SMA 1000 series

Delivering robust access security for all remote and mobile workers, through a powerful and granular access control engine

Industry challenges

As businesses move out of the confines of a secure building, managing access to sensitive corporate resources has become a top concern for CISOs. There is a need for an intelligent access security solution that provides policy-based access to guests, customers, partners and employees. Trends such as BYOD, cloud and remote working bring their own unique set of challenges, but fundamental problems remain.

- Unauthorized users gaining access to company data and applications
- Malware infected devices acting as conduits to infect company systems
- Maintaining a reliable service across different mobile platforms with zero impact to business
- Interception of company data in transit on unsecured public Wi-Fi networks
- Compliance with audit and regulatory requirements

SonicWall Solution

The SMA 1000 series is an advanced access security gateway that provides secure access to network and cloud resources from any device.

SMA Overview

Access Control Engine

The SMA 1000 series offers centralized, granular, policy-based enforcement of remote and mobile access to corporate apps and data, both on network and in the cloud. For organizations wishing to embrace agile working practices, such as BYOD, flexible working or off shore development, SMA becomes the central enforcement point across them all.

The SMA Access Control Engine ensures risks originating from users, endpoints or applications are evaluated prior to granting data access. Remediation actions, such as session quarantining and alerting are enforced to minimize user frustration and reduce helpdesk calls.

Secure access

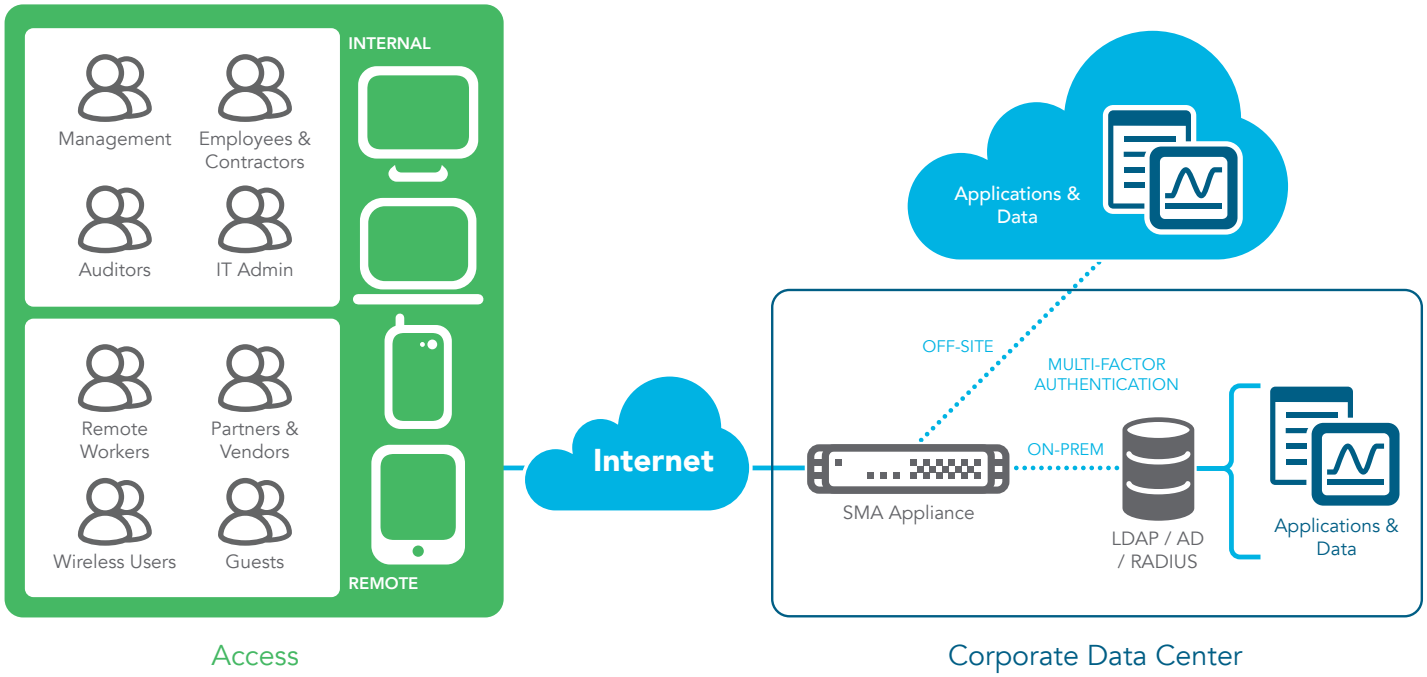
The SMA 1000 series empowers your users with secure remote access to the files, applications and resources they need to be productive with an intuitive client that is easy to deploy on Windows, Mac OSX, Linux, iOS, Android, Chrome OS, Windows Mobile and Kindle Fire devices. SMA delivers best-in-class security to minimize surface threats, while making organizations more secure by supporting latest encryption algorithms and ciphers.

