SONICWALL

SONICWALL SECURE MOBILE ACCESS (SMA)

基於用戶和設備身份、位置和信任，隨時隨地安全訪問跨多重雲環境的公司資源。

SonicWall SMA是一個統一安全訪問網關，可以使組織能夠隨時隨地從任何設備訪問關鍵任務型企業資源。SMA實施精細訪問控制策略引擎、情境感知設備身份認證、應用程序級別VPN和采用單點登錄的高級身份驗證，使組織能夠在多重雲環境中采用BYOD（自帶設備）和移動設備。

移動設備和BYOD（自帶設備）

對於希望采用BYOD（自帶設備）、靈活工作或第三方訪問的組織，SMA成為它們之間的關鍵強制實施點。SMA提供一流的安全性，以最大程度地減少表面威脅，同時通過支持最新的加密算法和密碼，確保組織更安全。SonicWall的SMA允許管理員提供安全的移動訪問和基於身份的權限，以便最終用戶可以快速、簡單地訪問所需的業務應用程序、數據和資源。同時，組織可以制定安全的BYOD（自帶設備）策略，以保護其公司網絡和數據免受惡意訪問和惡意軟件的攻擊。

遷移到雲

對於開始進行雲遷移之旅的組織，SMA提供了單點登錄(SSO)基礎設施，使用單個Web門戶在混合IT環境中對用戶進行身份驗證。無論公司資源是內部、在Web上還是在托管雲中，訪問體驗都一致且流暢。SMA還集成了行業領先的多因素身份驗證技術，以增強安全性。

托管服務提供商

無論是托管自有基礎設施的組織還是托管服務提供商，SMA提供統包解決方案，均可實現高度的業務連續性和可擴展性。SMA可以在單個設備上支持多達20,000個並行連接，並可以通過智能集群擴展成千上萬的用戶。數據中心可通過主動-主動集群和內置的動態負載平衡器降低成本，根據用戶需求將全局流量實時重新分配給最優化的數據中心。SMA工具集使服務提供商能夠在零停機時間內交付服務，從而使他們能夠履行非常積極的服務級別協議(SLA)。

SMA使IT部門能夠根據用戶情景，提供最佳體驗和最安全的訪問。SMA既可以作為增強的物理設備，也可以作為功能強大的虛擬設備使用，均可無縫地與現有的內部和/或雲基礎設施配合。組織可以為第三方或個人擁有的設備上的員工選擇一系列完全沒有客戶端的基於Web的安全訪問，也可以為所有設備類型的管理人員選擇更為傳統的基於客戶端的全隧道VPN訪問。無論是組織需要從單個位置向五個用戶提供可靠的安全訪問，還是跨全球分布的網絡擴展到數千個用戶，SonicWall SMA都可以提供解決方案。

