# Dell SonicWALL
# 产品线

SonicWALL

# 目 录


**概述** 3

**网络安全/防火墙解决方案**
网络安全解决方案综述 5
SuperMassive 解决方案 5
E-Class 解决方案 8
中小企业和分支机构解决方案 10
无线解决方案 16
升级服务、许可证和固件 17

**广域网加速解决方案**
广域网加速解决方案 19

**安全远程访问解决方案**
安全远程访问解决方案综述 21
E-Class 解决方案 22
附加功能 22
中小企业和分支机构解决方案 24
附加功能 25

**反垃圾邮件/电子邮件安全解决方案**
电子邮件安全解决方案综述 28
E-Class 解决方案 28
中小企业解决方案 30
升级服务 30

**备份和恢复解决方案**
备份和恢复解决方案综述 31
中小企业解决方案 31
许可证和服务 33

**策略和管理解决方案**
全球管理系统 35
Analyzer 35
Scrutinizer 35

**全球支持服务**
7×24 小时 E-Class 技术支持 36
5×8 和 7×24 小时动态技术支持 36
综合全球管理系统支持 37
重点技术支持 37
远程启动和配置服务 37

**客户优势计划**
Secure Upgrade Plus 计划 38
Customer Loyalty Bundle 计划 38

# 概 述

## 威胁管理

互联网威胁不再只是惹人厌烦，它已经演变成会严重影响企业运行的复杂的、恶意的攻击。Dell™ SonicWALL™ 解决方案无缝集成了网络安全、web 和电子邮件安全功能，可全面抵御复杂的、不断升级的威胁。Dell SonicWALL 网络安全解决方案增强了对病毒、蠕虫、木马、间谍软件和网络入侵的防御能力，无需牺牲性能即可提供企业级网络性能。Dell SonicWALL Web 安全解决方案提供了更强大的控制能力，可阻止不恰当的和非法的 web 网站，以及控制即时信息和点对点应用的使用。Dell SonicWALL 应用智能、控制和可视化功能可对非生产性应用进行控制，如网络交易、即时信息/聊天、点对点共享和流视频网站。Dell SonicWALL 电子邮件安全解决方案可有效阻止垃圾软件和钓鱼攻击，对 Dell SonicWALL 产品组合进行了补充，员工只能打开合法的电子邮件，不会有任何欺骗性邮件。Dell SonicWALL 智能解决方案大大简化了本地、远程和移动网络服务的集中化管理，同时能以更低的成本、更高的效率保护关键信息和通信资源。

## 移动性

移动技术的普及、越来越分散的企业员工、支持企业网访问的智能手机以及对业务连续性的需求使移动性成为企业不可或缺的条件。Dell SonicWALL 解决方案通过宽带和蜂窝连接等方式为规模各异的企业提供了移动解决方案。结合 Dell SonicWALL 下一代防火墙防护功能，Dell SonicWALL 网络安全解决方案可利用 IPSec 或 SSL VPN 提供安全的站对站连接或安全的远程访问。如配合使用这些设备和自配置 SonicPoint 接入点，可及时为临时网络提供安全的无线热点连接。Dell SonicWALL 防火墙在没有任何固定的互联网连接的情况下，几乎可在任何地方及时建立安全的 3G 蜂窝宽带。此外，Dell SonicWALL 专用 SSL VPN 利用标准的 web 浏览器或移动设备如无线智能手机和平板电脑，让用户几乎可在任何远程位置进行安全的移动访问。Dell SonicWALL SSL VPN 解决方案还提供了无与伦比的细粒度访问控制能力。

## 应用控制

Dell SonicWALL 应用智能和控制功能实现了应用的细粒度控制和实时可视化，可保障带宽优先级的执行，确保最高的网络安全性和生产力。作为 Dell SonicWALL 下一代防火墙的集成功能，Dell SonicWALL 应用智能和控制功能使用了 Dell SonicWALL 免重组深度包检测（RFDPI）*专利技术，可识别和控制应用，不管其采用的是何种端口或协议。利用不断扩展的签名数据库（目前可识别超过 3500 种应用和数百万种恶意软件威胁），应用智能和控制功能可保持对应用的细粒度控制，优先分配或遏制带宽使用，以及拒绝 web 网站访问。Dell SonicWALL 应用流监控功能提供了有关应用、入站和出站带宽、活动的网站连接和用户行为的实时监控图表。

## 合规性

网络内同样存在着安全威胁。不管是出于有意还是无意，员工都有可能泄露不应该泄露的内容、知识产权或机密数据，从而给企业带来重大损失，还会使企业面临违反行业或政府法规如美国医疗保险移动和责任法案（HIPAA）或萨班斯-奥克斯利法案（Sarbanes-Oxley）等风险。违法不仅会让企业面临罚款，还有可能被追究管理责任，失去客户的信任。利用同类最佳的加密技术和深度包检测技术，Dell SonicWALL 解决方案实现了“干净的 VPN”连接，可帮助企业满足相关法律法规。Dell SonicWALL SSL VPN 解决方案提供了数据加密和验证、细粒度访问控制、策略管理、记录功能和灵活的验证架构。Dell SonicWALL 电子邮件安全解决方案可帮助企业轻松创建出站策略，智能识别不合法的电子邮件，并提供了强大的监控和报告工具，以及一系列修复功能。此外，Dell SonicWALL 内容过滤服务可保护企业网络远离非法的或非生产性的 web 内容。最后，屡获殊荣的 Dell SonicWALL 全球管理系统（GMS®）利用集中化实时监控以及综合的策略和合规性报告功能提供了全面的审计追踪能力。

## 业务连续性

不管是因为重大灾难、流感爆发还是因为住宅区停电导致正常业务运营中断，都有可能令企业错失商机，损失应有的收入，甚至是名誉受损。Dell SonicWALL 针对各种规模的企业提供了业务连续性和恢复解决方案。采用 Dell SonicWALL SSL VPN 解决方案，远程员工在家里或其它临时地点都可保持与办公室同等的工作效率。Dell SonicWALL 备份和恢复解决方案为服务器、笔记本电脑和 PC 提供了自动的、实时的数据备份和灵活的灾难恢复选择。Dell SonicWALL 持续数据保护（CDP）系列解决方案可本地或远程保护文件安全，确保数据的及时恢复。

## 应用流量分析

Dell SonicWALL 应用流量分析解决方案让企业可深入了解应用流量、带宽利用率和安全威胁，同时提供强大的故障排除和取证能力。Dell SonicWALL 全球管理系统（GMS）和 Analyzer（分析程序）可利用 Dell SonicWALL 防火墙提供的应用流量分析数据，深入透彻地了解网络情况。Dell SonicWALL Scrutinizer（审查程序）可兼容第三方路由器和交换机。

*美国专利 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

## Dell SonicWALL 防火墙/网络安全解决方案

Dell SonicWALL 公司是领先的下一代防火墙提供商之一。作为下一代防火墙解决方案部署时，Dell SonicWALL 防火墙紧密集成了 RFDPI*专利技术，可提供优异的入侵防御、恶意软件防护、应用智能、控制和实时可视化以及 SSL 加密会话检测功能。Dell SonicWALL 下一代防火墙是智能的、具有高度自适应性的安全系统的必要组件，可扫描每个数据包的每个字节，实现最强的保护水平。与其它竞争性解决方案不同，单通道 RFDPI 引擎可对各种大小的文件和连接同时进行多威胁和应用扫描及分析，无需进行数据包重组。如此一来，Dell SonicWALL 防火墙可实现大规模扩展，将最先进的安全性扩展至不断增长的分布式企业网络。Dell SonicWALL 安全设备也可作为统一威胁管理（UTM）防火墙部署，提供全面的安全保护能力，融合了网关内容过滤、反垃圾软件、防病毒、反间谍软件、入侵防御以及应用智能和控制功能。

Dell SonicWALL 免重组深度包检测（RFDPI）*专利技术能以极高的速度对各种大小的文件和连接同时进行多威胁和应用扫描及分析。RFDPI 引擎远远超越了简单的全状态检测，可扫描多种应用类型和协议，确保网络远离内部和外部攻击。这种单一的代码库是从 TZ 105 到 Dell SonicWALL SuperMassive E10800 的每台 Dell SonicWALL 防火墙的核心。运行 SonicOS 的 SuperMassive E10800 是综合防御能力最强的下一代防火墙，获 NSS 实验室“推荐”级别。RFDPI 紧密融入到了防火墙平台，可通过防火墙接口或 Dell SonicWALL 全球管理系统（GMS）直接简化细粒度防火墙策略的管理。Dell SonicWALL 提供了一系列经实践检验的防火墙供企业选择，这些产品均支持大规模扩展，满足高性能网络的需求。此外，通过利用独一无二的 Dell SonicWALL 全球响应智能防御（GRID）网络的全球攻击识别和监测网络，Dell SonicWALL 防火墙现可提供出色的防御能力，未来还可阻止各种新型威胁。

*美国专利 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

综合防御能力最强的下一代防火墙，获 NSS 实验室“推荐”级别

运行 SonicOS 6.0 的 SuperMassive E10800

## Dell SonicWALL SuperMassive E10000 系列简介

SuperMassive E10000 系列是 Dell SonicWALL 公司专为大型网络设计的下一代防火墙平台，以数千兆位速率提供了可扩展性、可靠性和深度安全防护。SuperMassive E10000 系列旨在满足企业、政府、大学和服务提供商部署环境的需求，非常适合用于保障企业网、数据中心和服务器群的安全。SuperMassive E10000 系列采用了支持大规模扩展的多核设计和 SonicWALL RFDPI*专利技术，提供了业界领先的应用控制、入侵防御、恶意软件防护和 SSL 检测功能。

**SuperMassive E10800**

- 处理核心：96 个
- IPS 吞吐量：30Gbps
- 防火墙吞吐量：40Gbps
- 最大连接：12.0M
- 应用检测吞吐量：30Gbps
- 威胁防御吞吐量：12Gbps

**SuperMassive E10400**

- 处理核心：48 个
- 最大连接：6.0M
- 防火墙吞吐量：20Gbps
- 升级路径：可现场升级至 E10800
- 应用检测吞吐量：15Gbps
- IPS 吞吐量：15Gbps
- 威胁防御吞吐量：6.0Gbps

**SuperMassive E10200**

- 处理核心：24 个
- 最大连接：3.0M
- 防火墙吞吐量：10Gbps
- 升级路径：可现场升级至 E10400、E10800
- 应用检测吞吐量：7.5Gbps
- 威胁防御吞吐量：3.0Gbps
- IPS 吞吐量：7.5Gbps

*美国专利 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

# SuperMassive E10000 系列

| 特性 | E10200 | E10400 | E10800 |
|---|---|---|---|
| **系统规格** | | | |
| 操作系统 | SonicOS | | |
| 处理核心 | 24 | 48 | 96 |
| 10GbE 接口 | 6 个 10GbE SFP+端口 | | |
| 1GbE 接口 | 16 个 1GbE SFP 端口 | | |
| 管理界面 | 1GbE，1 个控制台 | | |
| 内存（RAM） | 16 GB | 32 GB | 64 GB |
| 存储 | 80 GB SSD，闪存 | | |
| 防火墙吞吐量 | 10 Gbps | 20 Gbps | 40 Gbps |
| 应用检测吞吐量 | 7.5 Gbps | 15 Gbps | 30 Gbps |
| IPS 吞吐量 | 7.5 Gbps | 15 Gbps | 30 Gbps |
| 反恶意软件检测吞吐量 | 3.0 Gbps | 6.0 Gbps | 12 Gbps |
| VPN 吞吐量 | 5.0 Gbps | 10 Gbps | 20 Gbps |
| 每秒连接数 | 160,000/秒 | 320,000/秒 | 640,000/秒 |
| 最大连接（SPI） | 3.0 M | 6.0 M | 12.0 M |
| 最大连接（DPI） | 2.5 M | 5.0 M | 10.0 M |
| **VPN** | | | |
| 点对点隧道 | 10,000 (20,000)* | 10,000 (40,000)* | 10,000 (80,000)* |
| IPSec VPN 客户端 | 2,000 (4,000)* | 2,000 (8,000)* | 2,000 (16,000)* |
| SSL VPN 许可证 | 50 (2,000)* | 50 (4,000)* | 50 (8,000)* |
| 加密 | DES，3DES，AES（128、192、256 位） | | |
| 验证 | MD5，SHA-1 | | |
| 密钥交换 | Diffie Hellman Groups 1，2，5，14 | | |
| 基于路由的 VPN | RIP，OSPF | | |
| **网络** | | | |
| IP 地址分配 | 静态（DHCP PPPoE、L2TP 和 PPTP 客户端）、内部 DHCP 服务器、DHCP 中继 | | |
| NAT 模式 | 1 对 1，多对 1，1 对多，多对多，灵活的 NAT（重复的 IPS），PAT，透明模式 | | |
| VLAN 接口 | 512 | | |
| 路由协议 | OSPF，RIPv1/v2，BGP*，静态路由，基于策略的路由，组播 | | |
| QoS | 带宽优先级，最大带宽，保证带宽，DSCP 标记，802.1p | | |
| 认证 | XAUTH/RADIUS，活动目录，SSO，LDAP，Novell，内部用户数据库，终端服务，Citrix | | |
| IPv6 | 支持 | | |
| VoIP | 全 H323-v1-5，SIP | | |
| 标准 | TCP/IP，ICMP，HTTP，HTTPS，IPSec，ISAKMP/IKE，SNMP，DHCP，PPPoE，L2TP，PPTP，RADIUS，IEEE 802.3 | | |
| **硬件** | | | |
| 电源 | 2 个热插拔冗余 850W 电源 | | |
| 风扇 | 2 个冗余风扇，可现场更换 | | |
| 显示屏 | 前端 LCD 显示屏 | | |
| 输入功率 | 100-240 VAC，60-50 Hz | | |
| 最大功耗（W） | 400 | 500 | 750 |
| 外形 | 4U 机架式 | | |
| 尺寸 | 17x18x7 英寸（43x43.5x17.8 厘米） | | |
| 重量 | 58 磅（26.3 千克） | 61 磅（27.7 千克） | 67 磅（30.3 千克） |
| WEEE 重量 | 59 磅（26.8 千克） | 62 磅（28.1 千克） | 68 磅（30.8 千克） |
| 装运重量 | 79 磅（35.8 千克） | 82 磅（37.2 千克） | 88 磅（39.9 千克） |
| 主要要求 | FCC A 级，CE，C-Tick，VCCI，Compliance MIC，UL，cUL，TUV/GS，CB，NOM，RoHS，WEEE | | |
| 工作环境 | 40-105°F，5-40°C | | |
| 湿度 | 10-90%，无冷凝 | | |

