SONICWALL

ACCESO MÓVIL SEGURO (SMA) DE SONICWALL

Acceso seguro en cualquier lugar y en cualquier momento a recursos corporativos en entornos multinube basados en la identidad, la ubicación y la confianza del usuario y del dispositivo.

El SMA de SonicWall es una gateway de acceso seguro unificado que permite a las organizaciones proporcionar acceso en cualquier momento, en cualquier lugar y desde cualquier dispositivo a los recursos corporativos críticos para la misión. El motor de políticas de control granular de 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 multinube.

Movilidad y BYOD
Para las organizaciones que desean adoptar políticas BYOD, modelos de trabajo flexible o acceso de terceros, el SMA se convierte en el punto de aplicación crítico para todos ellos. El SMA proporciona la mejor seguridad de su categoría para minimizar la superficie de ataque de las amenazas y aumenta la seguridad de las organizaciones gracias a su compatibilidad con los últimos algoritmos criptográficos y de cifrado. El SMA de SonicWall permite a los administradores proporcionar acceso móvil seguro y privilegios basados en identidades para que los usuarios finales puedan acceder de forma rápida y simple 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, el 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. El SMA también se integra con las principales tecnologías de autenticación multifactor del sector para mayor seguridad.

Proveedores de servicios gestionados
Tanto para organizaciones que alojan su propia infraestructura como para proveedores de servicios administrados, el SMA proporciona una solución de llave en mano para garantizar un alto nivel de continuidad y escalabilidad del negocio. El SMA puede admitir hasta 20.000 conexiones simultáneas en un solo dispositivo y ofrece escalabilidad para admitir cientos de miles de usuarios a través de la agrupación inteligente (clústeres). Los centros de datos pueden reducir costos gracias a la agrupación (clústeres) activa-activa y a un equilibrador de carga dinámico integrado, que reasigna en tiempo real el tráfico global al centro de datos más optimizado en función de la demanda de los usuarios. La serie de herramientas de SMA permite a los proveedores de servicios prestar servicios sin interrupciones, lo que les permite cumplir con SLA muy agresivos.

El SMA permite a los departamentos de TI brindar la mejor experiencia y el acceso más seguro en función del escenario de los usuarios. Disponible como dispositivos físicos reforzados o dispositivos virtuales potentes, el SMA se adapta perfectamente a la infraestructura existente local o en la nube. Las organizaciones pueden elegir entre una gama de acceso seguro basado en la web totalmente sin clientes para terceros o empleados en dispositivos personales, o un acceso VPN de túnel completo basado en los clientes más tradicional para ejecutivos en todo tipo de dispositivos. Tanto si las organizaciones necesitan proporcionar acceso seguro fiable a cinco usuarios desde una única ubicación, como si debe escalar su solución para miles de usuarios en redes distribuidas por todo el mundo, el SMA de SonicWall tiene una solución.

El SMA de SonicWall permite a las organizaciones adoptar la movilidad y la BYOD sin miedo, y trasladarse a la nube con facilidad. El SMA otorga mayor capacidad a los empleados y les proporciona una experiencia de acceso coherente.