SonicWall SMA使組織能夠放心地采用移動設備和BYOD（自帶設備），並輕松地遷移到雲中。SMA賦予員工力量，並為他們提供一致的訪問體驗。

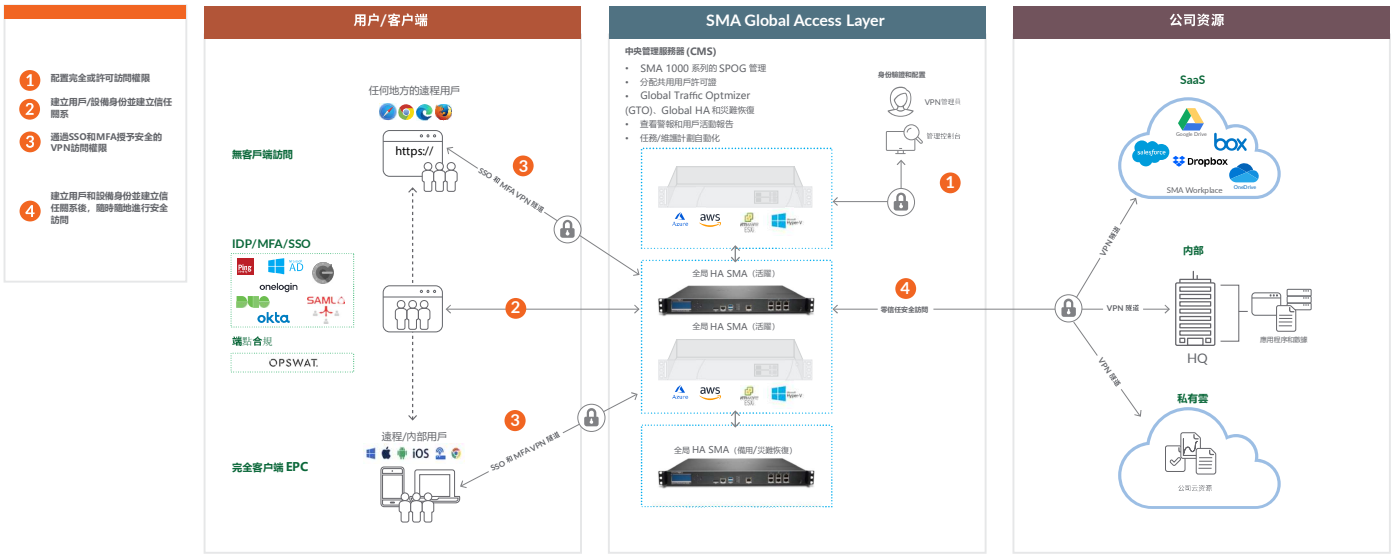
好處：

- 統一訪問所有網絡和雲資源，實現“任何時間、任何設備、任何應用程序”的安全訪問
- 利用穩健的訪問控制引擎定義精細策略，控制誰可以訪問哪些資源
- 通過使用單個URL向任何SaaS或本地托管應用程序提供聯合單點登錄，提高生產效率
- 通過在混合IT環境中整合基礎設施組件，降低總體擁有成本(TCO)並降低訪問管理的覆雜性
- 了解每個連接設備，並根據策略和端點的運行狀況授予訪問權限
- 使用CaptureATP沙箱掃描上傳到網絡中的所有文件，防止惡意軟件入侵
- 防範基於Web的攻擊，並提供與Web Application Firewall外接程序的PCI兼容性
- 利用GeoIP檢測和僵屍網絡防護防範DDoS和僵屍攻擊
- 使用基於Web瀏覽器的無客戶端HTML5訪問獲得安全保證的本機代理功能，而無需在端點設備上安裝和維護代理的開銷
- 借助實時監控和綜合報告，獲得制定明智決策所需的切實可行的洞察
- 在ESXi或Hyper-V上的私有雲中或在AWS或Microsof Azure公共雲環境中，部署為物理設備或虛擬設備。
- 支持根據實時需求動態頒发訪問許可證，並自動將端點定向到性能最高、延遲最低的連接
- 利用內置的負載平衡而無需額外的硬件或服務，從而降低前期成本，同時為設備故障轉移提供零用戶影響
- 可立即擴展容量，確保不受業務中斷或季節性高峰的影響

SMA 部署

增強的邊界網關，可隨時隨地從任何設備進行安全訪問

SMA提供對跨企業內部、雲和混合數據中心托管的公司資源的全面端到端安全遠程訪問。它應用基於身份的按策略強制實施的訪問控制、情境感知設備身份驗證和應用程序級別VPN，在建立用戶和設備身份、位置和信任之後，授予對數據、資源和應用程序的訪問權限。在ESXi或Hyper-V上的私有雲中或在AWS或Microsof Azure公共雲環境中，靈活部署為增強的Linux設備或虛擬設備。



SMA雲/內部部署

採用物理和虛擬設備進行靈活部署

SonicWall SMA可以部署為增強的高性能設備，也可以部署為虛擬設備，利用共享計算資源來優化利用率、簡化遷移並降低投資成本。硬件設備建立在多核體系結構之上，通過SSL加速、VPN吞吐量和強大的代理提供高性能，從而提供穩健的安全訪問。對於監管機構和聯邦機構，SMA還具有FIPS140-2二級認證。SMA虛擬設備在主要虛擬或雲平台（包括，Microsof Hyper-V、VMware ESX和AWS）上提供同樣強健的安全訪問功能。

跨設備分享用戶許可證

設備跨全球分布的組織可以從由於時間差導致的用戶許可證需求波動中受益。無論組織是部署完全VPN許可證還是基本ActveSync許可證，SMA的中央管理服務器都會將許可證重新分配給受管理的設備，不同地理區域的用戶對設備的需求已經達到頂峰，但由於非工作時間/夜間時間的原因，使用量有所下降。

情境感知設備的網絡可見性剖析

一流的情境感知身份驗證僅授予對受信任的設備和授權用戶的訪問權限。還會詢問筆記本電腦和PC是否存在安全軟件、客戶端證書和設備ID。在授予訪問權限之前，會詢問移動設備以獲取必需的安全信息，例如，越獄或root狀態、設備ID、證書狀態和操作系統版本。不允許不符合策略要求的設備訪問網絡，並且會通知用戶不合規情況。

單一Web門戶提供一致的體驗

用戶不需要記住所有單個應用程序URL並維護詳盡的書簽。SMA提供一個集中化訪問門戶，為用戶提供一個URL來從標準Web瀏覽器訪問所有關鍵任務型應用程序。用戶通過瀏覽器登錄後，瀏覽器窗口中會顯示一個可自定義的Web用戶門戶，提供單一玻璃視圖窗格來訪問任何SaaS或本地應用程序。門戶僅顯示與特定終端設備、用戶或組相關的鏈接和個性化書簽。該門戶與平台無關，並且支持所有主要設備平台，包括Windows、Mac OS、Linux、iOS和Android設備，並在所有這些設備上提供廣泛的瀏覽器支持。

在SaaS和本地應用程序兩者上聯合單點登錄

不再需要多個密碼，並停止使用不良的安全做法，如密碼重用。SMA為雲托管的SaaS應用程序和園區托管的應用程序提供聯合SSO。SMA與多種身份驗證、授權和計費服務器以及領先的多因素身份驗證技術集成，以增強安全性。SMA在檢查端點運行狀況狀態和合規性之後，才會將安全SSO交付給已授權的端點設備。訪問策略引擎可確保用戶僅能查看授權的應用程序，並在成功進行身份驗證後授予訪問權限。該解決方案即使在使用VPN

