SonicWall™ SonicOS 5.9.1.10

版本说明

2017 年 11 月

该版本说明提供了 SonicWall™ SonicOS 5.9.1.10 版本发布的相关信息。

主题：

关于 SonicOS 5.9.1.10

SonicWALL SonicOS 5.9.1.10是维护版本，增强了对KRACK漏洞的保护。SonicWALL TZ和SOHO无线防火墙以及SonicWALL无线接入点不会受到 KRACK 的攻击。然而，由于已受攻击的客户端可能会与接入点或防火墙通讯，将加入额外的保护层以拦截此类通讯。这将使所有的无线客户端的通讯安全。推荐升级至此版本以缓和所有的漏洞。

SonicOS 5.9.1.10提供所有功能并包含SonicOS 5.9.1.x之前版本存在的所有已解决问题且是一个支持5代平台和SOHO 设备的统一正式版本。

在 SonicWALL TZ 系列和一些较小的 NSA 系列平台（如 NSA 220）上，升级到 SonicOS 5.9.1.10 之后可能会影响性能。这是因为与 SonicOS 5.8 版本相比，SonicOS 5.9 版本中有大量的新功能、功能增强和漏洞修复。这些功能和更新对于提升网络安全至关重要。

如需其他版本的更多信息，请参阅之前的版本说明（可以访问 SonicWall 网站：https://www.mysonicwall.com/）。

本文档可能包含在某些国家或地区未发布的平台/版本的说明。

支持的平台

以下 SonicWall 网络安全平台支持 SonicOS 5.9.1.10 版本：

NSA E8510	NSA 2400	TZ 215	TZ 215 Wireless
NSA E8500	NSA 2400MX	TZ 210	TZ 210 Wireless
NSA E7500	NSA 250M	TZ 205	TZ 205 Wireless
NSA E6500	NSA 250M Wireless	TZ 200	TZ 200 Wireless
NSA E5500	NSA 240	TZ 105	TZ 105 Wireless
NSA E5000	NSA 220	TZ 100	TZ 100 Wireless
NSA 4500	NSA 220 Wireless	SOHO	
NSA 3500			

如需支持功能的信息，请参见以下章节中的表格：

- 根据平台支持的关键功能
- 根据平台支持的 SonicPoint 和无线功能
- 支持/不支持 IPv6 功能

根据平台支持的关键功能

该表格列出了 SonicOS 5.9 的关键功能并显示了支持该功能的设备系列。

功能 / 性能增强	NSA E-Class 系列	NSA 系列	TZ 215 系列	TZ 210 系列	TZ 205 系列	TZ 200 系列	TZ 105 系列	TZ 100 系列	SOHO 系列
Active/Active 集群	Y	N	N	N	N	N	N	N	N
Amazon VPC[1]	Y	Y	Y	Y	Y	Y	Y	Y	Y
应用程序规则增强	Y	Y	Y	Y	Y	N	Y	N	Y
AppFlow 报告	Y	Y	Y	Y	N	N	N	N	N
ArcSight Syslog 格式支持	Y	Y	Y	Y	Y	N	Y	N	Y
带宽管理增强	Y	Y	Y	Y	Y	Y	Y	Y	Y
BGP 高级路由	Y	Y[2]	Y[3]	N	N	N	N	N	N
CLI 增强[4]	Y	Y	Y	Y	Y	Y	Y	Y	Y
客户端 CFS 增强	Y	Y	Y	Y	Y	Y	Y	Y	Y
通用访问卡的支持	Y	Y	Y	Y	Y	Y	Y	Y	Y
访客管理支持	Y	Y	Y	Y	Y	N	Y	N	Y
IKE 失效对端检测	Y	Y	Y	Y	Y	Y	Y	Y	Y
IKEv2 配置负载支持	Y	Y	Y	Y	Y	Y	Y	Y	Y
IPv6	Y	Y	Y	Y	Y	N	Y	N	Y