* 配备可扩展许可证。
所有规格、特性和可用性可随时变更。

**Dell SonicWALL 企业级 E-Class NSA 系列采用了多核微处理器，可在不影响网络速度的情况下充分执行 RFDPI。**

## Dell SonicWALL 企业级解决方案：E-Class NSA 系列简介

Dell SonicWALL E-Class 网络安全设备（NSA）系列作为下一代防火墙提供了企业级性能，包括紧密集成的入侵防御系统、反恶意软件防护和应用智能、控制和可视化功能。通过结合 Dell SonicWALL 免重组深度包检测（RFDPI）*专利技术和强大的多核硬件平台，E-Class NSA 系列解决方案可分析和控制数千种独特的应用，即使是利用 SSL 加密的应用。集成式应用流量分析报告工具为 E-Class NSA 系列提供了强大的网络利用率监控功能。

E-Class NSA 系列经工程设计成为同类设备中扩展性最好、性能最佳、可靠性最高的多功能威胁管理设备。网关防病毒、反间谍软件和入侵防御功能可针对复杂的应用层和基于内容的攻击包括病毒、间谍软件、蠕虫、木马和软件漏洞如缓冲区溢出进行实时的网络安全防护。应用智能、控制和可视化功能可帮助企业全面了解网络流量，并提供了一套自定义策略，让管理员能以高度细粒度方式控制网络中的应用和用户，将安全防护提高到了新的高度。为了满足企业级网络的运营可靠性需求，E-Class NSA 系列在硬件和系统层面都融入了一系列高可用性功能，以最大程度地提高正常运行时间，扩大安全覆盖区域。E-Class NSA 系列还提供了一系列高级网络配置功能，可简化部署和集成，从而降低管理复杂性。这使 E-Class NSA 成为需要在各种环境下实现高性能网络安全的企业的最佳选择。此外，E-Class NSA 系列满足了联邦政府、州政府和地方政府的多功能安全需求，并符合相关的认证需求，如联邦信息处理标准（FIPS）、评估 IT 产品安全功能的国际标准（通用标准 3.1 EAL 4+）。E-Class NSA 系列的功能包括：

- 企业级 RFPDI，支持在每个接口针对每个数据包和每种协议进行入侵防御、恶意软件防护，同时支持应用智能、控制和可视化
- 创新的多核性能，使用了高达 16 个处理器核心，为外部和内部网络提供了高速多层威胁防御
- 利用 RFDPI 引擎，可消除文件大小不限和并发连接不限的流量所带来的威胁，实现最佳的扩展性
- 动态更新的、可自定义的安全防御机制
- 灵活的、安全的虚拟专用网（VPN）技术，包括用于站点间连接的 IPSec VPN，以及支持安全远程访问的 SSL VPN 和 IPSec VPN 客户端连接
- 不会对业务连续性和高可用性保护造成任何负面影响

*美国专利 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

### Dell SonicWALL E-Class NSA E8510 和 E8500

Dell SonicWALL NSA E8510 和 E8500 作为下一代防火墙，是专为需要深度包检测保护和应用控制功能的企业网设计的，同时确保优异的性能。NSA E8510 结合了紧密集成的入侵防御、先进的恶意软件保护功能以及强大的应用智能、控制和可视化功能。采用荣获专利的 Dell SonicWALL RFDPI*引擎，NSA E8510 和 E8500 可分析和控制数千种应用，即使这些应用采用了 SSL 进行加密。软件的精密性与硬件无比强大的功能相结合，应用流量在网络中几乎无处遁形，Dell SonicWALL RFDPI 引擎可同时检测所有端口上的数十万条连接，几乎达到了零延迟，且没有文件大小限制。

### Dell SonicWALL E-Class NSA E6500 和 E5500

Dell SonicWALL NSA E6500 和 E5500 是专为不断扩展的企业网设计的下一代防火墙，可提供高性能、可高度扩展的解决方案，满足企业网在扩展过程中的需求。NSA E6500 和 E5500 充分利用了荣获专利的 Dell SonicWALL RFDPI*引擎以及专用多核处理技术，实现了并行流量处理。如今，企业管理员可通过 Dell SonicWALL 打造的高性能安全平台应对不断升级的各种威胁。Dell SonicWALL 应用智能、控制和可视化功能可帮助企业实时了解网络流量，并提供了一套自定义策略，让管理员能以高度细粒度方式控制网络中的应用和用户，将安全防护提高到了新的高度。NSA E6500 和 E5500 标配了 8 个千兆铜缆以太网端口，实现了部署灵活性，并提供了 1 个 LCD 管理屏幕，简化了部署。

*美国专利 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

## Dell SonicWALL 中小企业和分支机构解决方案：NSA 系列简介

Dell SonicWALL 网络安全设备（NSA）系列融合了 Dell SonicWALL RFDPI* 引擎专利技术和强大的、支持大规模扩展的多核架构，可为各类规模的企业提供入侵防御、网关防病毒、网关反间谍软件以及应用智能和控制功能。通过将自动的、动态的安全功能融入单一安全平台，NSA 系列提供了全面的安全防护，同时确保了优异的性能。NSA 系列在单个经济实惠的访问平台上集成了高速入侵防御、文件和内容检测以及强大的应用智能、控制和可视化功能，提供一系列高级网络功能和灵活的配置能力，适用于各种环境，而且部署和管理都非常简单。NSA 系列采用了直观的 web 管理界面和简单易用的安装向导，简化了安装和配置。NSA 系列还提供了对虚拟局域网（VLAN）、企业级路由和 QoS 功能的支持，进一步增强了网络的安全性和性能。此外，NSA 系列符合相关认证要求，如 FIPS 和通用标准 EAL 4+。

### Dell SonicWALL NSA 4500

Dell SonicWALL NSA 4500 是一款旨在满足企业中央站点和大型分布式环境的下一代防火墙，以 8 核硬件平台为基础。NSA 4500 采用了 6 个可配置千兆以太网（GbE）接口，是实现企业边界保护和远程访问连接的最佳解决方案。

### Dell SonicWALL NSA 3500

Dell SonicWALL NSA 3500 是一款基于四核架构的下一代防火墙，带 6 个吉比特以太网接口。

### Dell SonicWALL NSA 2400

Dell SonicWALL NSA 2400 是一款基于多核硬件平台的下一代防火墙，带 6 个吉比特以太网接口。

*美国专利 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

### Dell SonicWALL NSA 250M 系列

Dell SonicWALL NSA 250M 系列作为模块化的下一代防火墙，为分支机构和分布式企业提供了全面的、先进的安全功能和可选的 802.11 双频无线功能。NSA 250M 可利用一系列模块进行扩展，如 T1/E1、DSL 和 SFP 模块，以提供部署灵活性和其它故障转移功能，还可降低收购和维护成本。

### Dell SonicWALL NSA 220 系列

Dell SonicWALL NSA 220 系列作为下一代防火墙，为分支机构和分布式企业提供了易于管理的、先进的安全功能和可选的 802.11 双频无线功能。

# 网络安全设备系列

| 特性 | NSA 220/W-N | NSA 250M/W-N | NSA 2400 | NSA 3500 | NSA 4500 |
|---|---|---|---|---|---|
| 支持的 SonicOS 版本 | SonicOS 5.8.1.1 | SonicOS 5.8.1.1 | SonicOS 增强版 5.6（或更高版） | SonicOS 增强版 5.6（或更高版） | SonicOS 增强版 5.6（或更高版） |
| 用户数和节点数 | 无限制 | 无限制 | 无限制 | 无限制 | 无限制 |
| 网络接口 | 7 个 10/100/1000 千兆端口，2 个 USB，1 个控制台接口 | 5 个 10/100/1000 千兆端口，2 个 USB，1 个控制台接口，1 个模块插槽 | 6 个 10/100/1000 千兆铜缆端口，1 个控制台接口，2 个 USB（备用） | 6 个 10/100/1000 千兆铜缆端口，1 个控制台接口，2 个 USB | 6 个 10/100/1000 千兆铜缆端口，1 个控制台接口，2 个 USB |
| 电源 | 36W 外部电源 | 36W 外部电源 | 单个 180W ATX 电源 | 单个 180W ATX 电源 | 单个 180W ATX 电源 |
| 冷却系统（风扇） | 无风扇/1 个风扇 | 2 个风扇 | 2 个风扇 | 2 个风扇 | 2 个风扇 |
| VLAN 接口 | 25 | 35 | 25 | 50 | 200 |
| 高可用性 | 主动/被动可选状态同步 | 主动/被动可选状态同步 | 主动/被动可选状态同步 | 主动/被动可选状态同步 | 主动/被动状态同步 |
| 全状态吞吐量 [1] | 600 Mbps | 750 Mbps | 775 Mbps | 1.5 Gbps | 2.75 Gbps |
| 3DES/AES 吞吐量 [2] | 150 Mbps | 200 Mbps | 300 Mbps | 625 Mbps | 1.0 Gbps |
| 网关防病毒吞吐量 [3] | 115 Mbps | 140 Mbps | 160 Mbps | 350 Mbps | 690 Mbps |
| 入侵防御吞吐量 [3] | 195 Mbps | 250 Mbps | 275 Mbps | 750 Mbps | 1.4 Gbps |
| 全面的 DPI 性能 [3] | 110 Mbps | 130 Mbps | 150 Mbps | 240 Mbps | 600 Mbps |
| IMIX 性能 [3] | 180 Mbps | 210 Mbps | 235 Mbps | 580 Mbps | 700 Mbps |
| 每秒新建连接 | 2,200 | 3,000 | 4,000 | 7,000 | 10,000 |
| 最大连接数 | 85,000 | 110,000 | 225,000 | 325,000 | 500,000 |
| 最大 DPI 连接数 | 32,000 | 64,000 | 125,000 | 175,000 | 250,000 |
| 点对点 VPN | 25 | 50 | 75 | 800 | 1,500 |
| 区域安全 | 支持 | 支持 | 支持 | 支持 | 支持 |
| 基于对象的管理 | 支持 | 支持 | 支持 | 支持 | 支持 |
| 基于策略的 NAT | 支持 | 支持 | 支持 | 支持 | 支持 |
| 多 ISP 故障转移 | 支持 | 支持 | 支持 | 支持 | 支持 |
| 负载均衡 | 支持 | 支持 | 支持 | 支持 | 支持 |
| 集成式无线交换机和控制器 | 支持 | 支持 | 支持 | 支持 | 支持 |
| 3G 无线故障转移 | 支持 | 支持 | – | 支持 | 支持 |
| 基于策略的路由 | 支持 | 支持 | 支持 | 支持 | 支持 |
| 综合反垃圾邮件服务 | 可选 | 可选 | 可选 | 可选 | 可选 |
| IP 语音（VoIP） | 支持 | 支持 | 支持 | 支持 | 支持 |
| IKEv2 VPN | 支持 | 支持 | 支持 | 支持 | 支持 |
| 安全远程管理（支持 SSHv2） | 支持 | 支持 | 支持 | 支持 | 支持 |
| SSL VPN 和 IPSec VPN 远程访问客户端 | 支持 | 支持 | 支持 | 支持 | 支持 |
| 安全虚拟辅助技术员 | 30 天试用期 | 30 天试用期 | 支持 | 支持 | 支持 |
| 基于路由的 VPN | 支持 | 支持 | 支持 | 支持 | 支持 |
| TSA 用户验证 | 支持 | 支持 | 支持 | 支持 | 支持 |
| 动态地址对象 | 支持 | 支持 | 支持 | 支持 | 支持 |
| 二层桥接模式 | 支持 | 支持 | 支持 | 支持 | 支持 |
| 2 层无线桥接 | 支持 | 支持 | 不支持 | 不支持 | 不支持 |
| 无线交换机和控制器 | 支持 | 支持 | 不支持 | 不支持 | 不支持 |
| 802.1q VLAN | 支持 | 支持 | 支持 | 支持 | 支持 |
| RIPv2 和 OSPF 路由 | 支持 | 支持 | 支持 | 支持 | 支持 |
| 单点登录（SSO） | 支持 | 支持 | 支持 | 支持 | 支持 |
| 应用智能和控制 | 可选 | 可选 | 可选 | 可选 | 可选 |
| 深度包检测 SSL | 可选 | 可选 | 可选 | 可选 | 可选 |
| SSL 控制 | 支持 | 支持 | 支持 | 支持 | 支持 |
| IPv6[4] | 不支持 | 不支持 | 支持 | 支持 | 支持 |
| 应用可视化 | 支持 | 支持 | 支持 | 支持 | 支持 |
| NetFlow/IPFIX | 支持 | 支持 | 支持 | 支持 | 支持 |

