SonicWall Secure Mobile Access (SMA)

SonicWall SMA es una pasarela de acceso seguro unificado para organizaciones que se enfrentan a retos en materia de movilidad, BYOD y migración a la nube.

SonicWall SMA es una pasarela de acceso seguro unificado que permite a las organizaciones proporcionar acceso en cualquier momento y desde cualquier lugar y dispositivo a los recursos corporativos críticos. El motor de políticas de control granular del acceso, la autorización de dispositivos con sensibilidad contextual, la VPN a nivel de aplicación y la autenticación avanzada con inicio de sesión único de SMA permiten a las organizaciones adoptar enfoques BYOD y de movilidad en un entorno de TI híbrido.

Movilidad y BYOD

Para las organizaciones que desean adoptar modelos BYOD, de trabajo flexible o de acceso de terceros, SMA se convierte en el punto de refuerzo crítico para todos ellos. SMA proporciona la mejor seguridad de su categoría para minimizar la superficie de ataque de las amenazas y aumenta la seguridad de las organizaciones al soportar los últimos algoritmos de cifrado. SonicWall SMA permite a los administradores proporcionar acceso móvil seguro y privilegios basados en roles para que los usuarios finales puedan acceder de forma rápida y sencilla a las aplicaciones, los datos y los recursos de negocio que necesiten. Al mismo tiempo, las organizaciones pueden establecer políticas BYOD seguras para proteger sus redes y sus datos corporativos contra el acceso no autorizado y los ataques de malware.

El traslado a la nube

Para aquellas organizaciones que emprenden el viaje a la nube, SMA ofrece una infraestructura de inicio de sesión único (SSO) que utiliza un único portal Web para autenticar a los usuarios en un entorno de TI híbrido. Tanto si el recurso corporativo está en una ubicación local, como en la Web o en una nube hospedada, la experiencia de acceso es coherente y fluida. Además, SMA se integra con tecnologías de autenticación multifactor líderes para una mayor seguridad.

Proveedores de servicios gestionados

Tanto para organizaciones que hospedan su propia infraestructura como para proveedores de servicios gestionados, SMA proporciona una solución de llave en mano para garantizar un alto nivel de continuidad de negocio y escalabilidad. SMA puede soportar hasta 20.000 conexiones simultáneas en un solo dispositivo, y ofrece escalabilidad para soportar cientos de miles de usuarios a través de la agrupación inteligente (clústeres). Los centros de datos pueden reducir costes gracias a la agrupación (clústeres) activa-activa y a un equilibrador de carga dinámico integrado que reasigna el tráfico global al centro de datos más optimizado en tiempo real en base a la demanda de los usuarios. Los conjuntos de herramientas de SMA permiten a los proveedores de servicios prestar sus servicios sin interrupciones y cumplir, de esta forma, los SLAs más exigentes.

Con SMA, los departamentos de TI pueden proporcionar la mejor experiencia y el acceso más seguro en función del escenario de los usuarios. Disponible como dispositivo físico reforzado o como potente dispositivo virtual, SMA encaja a la perfección en su infraestructura de TI. Las organizaciones pueden elegir entre diversas posibilidades que abarcan desde un acceso seguro basado en Web sin clientes para terceros o empleados que utilizan dispositivos personales, hasta un acceso más tradicional mediante túnel VPN y basado en cliente para ejecutivos desde cualquier tipo de dispositivo. Tanto si las organizaciones necesitan proporcionar acceso seguro fiable a cinco usuarios desde una única ubicación, como si deben escalar su solución para miles de usuarios en centros de datos distribuidos por todo el mundo, SonicWall SMA tiene una solución.

SonicWall SMA permite a las organizaciones adoptar iniciativas BYOD y de movilidad sin miedo alguno, así como trasladarse a la nube fácilmente. SMA aumenta las posibilidades del personal y les brinda una experiencia de acceso coherente.

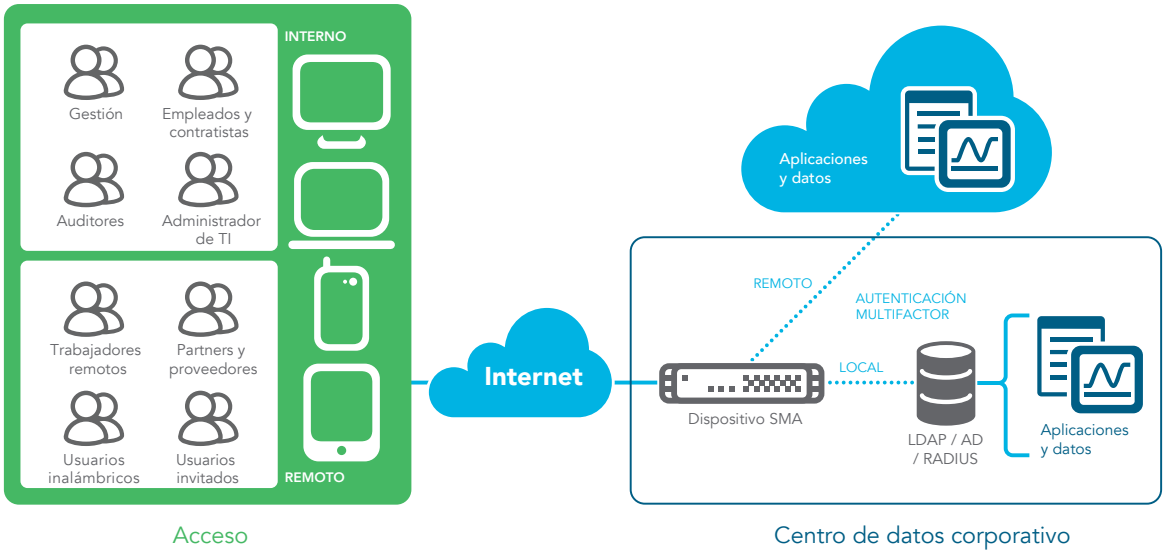
Ventajas:

- Acceso unificado a todos los recursos de la red y de la nube para poder acceder "en cualquier momento, desde cualquier dispositivo y a cualquier aplicación" de forma segura
- Controle quién accede a qué recursos mediante la definición de políticas granulares gracias al robusto motor de control del acceso
- Aumente la productividad al proporcionar funciones de inicio de sesión combinado a cualquier aplicación hospedada de forma local o SaaS con una sola URL
- Reduzca el TCO y la complejidad de la gestión del acceso al consolidar los componentes de la infraestructura en un entorno de TI híbrido
- Obtenga visibilidad de todos los dispositivos que se conectan y conceda acceso en base a políticas y al estado del punto terminal
- Prevenga los ataques de malware escaneando todos los archivos que se carguen en su red con el sandbox Capture ATP
- Ofrezca protección contra los ataques basados en Web y cumpla las normas de la PCI con el add-on Web Application Firewall
- Detenga los ataques DDoS y de zombis con detección basada en la dirección IP y la localización geográfica y protección contra botnets
- Disfrute de funciones nativas y seguras de agente utilizando acceso HTML5 sin clientes basado en navegador Web sin la necesidad de instalar ni mantener agentes en los dispositivos terminales
- Obtenga información relevante para tomar decisiones acertadas gracias a las funciones de monitorización en tiempo real e informes completos
- Simplifique la implementación con opciones flexibles de dispositivos virtuales y físicos según las necesidades de su empresa
- Permita la emisión dinámica de licencias de acceso en base a la demanda en tiempo real, con dirección automática de los puntos terminales a la conexión de mayor rendimiento y menor latencia
- Reduzca los costes iniciales con equilibrio de carga integrado sin hardware ni servicios adicionales, proporcionando al mismo tiempo funciones de reconexión de dispositivos sin impacto alguno sobre el usuario
- Protéjase contra las interrupciones del negocio o los picos estacionales escalando la capacidad de forma instantánea

Dispositivo SMA e implementación

Pasarela reforzada de borde de red para proporcionar acceso seguro en cualquier momento y desde cualquier lugar y dispositivo

SMA es una pasarela de seguridad de acceso avanzada que ofrece acceso seguro a los recursos de la red y de la nube desde cualquier dispositivo. SMA ofrece funciones de refuerzo centralizadas, granulares y basadas en políticas de acceso remoto y móvil a cualquier recurso corporativo puesto a disposición a través de un dispositivo reforzado basado en Linux. Disponible como dispositivo físico reforzado o como potente dispositivo virtual, SMA encaja a la perfección en cualquier infraestructura de TI existente.



Las soluciones SMA proporcionan acceso seguro para todos los usuarios, dispositivos y aplicaciones.

Implementación flexible con dispositivos físicos y virtuales

SonicWall SMA puede implementarse como dispositivo reforzado de alto rendimiento o como dispositivo virtual utilizando recursos informáticos compartidos para optimizar el uso, facilitar la migración y reducir los costes de capital. Los dispositivos de hardware se basan en una arquitectura multinúcleo de alto rendimiento con aceleración SSL, rendimiento VPN y proxies potentes para ofrecer un acceso seguro y eficaz. Para las organizaciones reguladas y federales, SMA también está disponible con certificación FIPS 140-2 de nivel 2. Los dispositivos virtuales SMA ofrecen las mismas prestaciones de acceso seguro y eficaz en las principales plataformas virtuales, como Microsoft Hyper-V y VMware ESX.

Licencias de usuario compartidas entre diferentes dispositivos

Las organizaciones con dispositivos distribuidos por todo el mundo pueden beneficiarse de la fluctuante demanda de licencias de usuarios consecuencia de las diferencias horarias. Tanto si una organización implementa licencias VPN completas como licencias ActiveSync básicas, la gestión centralizada de SMA toma las licencias de los dispositivos de zonas en las que el uso ha descendido por ser de noche o haber finalizado el horario de oficina y las asigna a los dispositivos gestionados donde la demanda de los usuarios ha aumentado.

Visibilidad de la red gracias a la creación de perfiles de dispositivos con sensibilidad contextual

Gracias al mejor sistema de autenticación sensible al contexto, únicamente acceden a los recursos los dispositivos de confianza y los usuarios autorizados. También se someten a interrogatorio los portátiles y PCs para obtener información sobre la presencia o ausencia de software de seguridad, los certificados de cliente y la ID de los dispositivos. El sistema interroga los dispositivos para obtener información esencial sobre la seguridad, como la existencia de jailbreaks y accesos root, la ID del dispositivo, así como información sobre certificados y versiones del SO, antes de permitir el acceso. Si un dispositivo no cumple los requisitos previstos en las políticas, no se permite su acceso a la red y se informa al usuario del incumplimiento.

Experiencia coherente desde un único portal Web

Los usuarios no necesitan recordar las URLs de cada una de las aplicaciones ni mantener marcadores exhaustivos. SMA proporciona un portal de acceso centralizado, de modo que los usuarios pueden acceder a todas las aplicaciones críticas de negocio con una sola URL desde un navegador Web estándar. Una vez que el usuario inicia sesión a través de un navegador, en la ventana del navegador aparece un portal Web personalizable para los usuarios, con una única consola, desde la que se puede acceder a cualquier aplicación SaaS o local. El portal solo muestra enlaces y marcadores personalizados relevantes para el punto terminal, usuario o grupo en cuestión. El portal soporta todas las principales plataformas de dispositivos, como Windows, Mac OS, Linux, iOS y Android, así como una amplia variedad de navegadores.

Inicio de sesión único combinado para aplicaciones SaaS y locales

Elimine la necesidad de tener múltiples contraseñas, y ponga fin a las malas prácticas de seguridad, como la reutilización de contraseñas. SMA proporciona un inicio de sesión único combinado a aplicaciones SaaS hospedadas en la nube y a aplicaciones hospedadas en campus. SMA se integra con múltiples servidores de autenticación, autorización y contabilidad, así como con tecnologías de autenticación multifactor líderes para ofrecer un mayor nivel de seguridad. Solo se proporciona inicio de sesión seguro a los dispositivos terminales autorizados después de que SMA haya comprobado el estado y la conformidad con las normas del punto terminal. El motor de políticas de acceso

garantiza que los usuarios solo puedan ver las aplicaciones autorizadas y les concede acceso solo después de que hayan pasado con éxito el proceso de autenticación.