功能 / 性能增强	NSA E-Class 系列	NSA 系列	TZ 215 系列	TZ 210 系列	TZ 205 系列	TZ 200 系列	TZ 105 系列	TZ 100 系列	SOHO 系列
IPv6 6rd	Y	Y	Y	Y	Y	N	Y	N	Y
IPv6 BGP	Y	Y	Y	Y	Y	N	Y	N	Y
IPv6 DHCP PD	Y	Y	Y	Y	Y	N	Y	N	Y
支持 IPv6 的后台服务器	Y	Y	Y	Y	Y	N	Y	N	Y
LDAP 用户群组监控	Y	Y	Y	Y	Y	Y	Y	Y	Y
LDAP 用户群组监控	Y	Y	Y	Y	Y	Y	Y	Y	Y
日志监控过滤输入框	Y	Y	Y	Y	Y	Y	Y	Y	Y
日志增强	Y	Y	Y	Y	Y	Y	Y	Y	Y
MOBIKE	Y	Y	Y	Y	Y	N	Y	N	Y
NetExtender WXAC 集成	Y	Y	Y	Y	Y	Y	Y	Y	Y
网络设备保护配置文件（NDPP 模式）	Y	Y	Y	Y	Y	Y	Y	Y	Y
基于路由的 VPN 有编号地址隧道接口	Y	Y[5]	N	N	N	N	N	N	N
一键配置覆盖	Y	Y	Y	Y	Y	N	Y	N	Y
OpenSSH 潜在安全增强	Y	Y	Y	Y	Y	Y	Y	Y	Y
路径 MTU 发现	Y	Y	Y	Y	Y	Y	Y	Y	Y
代理用户鉴别和登录	Y	Y	Y	Y	Y	Y	Y	Y	Y
DPI 引擎的免重组检测正则表达式	Y	Y	Y	Y	Y	N	Y	N	Y
IPSec 中的 SHA-2	Y	Y	Y	Y	Y	Y	Y	Y	Y
SNMPv3	Y	Y	Y	Y	Y	Y	Y	Y	Y
SSL VPN Mobile 连接书签	Y	Y	Y	Y	Y	Y	Y	Y	Y
SSL VPN 多核扩展性	Y	Y	Y	N	Y	N	N	N	Y
SSO RADIUS 计费	Y	Y[6]	N	N	N	N	N	N	N
TSR 增强	Y	Y	Y	Y	Y	Y	Y	Y	Y
UDP/ICMP 泛洪攻击保护	Y	Y	Y	Y	Y	N	Y	N	Y
有线模式 2.0	Y	Y[7]	N	N	N	N	N	N	N

功能 / 性能增强	NSA E-Class 系列	NSA 系列	TZ 215 系列	TZ 210 系列	TZ 205 系列	TZ 200 系列	TZ 105 系列	TZ 100 系列	SOHO 系列
WWAN 4G 支持	Y	Y	Y	Y	Y	Y	Y	N	Y
XD 查找访问规则	Y	Y	Y	Y	Y	Y	Y	Y	Y

1.所有平台都支持采用静态路由的 Amazon VPC VPN 连接。仅支持 BGP 的平台支持采用动态路由的 Amazon VPC VPN 连接。
2.NSA 240 不支持。NSA 250M 系列和 NSA 220 系列需要 BGP 许可证。
3.需要许可证。
4.NSA 240 和所有 TZ 系列支持有限的 CLI 命令集。
5.仅 NSA 250M 和更高的型号支持；NSA 2400MX 不支持。
6.仅 NSA 3500 和更高型号支持
7.仅 NSA 3500 和更高型号支持

根据平台支持的 SonicPoint 和无线功能

下表列出了 SonicOS 5.9 中的 SonicPoint 和无线功能以及支持这些功能的设备系列。

功能 / 性能增强	NSA E-Class 系列	NSA 系列	TZ 215 系列	TZ 210 系列	TZ 205 系列	TZ 200 系列	TZ 105 系列	TZ 100 系列	SOHO 系列
外部访客服务 Apache/PHP 支持	Y	Y	Y	Y	Y	Y	Y	Y	Y
外部指南服务 FQDN 支持	Y	Y	Y	Y	Y	Y	Y	Y	Y
访客管理支持	Y	Y	Y	Y	Y	N	Y	N	Y
内部无线 IDS 扫描日程[1]	N	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint 802.11e (WMM) OoS	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint 自动设置	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint 保留自定义配置	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint DFS 支持	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint 诊断增强	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint FairNet 支持	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint RADIUS 服务器故障切换	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint WPA TKIP 防御和 MIC 失败泛洪检测和保护	Y	Y	Y	Y	Y	Y	Y	Y	Y
SonicPoint 三层管理	Y	Y[2]	Y	N	N	N	N	N	N