[1] 测试方法：最大性能应符合 RFC 2544 的规定（用于防火墙）。实际性能可能会因网络状况和使用的服务而有所差异。
[2] VPN 吞吐量是使用符合 RFC 2544 规范、数据包大小为 1280 字节的 UDP 流量进行测定的。
[3] 全面的 DPI/网关 AV/反间谍软件/IPS 吞吐量使用工业标准 Spirent WebAvalanche HTTP 性能测试和 Ixia 测试工具进行测量。测试是采用穿越多个端口对的多点流量完成的。
[4] IPv6 功能需部署单独的固件。
*指全状态 HA 和扩展升级版。

# E-Class 网络安全设备系列

| 特性 | NSA E5500 | NSA E6500 | NSA E8500 | NSA E8510 |
|---|---|---|---|---|
| 支持的 SonicOS 版本 | SonicOS 增强版 5.6（或更高版） | SonicOS 增强版 5.6（或更高版） | SonicOS 增强版 5.6（或更高版） | SonicOS 增强版 5.81（或更高版） |
| 用户数和节点数 | 无限制 | 无限制 | 无限制 | 无限制 |
| 网络接口 | 8 个 10/100/1000 千兆铜缆端口，1 个 GbE HA 接口，1 个控制台接口，2 个 USB | 8 个 10/100/1000，4 个 10/100/1000 GbE，1 个 GbE HA 接口，1 个控制台接口，2 个 USB | 4 个 SFP（SX、LX 或 TX），4 个 10/100/1000 GbE，1 个 GbE HA 接口，2 个 USB，1 个控制台接口 | 2 个 SFP+10GbE，4 个 10/100/1000 GbE，1 个 GbE HA 接口，2 个 USB，1 个控制台接口 |
| 电源 | 单个 250W ATX 电源 | 单个 250W ATX 电源 | 两个 250W ATX 电源，可热插拔 | 两个 250W ATX 电源，可热插拔 |
| 冷却系统（风扇） | 2 个风扇，可热插拔 | 2 个风扇，可热插拔 | 2 个风扇，可热插拔 | 2 个风扇，可热插拔 |
| VLAN 接口 | 400 | 500 | 512 | 512 |
| 高可用性 | 主动/被动状态同步，主动/主动 DPI 状态同步 | 主动/被动状态同步，主动/主动 DPI 状态同步 | 主动/被动状态同步，主动/主动 DPI 状态同步 | 主动/被动状态同步，主动/主动 DPI 状态同步 |
| 全状态吞吐量 [1] | 3.9 Gbps | 5.0 Gbps | 8.0 Gbps | 8.0 Gbps |
| 3DES/AES 吞吐量 [2] | 1.7 Gbps | 2.7 Gbps | 4.0 Gbps | 4.0 Gbps |
| 网关防病毒吞吐量 [3] | 1.0 Gbps | 1.69 Gbps | 2.25 Gbps | 2.25 Gbps |
| 入侵防御吞吐量 [3] | 2.0 Gbps | 2.3 Gbps | 3.7 Gbps | 3.7 Gbps |
| 全面的 DPI 性能 [3] | 850 Mbps | 1.59 Gbps | 2.2 Gbps | 2.2 Gbps |
| IMIX 性能 [3] | 1.1 Gbps | 1.4 Gbps | 2.0 Gbps | 2.0 Gbps |
| 每秒新建连接 | 30,000 | 60,000 | 85,000 | 85,000 |
| 最大连接数 | 750,000 | 1,000,000 | 1,500,000 | 1,500,000 |
| 最大 DPI 连接数 | 500,000 | 600,000 | 1,250,000 | 1,250,000 |
| 点对点 VPN | 4,000 | 6,000 | 10,000 | 10,000 |
| 区域安全 | 支持 | 支持 | 支持 | 支持 |
| 基于对象的管理 | 支持 | 支持 | 支持 | 支持 |
| 基于策略的 NAT | 支持 | 支持 | 支持 | 支持 |
| 多 ISP 故障转移 | 支持 | 支持 | 支持 | 支持 |
| 负载均衡 | 支持 | 支持 | 支持 | 支持 |
| 集成式无线交换机和控制器 | 支持 | 支持 | 支持 | 支持 |
| 3G 无线故障转移 | 支持 | 支持 | 支持 | 支持 |
| 基于策略的路由 | 支持 | 支持 | 支持 | 支持 |
| 综合反垃圾邮件服务 | 可选 | 可选 | 可选 | 可选 |
| IP 语音（VoIP） | 支持 | 支持 | 支持 | 支持 |
| IKEv2 VPN | 支持 | 支持 | 支持 | 支持 |
| 安全远程管理（支持 SSHv2） | 支持 | 支持 | 支持 | 支持 |
| SSL VPN 和 IPSec VPN 远程访问客户端 | 支持 | 支持 | 支持 | 支持 |
| 安全虚拟辅助技术员 | 支持 | 支持 | 支持 | 支持 |
| 基于路由的 VPN | 支持 | 支持 | 支持 | 支持 |
| TSA 用户验证 | 支持 | 支持 | 支持 | 支持 |
| 动态地址对象 | 支持 | 支持 | 支持 | 支持 |
| 二层桥接模式 | 支持 | 支持 | 支持 | 支持 |
| 802.1q VLAN | 支持 | 支持 | 支持 | 支持 |
| RIPv2 和 OSPF 路由 | 支持 | 支持 | 支持 | 支持 |
| 单点登录（SSO） | 支持 | 支持 | 支持 | 支持 |
| 应用智能和控制 | 可选 | 可选 | 支持 | 支持 |
| 深度包检测 SSL | 可选 | 可选 | 支持 | 支持 |
| SSL 控制 | 支持 | 支持 | 支持 | 支持 |
| IPv6[4] | 支持 | 支持 | 支持 | 支持 |
| 应用可视化 | 支持 | 支持 | 支持 | 支持 |
| NetFlow/IPFIX | 支持 | 支持 | 支持 | 支持 |
| 链路聚合 | 支持 [5] | 支持 [5] | 支持 [5] | 支持 [5] |
| 端口冗余 | 支持 | 支持 | 支持 | 支持 |

[1] 测试方法：最大性能应符合 RFC 2544 的规定（用于防火墙）。实际性能可能会因网络状况和使用的服务而有所差异。
[2] VPN 吞吐量是使用符合 RFC 2544 规范、数据包大小为 1280 字节的 UDP 流量进行测定的。
[3] 全面的 DPI/网关 AV/反间谍软件/IPS 吞吐量使用工业标准 Spirent WebAvalanche HTTP 性能测试和 Ixia 测试工具进行测量。测试是采用穿越多个端口对的多点流量完成的。
[4] IPv6 功能需部署单独的固件。[5] 静态链路聚合。
*指全状态 HA 和扩展升级版。

TZ 系列是针对分布式网络环境最理想的安全平台，包括远程办公室、分支机构、中小企业和零售/POS 部署环境。

## Dell SonicWALL 分支机构和中小企业解决方案：TZ 系列简介

Dell SonicWALL TZ 系列是针对小型企业、零售环境、政府机构、远程站点和分支机构的最安全的统一威胁管理（UTM）防火墙。与消费级产品不同，TZ 系列提供了高效的反恶意软件、入侵防御、内容/URL 过滤和应用控制功能，并为笔记本电脑、智能手机和平板电脑提供了最广泛的、最安全的移动平台支持。它以最高的性能提供了深度包检测（DPI）功能，消除了其它产品可能带来的网络瓶颈，帮助企业提高了生产力。TZ 系列是目前市面上最安全、最先进且部署最广泛的安全平台。

此外，TZ 215 的 Dell SonicWALL 应用智能和控制功能确保业务关键应用能优先使用带宽，同时可遏制或阻止非生产性应用。TZ 215 还提供了先进的应用流量分析和报告功能，以便能深入了解带宽利用情况和安全威胁。

TZ 系列还集成了其它先进的网络功能如 IPSec、SSL VPN、多重 ISP 故障转移、负载均衡、可选集成式 802.11n 无线功能和网络分段，同时满足了 PCI 合规性。与其它 UTM 防火墙不同，TZ 系列为 Apple® iOS、Google® Android™、Windows、Mac OS 和 Linux 提供了本地 VPN 远程访问客户端。这一独特的客户端还提供了对 Clean VPN™ 的支持，该技术可清除 VPN 流量中的威胁。全新的 TZ 系列是多种单一功能产品的完美结合，通过单一解决方案提供了多种增值服务，同时降低了复杂性。

### TZ 215

Dell SonicWALL TZ 215 是针对小型企业和分支机构的最安全的、最高性能的统一威胁管理（UTM）防火墙。TZ 215 是专为小型企业、分布式企业、分支机构和零售环境设计的，集成了反恶意软件、入侵防御、应用控制和 URL 过滤功能，降低了成本和复杂性。它采用的是双核架构，在不影响网络性能的情况下提供了完整的深度包检测（DPI）功能，消除了其它产品可能会带来的瓶颈，让企业能有效提高生产力。TZ 215 还提供了应用控制功能，确保关键应用的带宽，同时遏制非生产性应用使用的带宽。先进的网络功能包括多重 ISP 故障转移、负载均衡、可选双频安全无线、IPSec VPN 支持、网络分段和 PCI 合规性功能。

### Dell SonicWALL TZ 205

Dell SonicWALL TZ 205 提供了强大的安全防护能力和业务级性能，使小型企业、零售环境、政府机构、远程站点和分支机构大大受益。与消费级产品不同，这款功能强大的统一威胁管理（UTM）防火墙集成了最有效的入侵防御、反恶意软件和内容/URL 过滤功能，并为笔记本电脑、智能手机和平板电脑提供了最广泛的、最安全的移动平台支持。TZ 205 以极高的性能提供了完整的深度包检测（DPI）功能，不仅保证了综合安全性，还实现了优异的性能。

## Dell SonicWALL TZ 105 系列

Dell SonicWALL TZ 105 是针对小型办公室、家庭办公室和小型零售环境的最安全的统一威胁管理（UTM）防火墙。与消费级产品不同，TZ 105 提供了经验证的、最有效的入侵防御、反恶意软件和内容/URL 过滤功能，并为笔记本电脑、智能手机和平板电脑提供了广泛的移动平台支持。它以极高的性能提供了完整的深度包检测（DPI）功能，消除了其它产品可能会带来的网络瓶颈，帮助企业在不增加成本的前提下提高了生产力。

| 特性 | TZ 105 系列 | TZ 205 系列 | TZ 215 系列 |
|---|---|---|---|
| 节点 | 无限制 | 无限制 | 无限制 |
| 网络接口 | 5 个 10/100 快速以太网接口，1 个 USB，1 个控制台接口 | 5 个 10/100/1000 千兆铜缆端口，1 个 USB，1 个控制台接口 | 7 个 10/100/1000 千兆铜缆端口，2 个 USB，1 个控制台接口 |
| 全状态包检测吞吐量 [1] | 200 Mbps | 500 Mbps | 500 Mbps |
| UTM 吞吐量 [3] | 25 Mbps | 40 Mbps | 60 Mbps |
| 3DES/AES 吞吐量 [2] | 75 Mbps | 100 Mbps | 130 Mbps |
| 最大连接数 | 8,000 | 12,000 | 48,000 |
| 最大 UTM 连接数 | 8,000 | 12,000 | 32,000 |
| 点对点 VPN 隧道 | 5 | 10 | 20 |
| 远程访问 IPSec VPN 隧道（最多） | 5 | 10 | 25 |
| 远程访问 IPSec VPN 隧道（捆绑的） | 可选升级 | 2 | 2 |
| 远程访问 SSL VPN 隧道（最多） | 5 | 10 | 10 |
| 远程访问 SSL VPN 隧道（捆绑的） | 1 | 1 | 2 |
| 安全虚拟辅助技术员（最多） | 不支持 | 1 | 2 |
| 安全虚拟辅助技术员（捆绑的） | 不支持 | 0 | 30 天试用期 |
| VLAN 接口 | 5 个，端口屏蔽 | 10 个，端口屏蔽 | 20 个，端口屏蔽 |
| 区域安全 | 支持 | 支持 | 支持 |
| 基于对象的管理 | 支持 | 支持 | 支持 |
| 基于策略的 NAT | 支持 | 支持 | 支持 |
| 多 ISP 故障转移 | 支持 | 支持 | 支持 |
| ISP 故障转移 | 支持 | 支持 | 支持 |
| 硬件故障转移 | 不支持 | 主动/被动 | 主动/被动 |
| 广域网负载均衡 | 支持 | 支持 | 支持 |
| 二层无线桥接 | 支持 | 支持 | 支持 |
| 无线交换机和控制器 | 支持 | 支持 | 支持 |
| 虚拟接入点（VAP） | 支持 [4] | 支持 [4] | 支持 [4] |
| 集成式接入点 | 可选 802.11n | 可选 802.11n | 可选 802.11n |
| 综合反垃圾邮件服务 | 可选 | 可选 | 可选 |
| 双频无线接入点 | 支持 | 支持（2×2） | 支持（3×3） |
| IP 语音（VoIP） | 支持 | 支持 | 支持 |
| PortShield 安全 | 支持 | 支持 | 支持 |
| 基于路由的 VPN | 支持 | 支持 | 支持 |
| 3G 无线故障转移 | 支持 | 支持 | 支持 |
| 带宽管理 | 不支持 | 支持 | 支持 |
| 应用智能和控制 | 不支持 | 支持 | 支持 |
| 应用可视化 | 不支持 | 支持 | 支持 |
| NetFlow/IPFIX | 不支持 | 支持 [5] | 支持 |