Prevención de brechas y amenazas avanzadas

SonicWall SMA proporciona una capa adicional de seguridad del acceso para mejorar su seguridad y reducir la superficie de ataque para las amenazas.

- SMA se integra con el sandbox multimotor basado en la nube SonicWall Capture ATP para escanear todos los archivos cargados por los usuarios desde puntos terminales no gestionados, o por los que se encuentran fuera de la red corporativa. De este modo, los usuarios gozan del mismo nivel de protección contra las amenazas avanzadas, como el ransomware o el malware de día cero, cuando están de viaje que cuando trabajan desde la oficina.[1]
- El servicio Web Application Firewall de SonicWall ofrece a las empresas una solución asequible y bien integrada para proteger las aplicaciones internas basadas en Web. Como resultado, los clientes pueden estar seguros de la confidencialidad de los datos, y de que los servicios Web internos no se verán comprometidos en el caso de que accedan usuarios maliciosos o no autorizados.
- Las funciones de detección de botnets y basadas en la dirección IP y la localización geográfica protegen a las organizaciones contra los ataques DDoS y zombis, y contra los puntos terminales comprometidos que se utilizan a modo de botnets.

Acceso fluido y seguro sin clientes basado en navegador

Puesto que SonicWall SMA funciona por completo sin clientes, no es necesario que el administrador instale manualmente un componente de cliente pesado en los ordenadores destinados a acceder de forma remota a los recursos de la red. De este modo, se elimina toda dependencia de Java y se reducen los gastos de TI, ampliando enormemente el concepto de acceso remoto. Esto significa que no se requieren tareas de preinstalación ni preconfiguración. Un trabajador remoto autorizado puede acceder de forma segura a los recursos corporativos desde cualquier ordenador en cualquier lugar del mundo. En su versión más pura, el acceso seguro se basa estrictamente en navegador, mediante HTML5, lo cual proporciona a los usuarios una experiencia fluida y unificada.

Proporcione una experiencia sin interrupciones

Para garantizar una experiencia de usuario fluida, SMA ofrece una VPN siempre disponible para dispositivos Windows gestionados. Los administradores pueden configurar los ajustes para establecer automáticamente una conexión VPN cada vez que un cliente de un punto terminal autorizado detecte una red pública o no fiable. Un solo evento de inicio de sesión en el dispositivo de Windows proporciona al usuario una conexión segura a los recursos corporativos. Los usuarios no tienen que iniciar sesión en sus clientes VPN ni mantener contraseñas adicionales. Esto proporciona a los usuarios móviles una experiencia fluida para acceder a recursos de misión crítica igual que si estuvieran en la oficina y permite a los administradores de TI mantener el control sobre los dispositivos gestionados, mejorando el estado de seguridad de la organización.

Gestión intuitiva y funciones completas de informes

SonicWall proporciona una plataforma de gestión intuitiva basada en Web para optimizar la gestión de los dispositivos, así como amplias funciones de informes. La GUI ofrece una forma sencilla y clara de gestionar uno o múltiples dispositivos y las correspondientes políticas. Cada página muestra cómo se configuran los ajustes en todos los equipos gestionados. La gestión unificada de políticas le ayuda a crear y monitorizar políticas de acceso y configuraciones. Una sola política puede controlar el acceso de sus usuarios, dispositivos y aplicaciones a los datos, los servidores y las redes. El personal de TI puede automatizar las tareas rutinarias y planificar actividades, librando a los equipos de seguridad de las tareas repetitivas para que puedan centrarse en las tareas de seguridad estratégicas, como en la respuesta a posibles incidentes. Los responsables de TI obtienen una visión de las tendencias de acceso de los usuarios y del estado de todo el sistema a través de funciones de informes fáciles de usar y de protocolización centralizada.

Ofrezca servicios disponibles las 24 horas

Las organizaciones deben mantener sus servicios sin interrupciones y con un alto nivel de fiabilidad para proporcionar un acceso seguro a las aplicaciones críticas de negocio en todo momento. Los dispositivos SMA soportan la tradicional alta disponibilidad activa-pasiva para organizaciones con un solo centro de datos, o bien alta disponibilidad global con agrupación (clústeres) activa-activa para centros de datos locales o distribuidos. Ambos modelos de alta disponibilidad ofrecen a los usuarios una experiencia fluida con reconexión y persistencia de sesión y sin impacto alguno.

Implemente el cliente VPN que mejor se adapte a sus necesidades

Elija entre una amplia variedad de clientes VPN para ofrecer acceso remoto seguro basado en políticas para varios puntos terminales, incluidos portátiles, teléfonos inteligentes y tablets.

Cliente VPN	SO soportado	Modelo de SMA soportado	Prestación más destacada
Mobile Connect	iOS, OS X, Android, Chrome OS, Windows 10	Todos los modelos	Proporcione autenticación biométrica, VPN por aplicación y refuerzo del control de los puntos terminales
Connect Tunnel (Cliente ligero)	Windows, Mac OS y Linux	6200, 7200, 8200v, 9000	Proporcione una experiencia "de oficina" completa con funciones eficaces de control de puntos terminales
NetExtender (Cliente ligero)	Windows y Linux	200, 400, 500v	Refuerce las políticas granulares de acceso y amplíe el acceso a la red por medio de clientes nativos

Reduzca los costes iniciales con un equilibrador de carga integrado

La funcionalidad de equilibrio de carga integrada en el dispositivo SMA proporciona el nivel de escalabilidad que cabe esperar para implementaciones de empresas medianas y grandes. Algunos modelos de dispositivos SMA ofrecen equilibrio de carga dinámico para asignar de forma inteligente cargas de sesiones y licencias de usuarios en tiempo real en base a la demanda. Las organizaciones no necesitan invertir en equilibradores de carga externos, lo cual reduce los coses iniciales.

