WatchGuard®
产 品 介 绍

Firebox® X Core™
e-Series

- **综合防御**让您的网络免受恶意攻击
- **预防御功能**可以预先阻止新出现的威胁
- **最新型网络安全管理**更加节约时间
- **不断更新的防病毒、防垃圾邮件及网络过滤服务**提供最新防御
- **全集成、可升级功能**让您物超所值
- **全球安全专家团队**随时为您效劳
- **完全符合RoHS/WEEE**及其他环保规定

综合统一威胁管理解决方案

Firebox® X Core™ 统一威胁管理(UTM)解决方案提供最全面的安全防御，在同一设备上集成了深度应用检测防火墙、VPN、预防御、防间谍软件、防毒病、防入侵、防垃圾邮件和URL过滤功能，在管理多台设备的解决方案中显著降低了管理时间与成本，并大大提高了对混合威胁的防御效率。

高级多层安全防御

Firebox X Core是在智能分层架构的基础上开发而来。 在此架构中，各安全保护层共同加强整体防御功能，同时层与层之间的协作通信减少并优化了处理过程。 因此，您无需牺牲网络性能即可获得安全防御。

预防御

在软件安全漏洞使新型的网络攻击变为可能的形势下，Firebox X Core的内置式预防御随时准备保障您客户网络的安全。这些预防御功能包括先进的代理技术，能够在新威胁出现之时就加以分辨和阻止，保障您能够不受影响，顺利开展业务。

直观的集中管理

WatchGuard® System Manager (WSM)提供直观的图形化用户界面，用于管理Firebox X Core UTM解决方案的所有功能。WSM提供综合日志系统、创建拖放VPN以及实时监控功能，而且不存在隐含成本，也无需购买更多硬件。只用一种界面即可管理安全解决方案(包括部署多台设备的情况)的所有方面，因此该产品更加节约您的时间及金钱。

综合安全功能提供更加精心的保护

每一项WatchGuard的安全服务与Firebox X Core的内置式预防御功能联手打造超强安全保护能力。所有新添加的安全分层均高度集成，而且定购价格均按每一设备(而非按用户数量)计算，因此绝对不会增加额外成本。所有服务均由WSM统一管理，用户可实时查看所有服务状态，而且，可以持续更新这些服务，获得最新的保护。

- **网关防病毒/入侵防御服务：**
  基于攻击特征的强大的安全保护，阻止间谍软件、木马、病毒及其它基于网络的漏洞攻击。
- ***spamBlocker***
  业内最佳的垃圾邮件过滤系统，阻止垃圾邮件的有效率可高达97%。
- ***WebBlocker***
  强化对员工在上班时间浏览网络内容的访问限制，同时，保护用户免受恶意网站的攻击。

专家指导与支持

WatchGuard LiveSecurity®服务为您提供全球安全专家团队支持，帮助您将复杂的IT管理工作变得更为便捷。您对LiveSecurity的订购包含了硬件保修和高级硬件更换，所以，若有硬件故障，WatchGuard将在收到您退回的设备之前就发送更换的设备给您，以最大限度地减少故障影响到的时间。LiveSecurity服务还提供软件更新、快速响应技术支持、最新漏洞攻击警告及培训资源。

保护您的投资

如果对比一下对多个安全解决方案进行的配置、管理及升级，您会明白为什么我们的Firebox X Core UTM解决方案会有更高的性价比。我们在一台设备上高度集成每一应用软件，并拥有全面保护功能，从最初购买到后续支持，无论是哪一方面，均能为您降低成本。

随着业务的发展，您可以轻松添加新功能，强化贵组织的安全保障。您可以在线下载许可密钥，将产品升级到更高型号，增大产品的处理能力。在无需购买新硬件的情况下，您可以将产品从Fireware®升级到Fireware® Pro高级设备软件，以提升网络表现，包括VLAN、高可用性、流量管理/服务质量管理(QoS)以及动态路由，满足更高的网络需要。当前市场上没有同类产品能够如此全面的保护您的投资。

我们的环保承诺

WatchGuard致力于提供更节省能源、可循环利用的设备和包装材料。我们完全遵照欧盟限制使用有害物质指令，并将环保责任融入我们的战略业务要求。

WatchGuard
Stronger Security, Simply Done™

防御基于网络的漏洞攻击

互联网是最有价值的商业工具之一，同时也对您的网络构成巨大威胁。未受到管理的网络用户可能会无意或故意造成漏洞，并借此引入bots及间谍软件，使公司的敏感数据受到威胁，并增加对技术支援的需要。出现漏洞的网络更容易受到域名服务器缓存毒害、缓存溢出以及拒绝服务(DoS)攻击。