功能 / 性能增强	NSA E-Class 系列	NSA 系列	TZ 215 系列	TZ 210 系列	TZ 205 系列	TZ 200 系列	TZ 105 系列	TZ 100 系列	SOHO 系列
基于配额流量的访客服务策略	Y	Y	Y	Y	Y	Y	Y	Y	Y
虚拟接入点 ACL 支持	Y	Y	Y	Y	Y	Y	Y	Y	Y
虚拟接入点 ACL 支持	Y	Y	Y	Y	Y	Y	Y	Y	Y
虚拟接入点日程	Y	Y	Y	Y	Y	Y	Y	Y	Y
无线客户端桥接支持[3]	N	Y	Y	Y	Y	Y	Y	Y	Y
无线 PCI 非法设备检测保护	Y	Y	Y	Y	Y	Y	Y	Y	Y
无线内置扫描日程[4]									

1.仅在有内置无线网络的系列平台支持。
2.NSA 240 不支持。
3.仅在有内置无线网络的系列平台支持。
4.仅在有内置无线网络的系列平台支持。

支持/不支持 IPv6 功能

以下表格总结了 SonicOS 5.9 中所支持的 IPv6 的功能。

如需查看支持 IPv6 的设备平台，请参考关于根据平台支持的 SonicPoint 和无线功能的章节。

支持的 IPv6 功能	不支持的 IPv6 功能

• 6 至 4 隧道（允许 IPv6 节点通过 IPv4 网络连接外部 IPv6 服务）
• 访问规则
• 地址对象
• 防间谍软件
• 应用程序防火墙
• 攻击预防：
  • Land 攻击
  • Ping of Death 攻击
  • Smurf
  • SYN Flood
• 连接缓存
• IPv6 连接限制
• 连接监控
• 内容过滤服务
• DHCP
• DNS 客户端
	• 反垃圾邮件
	• 命令行接口
	• DHCP over VPN
	• DHCP 中继
	• 用于 IPv6 地址的动态地址对象
	• 动态 DNS
	• FQDN
	• Global VPN Client (GVC)
	• GMS
	• H.323
	• 高可用性：
	  • 多播
	  • Oracle SQL/Net
	  • RTSP
	  • VoIP
	• IKEv1
	• IPv6 Syslog 消息
	• L2TP

支持的 IPv6 功能	不支持的 IPv6 功能

• DNS 查找和反向名称查找
• 动态路由 (RIPng 和 OSPFv3)
• EPRT
• EPSV
• FTP
• 网关防病毒
• 高可用性：
  • 连接缓存
  • FTP
  • IPv6 管理 IP 地址
  • NDP
  • SonicPoint
• 通过 IPv6 的 HTTP/HTTPS 管理
• ICMP
• IKEv2
• 入侵保护服务
• IP 欺骗保护
• IPv4 Syslog 消息，包括含 IPv6 地址的消息
• IPv6 BGP
• 支持 IPv6 的后台服务器
• 二层桥接模式
• 记录 IPv6 事件
• 登录唯一性
• 具有组播监听发现功能的组播路由
• NAT
• NAT 负载均衡
• 邻居发现协议
• 拥有 IPv6 地址的用户使用的 NetExtender 连接
• 数据包捕获
• Ping
• 基于策略的路由
• PPPoE
• 远程管理
• 使用 DPI 的 IPv6 流量安全服务
• 用于保障安全的有 IPSec 的站对站 IPv6 隧道
• SonicPoint IPv6 支持
• SNMP
• SSL VPN
• IPv6 流量的状态检查
• 用户状态
• 可视化
	• LDAP
	• MAC-IP 反欺骗
	• IPv6 与 IPv4 地址之间的 NAT
	• NAT 高可用性探测
	• NetBIOS over VPN
	• NTP
	• QoS 映射
	• RADIUS
	• RAS 组播转发
	• 基于路由的 VPN
	• 单点登录
	• SIP
	• SMTP 实时黑名单 (RBL) 过滤
	• SSH
	• 透明模式
	• ViewPoint
	• 虚拟助理
	• Web 代理