客戶端時也支持聯合 SSO，無論使用基於客戶端的安全訪問還是通過無客戶端的安全訪問，都可以為客戶提供無縫的身份驗證體驗。

防止違規和高級威脅

SonicWall SMA添加了一層訪問安全性，以改善您的安全狀況並減少威脅的影響範圍。

- SMA與SonicWall Capture ATP基於雲的多引擎沙盒集成，可掃描用戶利用非管理的端點上傳的所有文件或公司網絡外部用戶上傳的所有文件。這樣可以確保用戶在旅途中與在辦公室中一樣擁有相同級別的保護，免受勒索軟件或零日惡意軟件等高級威脅的侵害[1]。

- SonicWall Web Applicaton Firewall服務為企業提供了經濟實惠、良好集成的解決方案，以保護內部基於Web的應用程序。這使得客戶能夠確保數據的機密性，並且如果存在惡意或欺詐的經過驗證的用戶訪問，內部Web服務也不會受到損害。

- Geo-IP和僵屍網絡檢測可保護組織免受DDoS和僵屍攻擊，並防止遭到攻擊的端點成為僵屍網絡。

基於瀏覽器的無縫、安全的無客戶端訪問

SonicWall SMA的“無客戶端”性質意味著管理員無需將胖客戶端組件手動安裝到將用於遠程訪問的計算機上。這消除了對Java的依賴性和IT開銷，從而大大擴展了遠程訪問的概念。這意味著，由於不需要預先安裝或預先配置，授權的遠程員工可以在世界上任何地方，利用任何一台計算機，安全地訪問他們的公司資源。安全訪問用這種最簡單的方式，使用HTML5，並嚴格基於瀏覽器，從而為用戶提供無縫和統一的體驗。

提供“永遠在線”的體驗

為了提供無縫的用戶體驗，SMA為受管Windows設備提供“永遠在線”的VPN。管理員可以配置設置，以便在授權端點客戶端檢測到公用或不受信任的網絡時自動建立VPN連接。Windows設備的單一登錄事件為用戶提供與公司資源的安全連接。用戶不必登錄其VPN客戶端或維護其他密碼。這為移動用戶提供了無縫體驗，使他們能夠像在辦公室一樣訪問關鍵任務型資源，並使IT管理員能夠保持對托管設備的控制，從而改善組織的安全狀況。

直觀的管理和全面的報告

SonicWall提供一個基於Web的直觀管理平台 Central Management Server (CMS)，可簡化設備管理，同時提供廣泛的報告功能。GUI易於使用，使管理單個或多個設備和策略更加清晰。每個頁面顯示如何在所有受管理的機器上配置設置。統一策略管理可幫助您創建和監控訪問策略和配置。單個策略可以控制從您的用戶、設備和應用程序對數據、服務器和網絡的訪問。IT部門可以實現例行任務自動化並安排活動，使安全團隊從重覆性任務中解放出來，專注於諸如事件響應等戰略性安全任務。借助易於使用的報告和集中化日志記錄，IT部門可以洞察用戶訪問趨勢和系統範圍的運行狀況。

提供全天候服務可用性

組織要求維護其服務並以高度的可靠性使其正常運行，以便隨時提供對關鍵任務型應用程序的安全訪問。SMA設備為使用單個數據中心的組織提供傳統的主動-被動高可用性(HA)，或為本地或分布式數據中心提供具有主動-主動或主動-備用集群的全局HA。這兩種HA模型均可為用戶提供無障礙體驗，實現零影響的故障轉移和會話持續性。

部署適合您需求的VPN客戶端

從廣泛的VPN客戶端中進行選擇，為各種端點（包括筆記本電腦、智能手機和平板電腦）提供按策略強制實施的安全遠程訪問。

VPN 客戶端	支持的操作系統	支持的 SMA 型號	關鍵亮點
Mobile Connect	iOS、OS X、Android、Chrome OS、Windows 10	全部型號	提供生物身份驗證、按應用程序VPN和端點控制強制實施
Connect Tunnel（瘦客户端）	Windows、Mac OS 和 Linux	6200、6210、7200、7210、8200v、9000	借助穩健的端點控制提供完整的“辦公室”體驗
NetExtender（瘦客户端）	Windows 和 Linux	210、410、500v	實施精細的訪問策略，並通過本機客戶端擴展網絡訪問

使用內置負載平衡器降低前期成本

SMA設備內置的負載平衡功能可實現中型企業和公司部署所需的級別可擴展性。某些SMA設備型號可提供動態負載平衡，以根據需求智能地分配會話負載並實時分配用戶許可證。組織不需要投資外部負載平衡器，從而可減少前期成本。

為不可預見的事件投保

完整的業務連續性和災難恢覆解決方案必須能夠處理遠程訪問流量中的顯著峰值，同時仍保持安全性和成本控制。用於SMA的SonicWall Spike許可證包是附加許可證，使分布式業務可以擴展用戶數量並立即達到最大容量，從而實現無縫的業務連續性。Spike許可證的工作方式類似於保險單，可以應對從當前用戶數到數十個甚至數百個額外用戶的將來任何計劃內或計劃外的峰值。

