Secure Mobile Access 100 Series (SMA 210, 410, 500v)

Empower Remote Workforce without sacrificing security and ease of use

The SMA 100 series includes the SMA 210, 410 and 500v. It provides secure remote access optimized for small and medium businesses (50-100 employees). SMA 100 can be deployed on premises, in data centers or public clouds.

Its easy-to-use setup policy wizard and Cloud management system reduce deployment time and simplify the configuration of granular access policies. The result is a secure environment for any users to access corporate resources from anywhere.

SMA 100 Series Spec Preview. View full specs »

844 Mbps	400
Max SSL VPN Throughput (SMA 410)	Max Concurrent User Sessions (SMA 410)

HIGHLIGHTS

General Benefits:

- Supports VMWare ESXi, Hyper-V, KVM, AWS and Azure for hybrid-cloud deployments
- User-installable clients are available for macOS, Win10, Linux, ChromeOS, Android and iOS operating systems
- Deploys in minutes with setup and policy wizards
- Optional high-availability ensures zero-impact fail-over

Advanced Security Benefits

- Context-aware authentication limits access to only authorized users and trusted mobile devices
- Always-on VPN emulates in-office experience and maintains strong security posture
- Comes standard with secure clientless (web) access to resources via **HTML5** browser agents
- Integrates with the SonicWall Capture ATP, cloud-based multi-engine sandbox
- Built-in Web Application Firewall (WAF) to protect against web-based attacks and ensures PCI compliance
- Supports Geo IP detection and Botnet protection to stop DDoS and zombie attacks
- Integrates with Cloud Management and Reporting to provide real-time threat intelligence for VPN sessions, EPC, GEO IP/ BOTNET filtering, WAF and Capture ATP

Secure Remote Access Solution Optimized for Hybrid Cloud Environment

sonicwall.com/products

DATASHEET

With the modern workforce becoming increasingly mobile, maintaining effective security has become challenging. The SonicWall SMA 100 Series simplifies end-to-end secure remote access to any resources hosted across on-prem and cloud data centers, from more devices, without increasing the risk to your enterprise. Stringent access policies with layers of integrated advanced security features, and modern authentication ease administration and empower your workforce to work from anywhere.

EMPOWERING REMOTE WORKFORCE AND MOBILITY

For organizations wishing to embrace BYOD, enabling employees to work from anywhere, or securely enabling third-party access, the SMA 100 series can serve as the critical enforcement point. IT administrators have the flexibility to provision policy-based secure access and identity-based privileges to end-users and devices. It allows fast, simple access to the business resources, while at the same time, protects the corporate networks and data from rogue users and malware.

UNIFIED GATEWAY FOR MOBILE AND DESKTOP CLIENTS, OR WEB-BASED ACCESS

SMA 100 Series lowers IT costs by providing network managers with a centralized, secure access gateway for hundreds of users and devices.

It extends remote access to all network resources via SSL VPN for both internal and external users. These include web-based, client/server, host-based (such as virtual desktop), and back-connect applications (such as VoIP).

For mobile devices, the SMA 100 series supports special capabilities and policies to protect data at rest with SonicWall Mobile Connect. Authenticated users can securely browse, view intranet file shares and collaborate in a completely secure browser environment.

MODERN VPN FOR MIGRATION TO HYBRID CLOUD

For organizations embarking on cloud migration, the SMA 100 series provides flexible choices for any hybrid-cloud deployments, including physical, virtual appliances running on ESXi, Hyper-V, KVM, and virtual instances on AWS, Microsoft Azure public clouds.

Whether the corporate resource is on-premises, on the web, or in a hosted cloud, the SMA 100 series offers a single sign-on (SSO) with multi-factor authentication for added security. The result is a consistent and seamless user experience.

INTEGRATED ADVANCED SECURITY WITH END-POINT COMPLIANCE (EPC) AND ADVANCED THREAT PROTECTION (ATP)

To effectively reduce threat surfaces and empower users to work from anywhere and with any devices, the SMA 100 series consolidates several advanced security capabilities into one integrated solution.

SMA 100 relies on Endpoint Control (EPC) to grant network access to only authorized users and trusted devices. EPC validates the user and checks the device's health, making sure the operating system has the latest OS patches and malware-free.

Integration with the SonicWall Capture ATP, a cloud multi-engine sandbox, enables the SMA 100 to scan all files that users upload while outside the corporate network. The deep inspection of uploaded files ensures other users have the same level of protection from advanced threats (e.g., ransomware or zero-day malware) regardless of work locations.

To protect against botnet attacks, SMA 100 relies on Geo IP detection and Botnet protection to restrict any login attempt if the user location is out of the ordinary and unexpected.

GREATER CONTROL AND VISIBILITY WITH CLOUD MANAGEMENT AND REPORTING

SonicWall Cloud Management and Reporting (CSC) simplifies the management of the SMA 100 series both on-premises or across a hybrid-cloud environment. This robust cloud-based platform delivers single-pane-of-glass for security management, analytics, and real-time threat intelligence.

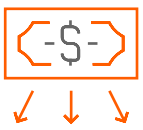
The simplicity extends to single-sign-on and support for the entire portfolio of SonicWall network, email, endpoint, mobile, and cloud security resources.

With SonicWall Cloud Management and Reporting (CSC), IT administrators can see everything connected to the network clearer than ever before.

INTEGRATED WEB APPLICATION FIREWALL (WAF)

Augment the perimeter firewall with the SMA 100 Series Web Application Firewall (WAF). SMA 100 Series WAF can detect sophisticated web-based attacks and protect web applications against web application malware.

Standard supports include OWASP Top Ten and PCI DSS compliance to protect against injection and cross-site scripting attacks (XSS), credit card and Social Security number theft, cookie tampering and cross-site request forgery (CSRF) from a malicious and rogue users.