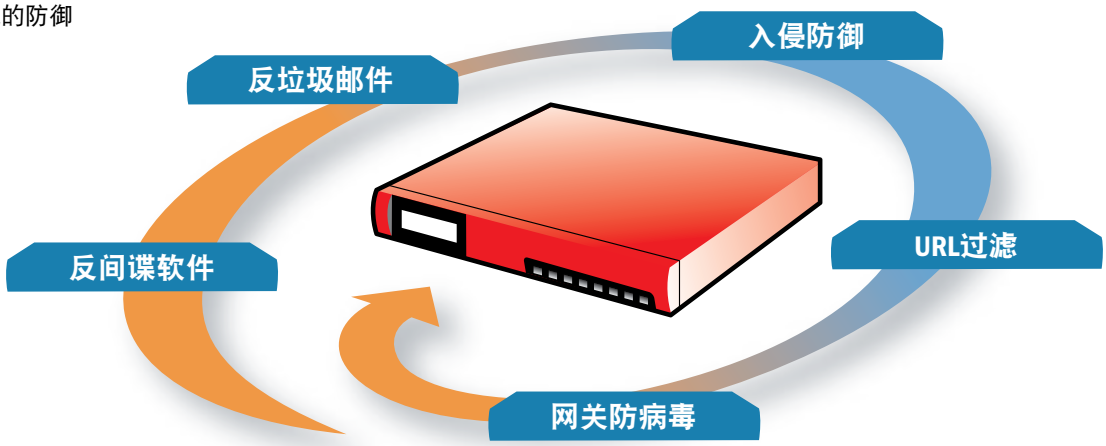
您需要：

- 从具有真正预防御功能的**Firebox X Core**开始。
- 订购**WebBlocker**，控制非授权网上浏览；订购**网关防病毒/入侵防御服务**，实时阻止可疑网络数据流和文件下载。

防御功能如何逐步增加

- 在应用软件的漏洞给了新型攻击可乘之机的情况下，运用强大的内置式代理技术的**预防御**可以保护您的网络免受未知威胁的危害。
- **网关防病毒**检查网络数据流中是否存在病毒、木马、bots及其它恶意程序。
- **隐藏Web服务器**可防止黑客使用您的系统信息攻击您的网络。
- **URL过滤**可控制用户上网，提高工作效率，保护网络带宽，降低安全风险，并减少在工作场所浏览不当内容所引起的法律责任。
- **多层反间谍软件功能**可以阻止用户访问已知间谍网址，阻止在网上浏览时，间谍软件进入网络，并阻止间谍软件连接其主机。
- **智能分层安全架构与域名服务器代理结合**，保护网路免受网络入侵、拒绝服务(DoS)攻击以及域名服务器(DNS)缓存毒害的侵扰。
- **强大的入侵防御系统功能**能够控制两类最常见的间谍软件散播工具－即时消息(IM)以及点对点(P2P)通讯。
- **集成日志、报告以及示警**能够提供网络活动的详细信息，并容许用户立即采取防御或纠正措施。

Firebox X的**集成安全服务**强化了在主要攻击领域的防御



阻止电子邮件携带的威胁

公司业务离不开电子邮件，因此电子邮件必须通畅、可靠地运行，不能危害网络安全。 但电子邮件却是网络上传播恶意代码的最常见载体。 再加上不断有垃圾邮件的攻击，用户的邮件服务器成为安全漏洞最大的地方。

您需要：

- 从具有真正预防御功能的**Firebox X Core**开始。
- 增加具有扫描电子邮件流功能的**网关防病毒/入侵防御服务**，可通过邮件流扫描功能来阻止已知间谍软件、病毒、木马及其他恶意软件。
- 订购**spamBlocker**，业内最好的实时区分合法通信与垃圾邮件攻击的产品。