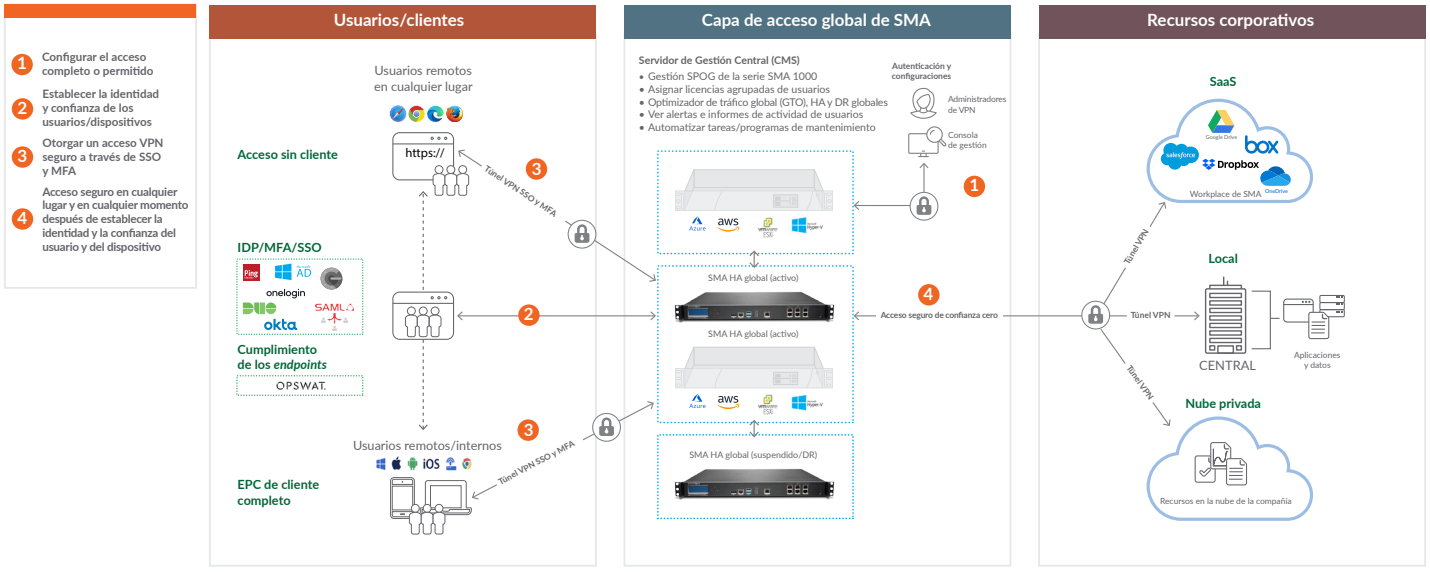
Ventajas:

- Acceso unificado a todos los recursos de red y nube para un acceso seguro "en cualquier momento, cualquier dispositivo, cualquier aplicación"
- Control de quién tiene acceso a qué recursos mediante políticas granulares con el robusto motor de control de acceso
- Aumento de la productividad mediante un inicio de sesión único federado en cualquier SaaS o aplicación alojada localmente con una única URL
- Menor TCO y menor complejidad de la gestión del acceso mediante la consolidación de los componentes de infraestructura en un entorno de TI híbrido
- Obtención de visibilidad de cada dispositivo de conexión y acceso en función a las políticas y la condición del *endpoint*
- Prevención de violaciones de software malicioso mediante el análisis de todos los archivos cargados en su red con el sandboxing de Capture ATP
- Protección contra ataques basados en la web y cumplimiento de la PCI con el complemento de firewall de aplicaciones web
- Detención de ataques DDoS y zombie con detección Geo IP y protección de botnets
- Funcionalidad segura de agente nativo mediante el uso del acceso HTML5 sin cliente basado en navegador web sin los gastos generales de instalación y mantenimiento de agentes en los dispositivos *endpoint*
- Acceso a información práctica que necesita para tomar las decisiones correctas con monitoreo en tiempo real y emisión de informes exhaustivos
- Implementación como un dispositivo físico o dispositivo virtual en nubes privadas en ESXi o Hyper-V, o en entornos de nube pública de AWS o Microsoft Azure
- Posibilidad de emisión dinámica de licencias de acceso en función a la demanda en tiempo real, con dirección de *endpoint* automatizada a la conexión de mayor rendimiento y menor latencia
- Reducción de los costos iniciales con equilibrio de carga integrado sin hardware o servicios adicionales, brindando al mismo tiempo un impacto cero de usuario en la conmutación por error de los dispositivos
- Seguro contra interrupciones de negocio o picos estacionales mediante la escalabilidad instantánea de la capacidad

Implementación del SMA

Una gateway de borde reforzado para un acceso seguro en cualquier momento, en cualquier lugar y desde cualquier dispositivo

El SMA ofrece un acceso remoto seguro, completo e integral a los recursos corporativos alojados en centros de datos locales, en la nube e híbridos. Aplica controles de acceso basados en la identidad e impuestos por políticas, autenticación de dispositivos con sensibilidad contextual y VPN a nivel de aplicación para otorgar acceso a datos, recursos y aplicaciones después de establecer la identidad, la ubicación y la confianza del usuario y del dispositivo. Pueden implementarse de forma flexible como un dispositivo Linux reforzado o dispositivo virtual en nubes privadas en ESXi o Hyper-V, o en entornos de nube pública de AWS o Microsoft Azure.



