SonicWALL 网络安全设备系列

网络安全

新一代统一威胁管理保护

- SonicWALL 新一代安全产品
- 可扩展多核硬件及免重组深度包检测
- 全状态高可用性及负载均衡功能
- 高性能及更低的总拥有成本（TCO）
- 先进的路由服务及网络功能
- 标准 VoIP
- 安全的分布式无线 LAN 服务
- 联网服务质量（QoS）

各种规模的企业都通过企业网络来访问内部和外部关键业务应用。一方面，网络优势不断为企业带来巨大利益，另一方面，他们受到攻击的挑战也日益巨增，这些攻击纷繁复杂，以经济利益为目的，是专门为了扰乱通信、降低性能和盗取数据而设计的。

恶意攻击通过利用更高的网络层穿透过时的状态包检测防火墙。单一功能产品能够增加安全级别，但整体成本更大且难以管理，同时，不易控制网络误用，并在抵御多方位攻击时也差强人意。SonicWALL®网络安全设备（NSA）系列则引发了网络安全革命，采用了突破性多核设计以及具有专利的免重组深度包检测（RFDPI™）技术*，让您无需牺牲网络性能即可获得全方位的安全保护。SonicWALL E-Class NSA 系列首次采用了该平台，如今该平台也适用于中型企业。

NSA 系列克服了现有安全解决方案的各种局限性，它能实时地对每一个数据包执行整体扫描，以检测当前出现的内部及外部威胁。依靠高速多核处理平台，NSA 系列能执行深度包检测功能，同时不会影响关键网络及应用的性能。

NSA 系列采用了新一代统一威胁管理（UTM）技术来抵御各种攻击，同时具有入侵防御、防病毒及反间谍软件功能以及 SonicWALL 应用智能服务的应用层控制功能。NSA 系列利用先进的路由、全状态高可用性以及高速 IPSec 和 SSL VPN 技术让您的分支机构、中央区域及分布式中小型企业网络倍添安全性、可靠性、功能性及生产力，同时还将成本及复杂程度降到最低。

NSA 系列包括 **SonicWALL NSA 240、NSA 2400、NSA 3500 和 NSA 4500**，提供各种解决方案，专为满足各种企业的网络安全需求而设计。

特性及优点

SonicWALL 新一代安全产品结合了更高层次的 UTM 技术，集成了入侵防御、网关防病毒及反间谍软件以及应用智能服务（Application Intelligence Service）可配置工具套件，以防止数据泄漏以及提供细粒度应用控制。

可扩展多核硬件及免重组深度包检测扫描并清除任意大小文件中的威胁，对并发连接没有限制而且网速不减。网络管理员可使用主级或次级调制解调器或 3G 无线接口来配置 NSA 240，确保产品的高度扩展能力可以满足未来的需求。

SonicOS 增强版 5.0 具有的**全状态高可用性及负载均衡功能**可充分利用网络带宽，保证最大的网络正常运行时间，让您随时能访问关键业务资源，并且确保 VPN 隧道及其它网络流量在故障切换时不会中断。

高性能及更低的总拥有成本（TCO）通过同时使用多核处理能力而实现，极大地增加了吞吐量和并行检测能力，同时降低了功耗。

先进的路由服务及网络功能结合了先进的网络安全技术，包括 802.1q VLAN、WAN/WAN 容错功能、基于域和对象的管理、负载均衡、先进的 NAT 模式及更多技术，为您提供灵活的细粒度配置及全面的安全防护能力。

标准 VoIP 功能为 VoIP 基础架构的每一个单元，从通信设备到适用于 VoIP 的设备，如 SIP Proxies、H.323 Gatekeepers 以及 Call Server，提供最高级别的安全保护。