[1] 测试方法：最大性能应符合 RFC 2544 的规定（用于防火墙）。实际性能可能会因网络状况和使用的服务而有所差异。
[2] VPN 吞吐量是使用符合 RFC 2544 规范、数据包大小为 1280 字节的 UDP 流量进行测定的。
[3] UTM/网关 AV/反间谍软件/IPS 吞吐量使用行业标准 Spirent WebAvalanche HTTP 性能测试和 Ixia 测试工具进行测量。测试是采用穿越多个端口对的多点流量完成的。
[4] 只有集成式无线射频支持虚拟接入点（VAP）。
[5] 请查看最新的版本注释，了解其可用性。

## Dell SonicWALL 干净的无线解决方案：SonicPoints 简介

Dell SonicWALL 利用创新的 Dell SonicWALL 干净的无线解决方案，让无线网络变得更安全、更简单，并且更具成本效益。Dell SonicWALL 干净的无线解决方案是第一款集成了 802.11n 和 802.11a/b/g 无线管理和同类最佳的下一代防火墙安全以及应用智能、控制和可视化功能以提供基于应用的策略控制的整体安全解决方案。Dell SonicWALL SonicPoint-N 系列无线访问点设备和 Dell SonicWALL 以太网供电注入器与 Dell SonicWALL 公司屡获殊荣的防火墙设备系列形成了互补，可在整个无线网络灵活提供全面的安全防护性能。Dell SonicWALL 干净的无线解决方案不止是单纯的安全无线解决方案，它可利用深度包检测技术让无线网变得和有线网一样安全，不仅可加密无线流量并清除流量中的网络威胁，同时可保护网络远离无线攻击，从而提供了双重安全保护。SonicPoint-Ni 和 SonicPoint-Ne 双频以及 SonicPoint-N 双射频都属于访问点，可用于提供无缝的、安全的无线局域网（WLAN）连接以及先进的功能和服务。Dell SonicWALL 让管理员可避免部署和单独管理与现有的有线网络并行的、昂贵的无线专用解决方案。

### Dell SonicWALL-N 双射频

Dell SonicWALL SonicPoint-N 双射频利用两台独立的收发机经 2.4GHz 和 5GHz 频段提供了安全的 802.11a/g/b/n 无线网络。Dell SonicWALL 的支持 SonicPoint 的 Clean Wireless™（干净无线）技术利用防火墙中的 Dell SonicWALL RFDPI* 专利技术的安全性实现了集成式接入点管理，消除了无线流量中的威胁。SonicPoint-N 双射频提供的总吞吐量高达 600Mbps，提供了更高的安全性和生产效率。

### SonicPoint-Ne 双频

Dell SonicWALL SonicPoint-Ne 双频访问点集成了 802.11a/b/g/n 管理和强制实施功能以及 Dell SonicWALL RFDPI* 专利技术，可灵活部署至 Dell SonicWALL 干净的无线网络。灵活的部署选项包括不带电源插座的 802.3af 以太网供电以及经交流电适配器进行直接供电。Dell SonicWALL SonicPoint-Ne 双频访问点尤为适合医院或诊所、专业办公室和其它需要带灯光和标识套、安静操作和可控 LED（除电源外）的谨慎的无线部署的部署场景。

### SonicPoint-Ni 双波段

Dell SonicWALL SonicPoint-Ni 双波段访问点集成了 802.11a/b/g/n 管理和强制实施功能以及 Dell SonicWALL RFDPI* 专利技术，可保障高度谨慎的 Dell SonicWALL 干净无线网络环境的安全。Dell SonicWALL SonicPoint-Ni 双波段访问点尤为适合医院或诊所、专业办公室和其它需要带内部天线、灯光和标识套、安静操作和可控 LED（除电源外）的谨慎的无线部署的部署场景。

*美国专利 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

### PoE 注入器

Dell SonicWALL PoE 注入器是符合 IEEE 802.3af 或 IEEE 802.3at 规范（SonicPoint-N 双射频）的电源注入器，采用了先进的自动感应算法，可自动检测是否存在兼容 PoE 的设备，将正确电源注入数据电缆。PoE 注入器属于即插即用设备，可轻松匹配无线以太网基础架构，无需配置或管理。

## 网络安全解决方案的先进安全服务

### Dell SonicWALL 网关防病毒、反间谍软件、入侵防御、应用智能和控制服务

网关防病毒、反间谍软件、入侵防御、应用智能和控制服务提供智能实时的网络安全保护，以抵御大范围的动态威胁，包括病毒、间谍软件、蠕虫、木马、软件漏洞利用（如缓存溢出）以及后门攻击和其它恶意代码。作为新增的安全层，这一功能强大的解决方案提供的应用层攻击防御不仅针对外部威胁，还包括网络内生成的所有威胁。Dell SonicWALL 网关防病毒、反间谍软件和入侵防御服务可检测大量电子邮件、web、文件传输和基于流的协议以及即时通讯（IM）和点对点（P2P）应用，避免潜在的安全威胁。Dell SonicWALL 应用智能和控制功能提供了对应用的细粒度控制和实时可视化，可保障带宽的优先分配，确保最高的网络安全性和生产力。

### Dell SonicWALL 内容过滤服务

内容过滤服务（CFS）增强了企业和学校的控制能力，可透明执行生产力和安全防护策略，阻止不恰当的、非法的和危险的 web 内容。Dell SonicWALL CFS 采用了动态的速率和缓存架构，可阻止多种具有争议性的 web 内容，完美结合了控制力和灵活性，可确保最高级别的生产力和安全保护。

### Dell SonicWALL 强制客户端防病毒和反间谍软件

强制客户端防病毒和反间谍软件配合 Dell SonicWALL 防火墙使用，可在网关层为台式机和笔记本电脑提供全面的强制病毒和间谍软件防护。Dell SonicWALL 防火墙确保所有电脑在访问网络之前都安装并运行了最新版本的防病毒和反间谍软件。病毒和间谍软件签名自动更新功能让技术人员无需逐一为设备安装防病毒软件，节省了时间。Dell SonicWALL 强制客户端防病毒和反间谍软件可与 McAfee®防病毒引擎一起购买。

### Dell SonicWALL 综合反垃圾邮件服务

综合反垃圾邮件服务（CASS）为中小企业提供了综合抵御垃圾邮件和病毒的能力，可及时部署于现有 Dell SonicWALL 网络安全设备。CASS 通过整合各种解决方案，加快了部署，简化了管理，减轻了负担，提供了单击反垃圾邮件服务，并且可在十分钟内完成高级配置。

*美国专利 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

### Dell SonicWALL DPI-SSL

对经 SSL 加密的流量进行深度包检测（DPI-SSL），可使用 Dell SonicWALL RFDPI 透明解密和扫描入站和出站 HTTPS 流量。如未检测到任何威胁或漏洞，便会对流量进行重新加密，并发送到原目标地址。

### Dell SonicWALL 安全虚拟援助

Secure Virtual Assist（安全虚拟援助）是一种远程技术支持工具。采用此工具，技术人员可控制客户 PC 或笔记本电脑，从而进行远程技术援助。经客户许可后，技术人员可通过 web 浏览器及时访问客户电脑，更轻松地进行远程诊断和问题修复。简单易用的客户 web 门户为 Windows 和 Mac 客户提供了熟悉的界面和体验。此外，技术人员和单独的客户端可改善支持队列的管理和时间安排。Dell SonicWALL 安全虚拟援助通过现有网络和认证基础机构实现了更紧密的集成。

## 网络安全设备的软件

### Dell SonicWALL VPN 客户端

针对客户端对主机的远程安全访问，Dell SonicWALL 提供了 SSL VPN 和 IPSec VPN 两种连接选择。采用 SSL VPN，Dell SonicWALL NetExtender 可通过 web 门户支持用户对 Windows、Mac 和基于 Linux 的系统进行无客户端远程访问，提供了连接和访问能力。采用 IPSec VPN，Dell SonicWALL 全球 VPN 客户端允许客户端系统下载 VPN 客户端，基于客户端提供更经典的 VPN 体验。

### SonicWALL Mobile Connect™

Mobile Connect 是针对 Apple® iOS 和 Google® Android™ 的单个统一的客户端应用，让智能手机和平板电脑用户可经由加密的 SSL VPN 连接以优异的网络级性能访问企业和学术资源。部署于 Dell SonicWALL 下一代防火墙时，它可创建一条干净的 VPN，将恶意软件从经由移动设备转发的通信中删除。

### Dell SonicWALL Analyzer 报告软件

Analyzer 是一种简单易用的 web 化应用流量分析和报告工具，可对网络的健康状况、性能和安全提供实时和历史性分析。Analyzer（分析程序）可支持 Dell SonicWALL 防火墙、备份/恢复设备，可保障远程访问设备的安全，同时利用应用流量分析来提供安全事件报告。

## 网络安全解决方案的固件

### SonicOS 增强版固件

SonicOS 增强版是功能强大的下一代操作系统，集成了大量先进功能，以满足当今和未来越发先进的网络在业务连续性、配置灵活性和管理方面的需求。

## Dell SonicWALL 广域网加速解决方案：WXA 系列简介

Dell SonicWALL 广域网加速设备（WXA）系列降低了应用延迟，节省了带宽，帮助设有远程和分支机构的中小企业大大改善了广域网应用性能和用户体验。初始数据传输完成后，WXA 系列随后只会经网络传输新的数据或更改数据，由此大大降低随后的数据量。WXA 可删除经广域网传输的重复数据，记住之前传输过的数据，利用识别符代替重复的字节序列，从而降低应用延迟，保存带宽。其它加速功能包括数据缓存、文件重复删除、元数据缓存和动态数据压缩。

WXA 系列包括 WXA 500 Live CD、WXA 2000 和 WXA 4000 硬件设备及 WXA 5000 虚拟设备。与单独的广域网加速产品不同，WXA 解决方案是 Dell SonicWALL E-Class NSA、NSA 和 TZ 系列设备的集成式附加组件，这些设备可作为下一代防火墙部署。这一集成式解决方案简化了集成其它组件（如 VPN）的 WXA 设备的安装、部署、配置、发送、管理和集成。与 Dell SonicWALL 应用智能和控制服务同时部署时，WXA 提供了独特的双重效益：优先处理应用流量和最大程度地降低网站之间的流量，从而实现最佳的网络性能。

**Dell SonicWALL WXA 500 Live CD**

WXA 500 Live CD 可经由可启动 Live CD 支持灵活的部署。

**Dell SonicWALL WXA 2000**

WXA 2000 可加速多达 120 名用户和 600 条广域网优化信息流的网络性能。

**Dell SonicWALL WXA 4000**

WXA 4000 可加速多达 240 名用户和 1200 条广域网优化信息流的网络性能。

**Dell SonicWALL WXA 5000 虚拟设备**

WXA 2000 支持在 VMWare®环境下进行灵活的虚拟机部署。

| 特性 | WXA 500 Live CD | WXA 2000 | WXA 4000 | WXA 5000 虚拟设备 |
|---|---|---|---|---|
| 平台 | 软件/CD | 硬件设备 | 硬件设备 | 虚拟设备（VMWare） |
| 最大用户数[1] | 20 | 120 | 240 | 360 |
| 最大连接数 | 100 | 600 | 1,200 | 1,800[3] |
| 字节缓存 | 支持 | | | |
| 压缩 | 支持 | | | |
| 管理 | 要求 SonicOS 5.8.1 或更高版 | | | |
| WFS 加速 | 支持[2] | 支持 | | |
| TCP/WFS 可视化 | 支持 | | | |
| SNMP | 支持 | | | |
| 系统记录 | 支持 | | | |
| 操作系统 | 增强型 Dell SonicWALL Linux OS | | | |
| 机架式机箱 | – | 1 RU | | – |
| CPU | – | Intel 2.0GHz 处理器 | Intel 2.0GHz 双核处理器 | – |
| RAM | – | 2 GB | 4 GB | – |
| 硬盘 | – | 250 GB | 2×250 GB | – |
| 冗余磁盘阵列（RAID） | – | – | RAID 1 | – |
| 尺寸 | 17.0×16.4×1.7 英寸/43.18×41.59×4.44 厘米 | | | |
| 重量 | – | 16 磅/7.26 千克 | | – |
| WEEE 重量 | – | 16 磅/7.37 千克 | | – |
| 功耗（W） | – | 86 | 101 | – |
| BTU | – | 293 | 344 | – |
| MTBF | 14.27 年 | | | |

| | 仅指 WXA 500 Live CD |
|---|---|
| 最小 CPU | 奔腾 4 或更高版 |
| 外部存储 | CD/DVD ROM Bay |
| 内存配置 | 最低 2GB RAM |
| 存储器配置 | 硬盘最少 80GB |
| 存储控制器 | SATA 控制器，支持 IDE 仿真 |
| 其它要求 | 浏览器/键盘 |

| | 仅指 WXA 5000 虚拟设备 |
|---|---|
| **Hypervisor** | ESX 和 ESXi（4.0 或更新版本） |
| 安装的操作系统 | 增强型 SonicLinux |
| 最小 CPU | 2×1.6GHz |
| 内存配置 | 4 GB |
| 可用磁盘容量 | 250 GB |
| VMware 硬件兼容性指南 | http://vmware.com/resources/compatibility/search.php |