防御功能如何逐步增加

- **内置式预防御**应用了强大的代理技术，预先阻止经常通过邮件携带恶意软件的文件类型。
- **spamBlocker**具有实时垃圾邮件检测功能，可以过滤高达97%的任何内容、语言或格式的垃圾邮件，极少犯错。
- **隐藏SMTP服务器**防止黑客使用您的系统信息攻击您的网络。
- **集成网关反病毒功能**可以向您提供更加精细的文件及附件防御服务，在病毒、蠕虫以及其它恶意程序穿透网络，影响您的电脑安全应用之前，将其击退。
- **电子邮件发送扫描**可以防止您将携带病毒、蠕虫以及其它恶意程序的电子邮件发送给您的合作伙伴、客户以及您网络之外的其他接收人。

规格

	Firebox® X550e WG50550 X550e UTM 套装产品 WG50553	Firebox® X750e WG50750 X750e UTM 套装产品 WG50753	Firebox® X1250e WG51250 X1250e UTM 套装产品 WG51253
防火墙处理能力†	300+ Mbps	300+ Mbps	300+ Mbps
VPN处理能力†	35 Mbps	50 Mbps	100 Mbps
网关防病毒/入侵防御服务	可选	可选	可选
URL过滤	可选	可选	可选
垃圾邮件过滤	可选	可选	可选
10/100 接口	4	8	0
10/100/1000 接口	0	0	8
安全域(含)	4	8	8
并行会话数	25,000	75,000	200,000
支持节点(LAN IP)	无限	无限	无限
串行端口	1	1	1
虚拟区域网(VLAN)*	25	25	25
分支办公室VPN通道(含/最大数量)	35/45	100/100	400/400
移动用户VPN通道(含/最大数量)	5/75	50/100	400/400
本地用户验证DB限制	250	1,000	5,000
可升级型号	否	是	否
Fireware® Pro高级应用软件	可选	可选	可选

† 传输速度视环境及配置而定

*用Fireware Pro高级软件更新，即可获得

特性

安全特性
- 状态包防火墙
- 深度应用检测防火墙
- 反间谍软件
- 应用层代理 - HTTP, SMTP, FTP, DNS, TCP
- 拒绝服务及分布式拒绝服务攻击防御
- Progressive分布式拒绝服务攻击防御
- 异常协议检测
- 行为分析
- 模式匹配
- 碎片封包重组防御
- 恶意封包防御
- 静态黑名单
- 动态黑名单
- 基于时间的规则
- 允许/拒绝即时通讯(IM)及点对点通讯

虚拟专用网
- 虚拟区域网(VLAN)*
  - 桥接(Bridging)
  - 标记
  - 路由模式
- VPN
  - 加密(DES, 3DES, AES 128-, 192-, 256-bit)
  - 网络协议安全
    - SHA-1, MD5
    - IKE预共享密钥, Firebox认证, 第三方认证
- PPTP服务器
- PPTP通道连接
- 对方失效检测(RFC 3706)
- 硬件加密
- 带Fireware规则的拖放式VPN通道

用户认证
- XAUTH
  - RADIUS®
  - LDAP
  - Windows® Active Directory
- RSA SecurID®
- 基于Web方式的
- 本地认证

IP地址分配
- 独立端口
- 静态
- PPPoE客户端
- DHCP服务器
- DHCP客户端
- DHCP中继
- 动态DNS客户端

高可用性*
- HA主/从模式
- 配置同步
- 会话同步
- VPN通道同步

多广域网容错
- VPN容错
- 广域网模式
  - 溢出*
  - Round Robin
  - 容错
  - ECMP
  - Weight Round Robin*

流量管理
- 服务质量(QoS)*
  - 8个优先级队列
  - Diffserve
  - 优化队列

路由
- 静态路由
- RIPv1, v2
- 动态路由*
  - BGP4
  - OSPF
- 基于政策的路由*

运行模式
- 透明/插入模式(第二层)
- 路由模式(第三层)

网络地址转换
- 静态网络地址转换(端口转换)
- 动态网络地址转换
- 一对一网络地址转换
- IPSec NAT穿越
- 基于策略的网络地址转换

日志/报告
- 多设备日志集合
- WebTrends®兼容报告(WELF)
- HTML报告
- XML日志格式
- 加密日志信道
- Syslog
- 简单网络管理协议(SNMP)

告警/通知
- 简单网络管理协议
- 电子邮件
- 管理系统预警

管理软件
- WatchGuard System Manager (WSM)

