SONICWALL

SONICWALL SECURE MOBILE ACCESS (SMA)

Secure anywhere, anytime access to corporate resources across multi-cloud environments based on user and device identity, location and trust.

SonicWall SMA is a unified secure access gateway that enables organizations to provide anytime, anywhere and any device access to mission critical corporate resources. SMA's granular access control policy engine, context aware device authorization, application level VPN and advanced authentication with single sign-on empowers organizations to embrace BYOD and mobility in a multi-cloud environment.

Mobility and BYOD

For organizations wishing to embrace BYOD, flexible working or third party access, SMA becomes the critical enforcement point across them all. SMA delivers best-in-class security to minimize surface threats, while making organizations more secure by supporting latest encryption algorithms and ciphers. SonicWall's SMA allows administrators to provision secure mobile access and identity-based privileges so end-users get fast, simple access to the business applications, data and resources they require. At the same time, organizations can institute secure BYOD policies to protect their corporate networks and data from rogue access and malware.

Move to the cloud

For organizations embarking on a cloud migration journey, SMA offers a single sign-on (SSO) infrastructure that uses a single web portal to authenticate users in a hybrid IT environment. Whether the corporate resource is on-premise, on the web or in a hosted cloud, the access experience is consistent and seamless. SMA also integrates with industry leading multi-factor authentication technologies for added security.

Managed service providers

For either organizations hosting their own infrastructure or for managed service providers, SMA provides turnkey solution to deliver a high degree of business continuity and scalability. SMA can support up to 20,000 concurrent connections on a single appliance, with the ability to scale upwards of hundreds of thousands users through intelligent clustering. Data centers can reduce costs with active-active clustering and a built-in dynamic load balancer, which reallocates global traffic to the most optimized data center in real-time based on user demand. SMA tool sets enable service providers to deliver services with zero downtime, allowing them to fulfill very aggressive SLAs.

SMA empowers IT departments to provide the best experience and the most secure access depending on the user scenario. Available as hardened physical appliances or powerful virtual appliances, SMA fits seamlessly into existing on-prem and/or cloud infrastructure. Organizations can choose from a range of fully clientless web-based secure access for third parties or employees on personally owned devices, or a more traditional client-based full tunnel VPN access for executives across all device types. Whether organizations need to provide reliable secure access to five users from a single location, or scale up to thousands' of users across globally distributed networks, SonicWall SMA has a solution.

SonicWall SMA enables organizations to embrace mobility and BYOD without fear, and move to the cloud with ease. SMA empowers workforces and provides them with a consistent access experience.

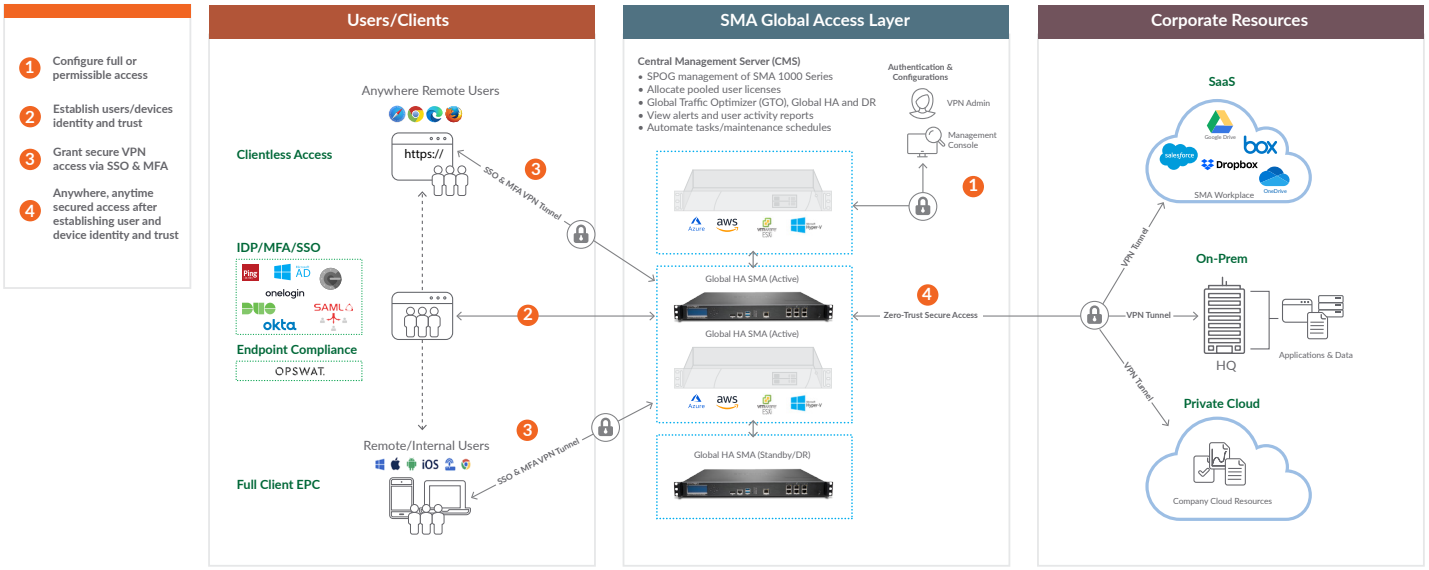
Benefits:

- Unified access to all network and cloud resources for "any time, any device, any application" secure access
- Control who has access to what resources by defining granular policies with the robust access control engine
- Increase productivity by delivering federated single sign-on to any SaaS or locally hosted application with a single URL
- Lower TCO and reduce complexity of access management by consolidating infrastructure components in a hybrid IT environment
- Gain visibility into every connecting device and grant access based on policies and the health of the endpoint
- Prevent malware breaches by scanning all files uploaded into your network with Capture ATP sandbox
- Protect against web based attacks and provide PCI compliance with Web Application Firewall add-on
- Stop DDoS and zombie attacks with Geo IP detection and Botnet protection
- Get secure, native agent functionality using web browser based clientless HTML5 access without the overhead of installing and maintaining agents on the endpoint devices
- Gain actionable insights you need to make the right decisions with real-time monitoring and comprehensive reporting
- Deploy as physical appliance or virtual appliance in private clouds on ESXi or Hyper-V, or in AWS or Microsoft Azure public cloud environments
- Enable dynamic issuance of access licenses based on real-time demand, with automated endpoint direction to the highest performing and lowest latency connection
- Reduce upfront costs with built-in load balancing without additional hardware or services, while providing zero user impact on appliance failover
- Insure against business disruptions or seasonal spikes by scaling capacity instantly

SMA Deployment

A hardened edge gateway for anytime, anywhere, any device secure access

SMA provides comprehensive end-to-end secure remote access to corporate resources hosted across on-prem, cloud and hybrid datacenters. It applies identity-based, policy enforced access controls, context-aware device authentication, and application level VPN to grant access to data, resources and applications after establishing user and device identity, location and trust. Flexibly deployed as a hardened Linux appliance or virtual appliance in private clouds on ESXi or Hyper-V, or in AWS or Microsoft Azure public cloud environments.



SMA Cloud / On-prem Deployment

Flexible deployment with physical and virtual appliances

SonicWall SMA can be deployed as a hardened, high-performance appliance or as a virtual appliance leveraging shared computing resources to optimize utilization, ease migration and reduce capital costs. The hardware appliances are built on a multi-core architecture that offers high performance with SSL acceleration, VPN throughput and powerful proxies to deliver robust secure access. For regulated and federal organizations, SMA is also available with FIPS 140-2 Level 2 certification. The SMA virtual appliances offer the same robust secure access capabilities on major virtual or cloud platforms including Microsoft Hyper-V, VMware ESX, and AWS.

Shared user licenses across the appliances

Organizations with appliances that are globally distributed can benefit from the fluctuating demands for user licenses due to time differences. Whether an organization deploys full VPN licenses or basic ActiveSync licenses, SMA's central management reallocates licenses to managed appliances where user demands have peaked from appliances in a different geographic area, where usage has fallen due to off-work/night hours.

Network visibility with context aware device profiling

Best-in-class, context-aware authentication grants access only to trusted devices and authorized users. Laptops and PCs are also interrogated for the presence or absence of security software, client certificates, and device ID. Mobile devices are interrogated for essential security information such as jailbreak or root status, device ID, certificate status and OS versions prior to granting access. Devices that do not meet policy requirements are not allowed network access and the user is notified of non-compliance.

Consistent experience from a single web portal

Users do not need to remember all the individual application URLs and maintain exhaustive bookmarks. SMA provides a centralized access portal, giving users one URL to access all mission critical applications from a standard web browser. After the user logs on through a browser, a customizable web user portal is displayed in the browser window, providing a single pane of glass view to access any SaaS or local application. The portal only displays links and personalized bookmarks relevant to the particular endpoint device, user or group. The portal is platform agnostic and supports all major device platforms including Windows, Mac OS, Linux, iOS and Android devices, and broad browser support across all these devices.

Federated single sign-on to both SaaS and local applications

Eliminate the need for multiple passwords, and stop bad security practices such as password reuse. SMA provides federated SSO to both cloud hosted SaaS applications and campus hosted applications. SMA integrates with multiple authentication, authorization, and accounting servers and leading multi-factor authentication technologies for added security. Secure SSO is delivered only to authorized endpoint devices after SMA checks

endpoint health status and compliance. Access policy engine ensures that users can see only the authorized applications and grants access after successful authentication. The solution supports federated SSO even when using VPN clients, providing customers a seamless authentication experience whether using client-based or clientless secure access.

Prevent breaches and advanced threats

SonicWall SMA adds a layer of access security to improve your security posture and reduce the surface area for threats.