[1] 根据每用户产生的流量大小不同，所支持的最大用户数也不同。
[2] WFS 加速功能仅在所提供硬件安装了 Live CD 镜像时可用。
[3] 最大流量取决于硬件规格，根据硬件配置可能会有所不同。所列规格指的是运行 WXA 虚拟设备的最低要求。

**Dell SonicWALL 安全远程访问解决方案为企业提供了细粒度访问控制能力以及易用性和易管理性。**

## Dell SonicWALL 安全远程访问解决方案

传统的企业局域网（LAN）边界正逐渐发展成为分布式的全球网络，可通过互联网、内联网和外联网连接员工、合作伙伴和客户。如今，移动员工迫切希望能通过比以往更多的设备（包括智能手机和平板电脑）随时随地访问更多资源。Dell SonicWALL 为各种规模的企业包括中小企业和大型的全球企业提供了可扩展的安全远程访问（SRA）解决方案。Dell SonicWALL Aventail E-Class SRA 系列以及面向中小企业的 Dell SonicWALL SRA 系列为实现安全远程访问、灾难恢复、安全无线网络和安全外联网提供了灵活的 SSL VPN 解决方案，可作为硬件或虚拟设备部署。

### Dell SonicWALL Aventail E-Class SRA 系列简介

Dell SonicWALL Aventail E-Class 安全远程访问（SRA）系列通过简化访问提高了生产力，并通过强制实施细粒度控制以及保持管理的简易性，降低了 IT 管理费用。领先分析机构评价 Dell SonicWALL Aventail 时，称其为行业领先产品，其获奖的 SSL VPN 充分满足了如今移动性不断增强的员工对安全远程访问的需求。Dell SonicWALL Aventail SRA 设备在 VMWare® 环境中提供了单一的、集中管理的网关或虚拟设备，用于控制网络资源访问，可通过以下方式提供强健的解决方案：

- 允许用户经由一系列端点设备平台，包括 Windows、Windows Mobile、Apple Mac OS、iOS、Linux®和 Google Android®安全远程访问关键业务应用和资源
- 提供无客户端浏览器访问或 web 交付瘦客户端访问，实现了“办公室化”体验
- 发生意外业务中断时，提供业务连续性和灾难恢复能力
- 针对支持多种设备平台的无线网提供集中化安全访问控制
- 确保业务合作伙伴外联网访问的安全，以增强协作效率
- 在不同的入口点强制实施访问策略，实现细粒度访问控制
- 增强对最新 Dell SonicWALL Workplace Portal 的门户访问、内容和设计的控制
- 提升安全性，在验证前检测出端点设备的固有风险；利用基于用户和端点设备的细粒度策略保护资源安全；然后为用户提供授权访问资源连接
- 在用户登录时或根据管理员定义的间隔时间反复进行端点控制（EPC）扫描，确保端点设备的安全性
- 无与伦比的细粒度控制能力，可根据对用户、访问设备和访问应用的信任程度为用户提供访问能力
- 面向当今和未来的坚实的网络访问控制（NAC）基础

**安全远程访问解决方案 — Dell SonicWALL Aventail E-Class SRA 系列**

**Dell SonicWALL Aventail E-Class SRA EX9000**

Dell SonicWALL Aventail E-Class 安全远程访问（SRA）系列经单一设备为企业多达 2 万名并发移动用户提供了功能全面的、简单易用的、无客户端或瘦客户端连接，媲美“办公室化”体验。E-Class SRA 可根据策略，允许用户经由 Windows、Windows Mobile、Apple Mac OS、iOS、Linux 和 Google Android 设备远程访问网络资源，提高了生产力，增强了业务连续性。

**安全远程访问解决方案 — Dell SonicWALL Aventail E-Class SRA 系列**

**Dell SonicWALL Aventail E-Class SRA EX7000**

Dell SonicWALL Aventail E-Class SRA EX7000 经单一设备为企业多达 5000 名并发移动用户提供了功能全面的、简单易用的、无客户端或瘦客户端连接，媲美“办公室化”体验。E-Class SRA 可根据策略，允许用户经由 Windows、Windows Mobile、Apple Mac OS、iOS、Linux 和 Google Android 设备远程访问网络资源，提高了生产力，增强了业务连续性。

**Dell SonicWALL Aventail E-Class SRA EX6000**

Dell SonicWALL Aventail E-Class SRA EX6000 经单一设备为企业多达 250 名并发移动用户提供了功能全面的、简单易用的、无客户端或瘦客户端连接，媲美“办公室化”体验。E-Class SRA 可根据策略，允许用户经由 Windows、Windows Mobile、Apple Mac OS、iOS、Linux 和 Google Android 设备远程访问网络资源，提高了生产力，增强了业务连续性。

**Dell SonicWALL Aventail E-Class SRA 虚拟设备**

Dell SonicWALL Aventail E-Class SRA 虚拟设备是一款加固的、性能经过优化的虚拟服务器，为移动企业机构提供了功能齐全的、易于管理的无客户端安全远程访问，单台虚拟设备可支持多达 250 名并发用户。E-Class SRA 虚拟设备可根据策略，允许用户经由 Windows、Windows Mobile、Apple Mac OS、iOS、Linux 和 Google Android 设备远程访问网络资源，提高了生产力，增强了业务连续性。

## 可选的 Dell SonicWALL Aventail E-Class 附加功能

**Dell SonicWALL Aventail 高级端点控制（EPC）™**

高级 EPC 结合了最先进的端点检测功能和最先进的数据保护技术。

**Dell SonicWALL Aventail 高级报告™**

高级报告功能提供了强大的远程资源访问分析能力。

**SonicWALL Mobile Connect**

Mobile Connect 是针对 Apple iOS 和 Google Android 的单个统一的客户端应用，让智能手机和平板电脑用户可经由加密的 SSL VPN 连接以优异的网络级性能访问企业和学术资源。

**Dell SonicWALL Aventail Connect Mobile™**

Connect Mobile 为智能手机设备提供了真实的“办公室化”体验。

**Dell SonicWALL Aventail 本地访问模块™**

本地访问模块支持针对基于服务器的应用的本地协议访问。

**Dell SonicWALL Aventail 临时增加用户授权™**

临时增加用户授权是一种灾难恢复“保险策略”，可为未来增加的远程用户提供支持。

**Dell SonicWALL 安全虚拟援助**

支持远程技术援助的远程支持工具。

**Dell SonicWALL Analyzer**

一种简单易用的应用流量分析和报告工具，可对网络的性能和安全提供实时和历史性分析。针对 Dell SonicWALL Aventail E-Class SRA 设备，Analyzer 提供了远程用户连接报告功能 ,还可为 Dell SonicWALL 防火墙和 CDP 设备提供报告功能。

| 特性 | 虚拟设备 | EX6000 | EX7000 | EX9000 |
|---|---|---|---|---|
| 并发用户许可证 | 5-250 | 25-250 | 50-5,000 | 100-20,000 |
| 基础端点控制（EPC）质询 | 包括 | 包括 | 包括 | 包括 |
| 高级 EPC （防病毒软件、个人防火墙、反间谍软件） | 附加 | 附加 | 包括 | 包括 |
| Aventail 安全桌面/缓存清理器 | 附加 | 附加 | 包括 | 包括 |
| 根据 EPC 质询结果允许、拒绝和隔离区域 | 包括 | 包括 | 包括 | 包括 |
| 细粒度访问控制 （用户和用户组、源 IP、服务/端口、目标 URL、主机名/IP 地址、IP 地址范围、子网、域） | 包括 | 包括 | 包括 | 包括 |
| 高级报告 | 附加 | 附加 | 附加 | 附加 |
| Analyzer | 附加 | 附加 | 附加 | 附加 |
| WorkPlace Portal | 包括 | 包括 | 包括 | 包括 |
| WorkPlace Mobile （针对手机浏览器优化的门户） | 包括 | 包括 | 包括 | 包括 |
| 本地访问模块 （Citrix、Windows Terminal Services 和 VMWare View） | 附加 | 附加 | 包括 | 包括 |
| 连接隧道（对基于 TCP 或 UDP 的应用的 Windows、Mac 和 Linux 访问） | 包括 | 包括 | 包括 | 包括 |
| Connect Mobile（Windows Mobile、Google Android） | 包括 | 包括 | 包括 | 包括 |
| Mobile Connect（iOS） | 附加 | 包括 | 包括 | 包括 |

**Dell SonicWALL SSL VPN 解决方案提供了经济实惠的、简单易用的且易于管理的安全远程访问。**

(SRA 1200, SRA 4200)

## 面向中小企业的 Dell SonicWALL 安全远程访问系列简介

Dell SonicWALL SRA 系列为各种规模的企业提供了经济实惠的、简单易用的且易于管理的、安全的无客户端远程网络和应用访问解决方案，而且无需预装任何客户端软件。只需一个标准 web 浏览器，用户即可在任何地方轻松、安全地访问企业局域网中的电子邮件、文件、内联网、应用、远程桌面、服务器和其它资源。Dell SonicWALL SSL VPN 解决方案无缝融入了几乎所有有线或无线网络拓扑，为用户提供强大的、可扩展的和低成本的远程企业资源访问。Dell SonicWALL SRA 系列可作为 VMWare 环境的设备或虚拟设备部署。

- 几乎可与所有防火墙进行无缝集成，因此企业可充分利用现有的网络基础架构。
- 无令牌双因子验证利用独特的临时密码，该密码由 SSL VPN 设备生成，然后发往远程用户的移动设备或电子邮件地址，提供了用户的网络用户名和密码，增强了对键盘记录程序的抵御。
- 针对 iOS 和 Google Android 的移动设备支持让远程员工可访问整个内联网和 web 化应用，为远程员工提供高度的灵活性。
- 采用细粒度策略配置控制功能，网络管理员可创建一定的策略，将用户局限在特定的应用/资源中，阻止其访问未授权资源。
- 应用卸载功能让用户可安全访问 web 应用，同时可充分利用强大的验证能力和细粒度访问策略功能。
- Dell SonicWALL Web 应用防火墙服务可检测并保护 web 应用( 包括 SSL VPN 设备自身 ) 远离 web 化攻击，降低潜在的丢失，满足数据保护合规性法规如 PCI-DSS。
- SRA 系列的端点控制 ( EPC ) 功能可识别基于 Windows 的端点，将其与授权用户连接起来，并可通过查找安全组件如防病毒和反间谍软件，评估设备的安全性
- 利用 Dell SonicWALL 安全虚拟援助进行远程支持让技术人员可为客户提供安全的按需技术援助，同时可充分利用现有基础架构。
- 安全虚拟访问让分布式企业和服务提供商机构中的授权终端用户可随时随地实现对无人照管的 Windows 电脑的安全远程访问。
- Secure Virtual Meeting ( 安全虚拟会议 ) 为 SMB 系列具备 SRA 的所有安全特点，可保护敏感的专有信息安全，同时以符合成本效益的方式实现协作
- 临时增加用户授权让管理员可准备灾难恢复计划来支持授权用户数量的临时增加。
- 与 Dell SonicWALL 网络安全设备( NSA )同时部署即可启动干净的 VPN，Dell SonicWALL NSA 可利用强大的深度包检测技术来扫描流量，以查找恶意威胁，如病毒、蠕虫、木马和间谍软件。

### Dell SonicWALL SRA 4200

Dell SonicWALL SRA 4200 为中型企业提供了强大的、简单易用的、经济实惠的安全远程访问解决方案，无需为 Windows、Windows Mobile、Apple Mac OS、iOS、Linux 和 Google Android 提供预装客户端软件，同时提供了可选的 Web 应用防火墙和多平台远程支持。只需一个标准 web 浏览器，用户即可在任何地方轻松、安全地访问企业局域网中的电子邮件、文件、内联网、应用、远程桌面、服务器和其它资源。SRA 4200 以及硬件辅助 SSL 卸载功能可支持大量远程访问用户，以及支持增值服务，提供远程 PC 支持、远程 PC 访问和 Web 应用防火墙。SRA 4200 的高可用性功能支持主动/被动配置，让企业能实现可靠的、安全的远程访问，即使是两台设备中的一台出现故障。

### Dell SonicWALL SRA 1200

Dell SonicWALL SRA 1200 为中小企业提供了简单易用的安全远程访问功能，用于访问企业电子邮件、文件和 web 化应用，无需为 Windows、Windows Mobile、Apple Mac OS、iOS、Linux 和 Google Android 提供预装客户端软件，同时提供了可选的 Web 应用防火墙和多平台远程支持。通过无缝融入几乎任何网络拓扑，SRA 1200 设备提供了经济实惠的且功能强大的远程访问、远程支持、远程 PC 控制和 Web 应用防火墙。

### 安全远程访问虚拟设备

Dell SonicWALL SRA 虚拟设备为中小型企业提供了加固的、性能经过优化的虚拟服务器，可采用无客户端方式经由更多操作系统平台包括 Windows、Windows Mobile、Apple Mac OS、iOS、Linux 和 Google Android 远程访问企业应用和资源，包括电子邮件、文件、内联网、web 化和传统应用、桌面和服务器。SRA 虚拟设备可快速部署于虚拟化环境，是一款经济实惠的解决方案，有助于中小企业降低总拥有成本。