支持的 IPv6 功能	不支持的 IPv6 功能
• IPv6 地址的 VLAN 接口 • VPN 策略 • 无线 • Wire 模式	

已解决的问题

本章节介绍此版本解决的问题。

无线

已解决的问题	问题 ID
WPA 2 (Wi – Fi 保护访问版本 2) 协议中的漏洞可能允许攻击程序解密或伪造客户端与 Wi – Fi 接入点之间的网络数据包。 在密钥协商期间，当易受攻击的客户端加入Wi – Fi网络时发生。	194397

已知问题

本节介绍此版本中存在的已知问题。

AppFlow

已知问题	问题 ID
公告板 > AppFlow 监控中的**用户**选项卡上的“创建规则”选项无效，日志消息显示在控制台上。 当试图为 RADIUS 用户创建一条规则来阻止 LAN 到 WAN 访问，但该用户已经属于一个具有 LAN 到 WAN 访问权限的组时发生。	167772
SSL VPN 用户未显示在**公告板 > AppFlow 监控**的**用户**选项卡上，仅显示“未知”用户。 当多个 (10) SSL VPN 用户连接到防火墙且 AppFlow 报告已启用时发生。	167149

应用程序控制

已知问题	问题 ID
应用程序规则匹配对象无法匹配文件名。 FTP 下载或上传，**防火墙 > 匹配对象**的**匹配类型**设置为**前缀匹配**，**输入表示**设置为**十六进制表示**且选中**启用反向匹配**选项时发生。 **解决方法：**当前缀匹配时不要启用反向匹配。	135634
入侵保护服务启用，否则应用程序控制策略将无法阻止 IPv6 流量。 当 IPS 禁用且在防火墙 > 应用程序控制高级创建应用程序控制策略来阻止 FTP 流量时发生。LAN 端 PC 仍可以使用 IPv6 地址来连接 FTP 服务器。 **解决方法：**启用 IPS。启用 IPS 后，应用程序控制策略将阻止 FTP 连接。	128410

命令行接口

已知问题	问题 ID
CLI 错误地提示网关防病毒未获得许可。 当使用 `show status` CLI 命令而设备上已许可 GAV 时发生。	160800
无法从 HA 对的备份设备上删除访问规则且进一步的配置也无法与备份设备同步。 当访问规则恢复默认设置 CLI 命令运行时发生。	141949

DPI-SSL

已知问题	问题 ID
无法清除缓存中的 SSL 代理连接数。 当客户端 DPI-SSL 已启用，并且 HTTPS 流量通过配置为“第 2 层桥接“模式的 X0 和 X2，然后 X0 和 X2 变为未分配模式时发生。	159332
来自安全站点的证书，例如 `https://mail.google.com`，未能如期望地更改为 SonicWall DPI-SSL 证书，流量无法检测。 在 **DPI-SSL > 客户端 SSL** 页面设置**启用 SSL 客户端检测**选项，SonicPoint-NDR 连接到设备，并在 WLAN 区域上启用访客服务，无线客户端连接到 SonicPoint 且用户登录到访客帐号时发生。	123097

固件

已知问题	问题 ID
Access 上的**恢复默认值**按钮无效。	182149

GVC 高级设置

已知问题	问题 ID
无法成功添加地址组。 当配置 VPN 策略时发生，尤其是当网关设置目标网络通过 VPN 隧道使用 DHCP 获取 IP 地址时。	182239

高可用性

已知问题	问题 ID
无法删除 OSPF/BGP/RIP 路由添加的路由策略。 当故障切换时发生。	182931

IPv6

已知问题	问题 ID
虽然无可用 6rd 前缀，但 6rd 隧道（IPv6 快速部署隧道）意外报告为可用。 当该隧道先前是可用且使用 DHCP 模式，然后禁用 DHCP 服务器并重启防火墙时发生。	157034
通过 6rd 接口发生的 IPv6 流量未转发。 当重启防火墙后发生。 **解决方法：**转至**网络 > 接口**页面，打开 6rd 接口的**编辑接口**对话框并在未做任何更改的情况下单击**确定**。流量即可转发。	143079