- SMA integrates with the SonicWall Capture ATP cloud-based multi-engine sandbox to scan all files uploaded by users with unmanaged endpoints, or by those outside the corporate network. This ensures users have the same level of protection from advanced threats, such as ransomware or zero-day malware, when they are on the road as they have in the office[1].
- SonicWall Web Application Firewall service offers businesses an affordable, well-integrated solution to secure internal web-based applications. This allows customers to ensure the confidentiality of data, and internal web services remain uncompromised should there be malicious or rogue authenticated user access.
- Geo-IP & Botnet detection protects organizations from DDoS and zombie attacks, and from compromised endpoints functioning as botnets.

Seamless and secure browser-based clientless access

The “clientless” nature of the SonicWall SMA means that there is no need for the administrator to install a fat client component manually to a computer that will be used for remote access. This removes any dependency on Java and overhead for IT, thereby greatly expanding the concept of remote access. It means that since there is no pre-installation or pre-configuration required, an authorized remote worker can sit down at any computer, anywhere in the world, and securely access their corporate resources. In its purest form, secure access is strictly browser-based using HTML5, providing a seamless and unified experience for the users.

Deliver an "Always On" experience

For a seamless user experience, SMA delivers Always On VPN for managed windows devices. Administrators can configure settings to automatically establish a VPN connection any time an authorized endpoint client detects a public or untrusted network. A single login event to the windows device provides the user with a secure connection to corporate resources. Users do not have to login to their VPN clients or maintain additional passwords. This provides a seamless experience to mobile users to access mission critical resources just as they were in the office and empowers IT admins to maintain control over managed devices, improving the security posture of the organization.

Intuitive management and comprehensive reporting

SonicWall provides an intuitive web-based management platform, Central Management Server (CMS), to streamline appliance management while providing extensive reporting capabilities. The easy-to-use GUI brings clarity to managing individual or multiple appliances and policies. Each page shows how settings are configured across all machines under management. Unified policy management helps you create and monitor access policies and configurations. A single policy can control access from your users, devices and applications, to data, servers and networks. IT can automate routine tasks and schedule activities, freeing up security teams from repetitive tasks to focus on strategic security tasks like incidence response. IT gains insights into user access trends and system-wide health through easy-to-use reporting and centralized logging.

Provide 24x7 service availability

Organizations have requirements to maintain their services and keep them up and running with a high degree of reliability to provide secure access to mission critical applications at all times. SMA appliances support traditional active-passive High Availability (HA) for organizations with single data centers, or global HA with active-active or active-standby clustering for local or distributed data centers. Both HA models deliver frictionless experience to users with zero-impact failover and session persistence.

Deploy the VPN client that suits your needs

Choose from a broad range of VPN clients to deliver policy-enforced secure remote access for various endpoints including laptops, smartphones and tablets.

VPN client	Supported OS	Supported SMA model	Key highlight
Mobile Connect	iOS, OS X, Android, Chrome OS, Windows 10	All models	Deliver biometric authentication, per app VPN and endpoint control enforcement
Connect Tunnel (Thin Client)	Windows, Mac OS and Linux	6200, 6210, 7200, 7210, 8200v, 9000	Provide a complete “in-office” experience with robust endpoint control
NetExtender (Thin Client)	Windows and Linux	210, 410, 500v	Enforce granular access policies and extend network access through native clients

Reduce upfront costs with built-in load balancer

The load balancing functionality built into the SMA appliance achieves the level scalability expected for medium-sized business and enterprise deployments. Select models of SMA appliance offer dynamic load balancing to intelligently assign session loads and allocate user licenses in real-time based on demand. Organizations do not need to invest in external load balancers, thus reducing upfront costs.

Get insurance against unforeseen events

A complete business continuity and DR solution must be able to handle a significant spike in remote access traffic, while still maintaining security and cost controls. SonicWall Spike license packs for the SMA are add-on licenses that enable distributed businesses to scale user count and reach maximum capacity instantly, enabling seamless business continuity. Spike licenses work like an insurance policy toward any future planned or unplanned spikes from current user counts to tens or even hundreds of additional users.

Features

Advanced authentication

Federated single sign-on[2]	SMA uses SAML 2.0 authentication to enable federated SSO via a single portal to both on-premises and cloud resources, while enforcing stacked multifactor authentication for added security.
Multifactor authentication	X.509 digital certificates Server-side and client-side digital certificates RSA SecurID, Dell Defender, Google Authenticator, Duo Security and other one-time password/two-factor authentication tokens Common Access Card (CAC) Dual or stacked authentication Captcha support, username/password
SAML Authentication	SMA can be configured as SAML Identity Provider (IdP), SAML Service Provider (SP) or proxy an existing on-prem IdP to enable federated single sign-on (SSO) using SAML 2.0 authentication.
Authentication repositories	SMA provides simple integrations with industry standard repositories for easy management of user accounts and passwords. User groups can be populated dynamically based on RADIUS, LDAP or Active Directory authentication repositories, including nested groups. Common or custom LDAP attributes can be interrogated for specific authorization or device registration verification.
Layer 3-7 application proxy	SMA provides flexible proxy options, for example vendor access can be provided through direct proxy, contractor access through reverse proxy and employee access to Exchange through ActiveSync.
Reverse proxy	The enhanced reverse proxy service with authentication allows administrators to configure application offloading portal & bookmarks, allowing users to connect seamlessly to remote applications and resources including RDP and HTTP. This feature supports all browsers including IE, Chrome and Firefox.
Kerberos constrained delegation	SMA provides authentication support using an existing Kerberos infrastructure, which does not need to trust front-end services to delegate a service.