## 可选的 Dell SonicWALL SSL VPN 附加功能

### Dell SonicWALL Web 应用防火墙服务

Dell SonicWALL 屡获殊荣的 Web 应用防火墙服务（WAF）是一种综合性的、经济实惠的、即插即用的合规性解决方案，充分利用现有的基础架构，作为可获许可的附加模块部署于 Dell SonicWALL 安全远程访问平台。Dell SonicWALL WAF 服务可利用动态更新的签名库来检测先进的 web 化攻击，保护 web 化应用包括 SSL VPN 门户，可应用 7 层流量的反向代理分析来抵御已知签名，一旦检测出 web 应用恶意软件即可拒绝访问，并将用户重定向到解释性错误页面。Dell SonicWALL WAF 还支持插入自定义规则链，使用自定义 Application Profiling（应用性能分析）来实现“虚拟补丁”，以抵御零天 web 应用威胁。Dell SonicWALL WAF 是满足 PCI 合规性以及提供 web 化 DLP（数据泄露保护）功能的关键性组件，可阻止或保护敏感信息如信用卡和 SSN 免于落入坏人之手。

## Dell SonicWALL SRA for SMB 的可选附加功能

### SonicWALL Mobile Connect

Mobile Connect 是针对 Apple iOS 和 Google Android 的单个统一的客户端应用，让智能手机和平板电脑用户可经由加密的 SSL VPN 连接以优异的网络级性能访问企业和学术资源。部署于 Dell SonicWALL 下一代防火墙时，它可创建一条干净的 VPN，将恶意软件从经由移动设备转发的通信中删除。

### Dell SonicWALL 安全虚拟援助

Secure Virtual Assist（安全虚拟援助）是一项远程支持工具，让技术人员可实现对终端用户的基于 Windows、Mac 或 Linux 的 PC 或笔记本电脑的控制，以提供远程技术援助。得到客户的许可后，技术人员可使用 web 浏览器及时访问电脑，远程快速诊断和修复问题，无需预安装的“肥”客户端。

### Dell SonicWALL 安全虚拟访问

Secure Virtual Access（安全虚拟访问）是一项远程 PC 控制工具，让授权终端用户可随时随地实现对无人照管的 Windows 电脑的安全远程访问。用户只需在具备互联网访问能力的 Windows PC 上安装虚拟访问代理，只要 PC 连接 Dell SonicWALL SSL VPN，用户即可在支持互联网连接的地方随时随地连接 PC。这对需要重新连接无法正常连接到 LAN 的家庭办公室电脑或小型办公室 PC 的远程员工来说尤为有用。

### Dell SonicWALL 安全虚拟会议

Secure Virtual Meeting（安全虚拟会议）可实现安全的、低成本的协作，减少了不必要的差旅开支。与其它虚拟会议解决方案不同，Dell SonicWALL 安全虚拟会议融合了 SRA for SMB 设备系列的所有安全特性，可全面保护敏感的专用通信安全。安全虚拟会议集成了现有的认证基础架构以及日程安排系统如 Microsoft Outlook™。

### SRA 系列的 Dell SonicWALL 端点控制功能

SRA 系列的端点控制（EPC）功能为中小型企业提供了企业级设备识别和询问功能。SRA 系列的端点控制功能可识别基于 Windows 的终端设备，并将其与授权用户联系起来。它也可通过检测关键组件如防病毒和反间谍软件，在经由 Dell SonicWALL NetExtender 客户端允许基于 Windows 设备的用户访问网络之前强制执行细粒度安全功能。设备询问名单包括领先厂商如 McAfee、Kaspersky Lab、Symantec®、Computer Associates®、Sophos®和许多其它公司所支持的防病毒、反间谍软件和个人防火墙解决方案，这大大降低了非 IT 管理设备的恶意软件进入网络的机会。

## Dell SonicWALL SRA for SMB 的可选附加功能

### Dell SonicWALL 临时增加用户授权

临时增加用户授权让客户可及时增加远程用户帐户，确保因暴动、地震和暴风雪等紧急情况导致的业务中断情况下的正常使用。

### Dell SonicWALL Analyzer

Analyzer（分析程序）是一项简单易用的应用流量分析和报告工具，可全面了解有关网络性能和安全性的实时和历时数据。针对 SRA 设备，分析程序提供了有关远程用户连接和 web 应用防火墙活动的报告。分析程序也可为 SonicWALL 防火墙和 CDP 设备提供报告。

| 部署 | SRA 1200 | SRA 4200 | SRA 虚拟设备 |
|---|---|---|---|
| 部署环境的类型和规模 | 员工不超过 50 名的小型企业 | 员工不超过 500 名的中型企业 | 各种规模的企业 |
| 包括/最大并发用户数量 | 5/50 | 25/500 | 5/50 |
| 虚拟访问/虚拟辅助最大并发用户数量 | 10 | 25 | 25 |

| 特性 | SRA 1200 | SRA 4200 | SRA 虚拟设备 |
|---|---|---|---|
| 安全虚拟访问 | 附加 | 附加 | 附加 |
| 安全虚拟援助 | 附加 | 附加 | 附加 |
| 安全虚拟会议 | 附加 | 附加 | 附加 |
| SRA 系列的端点控制 | 附加 | 附加 | 附加 |
| Analyzer | 附加 | 附加 | 附加 |
| Web 应用防火墙 | 附加 | 附加 | 附加 |
| 临时增加用户授权 | 附加 | 附加 | 附加 |
| 临时密码（OTP）验证 | 包括 | 包括 | 包括 |
| Vasco 支持 | 包括 | 包括 | 包括 |
| RSA 支持 | 包括 | 包括 | 包括 |
| Citrix（ICA）支持 | 包括 | 包括 | 包括 |
| NetExtender：支持多 IP 地址范围和路由 | 包括 | 包括 | 包括 |
| 可选的客户端认证支持 | 包括 | 包括 | 包括 |
| 图形使用监控 | 包括 | 包括 | 包括 |
| 创建系统备份选项 | 包括 | 包括 | 包括 |
| 反向代理：OWA 高级版和 Lotus Domino Access | 包括 | 包括 | 包括 |
| RADIUS 测试功能 | 包括 | 包括 | 包括 |
| 活动目录组支持 | 包括 | 包括 | 包括 |
| 虚拟主机/域名支持 | 包括 | 包括 | 包括 |
| 文件共享 Java 小程序 | 包括 | 包括 | 包括 |
| 诊断：DNS Lookup 和 Traceroute | 包括 | 包括 | 包括 |
| SNMPv2 | 包括 | 包括 | 包括 |
| 7 层负载均衡 | 包括 | 包括 | 包括 |
| 高可用性（HA） | – | 包括 | – |
| SSL 硬件辅助卸载 | – | 包括 | 根据底层硬件而定 |
| Mobile Connect（iOS） | 包括 | 包括 | 包括 |
| Mobile Connect （Android） | 包括 | 包括 | 包括 |

强大的、简单易用的电子邮件威胁防御

## Dell SonicWALL 电子邮件安全解决方案

利用 Dell SonicWALL 电子邮件安全解决方案保护企业远离入站和出站电子邮件威胁，避免违反相关法律法规。采用多种经实践检验的、荣获专利 [1] 的 Dell SonicWALL 威胁检测技术和独特的全球攻击识别和监测网络，实时有效地抵御垃圾邮件、钓鱼软件、病毒、僵尸、目录收集（DHA）、拒绝服务（Dos）和其它攻击。此外，电子邮件安全解决方案可利用先进的合规性扫描和管理功能，避免机密数据泄露和违规行为。

企业可以极低的成本轻松将电子邮件部署环境从 10 个邮箱扩展至 1 万个邮箱。Dell SonicWALL 电子邮件安全解决方案可作为可扩展的硬件设备、虚拟设备或软件灵活部署，包括针对 Microsoft Windows® Server 或 Small Business Server 优化的软件，以满足企业的预算和基础架构需求，从长期投资中获得最大回报。支持高可用性和可扩展分割模式配置，集中、可靠地管理企业级部署环境。管理直观、快速、简单。可将垃圾邮件管理安全委派给终端用户，同时保持对安全功能执行的最终控制。利用无缝的多 LDAP 同步化功能轻松管理用户和用户组账户。在大型分布式部署环境中，全新的多租户支持功能让企业可委派次级管理员来管理单个电子邮件安全部署环境中的多个组织单元的设置（如企业部门或 MSP 客户）。

## Dell SonicWALL E-Class 电子邮件安全系列

### Dell SonicWALL E-Class 电子邮件安全设备系列

Dell SonicWALL E-Class 电子邮件安全设备（ESA）ES6000 和 ES8300 为企业环境提供了全面的、有效的、可扩展的电子邮件安全。这一功能强大的、易于管理的解决方案集成了反垃圾邮件、防病毒和反钓鱼软件功能，以及内容过滤和出站电子邮件管理功能，避免泄露机密信息和违反法规遵从性。设备独特的优先扫描 MTA 提供了创新的信息分析能力和行业领先的信息投递率，为企业提供了优异的性能和扩展性。

### Dell SonicWALL E-Class 电子邮件安全软件

对于采用标准化专用硬件的企业，或者是拥有监控和备份系统或只是单纯希望获得终极部署灵活性的企业来说，Dell SonicWALL E-Class 电子邮件安全软件可通过单个软件平台提供 Dell SonicWALL E-Class 电子邮件安全设备的所有功能。这一电子邮件安全解决方案结合了最佳的防护能力和简单的控制以及高性能。

### Dell SonicWALL E-Class 电子邮件安全虚拟设备

Dell SonicWALL 电子邮件安全虚拟设备为 Dell SonicWALL 电子邮件安全提供了加固的、性能经过优化的虚拟服务器。采用过去那种“一台服务器、一种应用”模式，管理员通常并未充分利用硬件资源，并需要在服务器管理上花费大量时间。Dell SonicWALL 虚拟设备大大提高了资源和应用的效率和可用性。如需支持范围更广的部署环境和更高的扩展性，管理员可使用 Split-Config 模式在单台物理服务器或多台物理服务器上部署多台虚拟设备。

[1] 美国专利 7,814,545; 7,343,624; 7,665,140; 7,653,698; 7,546,348

# 面向中小企业的 Dell SonicWALL 电子邮件安全系列

## Dell SonicWALL 电子邮件安全设备系列

Dell SonicWALL 电子邮件安全设备专为中小企业设计，安装简单，并且可在 SMTP 网关有效阻止所有电子邮件威胁。这一功能强大的解决方案让企业可远离各种威胁，如垃圾邮件、钓鱼软件、病毒、拒绝服务（DOS）和目录收集攻击以及受僵尸攻击的设备。这些设备还提供了强健的出站电子邮件管理，满足了对策略和法规的遵从性。这些即插即用设备采用了增强型 SonicWALL OS，可在一小时内完成安装，确保电子邮件的安全。

## Dell SonicWALL 电子邮件安全软件

Dell SonicWALL 电子邮件安全软件非常适合希望能利用现有硬件部署电子邮件安全软件的中小企业。Dell SonicWALL 电子邮件安全软件具有 SMB 设备的所有功能，可通过简单易用的、基于 web 的管理界面帮助企业抵御所有入站和出站电子邮件威胁。

针对 Windows® Small Business Server（SBS）的 Dell SonicWALL 电子邮件安全软件可直接安装在 SBS 服务器硬件上，简化了安装，降低了总拥有成本。该软件还集成了 SBS 功能，可在邮件流量进入 SBS 之前使用高级连接管理，提供更出色的反垃圾邮件、反钓鱼软件和防病毒防护能力，避免 DHA 和 DOS 攻击。

## Dell SonicWALL 电子邮件安全虚拟设备

Dell SonicWALL 电子邮件安全虚拟设备为 Dell SonicWALL 电子邮件安全提供了加固的、性能经过优化的虚拟服务器。采用过去那种“一台服务器、一种应用”模式，管理员通常并未充分利用硬件资源，并需要在服务器管理上花费大量时间。Dell SonicWALL 虚拟设备大大提高了资源和应用的效率和可用性。如需支持范围更广的部署环境和更高的扩展性，管理员可使用 Split-Config 模式在单台物理服务器或多台物理服务器上部署多台虚拟设备。

## Dell SonicWALL 托管邮件安全

Dell SonicWALL 托管邮件安全为中小型企业提供了基于云的防护能力，能够以实惠的、可预测的、灵活的月费或年费制度来抵御垃圾邮件、钓鱼攻击和恶意软件。同时，它最大程度地简化了前期部署时间和成本，以及后续管理开支。Dell SonicWALL 托管邮件安全是唯一一款集成了多种防病毒技术的托管解决方案，包括 Dell SonicWALL GRID 防病毒、零时防病毒和 Kaspersky 实验室技术，实现了最佳的电子邮件安全。Dell SonicWALL GRID 网络技术和威胁研发小组每天会对数百万电子邮件进行严格的测试和评估，并不断进行更新分析，提供垃圾邮件阻止结果和防病毒和反间谍软件防护。Dell SonicWALL 零时病毒防护功能使用了可预测的、响应式技术，可在防病毒签名更新之前保护企业远离病毒感染。它可识别并立即隔离可疑的电子邮件，在病毒爆发时保护网络安全，直至防病毒签名更新完成。此外，Kaspersky 实验室技术增加了新的防病毒保护层，提供的防御能力比依靠单一防病毒技术的解决方案要强得多。

## Dell SonicWALL 电子邮件安全服务

### Dell SonicWALL 电子邮件安全防护升级和动态支持服务（5×8 或 7×24 小时）

电子邮件安全防护升级和动态支持服务是针对电子邮件安全设备和软件的一项必需的专享升级服务，因为该服务提供了实时反垃圾邮件、反钓鱼软件和防病毒软件升级以及软件/固件更新，对综合电子邮件威胁防护产品进行了补充。升级服务包括 5×8 小时或 7×24 小时技术支持、为设备提供 RMA 服务以及对因制造商疏忽造成产品瑕疵进行修复或更换。