Protéjase contra eventos imprevistos

Una solución completa de continuidad de negocio y recuperación de desastres debe ser capaz de soportar picos importantes en el tráfico de acceso remoto, manteniendo al mismo tiempo el control de la seguridad y de los costes. Los paquetes de licencias SonicWall Spike para SMA son licencias add-on que permiten a las empresas distribuidas escalar el número de usuarios y alcanzar su capacidad máxima de forma instantánea, permitiendo una continuidad del negocio sin fisuras. Gracias a las licencias Spike, puede añadir decenas o incluso cientos de usuarios adicionales, de modo que su empresa queda perfectamente protegida contra cualquier evento, ya sea previsto o imprevisto, que pueda provocar un pico en la demanda.

Prestaciones

Autenticación avanzada

Inicio de sesión único combinado[2]	SMA utiliza autenticación SAML 2.0 para permitir un inicio de sesión único combinado a través de un único portal para acceder a recursos tanto locales como en la nube, al tiempo que refuerza la autenticación stacked multifactor para proporcionar un mayor nivel de seguridad.
Autenticación multifactor	Certificados digitales X.509 Certificados digitales del lado del servidor y del lado del cliente RSA SecurID, Dell Defender, Google Authenticator, Duo Security y otros tokens de autenticación con contraseña de un solo uso/de doble factor Tarjeta Common Access Card (CAC) Autenticación dual o stacked Soporte de Captcha, nombre de usuario/contraseña
Autenticación SAML	SMA puede configurarse como Proveedor de identidades de SAML (IdP), Proveedor de servicios de SAML (SP) o como proxy para un IdP local existente para permitir el inicio de sesión único combinado utilizando autenticación SAML 2.0.
Repositorios de autenticación	SMA proporciona integraciones sencillas con repositorios estándar de la industria para simplificar la gestión de las cuentas y contraseñas de los usuarios. Se pueden crear grupos de usuarios (incluidos grupos anidados) de forma dinámica basados en repositorios de autenticación como RADIUS, LDAP o Active Directory. Se pueden interrogar atributos LDAP comunes o personalizados para una autorización específica o la verificación del registro de dispositivos.
Proxy de aplicaciones de capas 3-7	SMA ofrece opciones de proxy flexibles, por ejemplo, el acceso para proveedores puede proporcionarse a través de un proxy directo, para los contratistas a través de un proxy inverso y el acceso para los empleados a Exchange a través de ActiveSync.
Proxy inverso	El servicio de proxy inverso mejorado con autenticación permite a los administradores configurar un portal de descarga de aplicaciones y marcadores, para que los usuarios puedan conectarse fácilmente a las aplicaciones remotas y a los recursos, incluidos RDP y HTTP. Esta prestación soporta todos los navegadores, incluidos IE, Chrome y Firefox.
Delegación limitada de Kerberos	SMA ofrece soporte de autenticación utilizando una infraestructura Kerberos existente, que no necesita servicios front-end fiables para delegar un servicio.

Gestión del acceso

Motor de control del acceso (ACE)	Los administradores conceden o deniegan el acceso en base a las políticas de la organización y establecen medidas correctivas al poner sesiones en cuarentena. La política basada en objetos del motor ACE utiliza elementos de red, recurso, identidad, dispositivo, aplicación, datos y tiempo.
Control de puntos terminales (EPC)	El EPC permite al administrador reforzar las normas de acceso granulares en base al estado del dispositivo que se conecta. Dada la profunda integración con el SO, muchos elementos se combinan para la clasificación por tipos y la evaluación de riesgos. La interrogación EPC simplifica la creación de perfiles de equipos mediante una exhaustiva lista predefinida de soluciones antivirus, antispyware y de firewall personal para las plataformas Windows, Mac y Linux, que incluye la versión y el nivel de aplicabilidad del archivo de definiciones actualizado.
Control del acceso de las aplicaciones (AAC)	Los administradores pueden definir qué aplicaciones móviles específicas pueden acceder a qué recursos de la red a través de túneles de aplicaciones individuales. Las políticas AAC se refuerzan tanto en el cliente como en el servidor, ofreciendo una sólida protección del perímetro.

Seguridad superior

SSL VPN de capa 3	La serie SMA x000 ofrece prestaciones de túneles de capa 3 de alto rendimiento para una amplia variedad de dispositivos cliente en cualquier entorno.
Soporte de criptografía	Duración de sesión configurable Cifrado: AES de 128 + 256 bits, Triple DES, RC4 de 128 bits Hashes: MD5, SHA-256, SHA-1 Algoritmo de firma digital basado en curvas elípticas (ECDSA)
Soporte de cifrado avanzado	Gracias a los procedimientos de cifrado por defecto, los dispositivos SMA x000 proporcionan un robusto sistema de seguridad para el cumplimiento normativo listo para usar. Los administradores pueden ajustarlo según sus necesidades de rendimiento, seguridad y compatibilidad.
Certificaciones de seguridad	Certificado para FIPS 140-2 Nivel 2, ICSA SSL-TLS
Uso compartido y seguro de archivos	Detenga los ataques de día cero desconocidos, como el ransomware, en la pasarela, con implementación automática de definiciones. Los archivos cargados utilizando puntos terminales no gestionados con acceso seguro a las redes corporativas son inspeccionados por nuestro sandbox multimotor basado en la nube Capture ATP.
Web Application Firewall	Prevenga los ataques basados en Web y protocolos, ayudando a las empresas financieras, sanitarias, de comercio electrónico, etc. a conseguir entrar en el Top 10 de OWASP y a cumplir las normas de la PCI.
Detección de Geo IP y protección de botnets	Gracias a la detección de Geo IP y la protección de botnets, los clientes pueden permitir o restringir el acceso de los usuarios desde varias ubicaciones geográficas.

