

# SONICWALL SECURE MOBILE ACCESS (SMA)

基于用户和设备身份、位置和信任，随时随地安全访问跨多重云环境的公司资源。

SonicWall SMA 是一个统一安全访问网关，可以使组织能够随时随地从任何设备访问关键任务型企业资源。SMA 实施精细访问控制策略引擎、情境感知设备身份认证、应用程序级别 VPN 和采用单点登录的高级身份验证，使组织能够在多重云环境中采用 BYOD（自带设备）和移动设备。

## 移动设备和 BYOD（自带设备）

对于希望采用 BYOD（自带设备）、灵活工作或第三方访问的组织，SMA 成为它们之间的关键强制实施点。SMA 提供一流的安全性，以最大程度地减少表面威胁，同时通过支持最新的加密算法和密码，确保组织更安全。SonicWall 的 SMA 允许管理员提供安全的移动访问和基于身份的权限，以便最终用户可以快速、简单地访问所需的业务应用程序、数据和资源。同时，组织可以制定安全的 BYOD（自带设备）策略，以保护其公司网络和数据免受恶意访问和恶意软件的攻击。

## 迁移到云

对于开始进行云迁移之旅的组织，SMA 提供了单点登录 (SSO) 基础设施，使用单个 Web 门户在混合 IT 环境中对用户进行身份验证。无论公司资源是内部、在 Web 上还是在托管云中，访问体验都一致且流畅。SMA 还集成了行业领先的多因素身份验证技术，以增强安全性。

## 托管服务提供商

无论是托管自有基础设施的组织还是托管服务提供商，SMA 提供统包解决方案，均可实现高度的业务连续性和可扩展性。SMA 可以在单个设备上支持多达 20,000 个并行连接，并可以通过智能集群扩展成千上万的用户。数据中心可通过主动-主动集群和内置的动态负载均衡器降低成本，根据用户需求将全局流量实时重新分配给最优化的数据中心。SMA 工具集使服务提供商能够在零停机时间内交付服务，从而使他们能够履行非常积极的服务级别协议 (SLA)。

SMA 使 IT 部门能够根据用户情景，提供最佳体验和最安全的访问。SMA 既可以作为增强的物理设备，也可以作为功能强大的虚拟设备使用，均可无缝地与现有的内部和/或云基础设施配合。组织可以为第三方或个人拥有的设备上的员工选择一系列完全没有客户端的基于 Web 的安全访问，也可以为所有设备类型的管理人员选择更为传统的基于客户端的全隧道 VPN 访问。无论是组织需要从单个位置向五个用户提供可靠的安全访问，还是跨全球分布的网络扩展到数千个用户，SonicWall SMA 都可以提供解决方案。

SonicWall SMA 使组织能够放心地采用移动设备和 BYOD（自带设备），并轻松地迁移到云中。SMA 赋予员工力量，并为他们提供一致的访问体验。

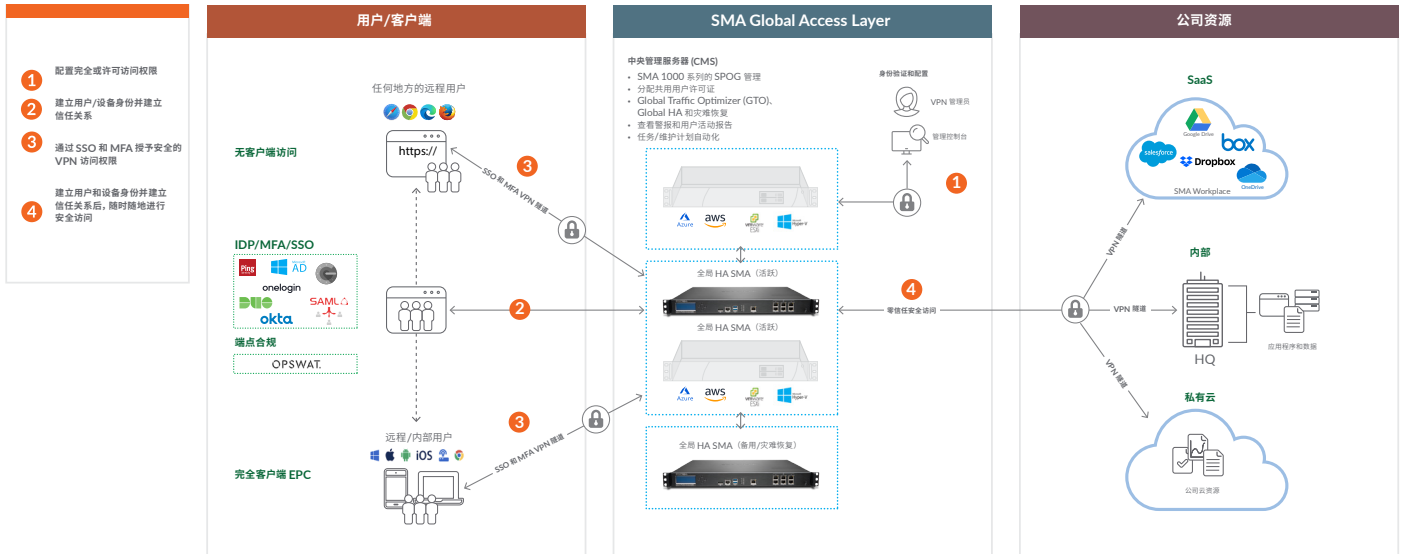
## 好处：

- 统一访问所有网络和云资源，实现“任何时间、任何设备、任何应用程序”的安全访问
- 利用稳健的访问控制引擎定义精细策略，控制谁可以访问哪些资源
- 通过使用单个 URL 向任何 SaaS 或本地托管应用程序提供联合单点登录，提高生产效率
- 通过在混合 IT 环境中整合基础设施组件，降低总体拥有成本 (TCO) 并降低访问管理的复杂性
- 了解每个连接设备，并根据策略和端点的运行状况授予访问权限
- 使用 Capture ATP 沙箱扫描上传到网络中的所有文件，防止恶意软件入侵
- 防范基于 Web 的攻击，并提供与 Web Application Firewall 外接程序的 PCI 兼容性
- 利用 Geo IP 检测和僵尸网络防护防范 DDoS 和僵尸攻击
- 使用基于 Web 浏览器的无客户端 HTML5 访问获得安全保证的本机代理功能，而无需在端点设备上安装和维护代理的开销
- 借助实时监控和综合报告，获得制定明智决策所需的切实可行的洞察
- 在 ESXi 或 Hyper-V 上的私有云中或在 AWS 或 Microsoft Azure 公共云环境中，部署为物理设备或虚拟设备。
- 支持根据实时需求动态颁发访问许可证，并自动将端点定向到性能最高、延迟最低的连接
- 利用内置的负载均衡而无需额外的硬件或服务，从而降低前期成本，同时为设备故障转移提供零用户影响
- 可立即扩展容量，确保不受业务中断或季节性高峰的影响