Implementación de SMA en la nube/local

Implementación flexible con dispositivos físicos y virtuales

El SMA de SonicWall 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 gubernamentales, el SMA 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 o en la nube, como Microsoft Hyper-V, VMware ESX y AWS.

Licencias de usuario compartidas por todos los dispositivos

Las organizaciones con dispositivos distribuidos globalmente pueden beneficiarse de la fluctuante demanda de licencias de usuario debido a las diferencias horarias. Ya sea que una organización implemente licencias completas de VPN o licencias básicas ActiveSync, la gestión central de SMA reasigna las licencias a los dispositivos administrados donde las demandas de los usuarios han llegado a su punto máximo desde dispositivos en una zona geográfica diferente, donde el uso ha disminuido debido a horarios nocturnos o no laborables.

Visibilidad de la red con perfiles de dispositivos con sensibilidad contextual

La mejor autenticación con sensibilidad contextual otorga acceso solamente a dispositivos confiables y usuarios autorizados. Las computadoras portátiles y PC también son interrogadas sobre la presencia o ausencia de software de seguridad, certificados de cliente e identificación del dispositivo. Los dispositivos móviles son interrogados sobre información de seguridad esencial, como estado del jailbreak o de raíz, identificación del dispositivo, estado del certificado y versiones del SO antes de otorgar el acceso. No se permite el acceso a la red a los dispositivos que no cumplen con los requisitos de las políticas y se notifica al usuario sobre el incumplimiento.

Experiencia coherente desde un único portal web

Los usuarios no necesitan recordar las URL de cada una de las aplicaciones ni mantener marcadores exhaustivos. El SMA es un portal de acceso centralizado que da a los usuarios solo una URL para acceder a todas las aplicaciones críticas para la misión desde un navegador web estándar. Una vez que el usuario inicia sesión a través de un navegador, se muestra un portal de usuario web personalizable en la ventana del navegador, lo que proporciona una vista de una única consola para acceder a cualquier aplicación local o SaaS. El portal sólo muestra enlaces y marcadores personalizados relevantes para un dispositivo, usuario o grupo de *endpoints* en particular. El portal es independiente de la plataforma y es compatible con todas las principales plataformas de dispositivos, lo que incluye Windows, Mac OS, Linux, iOS y Android, y es compatible con un amplio rango de navegadores en todos estos dispositivos.

Inicio de sesión único federado tanto en SaaS como en aplicaciones locales

Elimina la necesidad de múltiples contraseñas y da fin a malas prácticas de seguridad, como la reutilización de contraseñas. El SMA proporciona SSO federado tanto en aplicaciones SaaS alojadas en la nube como en aplicaciones alojadas en campus. El SMA se integra con múltiples servidores de autenticación, autorización y contabilidad, así como con tecnologías líderes de autenticación multifactor para ofrecer un mayor nivel de seguridad. Solo se proporciona inicio de sesión único seguro a los dispositivos *endpoint* autorizados después de que el SMA haya comprobado su condición y la conformidad con las normas.

El motor de políticas de acceso garantiza que los usuarios solo puedan ver las aplicaciones autorizadas y otorga acceso después de una autenticación exitosa. La solución admite SSO federado incluso cuando se utilizan clientes VPN, lo que brinda a los clientes una experiencia de autenticación fluida, ya sea mediante acceso seguro basado en clientes o sin clientes.

Prevención de infracciones y amenazas avanzadas

El SMA de SonicWall agrega una capa de seguridad de acceso para mejorar su posición en materia de seguridad y reducir el área de superficie para amenazas.