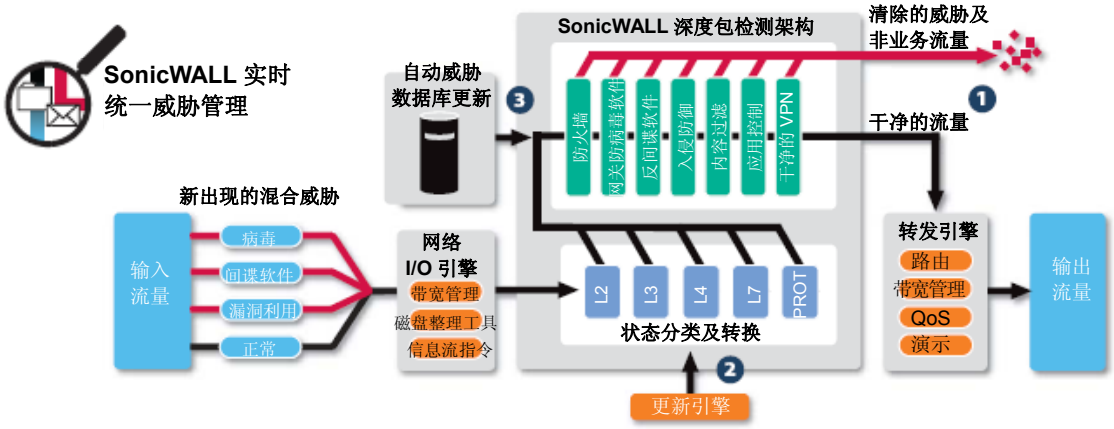
安全的分布式无线 LAN 服务让设备能够起到安全无线交换机及控制器的作用，它能够自动侦别并配置 SonicPoints™，SonicWALL 无线访问点保障了分布式网络环境中的远程访问安全。

联网服务质量（QoS）特性利用行业标准的 802.1p 及差异化服务编码点（DSCP）服务类别（CoS）指示符提供强大灵活的带宽管理，这对 VoIP、多媒体内容及关键业务应用起到至关重要的作用。

*美国专利号 7,310,815 — 一种分析和阻止数据流的方法和设备。

SONICWALL®

动态安全架构及管理

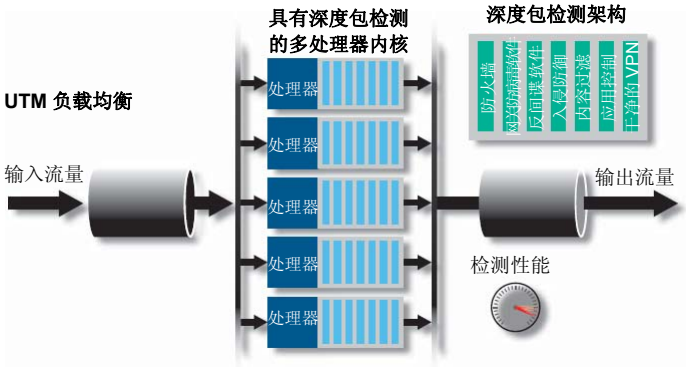


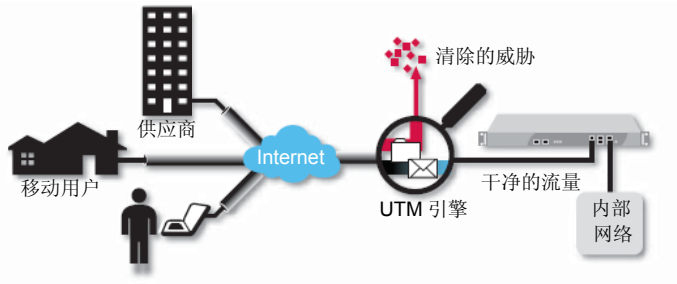
同级别最佳的保护

1. SonicWALL 深度包检测保护能抵御网络风险，如病毒、蠕虫、木马、间谍软件、钓鱼式攻击、新出现的威胁及 Internet 误用。应用智能服务能提供额外的高可配置性控制以防止应用层上的数据泄漏及带宽管理。
2. SonicWALL 免重组深度包检测（RFDPI）技术利用 SonicWALL 公司的多核架构对数据包进行实时检测，而无需将信息流量缓存在内存中。该功能可以扫描并清除任意大小文件中的威胁，对并发连接没有限制。
3. NSA 网络安全设备系列通过连续自动的安全更新提供动态的网络保护，对新出现的及不断演变的病毒进行清除而无需请求管理员干预。