### Dell SonicWALL 电子邮件防病毒升级服务

电子邮件防病毒升级服务会从病毒爆发的那一刻开始进行安全保护，直到采用 Dell SonicWALL 零时技术进行签名更新后为止。Dell SonicWALL 联手 McAfee 公司进行了签名升级，新增了一层保护层。

### Dell SonicWALL 电子邮件合规性升级服务

电子邮件合规性升级服务有助于企业满足相关法律法规的要求，并部署最佳的电子邮件使用方案。其功能包括详细附件扫描、合规性词典、许可框、记录 ID 匹配、加密路由、电子邮件归档、预定义策略和合规性报告。通过智能识别可能会违反合规性策略的电子邮件，监控并报告相应问题，同时强制实施多种策略，SonicWALL 可帮助企业轻松满足电子邮件合规性。

| 电子邮件安全设备 | SMB | | E-Class | |
|---|---|---|---|---|
| **型号** | **3300** | **4300** | **ES6000** | **ES8300** |
| 机架式机箱 | 1RU | 1RU | 1U 迷你型 | 2RU |
| CPU | Intel 2.0GHz | Intel 2.0GHz 双核处理器 | 3.2 GHz | Xeon 双核处理器 |
| 内存（RAM） | 2 GB | 4 GB | 2 GB | 4 GB |
| 硬盘驱动器 | 250 GB | 2×250 GB | 2×160 GB | 4×750 GB |
| 冗余磁盘阵列（RAID） | 不支持 | 支持 | 支持 | RAID 5 |
| 热插拔驱动 | 不支持 | 支持 | 不支持 | 支持 |
| 冗余电源 | 不支持 | 不支持 | 不支持 | 支持 |

| 电子邮件安全软件 | |
|---|---|
| 软件平台 | Microsoft Windows 2003 Server 或 Windows 2008 Server |

| 电子邮件安全虚拟设备 | |
|---|---|
| Hypervisor | ESXi™ 和 ESX™（4.0 版和更高版） |

## Dell SonicWALL 备份和恢复解决方案

Dell SonicWALL 持续数据保护（CDP）v.6 采用了全新的架构，提供了创新的备份和灾难恢复过程。直观的图形用户界面简化了 CDP 的部署、配置、管理和使用，可透明、自动保存和保护与业务有关的数据资产，避免数据从文件、设备和在基于位置的灾难中丢失。一键式用户主导恢复功能可削减 IT 费用，同时提高用户满意度和工作效率。

CDP 实现了无与伦比的灵活性，提供了多种灾难恢复选项，如站对站备份、异地备份、本地归档和通用系统恢复。CDP 可在本地或远程笔记本电脑、桌面和服务器上备份和恢复 Mac OS、Linux 或 Windows 平台。此外，CDP 支持 Microsoft SQL®、Exchange®、SharePoint®、Active Directory®和 Small Business Server®。

采用 CDP 的细粒度保护，管理员只需备份业务相关数据。CDP 让管理员可执行全球策略和日程表，或让用户设置自己的策略和日程表。重复数据删除技术可利用更少的磁盘空间来处理更多数据，优化了存储效率。此外，它在备份过程中只需经网络发送更少的流量，从而提高带宽效率。

## Dell SonicWALL 持续数据保护（CDP）系列

### Dell SonicWALL CDP 6080B

Dell SonicWALL CDP 6080B 为拥有多个工作站和多种服务器应用的大型企业提供了灵活的、大容量的数据备份和灾难恢复解决方案，该解决方案可自动保护业务资产，避免丢失。它可通过单个 web 化 GUI 支持 Windows、Linux 和 Mac OS 平台，在整个备份过程中提供了细粒度的、可全球执行的策略控制。先进的文件集备份和基于代理的重复删除加快了备份过程，优化了带宽，同时确保了数据连续性和保存了数据的多个版本。CDP 6080B 提供了强大的、全面的保护，实现了灵活的数据备份和灾难恢复，支持 RAID 5，容量高达 20TB（采用标准压缩比 2:1）。

### Dell SonicWALL CDP 5040B

Dell SonicWALL CDP 5040B 为拥有多个工作站和多种服务器应用的中小企业提供了灵活的、大容量的数据备份和灾难恢复解决方案，该解决方案可自动保护业务资产，避免丢失。它可通过单个 web 化 GUI 支持 Windows、Linux 和 Mac OS 平台，在整个备份过程中提供了细粒度的、可全球执行的策略控制。先进的文件集备份和基于代理的重复删除加快了备份过程，优化了带宽，同时确保了数据连续性和保存了数据的多个版本。CDP 5040B 提供了强大的、全面的保护，实现了灵活的数据备份和灾难恢复，支持 RAID 5，容量高达 10TB（采用标准压缩比 2:1）。

### Dell SonicWALL CDP 220

Dell SonicWALL CDP 220 为拥有多个工作站和服务器的小型企业、远程办公室或分支机构以及分布式环境提供了灵活的数据备份和灾难恢复解决方案，该解决方案可自动保护业务资产，避免丢失。它可通过单个 web 化 GUI 支持 Windows、Linux 和 Mac OS 平台，在整个备份过程中提供了细粒度的、可全球执行的策略控制。先进的文件集备份和基于代理的重复删除加快了备份过程，优化了带宽，同时确保了数据连续性和保存了数据的多个版本。CDP 220 提供了强大的、全面的保护，实现了灵活的数据备份和灾难恢复，容量高达 3.4TB（采用标准压缩比 2:1）。

### Dell SonicWALL CDP 210

Dell SonicWALL CDP 210 为拥有工作站的小型企业、远程办公室或分支机构提供了灵活的数据备份和灾难恢复解决方案，该解决方案可自动保护业务资产，避免丢失。它可通过单个 web 化 GUI 支持 Windows、Linux 和 Mac OS 平台，在整个备份过程中提供了细粒度的、可全球执行的策略控制。先进的文件集备份和基于代理的重复删除加快了备份过程，优化了带宽，同时确保了数据连续性和保存了数据的多个版本。CDP 210 提供了强大的、全面的保护，实现了灵活的数据备份和灾难恢复，容量高达 1.7TB（采用标准压缩比 2:1）。

## Dell SonicWALL 备份和灾难恢复许可证及服务

### Dell SonicWALL CDP 异地数据备份服务

CDP 异地数据备份服务提供了可全面管理的异地数据解决方案，实现了轻松的灾难恢复。如果本地 CDP 设备无法使用，IT 管理员可使用简单易用的用户界面经由 CDP 更换设备来轻松恢复任何已保存的数据修订版。数据中心的特点包括不间断电源系统（UPS）、紧急柴油发电机、地震保护、冗余火灾防御机制、洪水控制、HVAC 和 24 小时现场安全保障。

### Dell SonicWALL CDP 站点间备份

CDP 站点间备份服务面向的是需要对灾难保护解决方案进行管理的客户和零售商。站点间备份服务让企业可使用各种 CDP 设备进行异地备份。单台异地设备可为多台下游 CDP 设备提供灾难保护。灾难发生时，IT 管理员可经由简单易用的用户界面轻松恢复已保存的数据修订版。

### Dell SonicWALL CDP 通用系统恢复

通用系统恢复为整个服务器或工作站包括操作系统文件、程序、数据库和设置创建了精确的镜像。通过简单易用的、以向导为驱动的图形用户界面，可在数分钟内恢复整个系统。此外，它提供了本地归档功能，让企业能保存很长一段时间内的数据快照，满足行业和政府的合规性法规。

### Dell SonicWALL CDP 本地归档

CDP 本地归档功能让 IT 人员可将最新业务关键数据存储到 USB 设备。本地归档功能旨在帮助企业满足合规性要求，让管理员可浏览档案，存储单个文件。本地归档功能支持上游和下游 CDP 设备。

### 针对 Microsoft Exchange 的 Dell SonicWALL CDP 恢复管理器

针对 Microsoft® Exchange 的 CDP 恢复管理器让管理员可通过未安装的.edb 文件搜索、比较和存储单个、标准专用条目，包括单条信息、多个邮箱和公共文件夹，无需安装专用的恢复服务器。恢复管理器可消除专用恢复服务器的需求，节省成本。它还可根据发件人、收件人、日期、主题、信息关键字或附件关键字执行快速搜索，从而节省时间，通过以细粒度方式搜索 Exchange 和 Lotus® Domino 中已备份的附件内容、公共文件夹和公共文件夹分类，保存关键数据。

### Dell SonicWALL Analyzer

Analyzer 是一种简单易用的应用流量分析和报告工具，可对网络的性能和安全提供实时和历史性分析。针对 CDP 设备，Analyzer 提供了有关代理备份行为和设备容量利用率以及健康状况的报告。Analyzer 也为 Dell SonicWALL 防火墙和安全远程访问设备提供了报告。

| 特性 | CDP 210 | CDP 220 | CDP 5040B | CDP 6080B |
|---|---|---|---|---|
| **设备特性** | | | | |
| 用户（建议最大值）[1] | 50 | 50 | 100 | 250 |
| 服务器（建议最大值）[1] | 5 | 5 | 10 | 15 |
| 包含 Microsoft 应用许可证（如需更多，请另行购买）[2] | 0 | 1 | 3 | 3 |
| 包含文件服务器代理许可证（Windows、Apple 和 Linux）[3] | 1 | 1 | 1 | 1 |
| 包含工作站代理许可证（Windows 和 Apple）[3] | 10 | 50 | 100 | 250 |
| 外形规格 | 台式机 | 台式机 | 1U | 2U |
| RAID 支持 | – | – | RAID 5 | RAID 5 |
| 包含 RAM | 512 MB | 512 MB | 2 GB | 4 GB |
| 包含内部驱动（驱动机架数量） | 1 | 1 | 4 | 4 （最多 8 个） |
| 磁盘驱动容量、类型 | 1 TB SATA | 2 TB SATA | 2 TB SATA | 2 TB SATA |
| 总容量（包括扩展磁盘组）[4] | 1 TB | 2 TB | 6 TB | 6 TB（最大 12 TB）[4] |
| 总的可用容量（包括扩展磁盘组）[4] | 860 GB | 1.7 TB | 5 TB | 5 TB（10 TB）[4] |
| 总的可用容量（按标准 2:1 压缩） | 1.7 TB | 3.4 TB | 10 TB | 10 TB（20 TB）[4] |
| 网络接口 | 100baseT | 100baseT | 1 GbE | 1 GbE |
| 热插拔和冗余电源保护 | – | – | – | 支持 |
| 现场可更换的硬盘驱动器 | – | – | 支持 | 支持 |
| **备份和恢复** | | | | |
| 持续数据保护（CDP） | 支持 | 支持 | 支持 | 支持 |
| 卷映射拷贝服务（快照） | 支持 | 支持 | 支持 | 支持 |
| 高效文件集备份方法 | 支持 | 支持 | 支持 | 支持 |
| 基于全球策略的备份 | 支持 | 支持 | 支持 | 支持 |
| 基于年代顺序的数据版本 | 支持 | 支持 | 支持 | 支持 |
| 版本整理 | 支持 | 支持 | 支持 | 支持 |
| 基于代理程序的重复数据删除 | 支持 | 支持 | 支持 | 支持 |
| 细粒度恢复和 Exchange 数据恢复 | 支持 | 支持 | 支持 | 支持 |
| 灵活的灾难恢复功能选项 | 支持 | 支持 | 支持 | 支持 |
| 为动态数据和静态数据提供 AES 256 位加密 | 支持 | 支持 | 支持 | 支持 |
| 用户自恢复 | 支持 | 支持 | 支持 | 支持 |
| **管理和数据管理（策略和控制）** | | | | |
| 基于 web 和代理程序的管理界面 | 支持 | 支持 | 支持 | 支持 |
| 基于 Dell SonicWALL 全球管理系统的全球管理 | 支持 | 支持 | 支持 | 支持 |
| 基于对象的备份策略和控制 | 支持 | 支持 | 支持 | 支持 |
| 备份数据规则 | 支持 | 支持 | 支持 | 支持 |
| 版本控制 | 支持 | 支持 | 支持 | 支持 |
| 版本整理规则 | 支持 | 支持 | 支持 | 支持 |
| 异地设置 | 支持 | 支持 | 支持 | 支持 |
| 配额置备 | 支持 | 支持 | 支持 | 支持 |
| 带宽管理 | 支持 | 支持 | 支持 | 支持 |
| 报告、日志和通知 | 支持 | 支持 | 支持 | 支持 |
| Dell SonicWALL Analyzer | 附加 | 附加 | 附加 | 附加 |
| **应用支持** | | | | |
| Microsoft Exchange 2003、2007 和 2010 | 支持 | 支持 | 支持 | 支持 |
| 支持个别邮箱备份 | 支持 | 支持 | 支持 | 支持 |
| Microsoft SQL Server 2005 和 2008 | 支持 | 支持 | 支持 | 支持 |
| Microsoft SharePoint 2010 | 支持 | 支持 | 支持 | 支持 |
| 活动目录 | 支持 | 支持 | 支持 | 支持 |
| 系统状态 | 支持 | 支持 | 支持 | 支持 |
| Microsoft Outlook 2003、2007 和 2010 | 支持 | 支持 | 支持 | 支持 |
| **多平台系统支持** | | | | |
| Windows Server 2003 和 2008 R2（标准版和企业版） | 支持 | 支持 | 支持 | 支持 |
| Small Business Server 2003 和 2008 R2（标准版和高级版） | 支持 | 支持 | 支持 | 支持 |
| Windows XP、Vista 和 Win 7（所有版本） | 支持 | 支持 | 支持 | 支持 |
| Apple Mac OS X - Leopard（豹子）、Snow Leopard（雪豹）和服务器 | 支持 | 支持 | 支持 | 支持 |
| Linux（Debian、SuSE、Fedora、Red Hat 和 Ubuntu） | 支持 | 支持 | 支持 | 支持 |