- El SMA se integra con el sandbox multimotor basado en la nube Capture ATP de SonicWall para analizar todos los archivos cargados por usuarios con *endpoints* no gestionados o por aquellos ajenos a la red corporativa. Esto garantiza que los usuarios tengan el mismo nivel de protección contra amenazas avanzadas, como ransomware o malware de día cero, tanto en la oficina como cuando están en movimiento[1].
- El servicio de firewall de aplicaciones web de SonicWall ofrece a las empresas una solución asequible y bien integrada para proteger las aplicaciones internas basadas en la web. Esto permite a los clientes garantizar la confidencialidad de los datos y los servicios web internos no se verán comprometidos en caso de que exista un acceso de usuarios malintencionados o no autorizados.
- Geo-IP y la detección de botnets protege a las organizaciones de ataques DDoS y zombie y de *endpoints* comprometidos que funcionan como botnets.

Acceso ininterrumpido sin cliente y basado en navegador seguro

La naturaleza "sin clientes" del SMA de SonicWall implica que no es necesario que el administrador instale manualmente un componente de cliente pesado en una computadora que se utilizará para el acceso remoto. Esto elimina cualquier dependencia de Java y gastos generales de TI, lo que amplía considerablemente el concepto de acceso remoto. Significa que, dado que no se requiere preinstalación ni preconfiguración, un trabajador remoto autorizado puede sentarse en cualquier computadora, en cualquier lugar del mundo, y acceder de manera segura a sus recursos corporativos. En esencia, el acceso seguro se basa estrictamente en el navegador, utilizando HTML5, lo que proporciona una experiencia integrada y unificada para los usuarios.

Una experiencia "Always On"

Para una experiencia de usuario perfecta, el SMA ofrece una VPN Always On para dispositivos de Windows gestionados. Los administradores pueden configurar los ajustes para establecer automáticamente una conexión VPN cada vez que un cliente de *endpoint* autorizado detecte una red pública o no confiable. Un evento de inicio de sesión único en el dispositivo de Windows brinda al usuario una conexión segura a los recursos corporativos. No es necesario que los usuarios inicien sesión en sus clientes de VPN ni cuenten con contraseñas adicionales. Esto brinda una experiencia perfecta a los usuarios móviles para acceder a recursos críticos para la misión como si estuvieran en la oficina y permite a los administradores de TI mantener el control sobre los dispositivos gestionados, mejorando la posición de seguridad de la organización.

Gestión intuitiva y emisión de informes exhaustivos

SonicWall proporciona una plataforma de gestión intuitiva basada en la web, Central Management Server (CMS), para optimizar la gestión de los dispositivos, así como amplias funciones de emisión de informes. La GUI fácil de usar permite gestionar dispositivos y políticas de manera individual o múltiple. 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 datos, servidores y redes. La TI puede automatizar las tareas rutinarias y programar actividades, liberando a los equipos de seguridad de las tareas repetitivas para que puedan centrarse en las tareas de seguridad estratégicas, como en la respuesta ante posibles incidentes. La TI obtiene información sobre las tendencias de acceso de los usuarios y la condición en todo el sistema a través de emisión de informes fáciles de usar y registros centralizados.

Disponibilidad de servicio 24x7

Las organizaciones tienen requisitos para preservar sus servicios y mantenerlos en funcionamiento con un alto grado de confiabilidad para proporcionar acceso seguro a las aplicaciones críticas para la misión en todo momento. Los dispositivos de SMA admiten la alta disponibilidad (HA) activa-pasiva tradicional para organizaciones con centros de datos únicos, o HA global con agrupamiento (clústeres) activo-activo o activo-suspendido para centros de datos locales o distribuidos. Ambos modelos de HA proporcionan una experiencia sin inconvenientes a los usuarios con conmutación por error de impacto cero y persistencia de sesión.

Despliegue el cliente VPN que se adapte a sus necesidades

Elija entre una amplia variedad de clientes de VPN para ofrecer acceso remoto seguro aplicado por políticas para diversos *endpoints*, como computadoras portátiles, teléfonos inteligentes y tabletas.