Clientless access security

The SMA OS 12 HTML5 application agents provide a secure window to the most frequently utilized data types, while providing protection from malicious attacks and malware propagation. These feature rich agents keep parity with native application functions, which is critical for a great user experience. Clientless security provides zero-day device support, requires zero need for installation and thus leaves "zero" footprint, making it perfect for third party or un-managed end point access.

Benefits:

- Defines who has access to what resources through its fine-grained Access Control Engine
- Interrogates every connecting device and grants or denies access based on the health of the endpoint, via the Advanced Endpoint Control module
- Enables traffic optimization and zero impact failover, through its Global High Availability platform
- Ensures data protection and superior security by leveraging the latest ciphers
- Helps meet regulatory compliance with a comprehensive audit trail



SMA solutions provide secure access for all users, devices and applications.

Access management

Continual access enforcement both at the endpoint and at the edge helps secure corporate data from loss and theft. Through its robust and granular policy management engine, SMA ensures confidentiality and integrity of data. SMA validates every user, endpoint and application, before it enters the network, thus safeguarding data and empowering users.

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

SMA ensures that the highest security stance is maintained for compliance and data protection by utilizing the latest ciphers and strongest encryption available. SonicWall supports the federal, healthcare and finance industries with their regulatory requirements by routinely submitting all hardware models through rigorous industry security testing and certification.

Layer 3 SSL VPN	The SMA 1000 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: MD5, SHA-256, SHA-1 Elliptic Curve Digital Signature Algorithm (ECDSA)
Advanced ciphers support	SMA 1000 solutions 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

Global High Availability

The SMA 1000 series provides a turnkey solution to deliver a high degree of business continuity and scalability. Global High Availability (GHA) empowers the service owner through a series of tools to deliver a service with zero downtime and allows very aggressive SLAs to be fulfilled.

SonicWall 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	SMA OS 12 provides active/active configuration for high availability, whether deployed in a single datacenter or across multiple geographically-dispersed datacenters.
Scalable performance	SMA 1000 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

SMA provides a web-based management platform to streamline appliance management while providing extensive reporting capabilities.

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).
SONAR monitoring	SonicWall SONAR 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

SMA's extensibility program connects our product to complementary security solutions, and empowers our customers, partners and third-parties by integrating with industry leaders and providing powerful APIs.

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.
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

Advanced Authentication

The SMA 1000 series provides a consistent and simple user experience through single sign-on (SSO), while protecting against threat actors and credential harvesting.

Cloud single sign-on	SMA SAML IdP proxy enables SSO via a single portal to both traditional AD username/password and SaaS 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 and other one-time password/two-factor authentication tokens, using RADIUS protocol Common Access Card (CAC) Dual or stacked authentication Captcha support, username/password
SAML Gatekeeper Support	SMA provides air gap security to your campus hosted SAML IdP through credential chaining technology in its FIPS certified edge point appliance.
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.
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.

Intuitive user experience

A positive user experience ensures users adopt the strongest security policies and avoid shadow IT scenarios, which pose a serious risk of data loss.

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.
User portal	The WorkPlace portal provides users with a customizable and intuitive landing page of dynamically personalized resources.
Layer 3 tunneling	Administrators can choose Split-Tunnel or enforce Redirect-All mode with SSL/TLS tunneling and optional ESP fallback for maximum performance.
Session persistence	SMA provides session persistence across different locations without re-authentication.
Mobile OS integration	Mobile Connect is supported on all OS platforms, providing users complete flexibility in mobile device choice.