Access management

Access Control Engine (ACE)	Administrators grant or deny access based on organizational policies and set remediation actions when quarantining sessions. ACE object-based policy utilizes elements of network, resource, identity, device, application, data and time.
End Point Control (EPC)	EPC allows the administrator to enforce granular access control rules based on the health status of the connecting device. With deep OS integration, many elements are combined for type classification and risk factor assessment. EPC interrogation simplifies device profile setup using a comprehensive, predefined list of anti-virus, personal firewall and anti-spyware solutions for Windows, Mac and Linux platforms, including version and applicability of signature file update.
App Access Control (AAC)	Administrators can define which specific mobile applications are allowed to access which resources on the network through individual app tunnels. AAC policies are enforced both at the client and server, providing robust perimeter protection.

Superior security

Layer 3 SSL VPN	The SMA series delivers high performance layer-3 tunneling capabilities to a wide variety of client devices running in any environment.
Cryptography support	Configurable session length Ciphers: AES 128 + 256 bit, Triple DES, RC4 128 bit Hashes: SHA-256 Elliptic Curve Digital Signature Algorithm (ECDSA)
Advanced ciphers support	SMA appliances provide strong security stance out-of-the box for compliance, with default configuration ciphers, and administrators can further refine for performance, security strength, or compatibility.
Security certifications	Certified for FIPS 140-2 Level 2, ICSA SSL-TLS, In-progress for Common Criteria, UC-APL
Secure file share	Stop unknown, zero-day attacks such as ransomware at the gateway with automated remediation. Files uploaded using unmanaged endpoints with secure access to corporate networks are inspected by our cloud based multi-engine Capture ATP.
Web Application Firewall (WAF)	Prevent protocol and web-based attacks, helping financial, healthcare, e-commerce and other businesses attain OWASP Top 10 and PCI compliance.
Geo IP detection and botnet protection	Geo IP Detection and Botnet Protection allows customers with a mechanism to allow or restrict user access from various geographical locations.
TLS 1.3 support	Provide both security and performance improvement while reducing complexities over its predecessors.

Intuitive user experience

Always On VPN	Automatically establish a secure connection to the corporate network from company issued Windows devices to improve security, gain traffic visibility and remain in compliance
Secure Network Detection (SND)	SMA's network-aware VPN client detects when the device is off campus and auto-reconnects the VPN, bringing it down again when the device returns to a trusted network.
Clientless access to resources	SMA provides secure clientless access to resources via HTML5 browser agents delivering RDP, ICA, VNC, SSH and Telnet protocols.
Single sign-on portal	The WorkPlace portal provides easy to use, customizable, single pane view for secure access with Single sign-on (SSO) to any resource in a hybrid IT environment. No additional login or VPN is needed.
Layer 3 tunneling	Administrators can choose Split-Tunnel or enforce Redirect-All mode with SSL/TLS tunneling and optional ESP fallback for maximum performance.
HTML5 file explorer[1]	Modern file browser makes it easy for users to access file shares from any web browser.
Mobile OS integration	Mobile Connect is supported on all OS platforms providing users complete flexibility in mobile device choice.

Resilience

Global Traffic Optimizer (GTO)	SMA offers global traffic load-balancing with zero-impact to users. Traffic is routed to the most optimized and highest performing datacenter.
Dynamic high availability[2]	SMA supports Active/Passive and offers Active/Active configuration for high availability, whether deployed in a single datacenter or across multiple geographically-dispersed datacenters.
Universal session persistence[1]	Provide users a frictionless experience with zero impact failover. In the event of an appliance going offline, SMA's intelligent clustering reallocates users along with their session data without the need for re-authentication.
Scalable performance	SMA appliances scale performance exponentially by deploying multiple appliances, thus eliminating a single point of failure. Horizontal clustering fully supports mixing physical and virtual SMA appliances.
Dynamic licensing	User licenses no longer have to be applied to individual SMA appliances. Users can be distributed and reallocated dynamically among the managed appliances, based on user demand.

Central management & monitoring

Central Management System (CMS)	CMS provides centralized, web-based management for all SMA capabilities.
Custom alerts	Alerts can be configured to generate SNMP traps that are monitored by any IT infrastructure Network Management System (NMS). Administrators can also configure alerts for Capture ATP file scans and disk usage for immediate actioning.
Real-Time Dashboard	A real-time, customizable, dashboard allows the IT administrator to quickly and easily diagnose access issues, gaining valuable insight for troubleshooting.
SIEM integration	Real-time output to central SIEM data collectors allows security teams to correlate event driven activities, to understand the end-to-end workflow of a particular user or application. This is critical during security incident management and forensic analysis.
Scheduler	The scheduler enables users to schedule maintenance tasks such as deploying policies, replicating configuration settings and restarting services, without manual intervention