Clientes VPN	SO compatible	Modelo de SMA compatible	Aspecto clave
Mobile Connect	iOS, OS X, Android, Chrome OS, Windows 10	Todos los modelos	Ofrece autenticación biométrica, por VPN de la aplicación y control de *endpoints*
Connect Tunnel (cliente liviano)	Windows, Mac OS y Linux	6200, 6210, 7200, 7210, 8200v, 9000	Proporciona una experiencia completa "en la oficina" con un control robusto de los *endpoints*
NetExtender (cliente liviano)	Windows y Linux	210, 410, 500v	Aplica políticas de acceso granular y amplía el acceso a la red a través de clientes nativos

Reducción de los costos iniciales con el equilibrador de carga incorporado

La funcionalidad del equilibrio de carga integrada en el dispositivo de SMA logra una escalabilidad de nivel esperado para empresas y despliegues empresariales medianos. Algunos modelos de dispositivos de SMA ofrecen un equilibrio de carga dinámico para asignar de forma inteligente las cargas de sesión y asignar licencias de usuario en tiempo real en función de la demanda. No es necesario que las organizaciones inviertan en equilibradores de carga externos, lo que reduce los costos iniciales.

Seguro contra eventos imprevistos

Una solución completa de continuidad de negocio y DR debe ser capaz de manejar un aumento significativo en el tráfico de acceso remoto, manteniendo al mismo tiempo los controles de seguridad y costos. Los paquetes de licencias Spike de SonicWall para el SMA son licencias adicionales que permiten a las empresas distribuidas escalar la cantidad de usuarios y alcanzar la máxima capacidad de forma instantánea, lo que permite una continuidad fluida del negocio. Las licencias Spike funcionan como una póliza de seguro para cualquier aumento futuro planificado o no planificado de cantidad de usuarios actuales hasta decenas o incluso cientos de usuarios adicionales.

Prestaciones

Autenticación avanzada

Inicio de sesión único federado[2]	El SMA utiliza la autenticación SAML 2.0 para habilitar SSO federado a través de un único portal tanto para recursos locales como en la nube, al tiempo que aplica la autenticación de múltiples factores apilados para mayor 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 de dos factores/contraseña de un solo uso Tarjeta Common Access Card (CAC) Autenticación doble o apilada Soporte Captcha, nombre de usuario/contraseña
Autenticación SAML	El SMA puede configurarse como proveedor de identidad (IdP) SAML, proveedor del servicio (SP) SAML o actuar de proxy de un IdP existente local para permitir el inicio de sesión único (SSO) federado utilizando la autenticación SAML 2.0.
Repositorios de autenticación	El SMA proporciona integraciones sencillas con repositorios estándar de la industria para facilitar la gestión de las cuentas de usuario y contraseñas. Los grupos de usuarios se pueden rellenar dinámicamente en base a repositorios de autenticación de RADIUS, LDAP o Active Directory, incluidos los grupos anidados. Los atributos LDAP comunes o personalizados pueden ser interrogados sobre una autorización específica o la verificación del registro del dispositivo.
Proxy de la aplicación de capa 3-7	El SMA ofrece opciones de proxy flexibles; por ejemplo, el acceso del proveedor se puede proporcionar a través de proxy directo, el acceso del contratista a través de proxy inverso y el acceso del empleado a Exchange a través de ActiveSync.
Proxy inverso	El servicio proxy inverso mejorado con autenticación permite a los administradores configurar el portal de descarga de aplicaciones y los marcadores, lo que permite a los usuarios conectarse sin problemas a aplicaciones y recursos remotos, incluidos RDP y HTTP. Esta función es compatible con todos los navegadores, incluidos IE, Chrome y Firefox.
Delegación restringida de Kerberos	El SMA proporciona soporte de autenticación utilizando una infraestructura existente de Kerberos, que no necesita confiar en los servicios front-end para delegar un servicio.

Gestión de accesos

Motor de control de acceso (ACE)	Los administradores conceden o niegan el acceso según las políticas de la organización y establecen medidas de corrección al poner en cuarentena las sesiones. Las políticas basadas en objetos de ACE utilizan elementos de red, recurso, identidad, dispositivo, aplicación, datos y tiempo.
Control del *Endpoint* (EPC)	El EPC permite al administrador aplicar reglas de control de acceso granular basadas en la condición del dispositivo de conexión. Con una integración profunda en el SO, se combinan muchos elementos para la clasificación de tipos y la evaluación de factores de riesgo. La consulta de EPC simplifica la configuración del perfil del dispositivo mediante una lista completa y predefinida de soluciones antivirus, firewall personal y antispyware para las plataformas de Windows, Mac y Linux, incluida la versión y aplicabilidad de la actualización de archivos de firma.
Control de acceso a 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 de AAC se aplican tanto para el cliente como para el servidor, proporcionando una protección perimetral robusta.