# SMA 部署

## 增强的边界网关,可随时随地从任何设备进行安全访问

SMA 提供对跨企业内部、云和混合数据中心托管的公司资源的全面端到端安全远程访问。它应用基于身份的按策略强制实施的访问控制、情境感知设备身份验证和应用程序级别 VPN, 在建立用户和设备身份、位置和信任之后, 授予对数据、资源和应用程序的访问权限。在 ESXi 或 Hyper-V 上的私有云中或在 AWS 或 Microsoft Azure 公共云环境中, 灵活部署为增强的 Linux 设备或虚拟设备。



SMA 云/内部部署

## 采用物理和虚拟设备进行灵活部署

SonicWall SMA 可以部署为增强的高性能设备, 也可以部署为虚拟设备, 利用共享计算资源来优化利用率、简化迁移并降低投资成本。硬件设备建立在多核体系结构之上, 通过 SSL 加速、VPN 吞吐量和强大的代理提供高性能, 从而提供稳健的安全访问。对于监管机构和联邦机构, SMA 还具有 FIPS 140-2 二级认证。SMA 虚拟设备在主要虚拟或云平台 (包括, Microsoft Hyper-V、VMware ESX 和 AWS) 上提供同样强健的安全访问功能。

## 跨设备分享用户许可证

设备跨全球分布的组织可以从由于时间差导致的用户许可证需求波动中受益。无论组织是部署完全 VPN 许可证还是基本 ActiveSync 许可证, SMA 的中央管理服务器都会将许可证重新分配给受管理的设备, 不同地理区域的用户对设备的需求已经达到顶峰, 但由于非工作时间/夜间时间的原因, 使用量有所下降。

## 情境感知设备的网络可见性剖析

一流的情境感知身份验证仅授予对受信任的设备和授权用户的访问权限。还会询问笔记本电脑和 PC 是否存在安全软件、客户端证书和设备 ID。在授予访问权限之前, 会询问移动设备以获取必需的安全信息, 例如, 越狱或 root 状态、设备 ID、证

书状态和操作系统版本。不允许不符合策略要求的设备访问网络, 并且会通知用户不合规情况。

## 单一 Web 门户提供一致的体验

用户不需要记住所有单个应用程序 URL 并维护详尽的书签。SMA 提供一个集中化访问门户, 为用户提供一个 URL 来从标准 Web 浏览器访问所有关键任务型应用程序。用户通过浏览器登录后, 浏览器窗口中会显示一个可自定义的 Web 用户门户, 提供单一玻璃视图窗格来访问任何 SaaS 或本地应用程序。门户仅显示与特定终端设备、用户或组相关的链接和个性化书签。该门户与平台无关, 并且支持所有主要设备平台, 包括 Windows、Mac OS、Linux、iOS 和 Android 设备, 并在所有这些设备上提供广泛的浏览器支持。

## 在 SaaS 和本地应用程序两者上联合单点登录

不再需要多个密码, 并停止使用不良的安全做法, 如密码重用。SMA 为云托管的 SaaS 应用程序和园区托管的应用程序提供联合 SSO。SMA 与多种身份验证、授权和计费服务器以及领先的多因素身份验证技术集成, 以增强安全性。SMA 在检查端点运行状况状态和合规性之后, 才会将安全 SSO 交付给已授权的端点设备。访问策略引擎可确保用户仅能查看授权的应用程序, 并在成功进行身份验证后授予访问权限。该解决方案即使在使用 VPN 客户端时也支持联合 SSO, 无论使用

基于客户端的安全访问还是通过无客户端的安全访问，都可以为客户无缝的身份验证体验。

### 防止违规和高级威胁

SonicWall SMA 添加了一层访问安全性，以改善您的安全状况并减少威胁的影响范围。

- SMA 与 SonicWall Capture ATP 基于云的多引擎沙盒集成，可扫描用户上传的所有文件或公司网络外部用户上传的所有文件。这样可以确保用户在旅途中与在办公室中一样拥有相同级别的保护，免受勒索软件或零日恶意软件等高级威胁的侵害<sup>1</sup>。
- SonicWall Web Application Firewall 服务为企业提供了经济实惠、良好集成的解决方案，以保护内部基于 Web 的应用程序。这使得客户能够确保数据的机密性，并且如果存在恶意或欺诈的经过验证的用户访问，内部 Web 服务也不会受到损害。
- Geo-IP 和僵尸网络检测可保护组织免受 DDoS 和僵尸攻击，并防止遭到攻击的端点成为僵尸网络。

### 基于浏览器的无缝、安全的无客户端访问

SonicWall SMA 的“无客户端”性质意味着管理员无需将胖客户端组件手动安装到将用于远程访问的计算机上。这消除了对 Java 的依赖性和 IT 开销，从而大大扩展了远程访问的概念。这意味着，由于不需要预先安装或预先配置，授权的远程员工可以在世界上任何地方，利用任何一台计算机，安全地访问他们的公司资源。安全访问用这种最简单的方式，使用 HTML5，并严格基于浏览器，从而为用户提供无缝和统一的体验。

### 部署适合您需求的 VPN 客户端

从广泛的 VPN 客户端中进行选择，为各种端点（包括笔记本电脑、智能手机和平板电脑）提供按策略强制实施的安全远程访问。

| VPN 客户端               | 支持的操作系统                               | 支持的 SMA 型号                     | 关键亮点                         |
|-----------------------|---------------------------------------|--------------------------------|------------------------------|
| Mobile Connect        | iOS、OS X、Android、Chrome OS、Windows 10 | 全部型号                           | 提供生物身份验证、按应用程序 VPN 和端点控制强制实施 |
| Connect Tunnel (瘦客户端) | Windows、Mac OS 和 Linux                | 6200、6210、7200、7210、8200v、9000 | 借助稳健的端点控制提供完整的“办公室”体验        |
| NetExtender (瘦客户端)    | Windows 和 Linux                       | 210、410、500v                   | 实施精细的访问策略，并通过本机客户端扩展网络访问     |