Experiencia de usuario intuitiva

VPN siempre disponible	Establezca automáticamente una conexión segura a la red corporativa desde dispositivos Windows gestionados por la empresa para mejorar la seguridad, obtener visibilidad del tráfico y mantener el cumplimiento normativo.
Detección segura de red (SND)	El cliente VPN con reconocimiento de red de SMA detecta cuándo el dispositivo está fuera del campus y reconecta la VPN automáticamente, volviéndola a desconectar cuando el dispositivo regresa a una red de confianza.
Acceso a los recursos sin clientes	SMA brinda acceso seguro sin clientes a los recursos mediante agentes de navegador HTML5 proporcionando protocolos RDP, ICA, VNC, SSH y Telnet.
Portal de inicio de sesión único	El portal WorkPlace proporciona una vista sencilla y personalizable desde una única consola, para un acceso seguro con inicio de sesión único (SSO) a cualquier recurso de un entorno de TI híbrido. No se requieren inicio de sesión ni VPN adicionales.
Túneles de capa 3	Los administradores pueden elegir Split-Tunnel o reforzar el modo "Redirigir todo" con túneles SSL/TLS y fallback ESP opcional para maximizar el rendimiento.
Explorador de archivos HTML5[1]	El moderno navegador de archivos permite a los usuarios acceder fácilmente a archivos compartidos desde cualquier navegador Web.
Integración de SO móvil	Todas las plataformas de SO soportan Mobile Connect, lo cual proporciona a los usuarios total flexibilidad a la hora de elegir dispositivos móviles.

Resiliencia

Optimizador de tráfico global (GTO)	SMA ofrece equilibrio de carga del tráfico global sin impacto alguno para los usuarios. El tráfico es enrutado al centro de datos más optimizado y de mayor rendimiento.
Alta disponibilidad dinámica[2]	SMA soporta la configuración Activa/Pasiva y ofrece la configuración Activa/Activa para alta disponibilidad, ya sea implementada en un solo centro de datos o en múltiples centros de datos geográficamente dispersos.
Persistencia de sesión universal[1]	Proporcione a los usuarios una experiencia fluida con reconexión y sin impacto alguno. En caso de que un dispositivo se desconecte, la agrupación en clústeres inteligente de SMA reasigna a los usuarios, junto con los datos de su sesión, sin necesidad de que se repita la autenticación.
Rendimiento escalable	Los dispositivos SMA x000 pueden escalar su rendimiento de forma exponencial mediante la aplicación de múltiples dispositivos, eliminando así la existencia de un punto único de fallo. La agrupación horizontal soporta la mezcla de dispositivos SMA físicos y virtuales.
Licencias dinámicas	Ya no es necesario aplicar licencias de usuario a los dispositivos SMA individuales. Los usuarios pueden distribuirse y reasignarse dinámicamente entre los dispositivos gestionados, en base a la demanda.

Gestión centralizada y monitorización

Sistema de gestión central (CMS)	CMS proporciona gestión centralizada basada en Web para todas las funciones de SMA.
Alertas personalizadas	Se pueden configurar las alertas para generar traps SNMP monitorizados por el NMS (Sistema de gestión de red) de cualquier infraestructura de TI. Asimismo, los administradores pueden configurar alertas para que Capture ATP realice escaneados de archivos y para comprobar el uso del espacio en disco a fin de que se tomen medidas de inmediato.
Monitorización mediante SONAR	SonicWall SONAR permite a los administradores de TI diagnosticar los problemas de acceso de forma rápida y sencilla y obtener información valiosa para la resolución de problemas.
Integración con SIEM	La transmisión en tiempo real a recopiladores de datos SIEM centrales permite a los equipos de seguridad correlacionar actividades basadas en eventos para comprender el flujo de trabajo de extremo a extremo de un usuario o una aplicación en concreto. Esto resulta vital para la gestión de incidentes de seguridad y los análisis forenses.
Programador	El programador permite a los usuarios programar tareas de mantenimiento, como la implementación de políticas, la replicación de ajustes de configuración y el reinicio de servicios, sin intervención manual.

Ampliabilidad

APIs de gestión	Las APIs de gestión proporcionan un control administrativo programático completo de todos los objetos dentro de un solo entorno SMA o de un entorno CMS global.
APIs para usuarios finales	Las APIs para usuarios finales proporcionan control completo sobre todo el flujo de trabajo de inicio de sesión, autenticación y puntos terminales.
Autenticación de doble factor (2FA)	SMA proporciona 2FA al integrarse con las principales soluciones de contraseñas basadas en el tiempo y de un solo uso (TOTP), como Google Authenticator, Microsoft Authenticator, Duo security, etc.
Integración con MDM	SMA se integra con los principales productos de gestión móvil empresarial (FMM), como Airwatch y Mobile Iron.
Integración con productos de terceros	SMA se integra con proveedores líderes en el sector, como OPSWAT, para proporcionar protección contra las amenazas avanzadas

[1]*Disponible con SMA OS 12.1 o superior*

[2]*Mejorado en SMA 12.1*

Visión de conjunto de las prestaciones (comparación por modelos)