统一威胁管理负载均衡

包含了多种保护技术的单处理器设计受到单个中央处理器的严格限制。SonicWALL UTM 负载均衡技术将高速深度包检测及流量分类引擎应用到多个安全内核上，并行扫描应用程序和文件，而不会对网络性能或可扩展性产生显著影响。这就使在承载带宽密集和延时敏感的应用和业务的网络上扫描和控制安全威胁成为可能。





SonicWALL Clean VPN™

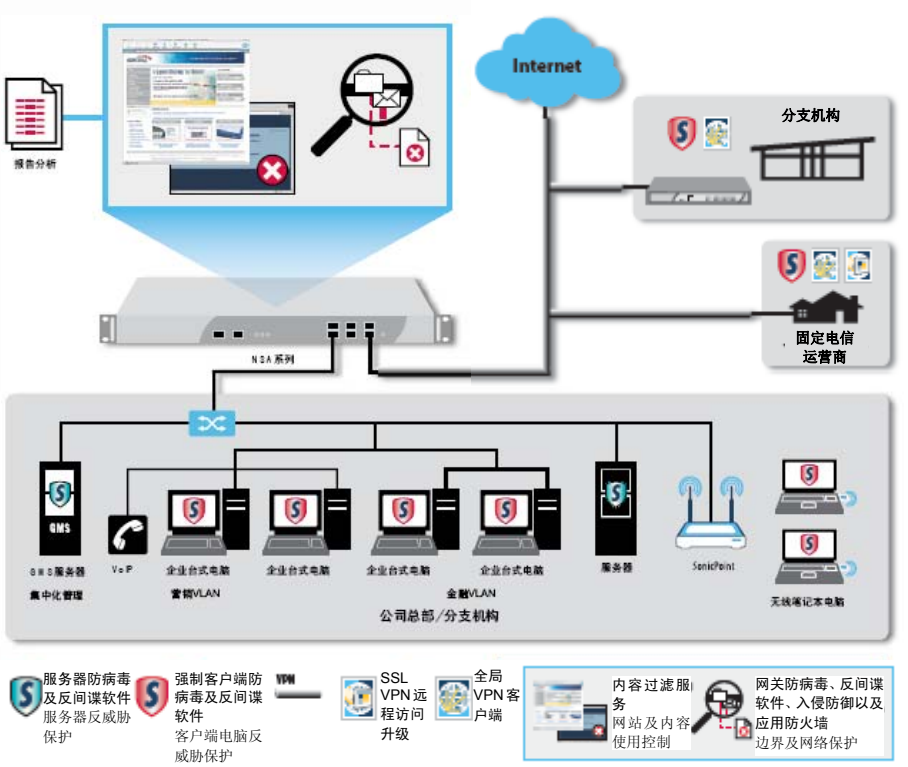
NSA 网络安全设备系列包括了极富创造性的 SonicWALL Clean VPN™ 技术，该技术让远程移动用户及分支机构的信息进入企业网络之前，就对其漏洞利用及恶意代码进行清除，而无需用户干预。

集中化策略管理

可利用 SonicWALL 全球管理系统（GMS）对 NSA 网络安全设备系列进行管理，该系统提供了强大、灵活、直观的管理工具，可对各种配置执行集中管理，实时查看监控数据并将策略与合规性报告结合在一起。

灵活和可自定义的部署选项——NSA 系列一览

每一种 SonicWALL NSA 网络安全设备解决方案都采用了突破性多核硬件设计以及具有专利的免重组深度包检测（RFDPI™）技术，针对各种内部和外部网络保护，提供新一代统一威胁管理保护，而无需牺牲网络性能。每一款 NSA 系列产品都融合了高速入侵防御、文档和内容检测、强大的应用智能服务控制以及众多先进的、具有高度灵活性的网络和配置功能。NSA 系列所采用的平台不仅易用性强，而且价格合理，便于在各种类型的企业、分支机构和分布式网络环境中部署和管理。



- SonicWALL **NSA 4500** 是那些需要高吞吐量和高性能的企业中心站点和大规模分布式环境的理想选择。
- SonicWALL **NSA 3500** 是那些对吞吐量和性能要求极高的企业、分支机构和分布式环境的理想选择。
- SonicWALL **NSA 2400** 是那些非常关注吞吐量和性能的中小型企业和分支机构环境的理想选择。
- SonicWALL **NSA 240** 是中小型企业和分支机构的理想选择。