### 提供“永远在线”的体验

为了提供无缝的用户体验，SMA 为受管 Windows 设备提供“永远在线”的 VPN。管理员可以配置设置，以便在授权端点客户端检测到公用或不受信任的网络时自动建立 VPN 连接。Windows 设备的单一登录事件为用户提供与公司资源的安全连接。用户不必登录其 VPN 客户端或维护其他密码。这为移动用户提供了无缝体验，使他们能够像在办公室一样访问关键任务型资源，并使 IT 管理员能够保持对托管设备的控制，从而改善组织的安全状况。

### 直观的管理和全面的报告

SonicWall 提供一个基于 Web 的直观管理平台 [Central Management Server \(CMS\)](#)，可简化设备管理，同时提供广泛的报告功能。GUI 易于使用，使管理单个或多个设备和策略更加清晰。每个页面显示如何在所有受管理的机器上配置设置。统一策略管理可帮助您创建和监控访问策略和配置。单个策略可以控制从您的用户、设备和应用程序对数据、服务器和网络的访问。IT 部门可以实现例行任务自动化并安排活动，使安全团队从重复性任务中解放出来，专注于诸如事件响应等战略性安全任务。借助易于使用的报告和集中化日志记录，IT 部门可以洞察用户访问趋势和系统范围的运行状况。

### 提供全天候服务可用性

组织要求维护其服务并以高度的可靠性使其正常运行，以便随时提供对关键任务型应用程序的安全访问。SMA 设备为使用单个数据中心的组织提供传统的主动-被动高可用性 (HA)，或为本地或分布式数据中心提供具有主动-主动或主动-备用集群的全局 HA。这两种 HA 模型均可为用户提供无障碍体验，实现零影响的故障转移和会话持续性。

## 使用内置负载均衡器降低前期成本

SMA 设备内置的负载均衡功能可实现中型企业和公司部署所需的级别可扩展性。某些 SMA 设备型号可提供动态负载均衡，以根据需求智能地分配会话负载并实时分配用户许可证。组织不需要投资外部负载均衡器，从而可减少前期成本。

## 为不可预见的事件投保

完整的业务连续性和灾难恢复解决方案必须能够处理远程访问流量中的显著峰值，同时仍保持安全性和成本控制。用于 SMA 的 SonicWall Spike 许可证包是附加许可证，使分布式业务可以扩展用户数量并立即达到最大容量，从而实现无缝的业务连续性。Spike 许可证的工作方式类似于保险单，可以应对从当前用户数到数十个甚至数百个额外用户的将来任何计划内或计划外的峰值。

## 特色



### 高级身份验证

|                     |   |
|---------------------|---|
| 联合单点登录 <sup>2</sup> | SMA 使用 SAML2.0 身份验证，通过单一门户启用对内部和云资源的联合 SSO，同时强制实施堆叠式多因素身份验证以增强安全性。  |
| 多因素身份验证             | X.509 数字证书<br>服务器端和客户端数字证书<br>RSA SecurID、Dell Defender、Google Authenticator、Duo Security 和其他一次性密码/双因素身份验证令牌<br>通用访问卡 (CAC)<br>双因素或堆叠身份验证<br>验证码支持，用户名/密码 |
| SAML 身份验证           | 可以将 SMA 配置为 SAML Identity Provider (IdP)、SAML Service Provider (SP) 或代理现有的 on-prem IdP，从而使用 SAML 2.0 身份验证启用联合单点登录 (SSO)。                                  |
| 身份验证存储库             | SMA 提供与行业标准存储库的简单集成，便于管理用户帐户和密码。<br>可以基于 RADIUS、LDAP 或 Active Directory 身份验证存储库 (包括嵌套组) 动态填充用户组。<br>可以询问通用或自定义 LDAP 属性，以进行特定的授权或设备注册验证。                   |
| 层 3-7 应用程序代理        | SMA 提供灵活的代理选项，例如，可以通过直接代理提供供应商访问，通过反向代理提供合同工访问，以及通过 ActiveSync 提供员工对 Exchange 的访问。  |
| 反向代理                | 实施身份验证的增强型反向代理服务使管理员可以配置应用程序卸载门户和书签，从而允许用户无缝连接到远程应用程序和资源，包括 RDP 和 HTTP。此功能支持所有浏览器，包括 IE、Chrome 和 Firefox。   |
| Kerberos 约束委派       | SMA 使用现有的 Kerberos 基础设施提供身份验证支持，不需要信任前端服务即可委派服务。  |



## 访问管理

|                |  |
|----------------|--|
| 访问控制引擎 (ACE)   | 管理员根据组织策略授予或拒绝访问权限，并在隔离会话时设置修正操作。ACE 基于对象的策略利用网络、资源、身份、设备、应用程序、数据和时间等元素。   |
| 端点控制 (EPC)     | EPC 允许管理员根据连接设备的运行状况强制实施精细的访问控制规则。借助深度操作系统集成，许多元素被组合起来进行类型分类和风险因素评估。EPC 询问使用针对 Windows、Mac 和 Linux 平台的防病毒、个人防火墙和防间谍软件解决方案的预定义全面列表（包括签名文件更新的版本和适用性），简化了设备配置文件的设置。 |
| 应用程序访问控制 (AAC) | 管理员可以定义允许哪些特定的移动应用程序通过单个应用程序隧道访问网络上的哪些资源。客户端和服务器上均强制实施 AAC 策略，从而提供稳健的外围保护。   |