Extensibility

Management APIs	Management APIs allow full programmatic administrative control over all objects within a single SMA or global CMS environment.
End User APIs	End User APIs provide complete control over all logon, authentication and endpoint workflow.
Two-factor authentication (2FA)	SMA delivers 2FA by integrating with leading time-based one-time password (TOTP) solutions such as Google Authenticator, Microsoft Authenticator, Duo security etc.
MDM integration	SMA integrates with leading enterprise mobile management (EMM) products such as Airwatch and Mobile Iron.
Other 3rd party integration	SMA integrates with industry leading vendors such as OPSWAT to provide advanced threat protection

[1]*Available with SMA OS 12.1 or higher*

[2] *Enhanced in SMA 12.1*

Feature Summary (comparison by model)

Category	Feature	210	410	500v	6210	7210	8200v
Deployment	Operating system	v9.0 onwards	v9.0 onwards	v9.0 onwards	v12.1 onwards	v12.1 onwards	v12.1 onwards
	Supported Hypervisors	–	–	VMware ESXi / Microsoft Hyper-V	–	–	VMware ESXi / Microsoft Hyper-V
	Supported Public Cloud Platforms	–	–	AWS/Azure	–	–	AWS/Azure
Throughput	Max concurrent user sessions	200	400	250	2,000	10,000	5,000
	Max SSL/TLS throughput	560 Mbps	844 Mbps	265 Mbps	1.3 Gbps	5.0 Gbps	1.58 Gbps
Web Application Firewall	Throughput	515 Mbps	672 Mbps	424 Mbps	–	–	–
	Transactions per second (TPS)	600	900	300	–	–	–
Client access	Layer 3 tunnel	•	•	•	•	•	•
	Split-tunnel and redirect-all	•	•	•	•	•	•
	Always On VPN	•	•	•	•	•	•
	Auto ESP encapsulation	–	–	–	•	•	•
	HTML5 (RDP, VNC, ICA, SSH, Telnet, Network Explorer)	•	•	•	•	•	•
	Secure Network Detection	–	–	–	•	•	•
	File browser (CIFS/NFS)	•	•	•	•	•	•
	Citrix XenDesktop/XenApp	•	•	•	•	•	•
	VMware View	–	–	–	•	•	•
	On Demand tunnel	–	–	–	•	•	•
	Chrome/Firefox extensions	–	–	–	•	•	•
	CLI tunnel support	–	–	–	•	•	•
	Mobile Connect (iOS, Android, Chrome, Win 10, Mac OSX)	•	•	•	•	•	•
	Net Extender (Windows, Linux)	•	•	•	–	–	–
	Connect Tunnel (Windows, Mac OSX, Linux)	–	–	–	•	•	•
	Exchange ActiveSync	•	•	•	•	•	•
Mobile access	Per app VPN	–	–	–	•	•	•
	App control enforcement	–	–	–	•	•	•
	App ID validation	–	–	–	•	•	•
User portal	Branding	•	•	•	•	•	•
	Customization	–	–	–	•	•	•
	Localization	•	•	•	•	•	•
	User defined bookmarks	•	•	•	•	•	•
	Custom URL support	•	•	•	•	•	•
	SaaS application support	–	–	–	•	•	•
Security	FIPS 140-2	–	–	–	•	•	–
	ICSA SSL-TLS	•	•	•	•	•	•
	Suite B ciphers	–	–	–	•	•	•
	Dynamic EPC interrogation	•	•	•	•	•	•
	Role Based Access Control (RBAC)	–	–	–	•	•	•
	Endpoint registration	•	•	•	•	•	•
	Secure File Share (Capture ATP)	•	•	•	•	•	•
	Endpoint quarantine	•	•	•	•	•	•
	OSCP CRL validation	–	–	–	•	•	•
	Cipher selection	–	–	–	•	•	•
	PKI and client certificates	•	•	•	•	•	•
	Geo IP filter	•	•	•	–	–	–
	Botnet filter	•	•	•	–	–	–
	Forward proxy	•	•	•	•	•	•
	Reverse proxy	•	•	•	•	•	•
Authentication and identity services	SAML 2.0	•	•	•	•	•	•
	LDAP, RADIUS	•	•	•	•	•	•
	Kerberos (KDC)	•	•	•	•	•	•
	NTLM	•	•	•	•	•	•
	SAML Identity Provider (IdP)	•	•	•	•	•	•
	Biometric device support	•	•	•	•	•	•
	Face ID support for iOS	•	•	•	•	•	•

SONICWALL®

Feature Summary (comparison by model con't)