安全服务和升级

网关防病毒、反间谍软件、入侵防御服务及应用智能服务提供智能实时的网络安全保护，以抵御复杂的应用层以及基于内容的攻击，包括病毒、蠕虫、木马、间谍软件及软件漏洞利用（如缓存溢出）。应用智能服务能提供一整套可配置的管理工具，这些工具是专为防止数据泄漏并且提供细粒度应用层控制而设计的。

强制客户端和服务器防病毒及反间谍软件利用一个单一的集成客户端为笔记本电脑、台式机及服务器提供全面的病毒及间谍软件防护，同时还能提供网络范围内的防病毒及反间谍软件策略、定义及软件更新的自动强制。

内容过滤服务通过采用创新性的评级架构，利用动态数据库阻止 56 类令人讨厌的 Web 内容，从而实现保护及生产力策略的强制。

ViewPoint 报告提供易用的、基于 Web 的各种功能，这些功能让系统管理员能立即获得网络性能及安全的综合性了解。ViewPoint 采用 Dashboard 和详细总结的方式为各种机构提供一系列历史报告，从而帮助他们进行 Internet 使用追踪，满足合规性要求并对其网络的安全状态进行监控。

SonicWALL 虚拟辅助服务（SonicWALL® Virtual Assist）是一项远程技术支持工具。采用此工具，技术人员可控制用户 PC 或笔记本电脑，从而进行远程技术援助。经用户许可后，技术人员可通过 Web 浏览器及时访问用户计算机，更轻松地进行远程诊断和问题修复，而无需预装“肥”客户端。

动态技术支持服务可根据用户的需要选择 5×8 或 7×24 小时技术支持服务。该服务包括世界级的技术支持、关键的固件升级、扩展性电子工具的使用以及即时的硬件更换，从而帮助企业获得最大的 SonicWALL 投资收益。

全球 VPN 客户端升级采用了可直接安装在基于 Windows 的计算机上的软件客户端，让远程用户可安全访问电子邮件、文件、内联网和应用，从而提高了员工的工作效率。升级许可证适用于各种规模的用户群，因此，企业可根据自身的发展进行扩展。

SSL VPN 远程访问升级为基于 PC、Mac 和 Linux 的系统提供了无客户端远程网络访问。由于采用了集成式 SSL VPN 技术，SonicWALL UTM 设备让用户可通过 NetExtender（一种可推送到用户设备的轻量级客户端软件）无缝、安全地访问来自各种客户端平台的电子邮件、文件、内联网和应用。NetExtender 的安装和配置都是自动的，用户无需介入。

SonicWALL 综合反垃圾邮件服务可在网关阻止垃圾邮件、钓鱼邮件以及带病毒的电子邮件。只要轻轻一点，就可马上激活此服务，及时阻止垃圾邮件，节省宝贵的网络带宽，无需重定向 MX 记录或向另一提供商发送电子邮件。