## 卓越的安全性

|                                |  |
|--------------------------------|--|
| 层 3 SSL VPN                    | SMA 系列为在任何环境中运行的各种客户端设备提供高性能层 3 隧道功能。  |
| 加密支持                           | 可配置会话长度<br>密码: AES 128 + 256 位、三重 DES、RC4 128 位<br>哈希: SHA-256<br>椭圆曲线数字签名算法 (ECDSA) |
| 高级密码支持                         | SMA 设备使用默认配置密码，提供强大的开箱即用安全机制，满足合规性，管理员可以进一步改进性能、安全强度或兼容性。                            |
| 安全认证                           | 通过 FIPS 140-2 二级认证、ICSA SSL-TLS 认证，正在进行通用标准 UC-APL 认证                                |
| 安全文件共享                         | 阻止未知的零日攻击，如在网关处阻止勒索软件，并进行自动修正。通过可安全访问公司网络的非托管端点上传的文件将由我们基于云的多引擎 Capture ATP 检查。      |
| Web Application Firewall (WAF) | 防止基于协议和 Web 的攻击，帮助金融、医疗、电子商务和其他企业满足 OWASP Top 10 (OWASP 前十大安全风险) 和 PCI 合规性。          |
| Geo IP 检测和僵尸网络保护               | Geo IP 检测和僵尸网络保护为客户提供了一种机制，可以允许或限制用户从不同地理位置访问。                                       |
| TLS 1.3 支持                     | 改进了安全和性能，同时与以前版本相比减少了复杂性。  |





## 直观的用户体验

|                          |  |
|--------------------------|--|
| “永远在线”的 VPN              | 从公司发放的 Windows 设备自动建立与公司网络的安全连接，以提高安全性、了解流量使用情况并保持合规性                          |
| 安全网络检测 (SND)             | SMA 的网络感知 VPN 客户端可检测设备何时离开园区，并自动重新连接 VPN，当设备返回到受信任的网络时再次将其关闭。                  |
| 对资源的无客户端访问               | SMA 通过交付 RDP、ICA、VNC、SSH 和 Telnet 协议的 HTML5 浏览器代理，提供对资源的无客户端安全访问。              |
| 单点登录门户                   | WorkPlace 门户提供易于使用、可自定义的单窗格视图，可通过单点登录 (SSO) 对混合 IT 环境中的任何资源进行安全访问。无需其他登录或 VPN。 |
| 层 3 隧道                   | 管理员可以使用 SSL/TLS 隧道和可选的 ESP 回退，选择分离隧道或强制实施全部重定向模式，实现最佳性能。                       |
| HTML5 文件浏览器 <sup>1</sup> | 现代文件浏览器使用户可以方便地使用任何 Web 浏览器访问文件共享。   |
| 移动操作系统集成                 | 所有操作系统平台均支持 Mobile Connect，从而为用户选择移动设备提供了充分灵活性。                                |



## 弹性

|                                |   |
|--------------------------------|---|
| Global Traffic Optimizer (GTO) | SMA 提供对用户零影响的全局流量负载均衡。流量被转到最优化且性能最高的数据中心。                       |
| 动态高可用性 <sup>2</sup>            | 无论是部署在单个数据中心中还是跨多个地理位置分散的数据中心中，SMA 均可支持主动/被动，并提供主动/主动配置以实现高可用性。 |
| 通用会话持久性 <sup>1</sup>           | 为用户提供零影响故障转移的无障碍体验。如果设备离线，则 SMA 的智能集群可重新分配用户及其会话数据，而无需进行重新身份验证。 |
| 性能可扩展                          | SMA 设备通过部署多个设备，呈指数级扩展性能，从而消除了单点故障。水平集群完全支持混合物理和虚拟 SMA 设备。       |
| 动态许可                           | 用户许可证不再必须应用于单个 SMA 设备。可以根据用户需求在托管设备之间动态地分配和重新分配用户。              |



## 中央管理与监控

|              |   |
|--------------|---|
| 中央管理系统 (CMS) | CMS 为所有 SMA 功能提供基于 Web 的集中化管理。  |
| 自定义警报        | 可以针对生成由任何 IT 基础设施网络管理系统 (NMS) 监控的 SNMP 陷阱配置警报。管理员还可以针对 Capture ATP 文件扫描和磁盘使用情况配置警报, 以备立即采取措施。 |
| 实时仪表板        | IT 管理员利用可定制的实时仪表板可以快速轻松地诊断访问问题, 从而为排除故障获取有价值的洞察。  |
| SIEM 集成      | 向中央 SIEM 数据收集器实时输出方便安全团队关联事件驱动的活动, 从而了解特定用户或应用程序的端到端工作流程。这在安全事件管理和取证分析期间至关重要。                 |
| 调度程序         | 调度程序使用户能够调度维护任务, 例如部署策略, 复制配置设置和重新启动服务, 而无需人工干预   |



## 扩展性

|               |  |
|---------------|--|
| 管理 API        | 管理 API 允许对单个 SMA 或全局 CMS 环境中的所有对象进行完全的程序化管理控制。   |
| 最终用户 API      | 最终用户 API 提供对所有登录、身份验证和端点工作流程的完全控制。   |
| 双因素身份验证 (2FA) | SMA 通过与基于时间的领先一次性密码 (TOTP) 解决方案 (例如, Google Authenticator、Microsoft Authenticator、Duo security 等) 集成来交付 2FA。 |
| MDM 集成        | SMA 集成了领先的企业移动管理 (EMM) 产品 (例如, Airwatch 和 Mobile Iron)。  |
| 其他第 3 方集成     | SMA 与 OPSWAT 等行业领先的供应商集成, 以提供高级威胁防护  |

<sup>1</sup> 适用于 SMA OS 12.1 或更高版本

<sup>2</sup> SMA 12.1 中增强

功能摘要 (按型号比较)