IPv6

已知问题	问题 ID
超出最大传输单元 (MTU) 的 IPv6 数据包将丢弃而不是分片。 当为接口设置 MTU，发送超出 MTU 的 IPv6 数据包时发生。	139108
应用程序规则策略仍阻止处于应用程序规则策略排除列表中的 IPv6 地址对象。 当 LAN 端 PC 的 IPv6 地址在应用程序规则策略的排除列表中尝试连接被该策略阻止的站点时发生。	128363

网络

已知问题	问题 ID
当管理员试图删除与 IP-Helper 策略相关的用户自定义 IP-Helper 协议时，管理员正确接收到错误消息。但如果还尝试删除该策略，然后尝试添加一个新的 DNS 型策略，则其原先试图删除的 IP-Helper 协议和相关策略会消失。	183072
来自 VPN 区域 的 DHCP ip-helper 策略不是从 VPN 区域 添加。 当添加隧道接口时发生。	182751
X1 接口从 PPTP 模式变为静态模式会导致 X1 不可访问且其 IP 地址变为 0.0.0.0。 当 X1 接口已在 PPTP 模式下获得一个 IP 地址，随后管理员在静态模式下重新配置 X1 并分配其一个静态 IP 地址时发生。 **解决方法：**重启防火墙以使 X1 又能访问。	160164
重启防火墙之后，使用 HTTPS 或 ping 无法访问 WAN 接口。 当 X0 (LAN) 配置了一个冗余端口且 X0 物理状态为“无链路”时发生。	156619
更改 WAN 模式之后，默认路由网关错误。 当 X1 在 L2TP 模式下配置并分配 IP，随后变为 PPTP 模式，但默认路由网关仍为从 L2TP 服务器获取的网关时发生。WAN 模式变回 L2TP 之后，默认路由网关为从 PPTP 服务器获取的网关。	154144
当有线模式对下的其它接口断开时，配对的接口无法断开。 当启用链路状态广播选项启用后，由于对端交换机断开而使有线模式接口断开时发生。	151827
禁用 DHCPv6 客户端也将禁用其它 DHCPv6 客户端。 当 X1 和 X2 都配置为 DHCPv6 自动模式，X1 更改为静态时发生。	147542
数据包无法通过有线模式对。 当目的链路本地 IPv6 地址和有线模式接口地址相同时发生。	144385
默认网关无法配置。 当 X2 配置为 WAN 接口且 IP 分配为静态时发生。	141973
IPv6 NAT 策略未能如期从防火墙删除。 当所有 IPv6 自定义策略删除且防火墙重启时发生。	141530
网关防病毒 (GAV) 在 IPv6 Wiremode > 安全模式下可能无效。 当在全局和每个区域启用 GAV 的情况下，使用有线模式 > 安全模式时发生。	139250
边界网关协议 (BGP) 验证无法和 IPv6 对端兼容。 当在防火墙和路由间配置 IPv6 对端，并在每端启用 BGP 验证时发生。	138888

安全服务

已知问题	问题 ID
不能按预期排除符合独立入侵保护特征的用户。 当对所有特征都已启用“安全服务 > 入侵保护”，同时启用了 WAN 和 LAN 区域的 IPS，然后管理员针对一个特定特征 ID，将用户配置在“排除的用户/组”中时发生。当该用户将包含该特征的流量从 WAN 侧发送到 LAN 上的计算机时，日志显示 IPS 拦截了流量，并且该用户的名称出现在日志中。	160458
即使某些 IP 地址在网关防病毒排除列表中，仍阻止这些 IP 地址。 当 FQDN 地址对象包含在网关防病毒排除列表中时发生。	121984

SSL VPN

已知问题	问题 ID
WLAN 区域上的“SSL VPN 增强”将用户重定向至 SSL VPN 门户登录页面，但登录页面未打开。 当从 WLAN 客户端机器浏览任何 HTTP 网站时发生。	161300