LOW TOTAL COST OF OWNERSHIP

The SMA 100 series is a cost-effective platform designed to reduce IT overhead and overall TCO. A built-in setup wizard can reduce security policy configuration time to minutes and significantly simplify an initial deployment.

Physical appliance specifications

Performance	SMA 210	SMA 410
Concurrent sessions/Users	Up to 200	Up to 400
SSL VPN Throughput* (at max CCU)	560 Mbps	844 Mbps
Web Application Firewall (WAF) Throughput	515 Mbps	672 Mbps
Web Application Firewall (WAF) Transactions per second (TPS)	600	900
Form factor	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)
Appliance weight	11 lbs (5 kgs)	11 lbs (5 kgs)
Encryption data acceleration (AES-NI)	NO	NO
Dedicated management port	NO	NO
SSL acceleration	NO	NO
Storage	4GB (Flash Memory)	4GB (Flash Memory)
Interfaces	(2) GB Ethernet, (2) USB, (1) console	(4) GB Ethernet, (2) USB, (1) console
Memory	4GB	8GB
TPM chip	NO	NO
Processor	4 cores	8 cores
MTBF (@ 25°C or 77°F) in hours	61,815	60,151

Operations and Compliance	SMA 210	SMA 410
Power	Fixed power supply	
Input rating	100-240VAC, 50-60MHz	
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	

Virtual appliance specifications

Specifications	SMA 500v
Concurrent sessions	Up to 250 users
SSL-VPN throughput* (at max CCU)	Up to 265 Mbps
Web Application Firewall (WAF) Throughput	424 Mbps
Web Application Firewall (WAF) Transactions per second (TPS)	300
Allocated memory	4 GB
Processor	2 cores
SSL acceleration	NO
Recommended disk size	32 GB
Operating system installed	Linux
Dedicated management port	NO

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

SMA 100 series feature summary

Deployment

- Recommended SMA Firmware (v 10.2 onwards)
- Supported Hypervisors (VMware ESXi/ Microsoft Hyper-V, KVM)
- Supported Public Cloud Platforms (AWS, Azure)

Client access

- Layer 3 tunnel
- Split-tunnel and redirect-all
- Always On VPN
- Secure network detection
- HTML5 (RDP, VNC, ICA, SSH, Telnet, Network Explorer)
- File browser (CIFS/NFS)
- Citrix XenDesktop/XenApp
- CLI tunnel support
- Mobile Connect (iOS, Android, ChromeOS, Win10, macOS)
- Net Extender (Win 10, Linux)
- Exchange ActiveSync
- Key File Auth Support for SSH over HTML5

User portal

- Branding
- Customization
- Localization
- User defined bookmarks
- Custom URL support
- SaaS application support

Security

- TLS 1.3 support
- 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
- 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 and Reporting

- Management interface (ethernet)
- Management interface (console)
- HTTPS administration
- SNMP MIBS
- Syslog and NTP
- Usage monitoring
- Configuration rollback
- Management REST APIs
- Authentication REST APIs
- Scheduled tasks
- Event-driven auditing
- Cloud Management and Reporting (CSC)
- On-Box System Reporting Enhancements

Networking

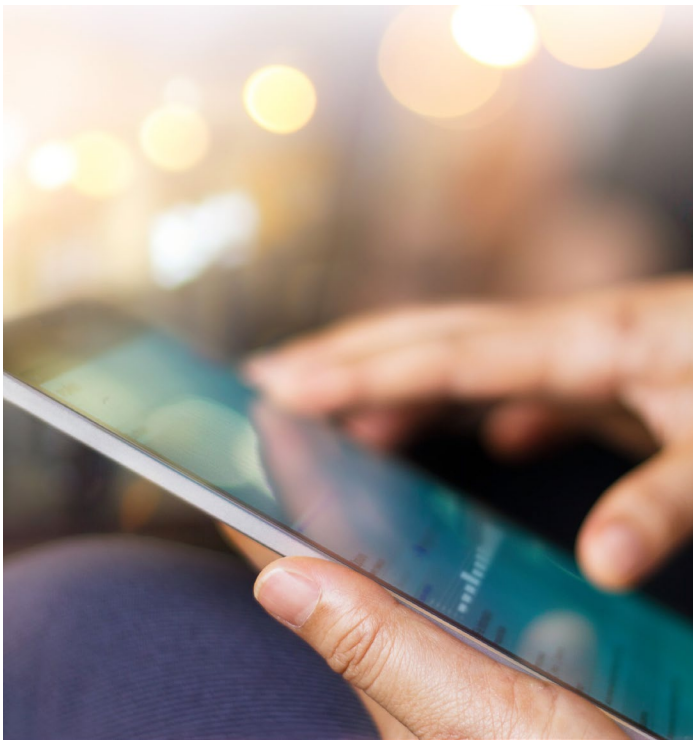
- IPv6
- TCP state replication
- Active/passive high availability
- Single or multiple FQDNs
- L3-7 smart tunnel proxy
- L7 application proxy

Integration

- 2FA TOTP support (Google Authenticator, MS Authenticator, DUO Security)
- EMM and MDM product support
- SIEM product support
- TPAM password vault

Licensing options

- Subscription based license
- Perpetual license with support
- Web Application Firewall (WAF)
- Spike licensing
- Tiered licensing



Easy-to-deploy, cost- effective and secure mobile access that addresses the needs of your increasingly mobile workforce.

To learn how you can be more successful in maintaining a healthy access security environment while achieving zero downtime, visit:

www.sonicwall.com/products/remote-access/secure-mobile-access-100-series

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. 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

SONICWALL