| 类别                                     | 功能   | 210      | 410      | 500v                            | 6210     | 7210     | 8200v                           |
|--|--|----------|----------|---------------------------------|----------|----------|---------------------------------|
| 部署                                     | 操作系统   | SMA 10.2 | SMA 10.2 | SMA 10.2                        | SMA 12.4 | SMA 12.4 | SMA 12.4                        |
|  | 支持的虚拟机监控程序   | -        | -        | VMware ESXi / Microsoft Hyper-V | -        | -        | VMware ESXi / Microsoft Hyper-V |
|  | 支持的公共云平台   | -        | -        | AWS/Azure                       | -        | -        | AWS/Azure                       |
| 吞吐量                                    | 最大并行用户会话数  | 50       | 250      | 250                             | 2,000    | 10,000   | 5,000                           |
|  | 最大 SSL/TLS 吞吐量                                     | 560 Mbps | 844 Mbps | 186 Mbps                        | 800 Mbps | 5.0 Gbps | 1.58 Gbps                       |
| 客户端访问                                  | 层 3 隧道   | •        | •        | •                               | •        | •        | •                               |
|  | 分离隧道和全部重定向   | •        | •        | •                               | •        | •        | •                               |
|  | “永远在线”的 VPN  | •        | •        | •                               | •        | •        | •                               |
|  | 自动 ESP 封装  | -        | -        | -                               | •        | •        | •                               |
|  | HTML5 (RDP、VNC、ICA、SSH、Telnet、网络浏览器)               | •        | •        | •                               | •        | •        | •                               |
|  | 安全网络检测   | -        | -        | -                               | •        | •        | •                               |
|  | 文件浏览器 (CIFS/NFS)                                   | •        | •        | •                               | •        | •        | •                               |
|  | Citrix XenDesktop/XenApp                           | •        | •        | •                               | •        | •        | •                               |
|  | VMware View  | -        | -        | -                               | •        | •        | •                               |
|  | On Demand Tunnel                                   | -        | -        | -                               | •        | •        | •                               |
|  | Chrome/Firefox 扩展                                  | -        | -        | -                               | •        | •        | •                               |
|  | CLI 隧道支持   | -        | -        | -                               | •        | •        | •                               |
|  | Mobile Connect (iOS、Android、Chrome、Win 10、Mac OSX) | •        | •        | •                               | •        | •        | •                               |
|  | Net Extender (Windows、Linux)                       | •        | •        | •                               | -        | -        | -                               |
| Connect Tunnel (Windows、Mac OSX、Linux) | -  | -        | -        | •                               | •        | •        |                                 |
| Exchange ActiveSync                    | •  | •        | •        | •                               | •        | •        |                                 |
| 移动访问                                   | 按应用程序 VPN  | -        | -        | -                               | •        | •        | •                               |
|  | 应用程序控制强制实施   | -        | -        | -                               | •        | •        | •                               |
|  | 应用程序 ID 验证   | -        | -        | -                               | •        | •        | •                               |
| 用户门户                                   | 品牌打造   | •        | •        | •                               | •        | •        | •                               |
|  | 自定义  | -        | -        | -                               | •        | •        | •                               |
|  | 本地化  | •        | •        | •                               | •        | •        | •                               |
|  | 用户定义的书签  | •        | •        | •                               | •        | •        | •                               |
|  | 自定义 URL 支持   | •        | •        | •                               | •        | •        | •                               |
| SaaS 应用程序支持                            | -  | -        | -        | •                               | •        | •        |                                 |
| 安全                                     | FIPS 140-2   | -        | -        | -                               | •        | •        | -                               |
|  | ICSA SSL-TLS                                       | •        | •        | •                               | •        | •        | •                               |
|  | Suite B 密码   | -        | -        | -                               | •        | •        | •                               |
|  | 动态 EPC 询问  | •        | •        | •                               | •        | •        | •                               |
|  | 基于角色的访问控制 (RBAC)                                   | -        | -        | -                               | •        | •        | •                               |
|  | 端点注册   | •        | •        | •                               | •        | •        | •                               |
|  | 安全文件共享 (Capture ATP)                               | •        | •        | •                               | •        | •        | •                               |
|  | 端点隔离   | •        | •        | •                               | •        | •        | •                               |
|  | OSCP CRL 验证  | -        | -        | -                               | •        | •        | •                               |
|  | 密码选择   | -        | -        | -                               | •        | •        | •                               |
|  | PKI 和客户端证书   | •        | •        | •                               | •        | •        | •                               |
|  | Geo IP 筛选器   | •        | •        | •                               | -        | -        | -                               |
| 僵尸网络筛选器                                | •  | •        | •        | -                               | -        | -        |                                 |
| 正向代理                                   | •  | •        | •        | •                               | •        | •        |                                 |
| 反向代理                                   | •  | •        | •        | •                               | •        | •        |                                 |
| 身份验证和身份服务                              | SAML 2.0   | -        | -        | -                               | •        | •        | •                               |
|  | LDAP、RADIUS  | •        | •        | •                               | •        | •        | •                               |
|  | Kerberos (KDC)                                     | •        | •        | •                               | •        | •        | •                               |
|  | NTLM   | •        | •        | •                               | •        | •        | •                               |
|  | SAML 标识提供程序 (IdP)                                  | •        | •        | •                               | •        | •        | •                               |
|  | 生物识别设备支持   | •        | •        | •                               | •        | •        | •                               |
|  | 针对 iOS 的 Face ID 支持                                | •        | •        | •                               | •        | •        | •                               |
|  | 双因素身份验证 (2FA)                                      | •        | •        | •                               | •        | •        | •                               |
| 多因素身份验证 (MFA)                          | -  | -        | -        | •                               | •        | •        |                                 |



功能摘要 (按型号比较 [续])