[1] 以上均为预估值，可随时变更，恕不另行通知。最大支持配置根据企业备份、网络负载以及异地上传而定。

[2] 许可证适用于以下 Microsoft 应用：Microsoft Exchange 2003、2007 和 2010（包括个别邮箱支持），Microsoft SQL Server 2005 和 2008，Microsoft SharePoint 2010，Micosoft Active Directory，Micosoft Small Business Server。

[3] 如要支持上述支持上限，需另外购买许可证。

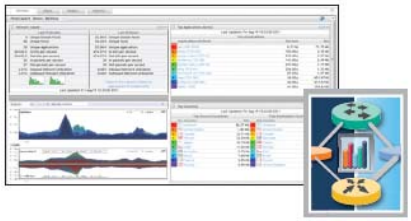
[4] 需购买 Dell SonicWALL 4 磁盘组升级工具包（01-SSC-9301）

# Dell SonicWALL 策略和管理解决方案

## Dell SonicWALL 全球管理系统

全球管理系统（GMS）为大型企业、分布式企业和服务提供商提供了强大的和直观的解决方案，以集中管理和快速部署 Dell SonicWALL 防火墙、反垃圾邮件、备份和恢复以及安全远程访问解决方案。可作为软件、硬件或虚拟设备灵活部署；Dell SonicWALL GMS 还提供了集中化实时监控功能、综合策略和合规性报告。针对企业客户，Dell SonicWALL GMS 简化了安全策略管理和设备部署，最大程度地降低了管理费用。对于服务提供商，Dell SonicWALL GMS 简化了多个客户端的安全管理，拓展了收入机会。如需更强的冗余能力和扩展性，可将 GMS 系统部署于集群配置。

- **GMS 软件** - SonicWALL GMS 可作为软件应用灵活部署在第三方 Windows 服务器上，充分利用现在基础架构。
- **通用管理设备 EM5000** - 屡获殊荣的 UMA 充分利用了增强型高性能设备，利用灵活的、强大的和直观的工具简化和自动化了多层策略管理、监控和合规性报告。多个 UMA 设备部署于同一群集时，经扩展可管理数千台 Dell SonicWALL 安全设备。
- **GMS 虚拟设备** - Dell SonicWALL GMS 虚拟设备为 Dell SonicWALL 全球管理系统提供了增强的、性能优化的虚拟设备代理。过去那种“一台服务器对应一种应用”的模式让管理员通常无法充分利用硬件资源，浪费了大量时间进行服务器管理。Dell SonicWALL 虚拟设备大大提高了资源和应用的效率和可用性。



## Dell SonicWALL Scrutinizer

Scruntizer（审查程序）是一项多厂商应用流量分析可视化和报告工具，用于衡量网络性能和利用率，排除故障，同时提高企业和服务提供商的生产效率。Scrutinizer 支持大量路由器、交换机、防火墙和数据流报告协议，可利用 Dell SonicWALL 防火墙导出的 IPFIX/NetFlow 数据深入、全面地了解应用流量分析。Scrutinizer 可轻松识别关键应用、对话、流量、协议、域、国家、子网以及有关可疑行为的警告。Scrutinizer 支持深度包检测应用流分析、主动的抖动/延迟监控、自动的报告和自定义面板。除为 MSP 和 ISP 提供多种专用功能外，Scrutinizer 还提供了历史和高级报告、基于角色的管理、高级分析和基于阀值的警告。Dell SonicWALL Scruntinizer 可作为 Windows 应用使用。

## Dell SonicWALL Analyzer

Analyzer 是一项简单易用的 web 化流量分析和报告工具，可实时了解网络的健康状况、性能和安全信息。Analyzer 支持 Dell SonicWALL 防火墙、备份/恢复设备和安全远程访问设备，同时利用应用流量分析提供安全事件报告，可帮助各种规模的企业提高员工生产效率，优化网络带宽利用率，增强安全意识。Dell SonicWALL 是唯一能够提供融合独立设备流量分析以及 Dell SonicWALL 防火墙生成的细粒度统计数据的完整的解决方案的防火墙提供商。Dell SonicWALL Analyzer 可作为 Windows 应用和虚拟设备使用。

## Dell SonicWALL 全球支持服务

Dell SonicWALL 提供了强健的全球支持服务组合，不仅可确保使用的是最新版的网络安全和数据备份恢复基础架构，还能很快解决可能发生的问题。然而，这并不足以确保网络的安全。因此，Dell SonicWALL 的支持服务还提供了关键的软件和固件更新和升级、最佳的技术支持、及时硬件更换和大量电子工具的使用。

### 针对 SuperMassive E10000 系列的 Dell SonicWALL 铂金技术支持

铂金技术支持和专业服务融合了技术支持和自定义服务，让 IT 部门能从 Dell SonicWALL 投资中获取最大的回报。Dell SonicWALL 铂金技术支持是一种自定义支持产品，包括一套全面的服务，用于保障操作的有效性和效率，所有服务由一组高级支持工程师管理和提供，他们非常了解企业的业务和技术要求。Dell SonicWALL 铂金技术支持以前瞻式服务和技术支持生命周期为基础，有着坚实的基础，可预见新兴安全需求，可动态适应和演变，以支持企业的业务目标。此外，铂金专业服务提供了现场安装和配置服务、培训和教育服务以及在现有 Dell SonicWALL 解决方案或其它厂商产品基础上的系统迁移。

- 高级技术支持工程师小组提供 7×24 小时技术支持
- 软件和固件更新和升级
- Advance Exchange 硬件更换（RMA）

### 7×24 小时 E-Class 技术支持

Dell SonicWALL E-Class 7×24 小时支持服务面向的是 Dell SonicWALL E-Class 解决方案客户，提供了企业级技术支持功能和高品质服务，确保企业网平滑、有效的运行。

- 7×24 小时通过电话、电子邮件和网络直接连线训练有素的高级技术支持工程师，寻求技术支持
- 订购固件更新和升级服务
- 一旦出现故障，可在下个工作日进行 Advance Exchange 硬件更换

### 5×8 小时和 7×24 小时动态技术支持

Dell SonicWALL 动态支持是专为需要通过不间断固件更新和高级技术支持实现连续保护的客户而设计的，根据需要可在正常办公时间或 7×24 小时提供。服务包括：

- 订购固件更新和升级服务
- 经由电话、电子邮件和网络寻求技术支持
- 一旦出现故障，可在下个工作日进行 Advance Exchange 硬件更换

### 综合全球管理系统支持（CGMS 支持）

对于需要 Dell SonicWALL 全球管理系统（GMS）来管理分布式网络的客户来说，Dell SonicWALL 提供了全面的 GMS 支持服务。这种保护伞式的支持服务为每台 Dell SonicWALL GMS 部署环境中的设备提供了 7×24 小时动态技术支持协议的所有效益。综合 GMS 技术支持服务包括：

- 7×24 小时动态技术支持合同的所有服务和优势
- GMS 应用的技术支持和软件更新
- 所有设备和服务享用一个到期日期，简化了管理

### 重点技术支持

业务关键客户需要业务关键技术支持。Dell SonicWALL 重点技术支持（FTS）旨在为大客户提供业界最高质量、最具响应度的技术支持服务。这一高级支持服务包括一套完整的主动服务，由指定的 Dell SonicWALL 安全工程师（SSE）进行管理，SSE 非常了解下辖客户的技术需求和业务。

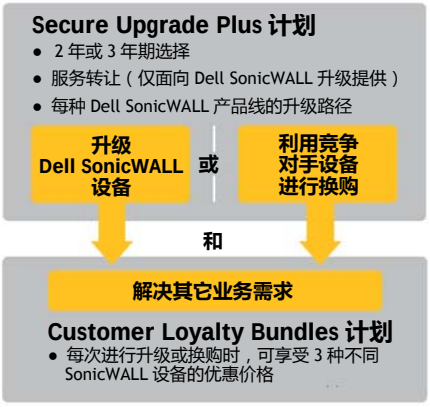
- 针对需要带指定资源的高端企业级技术支持的企业的自定义服务
- 提供 5×8 小时（FTS 标准和精简）或 7×24 小时（FTS 卓越）服务
- 及时联系主题专家（SME）和快速联系 Dell SonicWALL，加快事件报告，增强新功能处理

### Dell SonicWALL 远程启动和配置服务

远程启动和配置服务让各种规模的企业可在新网络或现有网络环境下快速、安全地配置和部署 Dell SonicWALL 设备。远程配置由获 CSSA 认证的技术人员使用 Dell SonicWALL 业经验证的方法进行，确保解决方案能够得到正确的配置和部署。该服务最大程度地降低了新设备的配置和部署成本，同时可释放宝贵的资源，以服务关键需求，从而增强了生产力。采用远程配置服务，企业的 Dell SonicWALL 设备可在几小时内安装完毕，且实现正常运行，从而能快速回收 Dell SonicWALL 投资。

## 客户优势计划

客户优势计划（Customer Advantage Program）为企业保持最新的基础架构提供了两种选择：Secure Upgrade Plus 计划和 Customer Loyalty Bundle 计划：




### Secure Upgrade Plus 计划

不管贵公司是升级旧的 Dell SonicWALL 设备，还是利用竞争对手产品进行换购，Secure Upgrade Plus 计划都会帮助您保护投资，让您能以更低的成本轻松升级。与单独购买硬件和一年的服务相比，大多数解决方案的年总成本可降低高达 50%。

Secure Upgrade Plus 计划包含多种 Dell SonicWALL 防火墙产品，包括最新的网络安全设备 NSA 220 和 NSA 250M 系列，以及其它指定的 Dell SonicWALL 产品线，包括安全远程访问（SSL VPN）和电子邮件安全（ES）。欲查看符合条件的 Dell SonicWALL 产品和竞争产品的完整列表，请参见“安全升级计划条款与条件”。参加 Secure Upgrade Plus 计划的客户购买其它产品时同样可享受 Customer Loyalty Bundle 优惠计划。

### Customer Loyalty Bundle 计划

Dell SonicWALL Customer Loyalty Bundle 计划是 Dell SonicWALL 对部署多种 Dell SonicWALL 产品线的客户而开展的答谢活动，感谢客户对 Dell SonicWALL 的长期信赖。符合条件的客户购买 Dell SonicWALL 其它产品线下的每种设备均可享受比 MSRP 低 30%的优惠。每次升级或换购时，客户均可以此优惠价选购其它产品线下的一种产品。Customer Loyalty Bundle 面向的是参加了 Secure Upgrade Plus 计划的客户，但只对升级或换购有效。

Dell SonicWALL 推出客户优势计划的目的是为了消除购买最新的、最高效的企业级网络安全系统和数据保护系统所产生的成本和复杂性，为客户提供更优质的服务。

## Dell SonicWALL 公司

Dell SonicWALL 主要提供智能网络安全和数据保护解决方案，帮助客户和合作伙伴动态保护、控制和扩展其全球网络。使用 Dell SonicWALL 全球响应智能防御（GRID）网络的数百万个共享接触点提供的信息，Dell SonicWALL 威胁中心可就威胁的本质和变化不断进行通信、反馈和分析。Dell SonicWALL 研究实验室会不断处理这些信息，提供能应对最新威胁的对策和动态更新。免重组深度包检测（RFDPI）*专利技术配合多核平行架构，能够以线速同时进行多威胁扫描和分析，提供技术架构，让整个解决方案能不断扩展，满足高带宽网络的部署需求。中小企业版和企业版均支持的 Dell SonicWALL 网络安全和数据保护解决方案可部署于大型校园环境、分布式企业环境、政府、零售环境和医院，以及服务提供商。

凭借简单易用的、高品质、高性能设备和服务，Dell SonicWALL 赢得了业界出版物如《网络世界》、《信息世界》、《PC magazine 个人计算机杂志》和《SC 杂志》的赞誉。Gartner 曾在 2011 年 SSL VPN 魔力象限报告中将 Dell SonicWALL 列入“远见者象限”，在最近的 2012 年统一威胁管理魔力象限报告中将 Dell SonicWALL 列入“领导者象限”。在 NSS 实验室的 2012 年下一代防火墙安全价值映射图™中，运行 SonicOS 的 Dell SonicWALL SuperMassive E10800 被评为是综合防御能力最强的下一代防火墙，获得了推荐评级。此 SonicOS 架构经过了实践检验，是每款 Dell SonicWALL 防火墙的核心组件。

Dell SonicWALL 提供了一系列业界领先的网络安全和数据保护解决方案，包括防火墙、安全远程访问/SSL VPN、反垃圾邮件/电子邮件安全和连续备份和恢复，以及集中化管理和报告功能，以及 7×24 小时技术支持服务。

SonicWALL 公司成立于 1991 年，于 2012 年被 Dell 公司收购。

*美国专利 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

©2012 Dell 公司版权所有。Dell SonicWALL 是 Dell 公司的商标，所有其它 Dell SonicWALL 产品和服务名称及标识是 Dell 公司的商标。本文提到的其它产品和公司名称可能是各自公司的商标和/或注册商标。
09/12 DSNWL 0293

SonicWALL