特色

高級身份驗證

聯合單點登錄[2]	SMA使用SAML2.0身份驗證，通過單一門戶啟用對內部和雲資源的聯合SSO，同時強制實施堆疊式多因素身份驗證以增強安全性。
多因素身份驗證	X.509數字證書 服務器端和客戶端數字證書 RSA SecurID、Dell Defender、Google Authentcator、Duo Security和其他一次性密碼/雙因素身份驗證令牌 通用訪問卡(CAC)雙因素或堆疊身份驗證 驗證碼支持，用戶名/密碼
SAML身份驗證	可以將SMA配置為SAML Identty Provider (IdP)、SAML Service Provider (SP)或代理現有的on-prem IdP，從而使用SAML 2.0身份驗證啟用聯合單點登錄(SSO)。
身份驗證存儲庫	SMA提供與行業標準存儲庫的簡單集成，便於管理用戶帳戶和密碼。 可以基於RADIUS、LDAP或Actve Directory身份驗證存儲庫（包括嵌套組）動態填充用戶組。可以詢問通用或自定義LDAP屬性，以進行特定的授權或設備注冊驗證。
層3-7應用程序代理	SMA提供靈活的代理選項，例如，可以通過直接代理提供供應商訪問，通過反向代理提供合同工訪問，以及通過ActveSync提供員工對Exchange的訪問。
反向代理	實施身份驗證的增強型反向代理服務使管理員可以配置應用程序卸載門戶和書簽，從而允許用戶無縫連接到遠程應用程序和資源，包括RDP和HTTP。此功能支持所有瀏覽器，包括IE、Chrome和Firefox。
Kerberos約束委派	SMA使用現有的Kerberos基礎設施提供身份驗證支持，不需要信任前端服務即可委派服務。

訪問管理

訪問控制引擎(ACE)	管理員根據組織策略授予或拒絕訪問權限，並在隔離會話時設置修正操作。ACE基於對象的策略利用網絡、資源、身份、設備、應用程序、數據和時間等元素。
端點控制(EPC)	EPC允許管理員根據連接設備的運行狀況強制實施精細的訪問控制規則。借助深度操作系統集成，許多元素被組合起來進行類型分類和風險因素評估。EPC詢問使用針對Windows、Mac和Linux平台的防病毒、個人防火墻和防間諜軟件解決方案的預定義全面列表（包括簽名文件更新的版本和適用性），簡化了設備配置文件的設置。
應用程序訪問控制(AAC)	管理員可以定義允許哪些特定的移動應用程序通過單個應用程序隧道訪問網絡上的哪些資源。客戶端和服務器上均強制實施AAC策略，從而提供穩健的外圍保護。

卓越的安全性

层 3 SSL VPN	SMA系列為在任何環境中運行的各種客戶端設備提供高性能層3隧道功能。
加密支持	可配置會話長度 密碼：AES 128 + 256位、三重DES、RC4 128 位哈希：SHA-256 橢圓曲線數字簽名算法(ECDSA)
高級密碼支持	SMA設備使用默認配置密碼，提供強大的開箱即用安全機制，滿足合規性，管理員可以進一步改進性能、安全強度或兼容性。
安全認證	通過FIPS 140-2二級認證、ICSA SSL-TLS認證，正在進行通用標準UC-APL認證
安全文件共享	阻止未知的零日攻擊，如在網關處阻止勒索軟件，並進行自動修正。通過可安全訪問公司網絡的非托管端點上傳的文件將由我們基於雲的多引擎Capture ATP檢查。
Web Application Firewall (WAF)	防止基於協議和Web的攻擊，幫助金融、醫療、電子商務和其他企業滿足OWASP Top 10（OWASP前十大安全風險）和PCI合規性。
Geo IP檢測和僵屍網絡保護	Geo IP檢測和僵屍網絡保護為客戶提供了一種機制，可以允許或限制用戶從不同地理位置訪問。
TLS 1.3 支持	改進了安全和性能，同時與以前版本相比減少了復雜性。

直觀的用戶體驗

“永遠在線”的VPN	從公司发放的Windows設備自動建立與公司網絡的安全連接，以提高安全性、了解流量使用情況並保持合規性
安全網絡檢測(SND)	SMA的網絡感知VPN客戶端可檢測設備何時離開園區，並自動重新連接VPN，當設備返回到受信任的網絡時再次將其關閉。
對資源的無客戶端訪問	SMA通過交付RDP、ICA、VNC、SSH和Telnet協議的HTML5瀏覽器代理，提供對資源的無客戶端安全訪問。
單點登錄門戶	WorkPlace門戶提供易於使用、可自定義的單窗格視圖，可通過單點登錄(SSO)對混合IT環境中的任何資源進行安全訪問。無需其他登錄或VPN。
層3隧道	管理員可以使用SSL/TLS隧道和可選的ESP回退，選擇分離隧道或強制實施全部重定向模式，實現最佳性能。
HTML5文件瀏覽器[1]	現代文件瀏覽器使用戶可以方便地使用任何Web瀏覽器訪問文件共享。
移動操作系統集成	所有操作系統平台均支持Mobile Connect，從而為用戶選擇移動設備提供了充分靈活性。