规格

NSA 4500
01-SSC-7012

NSA 4500 TotalSecure*（1 年）
01-SC-7032

NSA 3500
01-SSC-7016

NSA 3500 TotalSecure*（1 年）
01-SC-7033

NSA 2400
01-SSC-7020

NSA 2400 TotalSecure*（1 年）
01-SC-7035

NSA 240 TotalSecure*（1 年）
01-SSC-8760

PC 卡向 ExpressCard 转换的 SonicWALL 适配器（用于 NSA 240）
01-SSC-2887

欲了解有关 SonicWALL 网络安全解决方案的更多信息，请访问 **www.sonicwall.com/cn**。

*包括一年的网关防病毒、反间谍软件、入侵防御、应用智能服务、内容过滤服务、7x24 小时全天候动态技术支持服务以及 ViewPoint 报告。

防火墙	NSA 240	NSA 2400	NSA 3500	NSA 4500
SonicOS 版本	SonicOS 增强版 5.6（或更高）			
全状态吞吐量[1]	600 Mbps	775 Mbps	1.5 Gbps	2.75 Gbps
GAV 性能[2]	115 Mbps	160 Mbps	350 Mbps	690 Mbps
IPS 性能[2]	195 Mbps	275 Mbps	750 Mbps	1.4 Gbps
UTM 性能[2]	110 Mbps	150 Mbps	240 Mbps	600 Mbps
IMIX 性能[2]	195 Mbps	235 Mbps	580 Mbps	700 Mbps
最大连接数[3]	85,000/110,000[4]	225,000	325,000	500,000
最大 UTM 连接数	32,000/50,000[4]	125,000	175,000	250,000
每秒新建连接	2,000	4,000	7,000	10,000
支持的节点	无限制			
拒绝服务攻击防御	22 类 DoS、DDoS 和扫描攻击			
支持的 SonicPoint（最多）	16	32	32	64

VPN	NSA 240	NSA 2400	NSA 3500	NSA 4500
3DES/AES 吞吐量[5]	150 Mbps	300 Mbps	625 Mbps	1.0 Gbps
点对点 VPN 隧道	25/50[4]	75	800	1,500
捆绑的全局 VPN 客户端许可证（最多）	2（25）	10（250）	50（1,000）	500（3,000）
捆绑的 SSL VPN 许可证（最多）	2（15）	2（25）	2（30）	2（30）
捆绑的虚拟辅助服务（最多）	1 个，30 天试用期（最多 5 个）	1（5）	2（10）	2（10）
加密/认证/DH Group	DES、3DES、AES（128 位、192 位、256 位）、MD5、SHA-1/DH Groups 1, 2, 5, 14			
密钥交换	密钥交换 IKE、IKEv2、手动键、PKI（X.509）、L2TP over IPSec			
基于路由的 VPN	支持（OSPF、RIP）			
证书支持	Verisign、Thawte、Cybertrust、RSA Keon、Entrust 和 Microsoft CA for SonicWALL-to-SonicWALL VPN、SCEP			
失效对端检测（DPD）	支持			
DHCP over VPN	支持			
IPSec NAT 穿越	支持			
冗余 VPN 网关	支持			
支持的全局 VPN 客户端平台	Microsoft® Windows 2000、Windows XP、Microsoft® Vista 32 位/64 位、Windows 7			
支持的 SSL VPN 平台	Microsoft® Windows 2000 / XP / Vista 32/位 / Windows 7、Mac 10.4+、Linux FC 3+ / Ubuntu 7+ / OpenSUSE			

安全服务	NSA 240	NSA 2400	NSA 3500	NSA 4500
深度包检测服务	网关防病毒、反间谍软件、入侵防御和应用智能服务			
内容过滤服务 Premium 版	（CFS） HTTP URL、HTTPS IP、关键字和内容扫描 ActiveX、Java Applet 及 Cookie 封堵			
网关强制的客户端防病毒及反间谍软件	HTTP/S、SMTP、POP3、IMAP 及 FTP，强制的 McAfee™ 客户端电子邮件附件封堵			
综合反垃圾邮件服务	支持			
应用智能	提供应用层强制及带宽控制、网页流量管理、电子邮件、电子邮件附件及文件转发，通过关键字和短语进行文件文档扫描和限制			
DPI-SSL[6]	可透明解密 HTTPS 流量，并使用 SonicWALL 深度包检测技术（GAV/AS/IPS/应用智能服务/CFS）对流量进行扫描，以查找威胁，如果未发现任何威胁或漏洞，随后将重新加密流量，并将其发送到目标地址。该功能既适用于客户端，也适用于服务器。			

网络	NSA 240	NSA 2400	NSA 3500	NSA 4500
IP 地址分配	静态、（DHCP、PPPoE、L2TP 及 PPTP 客户端）、内部 DHCP 服务器、DHCP 中继			
NAT 模式	1 对 1、1 对多、多对 1、多对多、灵活的 NAT（重复的 IP）、PAT、透明模式			
VLAN 接口（802.1q）	10/25[4]	25	50	200
路由	OSPF、RIPv1/v2、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			
IPv6	适用于 IPv6			
认证	XAUTH/RADIUS、活动目录、SSO、LDAP、Novell、内部用户数据库、Terminal Services、Citrix			
内部数据库/单点登录用户	100/100 名用户	252/250 名用户	300/500 名用户	1000/1000 名用户
VoIP	全 H.323v1-5、SIP、Gatekeeper 支持、出站带宽管理、VoIP over WLAN、深度安全检测、大多数 VoIP 网关及通信设备之间的全面互通性			