Category	Feature	210	410	500v	6210	7210	8200v
Authentication and identity services con't	Two-factor authentication (2FA)	•	•	•	•	•	•
	Multi-factor authentication (MFA)	–	–	–	•	•	•
	Chained authentication	–	–	–	•	•	•
	One Time Passcode (OTP) via email or SMS	•	•	•	•	•	•
	Common Access Card (CAC) support	–	–	–	•	•	•
	X.509 certificate support	•	•	•	•	•	•
	Captcha integration	–	–	–	•	•	•
	Remote password change	•	•	•	•	•	•
	Form-based SSO	•	•	•	•	•	•
	Federated SSO	–	–	–	•	•	•
	Session persistence	–	–	–	•	•	•
	Auto logon	•	•	•	•	•	•
Access control	Group AD	•	•	•	•	•	•
	LDAP attributes	•	•	•	•	•	•
	Geolocation policies	•	•	•	–	–	–
	Continual endpoint monitoring	•	•	•	•	•	•
Management	Management interface (ethernet)	–	–	–	•	•	•
	Management interface (console)	–	–	–	•	•	•
	HTTPS administration	•	•	•	•	•	•
	SSH administration	–	–	–	•	•	•
	SNMP MIBS	•	•	•	•	•	•
	Syslog and NTP	•	•	•	•	•	•
	Usage monitoring	•	•	•	•	•	•
	Configuration rollback	•	•	•	•	•	•
	Centralized management	–	–	–	•	•	•
	Centralized reporting	–	–	–	•	•	•
	Management REST APIs	–	–	–	•	•	•
	Authentication REST APIs	–	–	–	•	•	•
	RADIUS accounting	–	–	–	•	•	•
	Scheduled tasks	–	–	–	•	•	•
	Centralized session licensing	–	–	–	•	•	•
	Event-driven auditing	–	–	–	•	•	•
Networking	IPv6	•	•	•	•	•	•
	Global load balancing	–	–	–	•	•	•
	Server load balancing	•	•	•	–	–	–
	TCP state replication	•	•	•	•	•	•
	Cluster state failover	–	–	–	•	•	•
	Active/passive high availability	–	•	•	•	•	•
	Active/active high availability	–	–	–	•	•	•
	Horizontal scalability	–	–	–	•	•	•
	Single or multiple FQDNs	–	–	–	•	•	•
	L3-7 smart tunnel proxy	•	•	•	•	•	•
	L7 application proxy	•	•	•	•	•	•
Integration	2FA TOTP support	•	•	•	•	•	•
	EMM and MDM product support	–	–	–	•	•	•
	SIEM product support	–	–	–	•	•	•
	TPAM password vault	–	–	–	•	•	•
	ESX hypervisor support	–	–	•	–	–	•
	Hyper-V hypervisor support	–	–	•	–	–	•
Licensing options	Subscription based license	–	–	–	•	•	•
	Perpetual license with support	•	•	•	•	•	•
	Web Application Firewall (WAF)	•	•	•	–	–	–
	Spike licensing	•	•	•	•	•	•
	Tiered licensing	–	–	–	•	•	•
	Virtual assist	•	•	•	–	–	–

** To learn more about VPN clients, visit: https://www.sonicwall.com/en-us/products/remote-access/vpn-client*

SONICWALL®

Benefits of upgrading to high end appliances

Higher performance | Increased throughput | Advanced features | Better scalability

Appliance Specifications

Choose from a range purpose-built secure mobile access (SMA) appliances.
Get flexible deployment options with virtual and physical appliances.

Physical appliance specifications

Performance	SMA 210	SMA 410	SMA 6210	SMA 7210
Concurrent sessions/Users	Up to 200	Up to 400	Up to 2,000	Up to 10,000
SSL VPN Throughput* (at max CCU)	560 Mbps	844 Mbps	Up to 800 Mbps	Up to 5.0 Gbps
Form factor	1U	1U	1U	1U
Dimensions	16.92 x 10.23 x 1.75 in (43x26x4.5cm)	16.92 x 10.23 x 1.75 in (43x26x4.5cm)	17.0 x 16.5 x 1.75 in (43 x 41.5x 4.5 cm)	17.0 x 16.5 x 1.75 in (43 x 41.5x 4.5 cm)
Appliance weight	11 lbs (5 kgs)	11 lbs (5 kgs)	17.7 lbs (8 kgs)	18.3 lbs (8.3 kgs)
Encryption data acceleration (AES-NI)	NO	NO	YES	YES
Dedicated management port	NO	NO	YES	YES
SSL acceleration	NO	NO	YES	YES
Storage	4GB (Flash Memory)	4GB (Flash Memory)	2 x 1TB SATA; RAID 1	2 x 1TB SATA; RAID 1
Interfaces	(2) GB Ethernet, (2) USB, (1) console	(4) GB Ethernet, (2) USB, (1) console	(6)-port 1GE, (2) USB, (1) console	(6)-port 1GE, (2)-port 10Gb SFP+, (2) USB, (1) console
Memory	4GB	8GB	8GB DDR4	16GB DDR4
TPM chip	NO	NO	YES	YES
Processor	4 cores	8 cores	4 cores	4 cores
MTBF (@ 25°C or 77°F) in hours	61,815	60,151	70,127	129,601
Operations and Compliance	**SMA 210**	**SMA 410**	**SMA 6210**	**SMA 7210**
Power	Fixed power supply	Fixed power supply	Fixed power supply	Dual power supply, hot swappable
Input rating	100-240VAC, 50-60MHz	100-240VAC, 50-60MHz	100-240 VAC, 1.1 A	100-240 VAC, 1.79 A
Power consumption	26.9 W	31.9 W	77 W	114 W
Total heat dissipation	92 BTU	109 BTU	264 BTU	389 BTU
Environmental	WEEE, EU RoHS, China RoHS			
Non-operating shock	110 g, 2 msec			
Emissions	FCC, ICES, CE, C-Tick, VCCI; MIC			
Safety	TUV/GS, UL, CE PSB, CCC, BSMI, CB scheme			
Operating temperature	0°C to 40°C (32°F to 104° F)			
FIPS certification	NO	NO	FIPS 140-2 Level 2 with anti-tamper protection	

