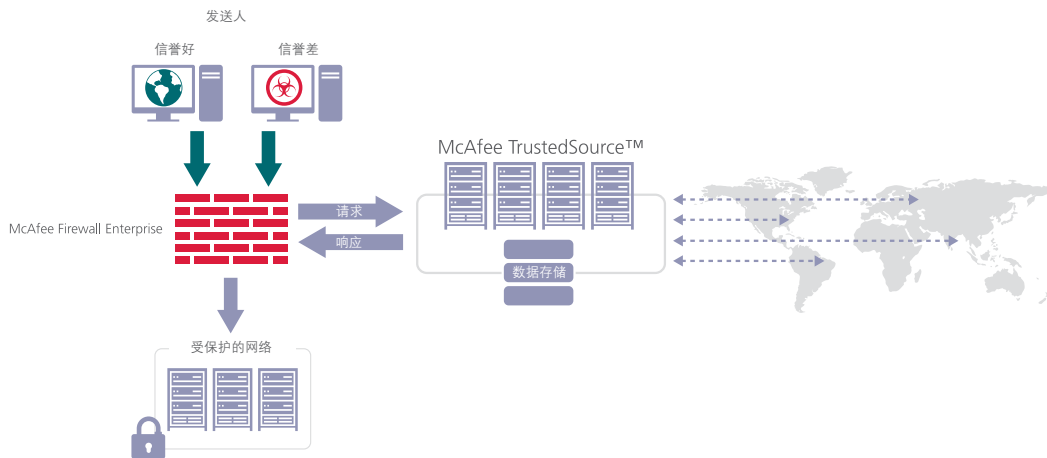
- 安全 DNS (单个或拆分)
- 安全 sendmail (单个或拆分)

设备和硬件

- 将大多数型号的保修服务升级到四小时响应
- 提供了虚拟化解决方案和各种不同的设备选项
- 单核、双核和四核处理器
- 基于 ASIC 的加速
- RAID HDD 配置
- 冗余电源

技术支持

- 全天候电话技术支持
- 使用基于 Web 的票证和知识库提供全天候技术支持



包含 McAfee TrustedSource 的 Global Threat Intelligence 可基于信誉允许或拒绝通信

保护

McAfee AppPrism 可帮助您降低应用程序级威胁带来的风险，同时优化对公司带宽的使用。AppPrism 由 McAfee Labs™ 提供强大的动力。其他威胁研究人员利用威胁研究和智能数据来不断识别和评估 31 类应用程序的风险，包括从匿名工具到视频和照片共享。

通过为站点、发送人和位置指定动态信誉，我们平均可以阻止 70% 的恶意通信（而且是在您发现这些通信之前阻止）。借助此功能，您甚至可以发现僵尸网络隐蔽的命令和控制 (C&C) 通道。

唯一提供信誉评价分析功能和全球威胁情报的防火墙

只有迈克菲在防火墙中纳入了信誉评价技术，而该技术仅是 McAfee Global Threat Intelligence 中的一个元素。在迈克菲，有超过四百名安全研究人员（比某些供应商的全体员工数还要多）就 Web、垃圾邮件、漏洞、主机和网络入侵、恶意软件和法规合规性研究进行协作。这种广度使他们可以识别每种新威胁和漏洞的特征。

这些人可借助全球一亿多台传感器提供的信息提供实时预测风险分析，以防范不断演化的多方面威胁。

与依赖于特征码的旧式防火墙不同，McAfee Labs 提供的自动化威胁反馈让您不用将防火墙脱机即可保持最新状态。随着高级持久性威胁（如极光行动）的增加，McAfee Global Threat Intelligence 可以为您提供精细的保护，帮助您扫除漏洞、避免出现违规行为并降低补救成本。

在一个集成式设备中提供多方位的安全保护

客户选择迈克菲的一个原因是，我们提供丰富的安全和合规性产品组合。现在，您可以轻松获得这些产品。面对 Web 2.0 应用程序中的复杂威胁（混合型利用漏洞攻击、网络钓鱼和有针对性的攻击），McAfee Firewall Enterprise 目前在每个防火墙设备中将多个关键威胁防护结合在一起。