彈性

Global Traffic Optimizer (GTO)	SMA提供對用戶零影響的全局流量負載平衡。流量被轉到最優化且性能最高的數據中心。
動態高可用性[2]	無論是部署在單個數據中心中還是跨多個地理位置分散的數據中心中，SMA均可支持主動/被動，並提供主動/主動配置以實現高可用性。
通用會話持久性[1]	為用戶提供零影響故障轉移的無障礙體驗。如果設備離線，則SMA的智能集群可重新分配用戶及其會話數據，而無需進行重新身份驗證。
性能可擴展	SMA設備通過部署多個設備，呈指數級擴展性能，從而消除了單點故障。水平集群完全支持混合物理和虛擬SMA設備。
動態許可	用戶許可證不再必須應用於單個SMA設備。可以根據用戶需求在托管設備之間動態地分配和重新分配用戶。

中央管理與監控

中央管理系統 (CMS)	CMS為所有SMA功能提供基於Web的集中化管理。
自定義警報	可以針對生成由任何IT基礎設施網絡管理系統(NMS)監控的SNMP陷阱配置警報。管理員還可以針對Capture ATP文件掃描和磁盤使用情況配置警報，以備立即采取措施。
實時儀表板	IT管理員利用可定制的實時儀表板可以快速輕松地診斷訪問問題，從而為排除故障獲取有價值的洞察。
SIEM 集成	向中央SIEM數據收集器實時輸出方便安全團隊關聯事件驅動的活動，從而了解特定用戶或應用程序的端到端工作流程。這在安全事件管理和取證分析期間至關重要。
調度程序	調度程序使用戶能夠調度維護任務，例如部署策略，覆制配置設置和重新啟動服務，而無需人工幹預

擴展性

管理 API	管理API允許對單個SMA或全局CMS環境中的所有對象進行完全的程序化管理控制。
最終用戶 API	最終用戶API提供對所有登錄、身份驗證和端點工作流程的完全控制。
雙因素身份驗證 (2FA)	SMA通過與基於時間的領先一次性密碼(TOTP)解決方案（例如，GoogleAuthentcator、Microsof Authentcator、Duo security等）集成來交付2FA。
MDM 集成	SMA集成了領先的企業移動管理(EMM)產品（例如，Airwatch和Mobile Iron）。
其他第 3 方集成	SMA與OPSWAT等行業領先的供應商集成，以提供高級威脅防護

[1]適用於*SMA OS 12.1*或更高版

[2]*SMA 12.1*中增強

功能摘要（按型號比較）

類別	功能	210	410	500v	6210	7210	8200v
部署	操作系統	SMA 10.2	SMA 10.2	SMA 10.2	SMA 12.4	SMA 12.4	SMA 12.4
	支持的虛擬機監控程序	–	–	VMware ESXi / Microsoft Hyper-V	–	–	VMware ESXi / Microsoft Hyper-V
	支持的公共雲平台	–	–	AWS/Azure	–	–	AWS/Azure
吞吐量	最大並行用戶會話數	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
客戶端訪問	層3隧道	•	•	•	•	•	•
	分離隧道和全部重定向	•	•	•	•	•	•
	“永遠在線”的VPN	•	•	•	•	•	•
	自動ESP封裝	–	–	–	•	•	•
	HTML5（RDP、VNC、ICA、SSH、Telnet 網絡瀏覽器）	•	•	•	•	•	•
	安全網絡檢測	–	–	–	•	•	•
	文件瀏覽器 (CIFS/NFS)	•	•	•	•	•	•
	Citrix XenDesktop/XenApp	•	•	•	•	•	•
	VMware View	–	–	–	•	•	•
	On Demand Tunnel	–	–	–	•	•	•
	Chrome/Firefox擴展	–	–	–	•	•	•
	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	•	•	•	•	•	•
移動訪問	按應用程序 VPN	–	–	–	•	•	•
	應用程序控制強制實施	–	–	–	•	•	•
	應用程序ID驗證	–	–	–	•	•	•
用戶門戶	品牌打造	•	•	•	•	•	•
	自定義	–	–	–	•	•	•
	本地化	•	•	•	•	•	•
	用戶定義的書簽	•	•	•	•	•	•
	自定義URL支持	•	•	•	•	•	•
	SaaS應用程序支持	–	–	–	•	•	•
安全	FIPS 140-2	–	–	–	•	•	–
	ICSA SSL-TLS	•	•	•	•	•	•
	Suite B 密碼	–	–	–	•	•	•
	動態EPC詢問	•	•	•	•	•	•
	基於角色的訪問控制(RBAC)	–	–	–	•	•	•
	端點注冊	•	•	•	•	•	•
	安全文件共享 (Capture ATP)	•	•	•	•	•	•
	端點隔離	•	•	•	•	•	•
	OSCP CRL 驗證	–	–	–	•	•	•
	密碼選擇	–	–	–	•	•	•
	PKI和客戶端證書	•	•	•	•	•	•
	Geo IP篩選器	•	•	•	–	–	–
	僵屍網絡篩選器	•	•	•	–	–	–
	正向代理	•	•	•	•	•	•
	反向代理	•	•	•	•	•	•
身份驗證和身份服務	SAML 2.0	–	–	–	•	•	•
	LDAP、RADIUS	•	•	•	•	•	•
	Kerberos (KDC)	•	•	•	•	•	•
	NTLM	•	•	•	•	•	•
	SAML 標識提供程序 (IdP)	•	•	•	•	•	•
	生物識別設備支持	•	•	•	•	•	•
	針對iOS 的 Face ID 支持	•	•	•	•	•	•
	雙因素身份驗證 (2FA)	•	•	•	•	•	•
	多因素身份驗證 (MFA)	–	–	–	•	•	•