** Throughput performance may vary based on deployment and connectivity. Published numbers are based on internal lab conditions*

Virtual appliance specifications

Specifications	SMA 500v (ESX/ESXi/Hyper-V)	SMA 8200v (ESX/ESXi/Hyper-V)
Concurrent sessions	Up to 250 users	Up to 5000
SSL-VPN throughput* (at max CCU)	Up to 186 Mbps	Up to 1.58 Gbps
Allocated memory	2GB	8 GB
Processor	1 core	4 cores
SSL acceleration	NO	YES
Applied disk size	2GB	64 GB (default)
Operating system installed	Linux	Hardened Linux
Dedicated management port	NO	YES

** Throughput performance may vary based on deployment and connectivity. Published numbers are based on internal lab conditions. SMA 8200v on Hyper-V scales up to 5000 concurrent sessions and provides up to 1.58 Gbps SSL-VPN throughput when running SMA OS 12.1 with Windows Server 2016*

Ordering Information

SKU	SONICWALL SECURE MOBILE ACCESS (SMA) APPLIANCE
02-SSC-2800	SMA 210 with 5 user license
02-SSC-2801	SMA 410 with 25 user license
01-SSC-8469	SMA 500v with 5 user license
02-SSC-0978	SMA 7210 with administrator test license
02-SSC-0976	SMA 6210 with administrator test license
01-SSC-8468	SMA 8200v (virtual appliance)
SKU	**SONICWALL SMA USER LICENSES**
01-SSC-9182	SMA 500V add 5 user (Also available for SMA 210)
01-SSC-2414	SMA 500V add 100 user (Also available for SMA 410)
01-SSC-7856	SMA 5 user license - stackable for 6210, 7210, 8200v
01-SSC-7860	SMA 100 user license - stackable for 6210, 7210, 8200v
01-SSC-7865	SMA 5000 user license - stackable for 7210, 8200v
SKU	**SONICWALL SMA SUPPORT CONTRACT**
01-SSC-9191	24X7 support for SMA 500V up to 25 user 1yr (Also available for SMA 210 & 410)
01-SSC-2326	24X7 support for SMA 6210 100 user 1yr - stackable
01-SSC-2350	24X7 support for SMA 7210 500 user 1yr - stackable
01-SSC-8434	24X7 support for SMA 8200V 5 user 1yr - stackable (Also available for SMA 6210, 7210)
01-SSC-8446	24X7 support for SMA 8200V 100 user 1yr - stackable (Also available for SMA 6210, 7210)
01-SSC-7913	24X7 support for SMA 8200V 5000 user 1yr - stackable (Also available for SMA 6210, 7210)
SKU	**CENTRAL MANAGEMENT FOR 6210, 7210, 8200V**
CMS appliance license	
01-SSC-8535	CMS base + 3 appliance license (Free - for Trials and use with subscription user licenses)
01-SSC-8536	CMS 100 appliances license 1yr (for use with subscription user licenses)
01-SSC-3369	CMS base + 3 appliances (Free - for use with perpetual user licenses)
01-SSC-3402	CMS 100 appliance license 1yr (for use with perpetual user licenses)
Central user licenses (subscription)	
01-SSC-2298	CMS pooled license 10 user 1yr
01-SSC-8539	CMS pooled license 1000 user 1yr
01-SSC-5339	CMS pooled license 50000 user 1yr
Central user licenses (perpetual)	
01-SSC-2053	CMS perpetual license 10 user
01-SSC-2058	CMS perpetual license 1000 user
01-SSC-2063	CMS perpetual license 50000 user
Support for central user licenses (perpetual)	
01-SSC-2065	CMS 24x7 support 1yr 10 user
01-SSC-2070	CMS 24x7 support 1yr 1000 user
01-SSC-2075	CMS 24x7 support 1yr 50000 user
Central ActiveSync licenses (subscription)	
01-SSC-2088	CMS pooled email license 10 user 1yr
01-SSC-2093	CMS pooled email license 1000 user 1yr
01-SSC-2087	CMS pooled email license 50000 user 1yr