| 类别                | 功能                             | 210 | 410 | 500v | 6210 | 7210 | 8200v |
|-------------------|--------------------------------|-----|-----|------|------|------|-------|
| 身份验证和身份服务 (续)     | 链式身份验证                         | -   | -   | -    | •    | •    | •     |
|                   | 通过电子邮件或短信发送一次性密码 (OTP)         | •   | •   | •    | •    | •    | •     |
|                   | 通用访问卡 (CAC) 支持                 | -   | -   | -    | •    | •    | •     |
|                   | X.509 证书支持                     | •   | •   | •    | •    | •    | •     |
|                   | 验证码集成                          | -   | -   | -    | •    | •    | •     |
|                   | 远程密码更改                         | •   | •   | •    | •    | •    | •     |
|                   | 基于表单的 SSO                      | •   | •   | •    | •    | •    | •     |
|                   | 联合 SSO                         | -   | -   | -    | •    | •    | •     |
|                   | 会话持久性                          | -   | -   | -    | •    | •    | •     |
| 自动登录              | •                              | •   | •   | •    | •    | •    |       |
| 访问控制              | 组 AD                           | •   | •   | •    | •    | •    | •     |
|                   | LDAP 属性                        | •   | •   | •    | •    | •    | •     |
|                   | 地理位置策略                         | •   | •   | •    | -    | -    | -     |
|                   | 持续端点监控                         | •   | •   | •    | •    | •    | •     |
| 管理                | 管理接口 (以太网)                     | -   | -   | -    | •    | •    | •     |
|                   | 管理接口 (控制台)                     | -   | -   | -    | •    | •    | •     |
|                   | HTTPS 管理                       | •   | •   | •    | •    | •    | •     |
|                   | SSH 管理                         | -   | -   | -    | •    | •    | •     |
|                   | SNMP MIBS                      | •   | •   | •    | •    | •    | •     |
|                   | Syslog 和 NTP                   | •   | •   | •    | •    | •    | •     |
|                   | 使用情况监控                         | •   | •   | •    | •    | •    | •     |
|                   | 配置回滚                           | •   | •   | •    | •    | •    | •     |
|                   | 集中化管理                          | -   | -   | -    | •    | •    | •     |
|                   | 集中化报告                          | -   | -   | -    | •    | •    | •     |
|                   | 管理 REST API                    | -   | -   | -    | •    | •    | •     |
|                   | 身份验证 REST API                  | -   | -   | -    | •    | •    | •     |
|                   | RADIUS 会计                      | -   | -   | -    | •    | •    | •     |
|                   | 计划的任务                          | -   | -   | -    | •    | •    | •     |
| 集中化会话许可           | -                              | -   | -   | •    | •    | •    |       |
| 事件驱动的审计           | -                              | -   | -   | •    | •    | •    |       |
| 联网                | IPv6                           | •   | •   | •    | •    | •    | •     |
|                   | 全局负载均衡                         | -   | -   | -    | •    | •    | •     |
|                   | 服务器负载均衡                        | •   | •   | •    | -    | -    | -     |
|                   | TCP 状态复制                       | •   | •   | •    | •    | •    | •     |
|                   | 集群状态故障转移                       | -   | -   | -    | •    | •    | •     |
|                   | 主动/被动高可用性                      | -   | •   | •    | •    | •    | •     |
|                   | 主动/主动高可用性                      | -   | -   | -    | •    | •    | •     |
|                   | 横向可扩展性                         | -   | -   | -    | •    | •    | •     |
|                   | 单个或多个 FQDN                     | -   | -   | -    | •    | •    | •     |
| 层 3-7 智能隧道代理      | •                              | •   | •   | •    | •    | •    |       |
| 层 7 应用程序代理        | •                              | •   | •   | •    | •    | •    |       |
| 集成                | 2FA TOTP 支持                    | •   | •   | •    | •    | •    | •     |
|                   | EMM 和 MDM 产品支持                 | -   | -   | -    | •    | •    | •     |
|                   | SIEM 产品支持                      | -   | -   | -    | •    | •    | •     |
|                   | TPAM 密码库                       | -   | -   | -    | •    | •    | •     |
|                   | ESX 虚拟机监控程序支持                  | -   | -   | •    | -    | -    | •     |
| Hyper-V 虚拟机监控程序支持 | -                              | -   | •   | -    | -    | •    |       |
| 许可选项              | 基于订阅的许可证                       | -   | -   | -    | •    | •    | •     |
|                   | 永久性许可证与支持                      | •   | •   | •    | •    | •    | •     |
|                   | Web Application Firewall (WAF) | •   | •   | •    | -    | -    | -     |
|                   | 峰值许可                           | •   | •   | •    | •    | •    | •     |
|                   | 分层许可                           | -   | -   | -    | •    | •    | •     |
| 虚拟协助              | •                              | •   | •   | -    | -    | -    |       |

\* 要了解有关 VPN 客户端的更多信息, 请访问: <https://www.sonicwall.com/en-us/products/remote-access/vpn-client>

## 升级到高端设备的好处

性能更高 | 吞吐量更大 | 高级功能 | 可扩展性更强

## 设备规格

从一系列特定用途的安全移动访问 (SMA) 设备中进行选择。利用虚拟和物理设备实现灵活的部署选项。



### 物理设备规格

| 性能                          | SMA 210                                      | SMA 410                                      | SMA 6210                                      | SMA 7210                                       |
|-----------------------------|--|--|---|--|
| 并行会话/用户                     | 最多 50  | 最多 250                                       | 最多 2,000                                      | 最多 10,000                                      |
| SSL VPN 吞吐量* (最大 CCU 时)     | 560 Mbps                                     | 844 Mbps                                     | 最高 800 Mbps                                   | 最高 5.0 Gbps                                    |
| 外形规格                        | 1U   | 1U   | 1U  | 1U   |
| 尺寸                          | 16.92 x 10.23 x 1.75 in<br>(43 x 26 x 4.5cm) | 16.92 x 10.23 x 1.75 in<br>(43 x 26 x 4.5cm) | 17.0 x 16.5 x 1.75 in<br>(43 x 41.5 x 4.5 cm) | 17.0 x 16.5 x 1.75 in<br>(43 x 41.5 x 4.5 cm)  |
| 设备重量                        | 11 lb (5 kg)                                 | 11 lb (5 kg)                                 | 17.7 lb (8 kg)                                | 18.3 lb (8.3 kg)                               |
| 加密数据加速 (AES-NI)             | 否  | 否  | 是   | 是  |
| 专用管理端口                      | 否  | 否  | 是   | 是  |
| SSL 加速                      | 否  | 否  | 是   | 是  |
| 存储                          | 4GB (闪存)                                     | 4GB (闪存)                                     | 2 x 1TB SATA; RAID 1                          | 2 x 1TB SATA; RAID 1                           |
| 接口                          | (2) GB 以太网, (2) USB, (1) 控制台                 | (4) GB 以太网, (2) USB, (1) 控制台                 | (6)-端口 1GE, (2) USB, (1) 控制台                  | (6)-端口 1GE, (2)-端口 10Gb SFP+, (2) USB, (1) 控制台 |
| 内存                          | 4GB  | 8GB  | 8GB DDR4                                      | 16GB DDR4                                      |
| TPM 芯片                      | 否  | 否  | 是   | 是  |
| 处理器                         | 4 核  | 8 核  | 4 核   | 4 核  |
| MTBF (@ 25°C 或 77°F), 以小时计算 | 61,815                                       | 60,151                                       | 70,127  | 129,601  |
| 运营与合规                       | SMA 210                                      | SMA 410                                      | SMA 6210                                      | SMA 7210                                       |
| 电源                          | 固定电源   | 固定电源   | 固定电源  | 双电源, 可热插拔                                      |
| 输入额定值                       | 100-240VAC, 50-60MHz                         | 100-240VAC, 50-60MHz                         | 100-240 VAC, 1.1 A                            | 100-240 VAC, 1.79 A                            |
| 功耗                          | 26.9 W                                       | 31.9 W                                       | 77 W  | 114 W  |
| 总散热                         | 92 BTU                                       | 109 BTU                                      | 264 BTU                                       | 389 BTU  |
| 环境                          | WEEE、欧盟 RoHS、中国 RoHS                         |  |   |  |
| 非运行冲击                       | 110 g, 2 msec                                |  |   |  |
| 排放                          | FCC、ICES、CE、C-Tick、VCCI; MIC                 |  |   |  |
| 安全                          | TUV/GS、UL、CE PSB、CCC、BSMI、CB 方案              |  |   |  |
| 工作温度                        | 0°C 至 40°C (32°F 至 104° F)                   |  |   |  |
| FIPS 认证                     | 否  | 否  | FIPS 140-2 二级, 带防篡改保护                         |  |