认证
- EAL4+
- West Coast Labs Checkmark
  - 该项认证包括防火墙、IPSec VPN、网络内容过滤、IPS

支持与维护
- 硬件1年保修
- 90天LiveSecurity®服务

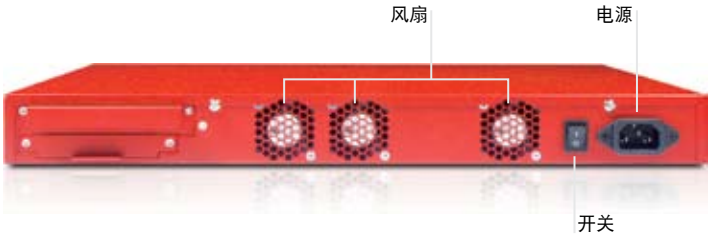
*提供Fireware® Pro高级操作系统更新

尺寸与电源

设备尺寸	1.75" x 16.75" x 14.25" (4.5 x 42.6 x 36.2 cm)
包装尺寸	7.25" x 21.75" x 19" (18.4 x 54.6 x 48.3 cm)
设备重量	9.68 lbs (4.39 Kg)
总重量	13.7 lbs (6.21 Kg)
WEEE重量	10.6 lbs (4.81 Kg)
交流电源	100-240 VAC（自动侦测）
消耗电源	U.S. 60 Watts
	其他国家：860 Cal/min或205 BTU/hr
机架式安装	是

环境指标

工作温度	32 – 113° F (0 – 45° C)
非工作状态温度	-40 – 158° F (-40 – 70° C)
工作湿度	10 - 85%
非工作状态湿度	131° F(55° C)时非冷凝湿度为10 - 95%
非工作状态随机振动	7 - 28 Hz 每Hz 0.001至0.01 G2
噪音	20 - 25° C时为54分贝
工作机械振动	11毫秒期间1/2正弦波，冲击力20G
符合WEEE/RoHS标准	是



准备升级为Fireware® Pro高级应用软件?

随着网络需求的增长，为满足更高的网络要求，您可将Firebox X Core从Fireware升级至Fireware Pro – WatchGuard的高级设备软件。现在Fireware Pro 9.x比以往版本功能更强大，可提供：

- **流量管理** – 确保业务关键应用获得足够的带宽
- **动态路由(BGP/OSPF)** – 通过路由表动态更新，实现网络灵活性、冗余度和效率最大化。
- **高可用性(主/从)** – 为主设备提供备援硬件及广域网容错和VPN容错。
- **虚拟区域网(VLAN)** – 创建逻辑关系上的网络配置，而非物理意义上的区域网，以降低对硬件的要求，增强对多种流量类型的控制，提供更强的相互操作性，并使子网的创建更为方便。
- **多广域网负载均衡** – 在多个ISP之间分配和平衡外发流量，以提高网络效率。
- **基于政策的路由** – 让用户可以按业务指定外发接口，以加强网络带宽的管理和降低费用。

欲了解关于Firebox X Core的详情，请访问
www.watchguard.com/appliances。
或致电北京：(010) 5877.1875/上海：(021) 5116.0557

Core™ UTM套装产品
一个解决方案，一个统一授权，更佳的性价比

采用极为方便的Firebox X Core e系列UTM套装产品包，您就可以享用您需要的综合统一威胁管理解决方案的一切。这个物超所值的套装产品包包括：

- Firebox X Core e系列X550e、X750e或X1250e安全设备
- WebBlocker*
- spamBlocker*
- 网关防病毒/入侵防御服务*
- LiveSecurity®服务*

从购买之初到此后的安全管理，Firebox X Core e系列套装产品让网络安全管理变得方便快捷，同时提供同类产品中最佳的UTM解决方案。赶紧购买吧，早买早省钱！

*订购一年

免费! **30天试用**

购买Firebox X Core，可获得以下产品的30天免费试用期：
网关防病毒/入侵防御服务，**spamBlocker**以及**WebBlocker**。
详情请联系经销商。

北京办事处
地址： 北京市朝阳门外大街16号中国人寿大厦525室邮编100020
电话： (86) 10.5877.1875 **传真：** (86) 10.5877.1876

上海办事处
地址： 上海市淮海中路333号瑞安广场1206室邮编200020
电话： (86) 21.5116.0557 **传真：** (86) 21.5116.0776

网址： www.watchguard.com/international/zh/
E-MAIL： information@watchguard.com

防火墙 IPSec VPN 网络内容过滤 IPS