Seguridad de alta calidad

SSL VPN de capa 3	La serie de SMA ofrece funciones de tunelización de la capa 3 de alto rendimiento a una amplia variedad de dispositivos clientes que funcionan en cualquier entorno.
Compatibilidad con cifrado	Duración de sesión configurable Cifras: AES 128 + 256 bits, Triple DES, RC4 128 bits Hashes: SHA-256 Algoritmo de firma digital de curva elíptica (ECDSA)
Compatibilidad con cifrado avanzado	Los dispositivos de SMA ofrecen una sólida posición de seguridad para cumplir con las normas, con cifrado de configuración predeterminado, y los administradores pueden refinar aún más el rendimiento, la seguridad o la compatibilidad.
Certificaciones de seguridad	Certificado para FIPS 140-2 Nivel 2, ICSA SSL-TLS, en camino a certificación para Common Criteria, UC-APL
Recurso compartido de archivos seguro	Detención de ataques desconocidos de día cero como el ransomware en la gateway con corrección automatizada. Los archivos cargados utilizando *endpoints* no gestionados con acceso seguro a redes corporativas son inspeccionados por nuestro Capture ATP multimotor basado en la nube.
Firewall de Aplicaciones Web (WAF)	Evite los ataques basados en protocolos y en la web, ayudando a las empresas financieras, de atención médica, de comercio electrónico y de otros tipos a lograr el cumplimiento de las normas OWASP Top 10 y PCI.
Detección Geo IP y protección de botnets	La detección Geo IP Detection y la protección de botnets permiten a los clientes disponer de un mecanismo para permitir o restringir el acceso del usuario desde diversas ubicaciones geográficas.
Compatibilidad con TLS 1.3	Ofrece seguridad y mejora del rendimiento al tiempo que reduce las complejidades con respecto a sus predecesores.

Experiencia de usuario intuitiva

VPN Always On	Establece automáticamente una conexión segura a la red corporativa desde dispositivos Windows proporcionados por la compañía para mejorar la seguridad, obtener visibilidad del tráfico y mantener el cumplimiento.
Detección de Red Segura (SND)	El cliente VPN consciente de la red de SMA detecta cuándo el dispositivo está fuera del campus y vuelve a conectarse automáticamente a la VPN, desconectándola de nuevo cuando el dispositivo vuelve a una red de confianza.
Acceso sin cliente a los recursos	El SMA proporciona acceso seguro sin cliente a los recursos a través de agentes de navegación HTML5 que ofrecen protocolos RDP, ICA, VNC, SSH y Telnet.
Portal de inicio de sesión único	El portal WorkPlace ofrece una vista de panel único, fácil de usar y personalizable para un acceso seguro con un inicio de sesión único (SSO) a cualquier recurso en un entorno de TI híbrido. No se necesita ningún otro inicio de sesión ni VPN.
Tunelización de capa 3	Los administradores pueden seleccionar Split-Tunnel o aplicar el modo Redirect-All con tunelización SSL/TLS y ESP opcional como alternativa para un rendimiento máximo.
Explorador de archivos HTML5[1]	El navegador de archivos moderno facilita a los usuarios el acceso a archivos compartidos desde cualquier navegador web.
Integración de SO móvil	Mobile Connect es compatible con todas las plataformas de SO, lo que proporciona a los usuarios una flexibilidad total en la elección de dispositivos móviles.