Feature summary

Client Access

- Layer 3 tunnel
- Split-tunnel and redirect-all
- Auto ESP encapsulation
- HTML5 (RDP/VNC/ICA/SSH)
- Secure Network Detection
- File browser (CIFS/NFS)
- Citrix XenDesktop/XenApp
- VMware View
- On Demand browser tunnel
- Chrome/Firefox extensions
- CLI tunnel support
- Multi client OS

Mobile

- 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
- Endpoint registration
- Endpoint quarantine
- OSCP CRL validation
- Cipher selection
- PKI and client certificates
- Forward proxy

Authentication

- LDAP, RADIUS
- Kerberos (KDC)
- NTLM
- SAML IdP gatekeeper
- Biometric device support
- Chained authentication
- Remote password change
- Forms based SSO
- Team ID session persistence
- Auto logon
- Reverse proxy

Access Control

- Group AD
- LDAP attributes
- Continual monitoring

Management

- Dedicated OOB (Serial and Eth)
- Global load balancing
- TCP state replication
- Cluster state failover
- Active/active high availability
- Horizontal clustering scalability
- Centralized management
- Device HTTPS and SSH admin
- SNMP MIBS
- Syslog and NTP
- Configuration rollback
- Burst licensing
- Centralized session licensing
- Event-driven auditing
- Single or multiple FQDNs
- L3-7 Smart Tunnel proxy
- L7 Application proxy
- Central reporting

Integration

- Management REST APIs
- Authentication REST APIs
- TPAM password vault
- EMM and MDM product support
- SIEM product support

Licensing Options

- Subscription (support included)
- Perpetual (support required)

Hardware appliance

SMA 6200 / 7200

SRA EX9000

Performance	SMA 6200	SMA 7200	SRA EX9000
Concurrent sessions / Users	Up to 2,500	Up to 10,000	Up to 20,000
SSL VPN Throughput (at max CCU)	Up to 400 Mbps	Up to 3.75Gbps	Up to 3.75 Gbps
Attributes	**SMA 6200**	**SMA 7200**	**SRA EX9000**
Form Factor	1U	1U	2U
Dimensions	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)	27.0 x 18.9 x 3.4 in (68.6 x 48.2x 8.8 cm)
Encryption Data Acceleration (AES-NI)	YES	YES	YES
Dedicated Management Port	YES	YES	YES
SSL Acceleration	YES	YES	YES
Hard Drive	2 X 500 GB SATA	2 X 500 GB SATA	2 X 2TB SATA
Interfaces	6 (6-port 1GE)	8 (6-port 1GE + 2-port 10Gb SFP+)	12 (8-port 1GE + 4-port 10Gb SFP+)
Memory	8GB DDR3	16GB DDR3	32 GB DDR3
TPM chip	YES	YES	NO
Processor	4 cores	4 cores	2 X 4 cores
MTBF	200,064 hours at 25°C (77°F)	233,892 hours at 25°C (77°F)	129,489 hours at 25°C (77°F)
Operations and Compliance	**SMA 6200**	**SMA 7200**	**SRA EX9000**
Power	Fixed power supply	Dual power supply, hot swappable	Dual power supply, hot swappable
Input rating	100-240 VAC, 1.1 A	100-240 VAC, 1.79 A	100-240 VAC, 2.8.5 A
Power Consumption	78 W	127 W	320 W
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)		
Certifications	FIPS 140-2 Level 2 with anti-tamper protection		

Virtual appliance specifications

	SMA 8200v (ESX/ESXI)	SMA 8200v (Hyper V)
Concurrent sessions	Up to 5000	Up to 250
SSL-VPN throughput (at max CCU)	Up to 1.58 Gbps	Up to 1.2 Gbps
Allocated memory	8 GB	
Processor	4 cores	
SSL acceleration	YES	
Applied disk size	64 GB (default)	Admin Configurable
Operating system installed	Hardened Linux	
Dedicated Management port	YES	

Core SKUs

SMA Appliance	SKU number
SMA 8200v	01-SSC-8468
SMA 6200	01-SSC-2300
SMA 7200	01-SSC-2301
SRA EX9000	01-SSC-9574
50 User CCU	01-SSC-7859
250 User CCU	01-SSC-7861
1,000 User CCU	01-SSC-7863
250 User 3 Year Support	01-SSC-2331
1,000 User 3 Year Support	01-SSC-2337

Optional SKUs

SMA Add-on	SKU Number
CMS Base (up to 3 Appliance)	01-SSC-8535
CMS up to 100 appliances 1yr	01-SSC-8536
50 User Pooled License*	01-SSC-2401
250 User Pooled License*	01-SSC-2403
1,000 User Pooled License*	01-SSC-8539
FIPS Add-on for SMA 7200	01-SSC-2406
FIPS Add-on for SMA 6200	01-SSC-2405
10 DAY 5- 1000 SPIKE FOR SMA 6200	01-SSC-2368

**GTO and SONAR included with pooled licensing*

About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, CA 95054
Refer to our website for additional information.
www.sonicwall.com

Datasheet-SMA-1000Series-US-KJ-24735