Categoría	Prestación	200	400	500v	6200	7200	9000	8200v
Rendimiento	Sesiones de usuarios simultáneas máximas	50	250	250	2.000	10.000	20.000	5.000
	Rendimiento SSL/TLS máx.	100 Mbps	368 Mbps	186 Mbps	400 Mbps	3,75 Gbps	3,75 Gbps	1,58 Gbps
Acceso cliente	Túnel capa 3	•	•	•	•	•	•	•
	Split-tunnel y redirigir todo	•	•	•	•	•	•	•
	VPN siempre disponible	•	•	•	•	•	•	•
	Autoencapsulado ESP	–	–	–	•	•	•	•
	HTML5 (RDP, VNC, ICA, SSH, Telnet, Network Explorer)	•	•	•	•	•	•	•
	Detección segura de red	–	–	–	•	•	•	•
	Navegador de archivos (CIFS/NFS)	•	•	•	•	•	•	•
	Citrix XenDesktop/XenApp	•	•	•	•	•	•	•
	Vista de VMware	–	–	–	•	•	•	•
	Túnel a demanda	–	–	–	•	•	•	•
	Extensiones Chrome/Firefox	–	–	–	•	•	•	•
	Soporte túnel CLI	–	–	–	•	•	•	•
	Mobile Connect (iOS, Android, Chrome, Win 10, Mac OSX)	•	•	•	•	•	•	•
	Net Extender (Windows, Linux)	•	•	•	–	–	–	–
	Connect Tunnel (Windows, Mac OSX, Linux)	–	–	–	•	•	•	•
	Exchange ActiveSync	•	•	•	•	•	•	•
Acceso móvil	VPN por aplicación	–	–	–	•	•	•	•
	Refuerzo del control de aplicaciones	–	–	–	•	•	•	•
	Validación ID de aplicación	–	–	–	•	•	•	•
Portal de usuarios	Adaptación a la marca	•	•	•	•	•	•	•
	Personalización	–	–	–	•	•	•	•
	Ubicación	•	•	•	•	•	•	•
	Marcadores definidos por los usuarios	•	•	•	•	•	•	•
	Soporte de URLs personalizadas	•	•	•	•	•	•	•
	Soporte de aplicaciones SaaS	–	–	–	•	•	•	•
Seguridad	FIPS 140-2	–	–	–	•	•	•	–
	ICSA SSL-TLS	–	–	–	•	•	•	•
	Cifrado Suite B	–	–	–	•	•	•	•
	Interrogación EPC dinámica	•	•	•	•	•	•	•
	Control del acceso basado en roles (RBAC)	–	–	–	•	•	•	•
	Registro de puntos terminales	•	•	•	•	•	•	•
	Uso compartido y seguro de archivos (Capture ATP)	•	•	•	•	•	•	•
	Protección antimalware de Capture	–	–	–	•	•	•	•
	Cuarentena de puntos terminales	•	•	•	•	•	•	•
	Validación CRL OSCP	–	–	–	•	•	•	•
	Selección de cifrado	–	–	–	•	•	•	•
	PKI y certificados de cliente	•	•	•	•	•	•	•
	Filtrado GeoIP	•	•	•	–	–	–	–
	Filtro de botnets	•	•	•	–	–	–	–
	Proxy directo	•	•	•	•	•	•	•
	Proxy inverso	•	•	•	•	•	•	•
Servicios de autenticación e identidad	SAML 2.0	–	–	–	•	•	•	•
	LDAP, RADIUS	•	•	•	•	•	•	•
	Kerberos (KDC)	•	•	•	•	•	•	•
	NTLM	•	•	•	•	•	•	•
	Proveedor de identidades de SAML (IdP)	–	–	–	•	•	•	•
	Soporte de dispositivos biométricos	•	•	•	•	•	•	•
	Soporte de identificador facial para iOS	•	•	•	•	•	•	•
	Autenticación de doble factor (2FA)	•	•	•	•	•	•	•
	Autenticación multifactor (MFA)	–	–	–	•	•	•	•

SONICWALL®

Visión de conjunto de las prestaciones (comparación por modelos, cont.)

Categoría	Prestación	200	400	500v	6200	7200	9000	8200v
Servicios de autenticación e identidad (cont.)	Autenticación encadenada	–	–	–	•	•	•	•
	Código de acceso de un solo uso (OTP)	•	•	•	•	•	•	•
	Compatibilidad con tarjetas Common Access Card (CAC)	–	–	–	•	•	•	•
	Soporte de certificado X.509	•	•	•	•	•	•	•
	Integración con Captcha	–	–	–	•	•	•	•
	Cambio de contraseña remoto	•	•	•	•	•	•	•
	SSO basado en formas	•	•	•	•	•	•	•
	SSO combinado	–	–	–	•	•	•	•
	Persistencia de sesión	–	–	–	•	•	•	•
	Inicio de sesión automático	•	•	•	•	•	•	•
Control de acceso	AD de grupo	•	•	•	•	•	•	•
	Atributos LDAP	•	•	•	•	•	•	•
	Políticas de ubicación geográfica	•	•	•	–	–	–	–
	Monitorización de puntos terminales continua	•	•	•	•	•	•	•
Gestión	Interfaz de gestión (ethernet)	–	–	–	•	•	•	•
	Interfaz de gestión (consola)	–	–	–	•	•	•	•
	Administración HTTPS	•	•	•	•	•	•	•
	Administración SSH	–	–	–	•	•	•	•
	SNMP MIBS	•	•	•	•	•	•	•
	Syslog y NTP	•	•	•	•	•	•	•
	Monitorización del uso	•	•	•	•	•	•	•
	Reversión de la configuración	•	•	•	•	•	•	•
	Gestión centralizada	–	–	–	•	•	•	•
	Informes centralizados	–	–	–	•	•	•	•
	APIs REST de gestión	–	–	–	•	•	•	•
	APIs REST de autenticación	–	–	–	•	•	•	•
	Contabilidad RADIUS	–	–	–	•	•	•	•
	Tareas planificadas	–	–	–	•	•	•	•
	Licencias de sesiones centralizadas	–	–	–	•	•	•	•
	Auditorías basadas en eventos	–	–	–	•	•	•	•
Interconexión	IPv6	•	•	•	•	•	•	•
	Equilibrio de carga global	–	–	–	•	•	•	•
	Equilibrio de carga de servidor	•	•	•	–	–	–	–
	Replicación de estado TCP	•	•	•	•	•	•	•
	Reconexión de estado de clúster	–	–	–	•	•	•	•
	Alta disponibilidad activa/pasiva	–	•	•	•	•	•	•
	Alta disponibilidad activa/activa	–	–	–	•	•	•	•
	Escalabilidad horizontal	–	–	–	•	•	•	•
	FQDNs individuales o múltiples	–	–	–	•	•	•	•
	Proxy de túnel inteligente capa 3-7	•	•	•	•	•	•	•
	Proxy de aplicación capa 7	•	•	•	•	•	•	•
Integración	Soporte de aplicaciones móviles con 2FA	•	•	•	•	•	•	•
	Soporte de productos FMM y MDM	–	–	–	•	•	•	•
	Soporte de productos SIEM	–	–	–	•	•	•	•
	Almacén de contraseñas TPAM	–	–	–	•	•	•	•
	Soporte de hipervisor ESX	–	–	•	–	–	–	•
	Soporte de hipervisor Hyper-V	–	–	–	–	–	–	•
Opciones de licencias	Licencia basada en suscripción	–	–	–	•	•	•	•
	Licencia perpetua con soporte	•	•	•	•	•	•	•
	Web Application Firewall (WAF)	•	•	•	–	–	–	–
	Licencias Spike	•	•	•	•	•	•	•
	Licencias escalonadas	–	–	–	•	•	•	•
	Virtual assist	•	•	•	–	–	–	–

** Para obtener más información sobre clientes VPN, visite: https://www.sonicwall.com/en-us/products/remote-access/vpn-client*

SONICWALL®

Ventajas de una actualización a un dispositivo de alta gama

Mayor rendimiento | Mayor capacidad de procesamiento | Prestaciones avanzadas | Escalabilidad mejorada

Especificaciones de los dispositivos

Elija entre una variedad de dispositivos creados específicamente para ofrecer acceso móvil seguro (SMA).
Obtenga opciones de implementación flexibles con dispositivos virtuales y físicos.