以前，防火墙仅限于访问控制和分段。您需要实施和维护数个不同的产品才能获得足够的保护，但这样代价太大。现在，一个产品即可实现下面所有功能：

- McAfee AppPrism - 完全应用程序发现和控制
- 入侵防护
- 全球信誉分析
- 使用 McAfee SmartFilter® 技术进行 URL 过滤
- 加密应用程序过滤
- 防病毒、防间谍软件和反垃圾邮件

我们在构建多方位解决方案方面所具有的丰富经验帮助我们提供了所有这些保护，而且不会降低性能和工作效率，也不收取额外的费用。

McAfee Firewall Enterprise 产品系列

Firewall Enterprise 产品系列包括适用于各种企业规模的设备及其随附产品（如 McAfee Firewall Enterprise Profiler、McAfee Firewall Enterprise Control Center 和 McAfee Firewall Reporter）。这些产品协同工作可简化管理活动并降低运营成本。灵活的混合提供选项包含物理设备、多防火墙设备、虚拟设备和针对 Riverbed Steelhead 设备的解决方案。通过在 Crossbeam 的 X 系列硬件上运行的 McAfee Firewall Enterprise for Crossbeam 解决方案，可以提供运营商级的安全性能，速度高达 40 Gbps。有关详细信息，请咨询销售代表。

精细控制实现了易管理性

可靠的安全性还必须易于配置。管理员使用直观的 McAfee Firewall Enterprise 管理控制台可以通过一个屏幕创建规则，并可以有选择地应用防御措施，例如应用程序过滤器、IPS 特征码和 URL 过滤。新的软件功能更新可通过 Internet 自动提供，从而减少了维护工作。只通过一次单击便可确定计划。

McAfee Firewall Enterprise 产品系列包括用于简化管理的附加工具：McAfee Firewall Reporter 和 McAfee Firewall Enterprise Control Center。

包含的 Firewall Reporter 软件不用支付额外的成本，该软件可以将审核流转换为可操作的信息。这种屡获殊荣的安全事件管理 (SEM) 工具提供集中监控和关联的警报和报告。您可以从 500 多个图形报告中进行选择来描绘网络通信并帮助满足所有的主要法规要求。

McAfee Firewall Enterprise Control Center 单独出售，可针对多个 McAfee Firewall Enterprise 设备提供集中式防火墙策略管理。借助它可最大程度提高运行效率，简化策略控制，优化规则，简化软件更新以及证明法规合规性。您甚至可以比较所有 Control Center 管理的设备上的策略配置，以确保跨网络的一致性。强大的配置管理允许您以集中方式跟踪和验证所有策略更改。

而且，Control Center 与 McAfee ePolicy Orchestrator® (ePO™) 集成，让 ePO 可以深入了解防火墙运行状况数据和报告。

最安全的防火墙硬件平台

从根本上讲，McAfee Firewall Enterprise 运行在高速、高度可靠的 McAfee SecureOS 操作系统上。获得专利的 McAfee Type Enforcement® 技术会保护操作系统本身，以实现无与伦比的平台安全性。这也可能是 SecureOS 拥有一个无与伦比的 CERT 公告记录的原因：从来都不需要紧急安全补丁程序。

预先配置的操作系统安全策略可防止遭受破坏，并且整个操作系统分成各个不同的部分，这样攻击者便无法干扰其工作。

这些额外的措施使我们的防火墙成为第一个获得 Common Criteria EAL 4+ 认证并符合 US DoD Protection Profile 规范的防火墙。

凭借我们的创新和高级安全性，McAfee Firewall Enterprise 可为全球 15000 个网络提供保护，包括数千个政府机构、Fortune 500（财富 500 强）、十大金融机构中的七大金融机构。让我们为您提供保护，您可高枕无忧。

产品简介 McAfee Firewall Enterprise 设备



用于保护虚拟基础设施的虚拟
防火墙



通过单台设备实现 WAN 优化
和分支办公室安全



Crossbeam X 系列防火墙性能
能高达 40 Gbps



硬件规格 ¹	S1104	410	510	1100	2100	2150	2150 VX-XX	4150
外形尺寸	小型 1U	小型 1U	小型 1U	企业级 1U	企业级 2U	企业级 2U	企业级 2U	企业级 5U
不受限制的用户许可证	是	是	是	是	是	是	是	是
建议的用户数	200	300	600	大中型	大中型	大型	大型	企业级
RAID	N/A	N/A	N/A	RAID 1	RAID 1	RAID 5	RAID 5	RAID 5
电源	单个	单个	单个	两个	两个	两个	两个	两个
铜线接口 (基本/最大)	4 Gb	8 Gb	8 Gb	10/16 Gb	10/22 Gb	10/22 Gb	22/24 Gb	14/26 Gb
光纤接口选项 (最大)	N/A	N/A	N/A	6	12	12	N/A	12
10 Gb 接口选项 (最大)	N/A	N/A	N/A	6	6	6	6	6
加密过滤加速卡选项	N/A	N/A	N/A	是	是	是	是	是