功能摘要（按型號比較[續]）

類別	功能	210	410	500v	6210	7210	8200v
身份驗證和身份服務（續）	鏈式身份驗證	–	–	–	•	•	•
	通過電子郵件或短信发送一次性密碼 (OTP)	•	•	•	•	•	•
	通用訪問卡 (CAC) 支持	–	–	–	•	•	•
	X.509 證書支持	•	•	•	•	•	•
	驗證碼集成	–	–	–	•	•	•
	遠程密碼更改	•	•	•	•	•	•
	基於表單的 SSO	•	•	•	•	•	•
	聯合 SSO	–	–	–	•	•	•
	會話持久性	–	–	–	•	•	•
	自動登錄	•	•	•	•	•	•
訪問控制	組 AD	•	•	•	•	•	•
	LDAP屬性	•	•	•	•	•	•
	地理位置策略	•	•	•	–	–	–
	持續端點監控	•	•	•	•	•	•
管理	管理接口（以太網）	–	–	–	•	•	•
	管理接口（控制台）	–	–	–	•	•	•
	HTTPS 管理	•	•	•	•	•	•
	SSH 管理	–	–	–	•	•	•
	SNMP MIBS	•	•	•	•	•	•
	Syslog 和 NTP	•	•	•	•	•	•
	使用情況監控	•	•	•	•	•	•
	配置回滾	•	•	•	•	•	•
	集中化管理	–	–	–	•	•	•
	集中化報告	–	–	–	•	•	•
	管理 REST API	–	–	–	•	•	•
	身份驗證 REST API	–	–	–	•	•	•
	RADIUS會計	–	–	–	•	•	•
	計劃的任務	–	–	–	•	•	•
	集中化會話許可	–	–	–	•	•	•
	事件驅動的審計	–	–	–	•	•	•
聯網	IPv6	•	•	•	•	•	•
	全局負載平衡	–	–	–	•	•	•
	服務器負載平衡	•	•	•	–	–	–
	TCP 狀態復制	•	•	•	•	•	•
	集群狀態故障轉移	–	–	–	•	•	•
	主動/被動高可用性	–	•	•	•	•	•
	主動/主動高可用性	–	–	–	•	•	•
	橫向可擴展性	–	–	–	•	•	•
	單個或多個 FQDN	–	–	–	•	•	•
	層3-7智能隧道代理	•	•	•	•	•	•
	層7應用程序代理	•	•	•	•	•	•
集成	2FA TOTP 支持	•	•	•	•	•	•
	EMM 和 MDM 產品支持	–	–	–	•	•	•
	SIEM產品支持	–	–	–	•	•	•
	TPAM密碼庫	–	–	–	•	•	•
	ESX 虛擬機監控程序支持	–	–	•	–	–	•
	Hyper-V 虛擬機監控程序支持	–	–	•	–	–	•
許可選項	基於訂閱的許可證	–	–	–	•	•	•
	永久性許可證與支持	•	•	•	•	•	•
	Web Application Firewall (WAF)	•	•	•	–	–	–
	峰值許可	•	•	•	•	•	•
	分層許可	–	–	–	•	•	•
	虛擬協助	•	•	•	–	–	–

* 要了解有關*VPN*客戶端的更多信息，請訪問：*https://www.sonicwall.com/en-us/products/remote-access/vpn-client*

升級到高端設備的好處

性能更高 | 吞吐量更大 | 高級功能 | 可擴展性更強

設備規格

從一系列特定用途的安全移動訪問(SMA)設備中進行選擇。利用虛擬和物理設備實現靈活的部署選項。

物理設備規格

性能	SMA 210	SMA 410	SMA 6210	SMA 7210
並行會話/用戶	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
外形規格	1U	1U	1U	1U
尺寸	16.92 x 10.23 x 1.75 in (43 x 26 x 4.5cm)	16.92 x 10.23 x 1.75 in (43 x 26 x 4.5cm)	17.0 x 16.5 x 1.75 in (43 x 41.5 x 4.5 cm)	17.0 x 16.5 x 1.75 in (43 x 41.5 x 4.5 cm)
設備重量	11 lb (5 kg)	11 lb (5 kg)	17.7 lb (8 kg)	18.3 lb (8.3 kg)
加密數據加速 (AES-NI)	否	否	是	是
專用管理端口	否	否	是	是
SSL 加速	否	否	是	是
存儲	4GB（閃存）	4GB（閃存）	2 x 1TB SATA; RAID 1	2 x 1TB SATA; RAID 1
接口	(2) GB 以太網，(2) USB，(1)控制台	(4) GB以太網，(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
內存	4GB	8GB	8GB DDR4	16GB DDR4
TPM 芯片	否	否	是	是
處理器	4 核	8 核	4 核	4 核
MTBF（@ 25°C 或 77°F），以小時計算	61,815	60,151	70,127	129,601
運營與合規	**SMA 210**	**SMA 410**	**SMA 6210**	**SMA 7210**
電源	固定電源	固定電源	固定電源	雙電源，可熱插拔
輸入額定值	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
總散熱	92 BTU	109 BTU	264 BTU	389 BTU
環境	WEEE、歐盟 RoHS、中國 RoHS			
非運行沖擊	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			
工作溫度	0°C 至 40°C（32°F 至 104° F）			
FIPS 認證	否	否	FIPS 140-2 二級，帶防篡改保護	