\* 吞吐量性能可能会因部署和连接而异。公布的数字基于内部实验室条件

### 虚拟设备规格

| 规格                      | SMA 500v (ESX/ESXi/Hyper-V) | SMA 8200v (ESX/ESXi/Hyper-V) |
|-------------------------|-----------------------------|------------------------------|
| 并行会话                    | 最多 250 个用户                  | 最多 5,000                     |
| SSL-VPN 吞吐量* (最大 CCU 时) | 最高 186 Mbps                 | 最高 1.58 Gbps                 |
| 分配的内存                   | 2 GB                        | 8 GB                         |
| 处理器                     | 1 核                         | 4 核                          |
| SSL 加速                  | 否                           | 是                            |
| 应用的磁盘大小                 | 2 GB                        | 64 GB (默认)                   |
| 已安装操作系统                 | Linux                       | 加固 Linux                     |
| 专用管理端口                  | 否                           | 是                            |

\* 吞吐量性能可能会因部署和连接而异。公布的数字基于内部实验室条件。在 Windows Server 2016 上运行 SMA OS 12.1 时, Hyper-V 上的 SMA 8200v 最多可扩展到 5,000 个并行会话, 并提供高达 1.58 Gbps SSL-VPN 吞吐量

订购信息

| SKU                           | SONICWALL SECURE MOBILE ACCESS (SMA) 设备                 |
|-------------------------------|---|
| 02-SSC-2800                   | SMA 210, 带 5 个用户许可证                                     |
| 02-SSC-2801                   | SMA 410, 带 25 个用户许可证                                    |
| 01-SSC-8469                   | SMA 500v, 带 5 个用户许可证                                    |
| 02-SSC-0978                   | SMA 7210, 带管理员测试许可证                                     |
| 02-SSC-0976                   | SMA 6210, 带管理员测试许可证                                     |
| 01-SSC-8468                   | SMA 8200v (虚拟设备)  |
| SKU                           | SONICWALL SMA 用户许可证                                     |
| 01-SSC-9182                   | SMA 500V 增加 5 个用户 (也适用于 SMA 210)                        |
| 01-SSC-2414                   | SMA 500V 增加 100 个用户 (也适用于 SMA 410)                      |
| 01-SSC-7856                   | SMA 5 个用户许可证 - 可堆叠用于 6210、7210、8200v                    |
| 01-SSC-7860                   | SMA 100 个用户许可证 - 可堆叠用于 6210、7210、8200v                  |
| 01-SSC-7865                   | SMA 5,000 个用户许可证 - 可堆叠用于 7210、8200v                     |
| SKU                           | SONICWALL SMA 支持合同                                      |
| 01-SSC-9191                   | 为 SMA 500V 最多 25 个用户提供 1 年全天候支持 (也适用于 SMA 210 和 410)    |
| 01-SSC-2326                   | 为 SMA 6210 的 100 个用户提供 1 年全天候支持 - 可堆叠                   |
| 01-SSC-2350                   | 为 SMA 7210 的 500 个用户提供 1 年全天候支持 - 可堆叠                   |
| 01-SSC-8434                   | 为 SMA 8200V 的 5 个用户提供 1 年全天候支持 (也适用于 SMA 6210、7210)     |
| 01-SSC-8446                   | 为 SMA 8200V 的 100 个用户提供 1 年全天候支持 (也适用于 SMA 6210、7210)   |
| 01-SSC-7913                   | 为 SMA 8200V 的 5,000 个用户提供 1 年全天候支持 (也适用于 SMA 6210、7210) |
| SKU                           | 针对 6210、7210、8200V 的中央管理                                |
| <b>CMS 设备许可证</b>              |   |
| 01-SSC-8535                   | CMS 基本 + 3 个设备许可证 (免费 - 试用版和与订阅用户许可证一起使用)               |
| 01-SSC-8536                   | CMS 100 设备许可证 1 年 (用于与订阅用户许可证一起使用)                      |
| 01-SSC-3369                   | CMS 基本 + 3 个设备许可证 (免费 - 与永久性用户许可证一起使用)                  |
| 01-SSC-3402                   | CMS 100 设备许可证 1 年 (与永久性用户许可证一起使用)                       |
| <b>中央用户许可证 (订阅)</b>           |   |
| 01-SSC-2298                   | CMS 共用许可证 10 个用户 1 年                                    |
| 01-SSC-8539                   | CMS 共用许可证 1,000 用户 1 年                                  |
| 01-SSC-5339                   | CMS 共用许可证 50,000 个用户 1 年                                |
| <b>中央用户许可证 (永久性)</b>          |   |
| 01-SSC-2053                   | CMS 永久性许可证 10 个用户                                       |
| 01-SSC-2058                   | CMS 永久性许可证 1,000 个用户                                    |
| 01-SSC-2063                   | CMS 永久性许可证 50,000 个用户                                   |
| <b>支持中央用户许可证 (永久性)</b>        |   |
| 01-SSC-2065                   | CMS 全天候支持 1 年 10 个用户                                    |
| 01-SSC-2070                   | CMS 全天候支持 1 年 1,000 个用户                                 |
| 01-SSC-2075                   | CMS 全天候支持 1 年 50,000 个用户                                |
| <b>中央 ActiveSync 许可证 (订阅)</b> |   |
| 01-SSC-2088                   | CMS 共用电子邮件许可证 10 个用户 1 年                                |
| 01-SSC-2093                   | CMS 共用电子邮件许可证 1,000 个用户 1 年                             |
| 01-SSC-2087                   | CMS 共用电子邮件许可证 50,000 个用户 1 年                            |