系统

已知问题	问题 ID
LCD 面板的配置模式无法访问并显示无效编码的错误消息。 当管理员从 LCD 面板选择配置选项并输入刚在系统 > 管理员页面更改的PIN编码时发生。	130379
在一键配置下修改密码并重启设备后，SonicWall GMS 不能和 SonicOS 同步。 当通过 GMS 的一键配置更改密码的复杂度时发生。状态防火墙安全需要密码包含字母、数字和标点字符。如果设备的密码太简单，例如默认的“password”，重启之后 GMS 无法登录，无法弹出提示修改密码的提示框。	124998

升级

已知问题	问题 ID
NTP 服务器身份验证类型从 **MD5** 变为**无身份验证**。 当从 5.8.1.15 升级到 5.9.1.8 之后发生。	183577

用户界面

已知问题	问题 ID
系统 > 状态页面的**最新警报**部分未显示任何警报。 当启用或禁用接口或发生其他已知会引发警报的事件时发生。	160868
“单击此处以进行 UTM 管理”中的超链接无效。 当登录至 SSL VPN 虚拟办公室入口的 IPv6 地址时发生。	157523

VoIP

已知问题	问题 ID
SonicOS 丢弃从 WAN 到二层桥接接口的 SIP 数据包，且无法建立 VoIP 呼叫。可以在相同的路径进行 Ping。当使用主要 LAN 接口时呼叫可以建立。 当接口 X5 (LAN) 配置为二层桥接模式且桥接到 X0 (LAN) 时发生。Cisco 电话连接到 X5 并用来呼叫 WAN 端的电话，但是呼叫无法建立。	128225

VPN

已知问题	问题 ID
中央防火墙后的客户端可以 ping 远程防火墙后的 LAN 设备，即使该设备位于“排除 LAN 设备”表中也能访问。 当远程防火墙配置为使用 VPN 上的 DHCP，并且将 LAN 设备配置为远程防火墙上的“LAN 上静态设备”，再将其添加到“排除 LAN 设备”表中时发生。	166617
VPN 协商失败且发起者的日志无法显示"IKEv2 协商完成"。 当 VPN 策略绑定到接口而不是默认路由接口时发生。当 VPN 策略绑定到 IPv6 地址时可以发现。	148167
流量无法通过错误的 VPN 隧道。 当两个 VPN 隧道接口配置 Amazon VPC 并添加两个编号隧道接口和基于 Amazon VPC 配置的 BGP 邻居时发生。 当隧道 1 断开，流量切换到隧道 2。当隧道 1 恢复时，流量仍保持在隧道 2。当隧道 2 断开时，流量切换到隧道 1。 当隧道 2 恢复时，流量停止了。路由表显示数据包通过隧道 1，但数据抓包未显示数据包通过隧道 2。	135205
活动 IPv6 VPN 隧道未在前端防火墙的 VPN > 设置页面显示。 在头端和远端设备上创建两条 IPv6 VPN 隧道时发生。VPN > 设置页面显示 “目前有 2 条活动的 IPv6 隧道”，但在活动 VPN 隧道表只显示了一条隧道。	128633
在 NSA 240 和 NSA 7500 之间无法建立 OSPF 连接。 当在 NSA 240 和 NSA 7500 之间配置 VPN 隧道并在 NSA 240 上启用高级路由时发生。在 NSA 7500 上创建编号隧道接口并绑定到 VPN 隧道。在 NSA 240 上创建 VLAN 并配置和 NSA 7500 上的隧道接口相同子网的 IP 地址。两台设备上都启用了 OSPF，但 NSA 240 无法响应 OSPF “Hello” 数据包且 OSPF 连接无法建立。	128419

系统兼容性

本节提供了该版本关于硬件和软件兼容的额外信息。

无线 3G/4G 宽带设备

SonicOS 5.9.1.10 为各种 PC 卡、USB 设备和无线服务提供商提供支持。如需支持的设备的最新列表，请访问 https://www.sonicwall.com/supported-wireless-broadband-cards-devices/。