* 吞吐量性能可能會因部署和連接而異。公布的數字基於內部實驗室條件

虛擬設備規格

規格	SMA 500v (ESX/ESXi/Hyper-V)	SMA 8200v (ESX/ESXi/Hyper-V)
並行會話	最多 250 个用户	最多 5,000
SSL-VPN 吞吐量*（最大 CCU時）	最高 186 Mbps	最高 1.58 Gbps
分配的內存	2 GB	8 GB
處理器	1 核	4 核
SSL 加速	否	是
應用的磁盤大小	2 GB	64 GB（默認）
已安裝操作系統	Linux	加固 Linux
專用管理端口	否	是

*吞吐量性能可能會因部署和連接而異。公布的數字基於內部實驗室條件。在Windows Server 2016上運行SMA OS 12.1時，Hyper-V上的SMA 8200v最多可擴展到5,000個並行會話，並提供高達1.58 Gbps SSL-VPN吞吐量

訂購信息

SKU	SONICWALL SECURE MOBILE ACCESS (SMA) 設備
02-SSC-2800	SMA 210，帶5個用戶許可證
02-SSC-2801	SMA 410，帶25個用戶許可證
01-SSC-8469	SMA 500v，帶5個用戶許可證
02-SSC-0978	SMA 7210，帶管理員測試許可證
02-SSC-0976	SMA 6210，帶管理員測試許可證
01-SSC-8468	SMA 8200v（虛擬設備）
SKU	**SONICWALL SMA 用戶許可證**
01-SSC-9182	SMA 500V 增加5個用戶（也適用於 SMA 210）
01-SSC-2414	SMA 500V 增加100個用戶（也適用於 SMA 410）
01-SSC-7856	SMA 5 個用戶許可證-可堆疊用於 6210、7210、8200v
01-SSC-7860	SMA 100個用戶許可證-可堆疊用於 6210、7210、8200v
01-SSC-7865	SMA 5,000 個用戶許可證-可堆疊用於 7210、8200v
SKU	**SONICWALL SMA 支持合同**
01-SSC-9191	為 SMA 500V 最多 25 個用戶提供1年全天候支持（也適用於 SMA 210 和 410）
01-SSC-2326	為 SMA 6210 的 100個用戶提供1年全天候支持-可堆疊
01-SSC-2350	為 SMA 7210 的 500 個用戶提供1年全天候支持-可堆疊
01-SSC-8434	為 SMA 8200V 的 5 個用戶提供1年全天候支持（也適用於 SMA 6210、7210）
01-SSC-8446	為 SMA 8200V 的 100 个個用戶提供1年全天候支持（也適用於 SMA 6210、7210）
01-SSC-7913	為 SMA 8200V 的 5,000 个個用戶提供1年全天候支持（也適用於 SMA 6210、7210）
SKU	**针对 6210、7210、8200V 的中央管理**
CMS 設備許可證	
01-SSC-8535	CMS 基本 + 3 個設備許可證（免費-試用版和與訂閱用戶許可證一起使用）
01-SSC-8536	CMS 100 設備許可證1年（用於與訂閱用戶許可證一起使用）
01-SSC-3369	CMS 基本 + 3 個設備許可證（免費-試用版和與訂閱用戶許可證一起使用）
01-SSC-3402	CMS 100 設備許可證1年（用於與訂閱用戶許可證一起使用）
中央用戶許可證（訂閱）	
01-SSC-2298	CMS 共用許可證10 個用戶1年
01-SSC-8539	CMS 共用許可證 1,000 個用戶1年
01-SSC-5339	CMS共用許可證 50,000 個用戶1年
中央用戶許可證（永久性）	
01-SSC-2053	CMS永久性許可證 10 個用戶
01-SSC-2058	CMS永久性許可證 1,000 個用戶
01-SSC-2063	CMS 永久性許可證 50,000 個用戶
支持中央用戶許可證（永久性）	
01-SSC-2065	CMS 全天候支持 1 年 10 個用戶
01-SSC-2070	CMS 全天候支持 1 年 1,000 個用戶
01-SSC-2075	CMS 全天候支持 1 年 50,000 個用戶
中央Active Sync許可證（訂閱）	
01-SSC-2088	CMS 共用電子郵件許可證 10 個用户 1 年
01-SSC-2093	CMS 共用電子郵件許可證 1,000 個用户 1 年
01-SSC-2087	CMS 共用電子郵件許可證 50,000 個用户 1 年