订购信息 (续)

| SKU                      | 针对 6210、7210、8200V 的中央管理                                   |
|--------------------------|--|
| <b>中央峰值许可证</b>           |  |
| 01-SSC-2111              | CMS 峰值 1,000 个用户 5 天                                       |
| 01-SSC-2115              | CMS 峰值 50,000 个用户 5 天                                      |
| <b>Capture 外接程序 (订阅)</b> |  |
| 联系您的经销商                  |  |
| * 订阅许可证包括全天候支持           |  |
| SKU                      | SONICWALL SMA 外接程序   |
| 01-SSC-2406              | SMA 7210 FIPS 外接程序   |
| 01-SSC-2405              | SMA 6210 FIPS 外接程序   |
| 01-SSC-9185              | SMA 500V Web Application Firewall 1 年 (也适用于 SMA 210 和 410) |
| SKU                      | SONICWALL SMA 安全升级   |
| 02-SSC-2794              | SMA 210 安全升级增强版, 5 个用户捆绑包, 全天候支持, 最多支持 25 个用户 1 年          |
| 02-SSC-2795              | SMA 210 安全升级增强版, 5 个用户捆绑包, 全天候支持, 最多支持 25 个用户 3 年          |
| 02-SSC-2798              | SMA 410 安全升级增强版, 25 个用户捆绑包, 全天候支持, 最多支持 100 个用户 1 年        |
| 02-SSC-2799              | SMA 410 安全升级增强版, 25 个用户捆绑包, 全天候支持, 最多支持 100 个用户 3 年        |
| 02-SSC-2893              | SMA 6210 安全升级增强版, 全天候支持, 最多支持 100 个用户 1 年                  |
| 02-SSC-2894              | SMA 6210 安全升级增强版, 全天候支持, 最多支持 100 个用户 3 年                  |
| 02-SSC-2895              | SMA 7210 安全升级增强版, 全天候支持, 最多支持 250 个用户 1 年                  |
| 02-SSC-2896              | SMA 7210 安全升级增强版, 全天候支持, 最多支持 250 个用户 3 年                  |
| 02-SSC-0860              | SMA 8200V 安全升级增强版, 全天候支持, 最多支持 100 个用户 1 年                 |
| 02-SSC-0862              | SMA 8200V 安全升级增强版, 全天候支持, 最多支持 100 个用户 3 年                 |
| 02-SSC-2807              | SMA 500V 安全升级增强版, 全天候支持, 最多支持 100 个用户 1 年                  |
| 02-SSC-2808              | SMA 500V 安全升级增强版, 全天候支持, 最多支持 100 个用户 3 年                  |
| SKU                      | SMA 的峰值许可证 (达到容量所需的增量)                                     |
| 01-SSC-2240              | SMA 210 10 天 50 个用户峰值许可证 (也适用于 SMA 410 和 500v)             |
| 01-SSC-7873              | SMA 8200v 10 天 5-2,500 个用户峰值许可证 (也适用于 SMA 6210、7210)       |
| 02-SSC-4490              | SMA 500V 30 天 250 个用户峰值许可证                                 |
| 02-SSC-4489              | SMA 500V 60 天 250 个用户峰值许可证                                 |
| 02-SSC-4488              | SMA 200/210 30 天 50 个用户峰值许可证                               |
| 02-SSC-4487              | SMA 200/210 60 天 50 个用户峰值许可证                               |
| 02-SSC-4486              | SMA 400/410 30 天 250 个用户峰值许可证                              |
| 02-SSC-4485              | SMA 400/410 60 天 250 个用户峰值许可证                              |
| 02-SSC-4471              | SMA CMS 峰值外接程序许可证 100 个用户 30 天                             |
| 02-SSC-4473              | SMA CMS 峰值外接程序许可证 500 个用户 30 天                             |
| 02-SSC-4475              | SMA CMS 峰值外接程序许可证 1,000 个用户 30 天                           |
| 02-SSC-4477              | SMA CMS 峰值外接程序许可证 5,000 个用户 30 天                           |
| 02-SSC-4479              | SMA CMS 峰值外接程序许可证 10,000 个用户 30 天                          |
| 02-SSC-4481              | SMA CMS 峰值外接程序许可证 25,000 个用户 30 天                          |
| 02-SSC-4483              | SMA CMS 峰值外接程序许可证 50,000 个用户 30 天                          |
| 02-SSC-4472              | SMA CMS 峰值外接程序许可证 100 个用户 60 天                             |
| 02-SSC-4474              | SMA CMS 峰值外接程序许可证 500 个用户 60 天                             |
| 02-SSC-4476              | SMA CMS 峰值外接程序许可证 1,000 个用户 60 天                           |

## 订购信息 (续)

| SKU         | SMA 的峰值许可证 (达到容量所需的增量)            |
|-------------|-----------------------------------|
| 02-SSC-4478 | SMA CMS 峰值外接程序许可证 5,000 个用户 60 天  |
| 02-SSC-4480 | SMA CMS 峰值外接程序许可证 10,000 个用户 60 天 |
| 02-SSC-4482 | SMA CMS 峰值外接程序许可证 25,000 个用户 60 天 |
| 02-SSC-4484 | SMA CMS 峰值外接程序许可证 50,000 个用户 60 天 |

\* 还提供多年 SKU 和支持合同。有关 SKU 的完整列表, 请联系您的经销商或销售人员。

### 合作伙伴支持服务

需要帮助规划、部署或优化 SonicWall 解决方案吗? SonicWall 高级服务合作伙伴接受过培训, 可为您提供世界一流的专业服务。详情请访问 [www.sonicwall.com/PES](http://www.sonicwall.com/PES)。

### 关于 SonicWall

SonicWall 已经致力于打击网络犯罪超过 27 年, 为全世界的中小企业、公司和政府机构提供防护。在 SonicWall Capture Labs 研究的支持下, 我们备受赞誉的实时漏洞检测和预防解决方案在超过 215 个国家和地区确保了超过一百万个网络及其电子邮件、应用程序和数据的安全。这些组织的运作效率更高, 对安全的担忧也更少。有关更多信息, 请访问 [www.sonicwall.com](http://www.sonicwall.com) 或在 [Twitter](#)、[领英](#)、[Facebook](#) 和 [Instagram](#) 上关注我们。