Especificaciones de los dispositivos físicos

Rendimiento	SMA 200	SMA 400	SMA 6200	SMA 7200	SRA EX9000
Sesiones/Usuarios simultáneos	Hasta 50	Hasta 250	Hasta 2.000	Hasta 10.000	Hasta 20.000
Rendimiento SSL VPN* (con CCU máx.)	Hasta 100 Mbps	Hasta 368 Mbps	Hasta 400 Mbps	Hasta 3,75 Gbps	Hasta 3,75 Gbps
Factor de forma	1U	1U	1U	1U	2U
Dimensiones	43 x 26 x 4,5 cm (16,92x10,23x1,75 pulgadas)	43 x 26 x 4,5 cm (16,92x10,23x1,75 pulgadas)	43 x 41,5 x 4,5 cm (17,0 x 16,5 x 1,75 pulgadas)	43 x 41,5 x 4,5 cm (17,0 x 16,5 x 1,75 pulgadas)	68,6 x 48,2 x 8,8 cm (27,0 x 18,9 x 3,4 pulgadas)
Peso del dispositivo	5 kg (11 libras)	5 kg (11 libras)	7,3 kg (16 libras)	8,3 kg (18,3 libras)	22,3 kg (49,1 libras)
Aceleración de cifrado y descifrado (AES-NI)	NO	NO	SÍ	SÍ	SÍ
Puerto de gestión dedicado	NO	NO	SÍ	SÍ	SÍ
Aceleración SSL	NO	NO	SÍ	SÍ	SÍ
Almacenamiento	2GB (Memoria Flash)	2GB (Memoria Flash)	2 X 500 GB SATA	2 X 500 GB SATA	2 X 2TB SATA
Interfaces	(2) GB Ethernet, (2) USB, (1) consola	(4) GB Ethernet, (2) USB, (1) consola	6 (6 puertos 1GE)	8 (6 puertos 1GE + 2 puertos 10Gb SFP+)	12 (8 puertos 1GE + 4 puertos 10Gb SFP+)
Memoria	2GB	4GB	8GB DDR3	16GB DDR3	32 GB DDR3
Chip TPM	NO	NO	SÍ	SÍ	NO
Procesador	2 núcleos	4 núcleos	4 núcleos	4 núcleos	2 X 4 núcleos
MTBF (@ 25°C o 77°F) en horas	61.815	60.151	200.064	233.892	129.489
Operaciones y conformidad con normas	**SMA 200**	**SMA 400**	**SMA 6200**	**SMA 7200**	**SRA EX9000**
Alimentación	Alimentación fija	Alimentación fija	Alimentación fija	Alimentación dual de cambio en caliente	Alimentación dual de cambio en caliente
Corriente de entrada	100-240 V CA, 50-60 MHz	100-240 V CA, 50-60 MHz	100-240 V CA, 1,1 A	100-240 V CA, 1,79 A	100-240 V CA, 2,85 A
Consumo eléctrico	26,9 W	31,9 W	78 W	127 W	320 W
Disipación de calor total	92 BTU	109 BTU	266 BTU	432 BTU	1091 BTU
Entorno	WEEE, EU RoHS, China RoHS				
Resistencia al impacto (en reposo)	110 g, 2 ms				
Emisiones	FCC, ICES, CE, C-Tick, VCCI; MIC				
Seguridad	TÜV/GS, UL, CE PSB, CCC, BSMI, CB Scheme				
Temperatura de servicio	0°C a 40°C (32°F a 104° F)				
Certificación FIPS	NO	NO	FIPS 140-2 nivel 2 con protección antimanipulación		

** El rendimiento de la transferencia de datos puede variar en función de la implementación y la conectividad. Los números publicados se basan en las condiciones internas del laboratorio*

Especificaciones de los dispositivos virtuales

Especificaciones técnicas	SMA 500v (ESX/ESXI)	SMA 8200v (ESX/ESXI)	SMA 8200v (Hyper-V)
Sesiones simultáneas	Hasta 250 usuarios	Hasta 5.000	Hasta 250
Rendimiento SSL-VPN* (con CCU máx.)	Hasta 186 Mbps	Hasta 1,58 Gbps	Hasta 1,2 Gbps
Memoria asignada	2GB	8 GB	
Procesador	1 núcleo	4 núcleos	
Aceleración SSL	NO	SÍ	
Tamaño del disco aplicado	2GB	64 GB (por defecto)	Configurable por el administrador
Sistema operativo instalado	Linux	Linux reforzado	
Puerto de gestión dedicado	NO	SÍ	

** El rendimiento de la transferencia de datos puede variar en función de la implementación y la conectividad. Los números publicados se basan en las condiciones internas del laboratorio. SMA 8200v en Hyper-V puede escalarse hasta 5.000 sesiones simultáneas y proporciona un rendimiento SSL-VPN de hasta 1,58 Gbps al ejecutar SMA OS 12.1 con Windows Server 2016*