Ordering Information con't

SKU	CENTRAL MANAGEMENT FOR 6210, 7210, 8200V
Central spike licenses	
01-SSC-2111	CMS spike 1000 user 5days
01-SSC-2115	CMS spike 50000 user 5days
Capture add-on (subscription)	
Contact your reseller ** Subscription licenses have 24X7 support included*	
SKU	**SONICWALL SMA ADD-ONS**
01-SSC-2406	SMA 7210 FIPS add-on
01-SSC-2405	SMA 6210 FIPS add-on
01-SSC-9185	SMA 500V Web Application Firewall 1 YR (Also available for SMA 210 & 410)
SKU	**SONICWALL SMA SECURE UPGRADE**
02-SSC-2794	SMA 210 Secure Upgrade Plus, 5 User Bundle with 24X7 support up to 25 users 1yr
02-SSC-2795	SMA 210 Secure Upgrade Plus, 5 User Bundle with 24X7 support up to 25 users 3yr
02-SSC-2798	SMA 410 Secure Upgrade Plus, 25 User Bundle with 24X7 support up to 100 users 1yr
02-SSC-2799	SMA 410 Secure Upgrade Plus, 25 User Bundle with 24X7 support up to 100 users 3yr
02-SSC-2893	SMA 6210 Secure Upgrade Plus, 24X7 support up to 100 users 1yr
02-SSC-2894	SMA 6210 Secure Upgrade Plus, 24X7 support up to 100 users 3yr
02-SSC-2895	SMA 7210 Secure Upgrade Plus, 24X7 support up to 250 users 1yr
02-SSC-2896	SMA 7210 Secure Upgrade Plus, 24X7 support up to 250 users 3yr
02-SSC-0860	SMA 8200V Secure Upgrade Plus, 24X7 support up to 100 users 1yr
02-SSC-0862	SMA 8200V Secure Upgrade Plus, 24X7 support up to 100 users 3yr
02-SSC-2807	SMA 500V Secure Upgrade Plus, 24X7 support up to 100 users 1yr
02-SSC-2808	SMA 500V Secure Upgrade Plus, 24X7 support up to 100 users 3yr
SKU	**SPIKE LICENSE FOR SMA (INCREMENTAL NEEDED TO REACH CAPACITY)**
01-SSC-2240	SMA 210 10 day 50 user spike license (Also available for SMA 410 and 500v)
01-SSC-7873	SMA 8200v 10 day 5-2500 user spike license (Also available for SMA 6210, 7210)
02-SSC-4490	SMA 500V 30 DAY 250 USER SPIKE LICENSE
02-SSC-4489	SMA 500V 60 DAY 250 USER SPIKE LICENSE
02-SSC-4488	SMA 200/210 30 DAY 50 USER SPIKE LICENSE
02-SSC-4487	SMA 200/210 60 DAY 50 USER SPIKE LICENSE
02-SSC-4486	SMA 400/410 30 DAY 250 USER SPIKE LICENSE
02-SSC-4485	SMA 400/410 60 DAY 250 USER SPIKE LICENSE
02-SSC-4471	SMA CMS SPIKE ADD-ON LICENSE 100 USER 30 DAYS
02-SSC-4473	SMA CMS SPIKE ADD-ON LICENSE 500 USER 30 DAYS
02-SSC-4475	MA CMS SPIKE ADD-ON LICENSE 1,000 USER 30 DAYS
02-SSC-4477	SMA CMS SPIKE ADD-ON LICENSE 5,000 USER 30 DAYS
02-SSC-4479	SMA CMS SPIKE ADD-ON LICENSE 10,000 USER 30 DAYS
02-SSC-4481	MA CMS SPIKE ADD-ON LICENSE 25,000 USER 30 DAYS
02-SSC-4483	SMA CMS SPIKE ADD-ON LICENSE 50,000 USER 30 DAYS
02-SSC-4472	SMA CMS SPIKE ADD-ON LICENSE 100 USER 60 DAYS
02-SSC-4474	SMA CMS SPIKE ADD-ON LICENSE 500 USER 60 DAYS
02-SSC-4476	SMA CMS SPIKE ADD-ON LICENSE 1,000 USER 60 DAYS

Ordering Information con't

SKU	SPIKE LICENSE FOR SMA (INCREMENTAL NEEDED TO REACH CAPACITY)
02-SSC-4478	SMA CMS SPIKE ADD-ON LICENSE 5,000 USER 60 DAYS
02-SSC-4480	SMA CMS SPIKE ADD-ON LICENSE 10,000 USER 60 DAYS
02-SSC-4482	SMA CMS SPIKE ADD-ON LICENSE 25,000 USER 60 DAYS
02-SSC-4484	SMA CMS SPIKE ADD-ON LICENSE 50,000 USER 60 DAYS

** Multi-year SKUs and support contracts are also available. For a complete list of SKUs contact your reseller or sales*

Partner Enabled Services

Need help to plan, deploy or optimize your SonicWall solution? SonicWall Advanced Services Partners are trained to provide you with world class professional services. Learn more at www.sonicwall.com/PES.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era in a work reality where everyone is remote, mobile and unsecure. SonicWall safeguards organizations mobilizing for their new business normal with seamless protection that stops the most evasive cyberattacks across boundless exposure points and increasingly remote, mobile and cloud-enabled workforces. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

Datasheet-SecureMobileAccess-US-VG-2883