Resiliencia

Optimizador Global de Tráfico (GTO)	El SMA ofrece un equilibrio de carga de tráfico global con impacto cero para los usuarios. El tráfico se enruta al datacenter más optimizado y de mayor rendimiento.
Alta disponibilidad dinámica[2]	El SMA es compatible con configuración Activa/Pasiva y ofrece configuración Activa/Activa para una alta disponibilidad, ya sea que esté desplegada en un solo datacenter o en varios dispersos geográficamente.
Persistencia de sesión universal[1]	Proporciona a los usuarios una experiencia sin inconvenientes con conmutación por error de impacto cero. En caso de que un dispositivo se desconecte, los clústeres inteligentes de SMA reasignan a los usuarios junto con sus datos de sesión sin necesidad de volver a autenticarse.
Rendimiento escalable	Los dispositivos de SMA escalan el rendimiento exponencialmente desplegando múltiples dispositivos, eliminando así un único punto de falla. Los clústeres horizontales son totalmente compatibles con la mezcla de dispositivos de SMA físicos y virtuales.
Licencias dinámicas	Ya no es necesario que las licencias de usuario se apliquen a los dispositivos de SMA individualmente. Los usuarios se pueden distribuir y reasignar dinámicamente entre los dispositivos gestionados, en función de la demanda del usuario.

Gestión y monitoreo centrales

Sistema de Gestión Central (CMS)	El CMS proporciona gestión centralizada basada en la web para todas las funciones de SMA.
Alertas personalizadas	Las alertas pueden configurarse para generar trampas SNMP que son supervisadas por cualquier Sistema de Gestión de Redes (NMS) de infraestructura de TI. Los administradores también pueden configurar alertas para análisis de archivos Capture ATP y uso del disco para una acción inmediata.
Panel de control en tiempo real	Un panel de control en tiempo real y personalizable permite al administrador de TI diagnosticar de forma rápida y sencilla los problemas de acceso y obtener información valiosa para la solución de problemas.
Integración de SIEM	La salida en tiempo real a los recopiladores de datos centrales de Gestión de Eventos e Información de Seguridad (SIEM) permite que los equipos de seguridad correlacionen las actividades impulsadas por eventos para comprender el flujo de trabajo integral de un usuario o aplicación en particular. Esto es fundamental durante la gestión de incidentes de seguridad y el análisis forense.
Programador	El programador permite a los usuarios programar tareas de mantenimiento como la implementación de políticas, la replicación de ajustes de configuración y los servicios de reinicio, sin intervención manual.

Extensibilidad

API de gestión	Las API de gestión permiten un control administrativo programático completo de todos los objetos dentro de un único entorno de SMA o CMS global.
API de usuario final	Las API de usuario final proporcionan un control completo de inicio de sesión, autenticación y flujo de trabajo de *endpoints*.
Autenticación de dos factores (2FA)	El SMA ofrece 2FA integrándose con las principales soluciones de contraseñas de un solo uso (TOTP) basadas en el tiempo, como Google Authenticator, Microsoft Authenticator, Duo security, etc.
Integración de MDM	El SMA se integra con los principales productos de gestión de movilidad enterprise (EMM), como Airwatch y Mobile Iron.
Otras integraciones de terceros	El SMA se integra con proveedores líderes del sector como OPSWAT para proporcionar protección avanzada contra amenazas.

[1] *Disponible con SO de SMA 12.1 o superior*

[2] *Mejorado en SMA 12.1*

Resumen de funciones (comparación por modelo)