Información de pedido

SKU	DISPOSITIVO SONICWALL SECURE MOBILE ACCESS (SMA)
01-SSC-2231	SMA 200 con licencia para 5 usuarios
01-SSC-2243	SMA 400 con licencia para 25 usuarios
01-SSC-8469	SMA 500v con licencia para 5 usuarios
01-SSC-2301	SMA 7200 con licencia de prueba para el administrador
01-SSC-2300	SMA 6200 con licencia de prueba para el administrador
01-SSC-9574	SRA EX9000 (dispositivo básico)
01-SSC-8468	SMA 8200v (dispositivo virtual)
SKU	**LICENCIAS DE USUARIO DE SONICWALL SMA**
01-SSC-9182	SMA 500V, 5 usuarios adicionales (también disponible para SMA 200)
01-SSC-2414	SMA 500V, 100 usuarios adicionales (también disponible para SMA 400)
01-SSC-7856	SMA, licencia para 5 usuarios - apilable para 6200, 7200, EX9000, 8200v
01-SSC-7860	SMA, licencia para 100 usuarios - apilable para 6200, 7200, EX9000, 8200v
01-SSC-7865	SMA, licencia para 5.000 usuarios - apilable para 7200, EX9000, 8200v
01-SSC-5286	SMA, licencia de alta disponibilidad para 5 usuarios - apilable para 6200, 7200, EX9000
01-SSC-5290	SMA, licencia de alta disponibilidad para 100 usuarios - apilable para 6200, 7200, EX9000
01-SSC-5295	SMA, licencia de alta disponibilidad para 5.000 usuarios - apilable para 7200, EX9000
SKU	**CONTRATO DE SOPORTE PARA SONICWALL SMA**
01-SSC-9188	Soporte 8X5 para SMA 500V, hasta 25 usuarios, 1 año (también disponible para SMA 200 y 400)
01-SSC-9191	Soporte 24X7 para SMA 500V, hasta 25 usuarios, 1 año (también disponible para SMA 200 y 400)
01-SSC-8434	Soporte 24X7 para SMA 8200V, 5 usuarios, 1 año - apilable (también disponible para SMA 6200, 7200 y EX9000)
01-SSC-8446	Soporte 24X7 para SMA 8200V, 100 usuarios, 1 año - apilable (también disponible para SMA 6200, 7200 y EX9000)
01-SSC-7913	Soporte 24X7 para SMA 8200V, 5.000 usuarios, 1 año - apilable (también disponible para SMA 6200, 7200 y EX9000)
SKU	**GESTIÓN CENTRALIZADA PARA 6200, 7200, EX9000, 8200V**
Licencia para dispositivos CMS	
01-SSC-8535	Licencia CMS base + 3 dispositivos (Gratis - para pruebas y uso con licencias de usuario de suscripción)
01-SSC-8536	Licencia CMS para 100 dispositivos, 1 año (para uso con licencias de usuario de suscripción)
01-SSC-3369	CMS Base + 3 dispositivos (Gratis - para uso con licencias de usuario perpetuas)
01-SSC-3402	Licencia CMS para 100 dispositivos, 1 año (para uso con licencias de usuario perpetuas)
Licencias para usuarios centrales (suscripción)	
01-SSC-2298	Licencia agrupada para CSM, 10 usuarios, 1 año
01-SSC-8539	Licencia agrupada para CSM, 1.000 usuarios, 1 año
01-SSC-5339	Licencia agrupada para CSM, 50.000 usuarios, 1 año
Licencias para usuarios centrales (perpetuas)	
01-SSC-2053	Licencia perpetua de CMS para 10 usuarios
01-SSC-2058	Licencia perpetua de CMS para 1.000 usuarios
01-SSC-2063	Licencia perpetua de CMS para 50.000 usuarios
Soporte de licencias para usuarios centrales (perpetuas)	
01-SSC-2065	1 año de soporte 24x7 para CMS (10 usuarios)
01-SSC-2070	1 año de soporte 24x7 para CMS (1.000 usuarios)
01-SSC-2075	1 año de soporte 24x7 para CMS (50.000 usuarios)

Información de pedido (cont.)

Licencia ActiveSync central (suscripción)	
01-SSC-2088	Licencia agrupada de e-mail CSM, 50.000 usuarios, 1 año
01-SSC-2093	Licencia agrupada de e-mail CSM, 1.000 usuarios, 1 año
01-SSC-2087	Licencia agrupada de e-mail CSM, 10 usuarios, 1 año
Licencias spike centrales	
01-SSC-2111	Spike para CSM, 1.000 usuarios, 5 días
01-SSC-2115	Spike para CSM, 50.000 usuarios, 5 días
Add-on de Capture (suscripción)	
01-SSC-2116	Licencia de prueba CMS Capture 1 año para SMA
** Las licencias de suscripción incluyen soporte 24x7*	
SKU	**ADD-ONS DE SONICWALL SMA**
01-SSC-2406	Add-on SMA 7200 FIPS
01-SSC-2405	Add-on SMA 6200 FIPS
01-SSC-9185	SMA 500V Web Application Firewall, 1 año (También disponible para SMA 200 y 400)
SKU	**ADD-ONS DE SONICWALL SMA**
01-SSC-5967	Virtual assist, hasta 1 técnico simultáneo (SMA 200,400,500v)
01-SSC-5971	Virtual assist, hasta 10 técnicos simultáneos (SMA 200,400,500v)
SKU	**LICENCIA SPIKE PARA SMA (INCREMENTO NECESARIO PARA ALCANZAR CAPACIDAD)**
01-SSC-2240	Licencia spike de 10 días para 50 usuarios de SMA 200 (también disponible para SMA 400 y 500v)
01-SSC-7873	Licencia spike de 10 días para 5-2.500 usuarios de SMA 8200v (también disponible para SMA 6200, 7200 y EX9000)

** También hay disponibles números SKU y contratos de soporte de varios años. Para una lista completa de SKUs, póngase en contacto con su revendedor o representante de ventas*

Acerca de nosotros

SonicWall lleva más de 25 años combatiendo la industria del crimen cibernético, defendiendo a las empresas pequeñas, medianas y grandes de todo el mundo. Nuestra combinación de productos y partners nos ha permitido crear una solución de defensa cibernética en tiempo real adaptada a las necesidades específicas de más de 500.000 negocios en más de 150 países, para que usted pueda centrarse por completo en su negocio sin tener que preocuparse por las amenazas.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Para más información, consulte nuestra página Web
www.sonicwall.com

Datasheet-SecureMobileAccess-US-KJ-MKTG3047