訂購信息（續）

SKU	針對 6210、7210、8200V 的中央管理
中央峰值許可證	
01-SSC-2111	CMS 峰值 1,000 個用户 5 天
01-SSC-2115	CMS 峰值 50,000 個用户 5 天
Capture 外接程序（訂閱）	
聯系您的經銷商 *訂閱許可證包括全天候支持	
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（也適用於 SMA 210 和 410）
SKU	**SONICWALL SMA 安全升級**
02-SSC-2794	SMA 210 安全升級增強版，5 個用戶捆綁包，全天候支持，最多支持 25 個用户 1 年
02-SSC-2795	SMA 210 安全升級增強版，5 個用戶捆綁包，全天候支持，最多支持 25 個用户 3 年
02-SSC-2798	SMA 410 安全升級增強版，25 個用戶捆綁包，全天候支持，最多支持 100 個用户 1 年
02-SSC-2799	SMA 410 安全升級增強版，25 個用戶捆綁包，全天候支持，最多支持 100 個用户 3 年
02-SSC-2893	SMA 6210 安全升級增強版，全天候支持，最多支持 100 個用户 1 年
02-SSC-2894	SMA 6210 安全升級增強版，全天候支持，最多支持 100 個用户 3 年
02-SSC-2895	SMA 7210 安全升級增強版，全天候支持，最多支持 250 個用户 1 年
02-SSC-2896	SMA 7210 安全升級增強版，全天候支持，最多支持 250 個用户 3 年
02-SSC-0860	SMA 8200V 安全升級增強版，全天候支持，最多支持 100 個用户 1 年
02-SSC-0862	SMA 8200V 安全升級增強版，全天候支持，最多支持 100 個用户 3 年
02-SSC-2807	SMA 500V 安全升級增強版，全天候支持，最多支持 100 個用户 1 年
02-SSC-2808	SMA 500V 安全升級增強版，全天候支持，最多支持 100 個用户 3 年
SKU	**SMA 的峰值許可證（達到容量所需的增量）**
01-SSC-2240	SMA 210 10 天 50個用戶峰值許可證（也適用於 SMA 410 和 500v）
01-SSC-7873	SMA 8200v 10 天 5-2,500 個用戶峰值許可證（也適用於 SMA 6210、7210）
02-SSC-4490	SMA 500V 30 天 250 個用戶峰值許可證
02-SSC-4489	SMA 500V 60 天 250 個用戶峰值許可證
02-SSC-4488	SMA 200/210 30 天 50 個用戶峰值許可證
02-SSC-4487	SMA 200/210 60 天 50 個用戶峰值許可證
02-SSC-4486	SMA 400/410 30 天 250 個用戶峰值許可證
02-SSC-4485	SMA 400/410 60 天 250 個用戶峰值許可證
02-SSC-4471	SMA CMS 峰值外接程序許可證 100 個用户 30 天
02-SSC-4473	SMA CMS 峰值外接程序許可證500 個用户 30 天
02-SSC-4475	SMA CMS 峰值外接程序許可證 1,000 個用户 30 天
02-SSC-4477	SMA CMS 峰值外接程序許可證 5,000 個用户 30 天
02-SSC-4479	SMA CMS 峰值外接程序許可證 10,000 個用户 30 天
02-SSC-4481	SMA CMS 峰值外接程序許可證 25,000 個用户 30 天
02-SSC-4483	SMA CMS 峰值外接程序許可證 50,000 個用户 30 天
02-SSC-4472	SMA CMS 峰值外接程序許可證 100 個用户 60 天
02-SSC-4474	SMA CMS 峰值外接程序許可證 500 個用户 60 天
02-SSC-4476	SMA CMS 峰值外接程序許可證 1,000 個用户 60 天

訂購信息（續）

SKU	SMA 的峰值許可證（達到容量所需的增量）
02-SSC-4478	SMA CMS 峰值外接程序許可證 5,000 個用户 60 天
02-SSC-4480	SMA CMS 峰值外接程序許可證 10,000 個用户 60天
02-SSC-44	SMA CMS 峰值外接程序許可證 25,000 個用户 60 天
02-SSC-4484	SMA CMS 峰值外接程序許可證 50,000 個用户 60 天

*還提供多年SKU和支持合同。有關SKU的完整列表，請聯系您的經銷商或銷售人員。

合作夥伴支持服務

需要幫助規劃、部署或優化SonicWall解決方案嗎？SonicWall高級服務合作夥伴接受過培訓，可為您提供世界一流的專業服務。詳情請訪問 www.sonicwall.com/PES

關於 SonicWall

SonicWall已經致力於打擊網絡犯罪超過27年，為全世界的中小企業、公司和政府機構提供防護。在SonicWall Capture Labs研究的支持下，我們備受讚譽的實時漏洞檢測和預防解決方案在超過215個國家和地區確保了超過一百萬個網絡及其電子郵件、應用程序和數據的安全。這些組織的運作效率更高，對安全的擔憂也更少。有關更多信息，請訪問 www.sonicwall.com 或在領英、Twitter、Facebook和Instagram 上關注我們。

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
有關詳情，請訪問我們的網站。
www.sonicwall.com

Datasheet-SecureMobileAccess-US-VG-1834