法规合规性 FCC (仅限美国) B 类、ICES (加拿大) B 类、CE 标准 (EN 55022 B 类、EN55024、EN61000-3-2、EN61000-3-3)、VCC (日本) B 类、BSMI (台湾) A 类、C-Tick (澳大利亚/新西兰) B 类、SABS (南非) B 类、MIC (韩国) B 类、UL 60950、CAN/CSA C22.2 编号 60950 和 IEC 60950

性能¹

防火墙性能 (最高) ²	750 Mbps	1.5 Gbps	3 Gbps	7.5 Gbps	7.5 Gbps	10 Gbps	10 Gbps	12 Gbps
威胁预防 ²	250 Mbps	500 Mbps	1.5 Gbps	3 Gbps	3 Gbps	5 Gbps	5 Gbps	6 Gbps
AppPrism ²	250 Mbps	500 Mbps	1 Gbps	3 Gbps	4 Gbps	4 Gbps	4 Gbps	5 Gbps
并发会话数 ²	200000	500000	750000	950000	950000	1100000	1100000	1300000
每秒的新会话数 ²	5000	15000	20000	25000	25000	30000	30000	35000
IPSec VPN 吞吐量 (AES) ²	60 Mbps	200 Mbps	275 Mbps	300 Mbps	300 Mbps	400 Mbps	400 Mbps	700 Mbps
IPSec VPN 最大通道数 ²	250	500	1000	2000	2000	4000	4000	8000

尺寸、重量和环境

宽度	42.93 厘米	44.70 厘米	44.70 厘米	48.20 厘米	44.30 厘米	44.30 厘米	44.30 厘米	48.25 厘米
长度	21.59 厘米	42.54 厘米	54.60 厘米	77.20 厘米	68.10 厘米	68.10 厘米	68.10 厘米	62.10 厘米
高度	3.81 厘米	4.20 厘米	4.20 厘米	4.26 厘米	8.64 厘米	8.64 厘米	8.64 厘米	21.77 厘米
重量	4.96 千克	6.94 千克	11.80 千克	17.70 千克	26.10 千克	26.10 千克	26.10 千克	35.00 千克
电源详细信息	100 W 110/220 V	345 W 110/220 V	345 W 110/220 V	双 717 W 110/220 V	双 870 W 110/220 V	双 870 W 110/220 V	双 870 W 110/220 V	双 870 W 110/220 V
工作温度	0°C – 50°C	10°C – 35°C	10°C – 35°C	10°C – 35°C	10°C – 35°C	10°C – 35°C	10°C – 35°C	10°C – 35°C

1. 所有规格和性能结果都基于 F 系列和 S 系列的设备。

2. V8 性能数据表示根据最佳测试条件下度量的系统的最大功能。部署和策略考虑事项可能会影响性能结果。

迈克菲 (上海) 软件有限公司

北京朝阳门外大街 16 号中国人寿大厦 1709 室

邮编: 100020

电话: (8610) 85722000

传真: (8610) 85752299

上海市卢湾区湖滨路 222 号企业天地 1 号楼 1101 室

邮编: 200021

电话: (8621) 23080699

传真: (8621) 63406606

广州市天河区体育东路 118 号财富广场西塔 15 楼 106 室

邮编: 510620

电话: (8620) 38860668

传真: (8620) 38860638

销售热线: 800-810-0369 www.mcafee.com/cn



McAfee、迈克菲和 McAfee 徽标是 McAfee, Inc. 和/或其子公司在美国和/或其他国家或地区的注册商标或商标。其他标志和商标可能已声明为其他公司的财产。本文中的产品计划、规格和描述仅供参考, 如有更改, 恕不另行通知, 并且在提供时不作任何类型的明示或默示担保。
版权所有 © 2011 McAfee, Inc.

19101ds_firewall-enterprise_1210_fnl_ETMG