系统	NSA 240	NSA 2400	NSA 3500	NSA 4500
区域安全	支持			
时间表	一次，定期的			
基于对象/基于组的管理	支持			
动态域名（DDNS）	支持			
管理及监控	Web GUI（HTTP、HTTPS）、命令行（SSH、控制台）、SNMPv2；SonicWALL GMS 全球管理系统			
日志及报告	ViewPoint®、本地日志、Syslog、Solera Networks			
高可用性	可选主动/被动状态同步[4]	可选主动/被动状态同步		主动/被动状态同步
内部数据库/单点登录用户	可选[2]	可选	支持	支持
负载均衡	是，（出方向的流量基于百分比、轮循及带宽溢出）（进入方向的轮循、随机分布、静态 IP、网段重新影射以及对称重新影射）			
标准	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
无线标准	802.11 a/b/g/n, WPA2, WPA, TKIP, 802.1x, EAP-PEAP, EAP-TTLS			

硬件	NSA 240	NSA 2400	NSA 3500	NSA 4500
接口	（3 个）GE 千兆端口+（6 个）10/100，2 个 USB，PC 卡插槽（可选 3G/模拟调制解调器），1 个控制台接口	（6 个）10/100/1000 铜缆千兆端口，1 个控制台接口，2 个 USB		
内存（RAM）	256MB	512MB	512MB	512MB
闪存	32MB Compact Flash	512MB Compact Flash		
3G 无线/调制解调器 7*	带 3G USB 适配器/调制解调器			
电源	36W 外部	单个 180W ATX 电源		
风扇	无	2 个风扇		
输入功率	10-240V, 50-60Hz	100-240Vac, 60-50Hz		
最大功耗	15W	42W	64W	66W
总散热量	51.1BTU	144BTU	219BTU	225BTU
认证	VPNC、ICSA 防火墙 4.1		EAL4+、FIPS 140-2 Level 2、VPNC、ICSA 防火墙 4.1	
待定认证	EAL-4+、FIPS 140-2		—	—
外观及尺寸	7.125×1.5×10.5 英寸/18.10×3.81×26.67 厘米	1U 机架式/17×10.25×1.75 英寸/43.18×26×4.44 厘米		1U 机架式/17×13.25×1.75 英寸/43.18×33.65×4.44 厘米
重量	2.55 磅/1.16 千克	8.05 磅/3.65 千克		11.30 磅/5.14 千克
WEEE 重量	3.15 磅/1.43 千克	8.05 磅/3.65 千克		11.30 磅/5.14 千克
主要要求	FCC A 级、CES A 级、CE、C-Tick、VCCI、Compliance MIC、UL、cUL、TUV/GS、CB、NOM、RoHS、WEEE			
运行环境	32-105°F，0-40℃	40-105°F，5-40℃		
MTBF	9.5 年	16.0 年	14.3 年	14.1 年
湿度	0-95%，无冷凝	10-90%，无冷凝		

[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] UTM/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。 [3] 启用 UTM 服务后，实际的最大连接数量降低了。 [4] 仅指 NSA 240 全状态 HA 和扩展升级版。 [5] 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。 [6] NSA 3500 及更高版本支持此功能。 [7] NSA 2400 不支持此功能。 *不包括 USB 3G 卡和调制解调器。欲了解所支持的 USB 设备的有关信息，请访问 http://www.sonicwall.com/us/products/cardsupport.html。

认证

Common Criteria EAL4+ CERTIFIED

FIPS VALIDATED 140-2

ICSA labs CERTIFIED FIREWALL - CORPORATE

SonicWALL 中国联系方式
销售热线：021-65100909 转 42888
电子邮件：china@sonicwall.com
www.sonicwall.com/cn

SonicWALL 综合性安全防御解决方案系列

网络安全 | 安全远程访问 | 网页及 EMAIL 安全 | 备份恢复 | 策略管理

SONICWALL

02/10 SW 883