注： 当连接到 SonicWall 设备时，大部分 3G/4G 设备的性能和数据吞吐量将比直接与个人计算机相连时要低。SonicOS 使用 PPP 接口而不是这些设备的专用接口。该性能与从 Linux 机器或其他 4G 路由器连接的性能差不多。

GMS 支持

对运行 SonicOS 5.9.1.10 的 SonicWall SOHO 设备执行 GMS 管理，需要 SonicWall 全局管理系统 (GMS) 7.2 服务包 5（或更高版本）或 GMS 8.1（或更高版本）。

WXA 支持

支持 SonicWall WXA 系列设备（WXA 6000 软件、WXA 500 Live CD、WXA 5000 虚拟设备、WXA 2000/4000 设备）与运行 SonicOS 5.9.1.10 的 SonicWall 安全设备配合使用。WXA 系列设备的建议固件版本为 WXA 1.3.2。

浏览器支持

可视化的 SonicOS 使用了大部分最新浏览器都支持的诸如 HTML5 等高级浏览器技术。SonicWall 建议使用最新的 Chrome、Firefox、Internet Explorer 或 Safari 浏览器来管理 SonicOS。该版本支持以下 Web 浏览器：

- Chrome 18.0 或更高版本（建议使用可以显示公告板实时图表的浏览器）
- Firefox 16.0 或更高版本
- Internet Explorer 9.0 及更高版本（不使用兼容模式）
- Safari 5.0 或更高版本，在非 Windows 机器上运行

注： 在 Windows 机器上，SonicOS 管理不支持 Safari。

注： 不推荐使用移动设备浏览器进行 SonicWall 设备系统管理。

产品许可

SonicWall 网络安全设备必须在 MySonicWall 上注册才能启用所有的功能和享受 SonicWall 安全服务、固件升级和技术支持。请在以下网址登录或注册 MySonicWall 帐户：https://mysonicwall.com/。

SonicOS 中安全服务的数量是需要单独授权的。一项服务获得授权后才能完全访问其功能。SonicOS 使用 SonicWall 许可证管理器定期检查许可证状态。**系统 > 状态**页面会显示每项安全服务的许可证状态。

升级信息

如需获取最新固件、升级 SonicWall 设备中的固件镜像以及从其他设备导入配置设置的信息，请参见 *SonicOS 5.9* 升级指南（可从支持门户获取，网址为：https://support.sonicwall.com/zh-cn/technical-documents）。

重要提示： 如果运行 SonicOS 5.9 的设备上配置了 VPN 隧道接口，则将设备升级到 SonicOS 5.9 之前，请阅读 *SonicOS 5.9* 升级指南中的“关于 VPN 隧道接口的升级注意事项”。

注： 对于 SonicWall TZ 系列和一些较小的 NSA 系列平台（如 NSA 220），升级到 SonicOS 5.9.1.10 之后可能会影响性能。这是因为与 SonicOS 5.8 版本相比，SonicOS 5.9 版本中有大量的新功能、性能增强和漏洞修复。这些功能和更新对于提升网络安全是必要的。

SonicWall 支持

购买了拥有有效支持维护合同的 SonicWall 产品的客户和试用版本的客户都可以获得技术支持。

支持门户提供了各种自助工具，使您可以快速并独立地解决问题，一年 365 天，一天 24 小时不间断。如需访问支持门户，请访问 https://support.sonicwall.com/zh-cn/。

支持门户使您能够：

- 查看知识库文章和技术文档
- 下载软件
- 查看视频教程
- 与用户论坛中的同行和专家合作
- 获得许可帮助
- 访问 MySonicWall
- 了解 SonicWall 的专业服务
- 注册培训和认证

如需联系 SonicWall 支持，请访问 https://support.sonicwall.com/zh-cn/contact-support。

图例

警告：“警告”图标用来提示可能造成财产损失或人员伤亡的情况。

小心：“小心”图标用来提示如不按照相应说明进行操作，可能引起硬件损坏或数据丢失。

重要提示、注意、提示、手机或视频：信息图标表示支持的信息。

最后更新日期：2017 年 11 月

232-004104-00 修订版 A