Categoría	Función	210	410	500v	6210	7210	8200v
Implementación	Sistema operativo	v9.0 en adelante	v9.0 en adelante	v9.0 en adelante	v12.1 en adelante	v12.1 en adelante	v12.1 en adelante
	Hipervisores compatibles	–	–	VMware ESXi/ Microsoft Hyper-V	–	–	VMware ESXi/ Microsoft Hyper-V
	Plataformas de nubes públicas compatibles	–	–	AWS/Azure	–	–	AWS/Azure
Rendimiento	Cant. máx. de sesiones de usuario simultáneas	200	400	250	2.000	10.000	5.000
	Rendimiento máx. de SSL/TLS	560 Mbps	844 Mbps	265 Mbps	1,3 Gbps	5,0 Gbps	1,58 Gbps
Acceso del cliente	Túnel de capa 3	•	•	•	•	•	•
	Split-tunnel y redirect-all	•	•	•	•	•	•
	VPN Always On	•	•	•	•	•	•
	Encapsulación automática de ESP	–	–	–	•	•	•
	HTML5 (RDP, VNC, ICA, SSH, Telnet, Network Explorer)	•	•	•	•	•	•
	Detección de red segura	–	–	–	•	•	•
	Navegador de archivos (CIFS/NFS)	•	•	•	•	•	•
	Citrix XenDesktop/XenApp	•	•	•	•	•	•
	Vista de VMware	–	–	–	•	•	•
	Túnel según demanda	–	–	–	•	•	•
	Extensiones de Chrome/Firefox	–	–	–	•	•	•
	Compatibilidad con 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	–	–	–	•	•	•
	Ejecución del control de aplicaciones	–	–	–	•	•	•
	Validación de ID de la aplicación	–	–	–	•	•	•
Portal de usuario	Marca	•	•	•	•	•	•
	Personalización	–	–	–	•	•	•
	Localización	•	•	•	•	•	•
	Marcadores definidos por el usuario	•	•	•	•	•	•
	Soporte personalizado de URL	•	•	•	•	•	•
	Soporte de aplicación SaaS	–	–	–	•	•	•
Seguridad	FIPS 140-2	–	–	–	•	•	–
	ICSA SSL-TLS	•	•	•	•	•	•
	Conjuntos de cifrado B	–	–	–	•	•	•
	Consulta dinámica de EPC	•	•	•	•	•	•
	Control de acceso basado en funciones (RBAC)	–	–	–	•	•	•
	Registro de *endpoints*	•	•	•	•	•	•
	Recurso compartido de archivos seguro (Capture ATP)	•	•	•	•	•	•
	Cuarentena de *endpoints*	•	•	•	•	•	•
	Validación de CRL OSCP	–	–	–	•	•	•
	Selección de cifras	–	–	–	•	•	•
	PKI y certificados de cliente	•	•	•	•	•	•
	Filtro de Geo IP	•	•	•	–	–	–
	Filtro de botnets	•	•	•	–	–	–
	Proxy de reenvío	•	•	•	•	•	•
	Proxy inverso	•	•	•	•	•	•
Servicios de autenticación e identidad	SAML 2,0	•	•	•	•	•	•
	LDAP, RADIUS	•	•	•	•	•	•
	Kerberos (KDC)	•	•	•	•	•	•
	NTLM	•	•	•	•	•	•
	Proveedor de identidad (IdP) de SAML	•	•	•	•	•	•
	Compatibilidad con dispositivo biométrico	•	•	•	•	•	•
	Compatibilidad con Face ID para iOS	•	•	•	•	•	•
	Autenticación de dos factores (2FA)	•	•	•	•	•	•
	Autenticación multifactor (MFA)	–	–	–	•	•	•

Resumen de funciones (continuación de comparación por modelo)

Categoría	Función	210	410	500v	6210	7210	8200v
Continuación de servicios de autenticación e identidad	Autenticación encadenada	–	–	–	•	•	•
	Contraseña de un solo uso (OTP) por correo electrónico o SMS	•	•	•	•	•	•
	Compatibilidad con tarjetas Common Access Card (CAC)	–	–	–	•	•	•
	Compatibilidad con certificados X.509	•	•	•	•	•	•
	Integración Captcha	–	–	–	•	•	•
	Cambio remoto de contraseña	•	•	•	•	•	•
	SSO basado en formularios	•	•	•	•	•	•
	SSO federado	–	–	–	•	•	•
	Persistencia de la sesión	–	–	–	•	•	•
	Inicio de sesión automático	•	•	•	•	•	•
Control de acceso	Grupo AD	•	•	•	•	•	•
	Atributos LDAP	•	•	•	•	•	•
	Políticas de geolocalización	•	•	•	–	–	–
	Monitoreo continuo de *endpoints*	•	•	•	•	•	•
Gestión	Interfaz de gestión (ethernet)	–	–	–	•	•	•
	Interfaz de gestión (consola)	–	–	–	•	•	•
	Administración HTTPS	•	•	•	•	•	•
	Administración SSH	–	–	–	•	•	•
	SNMP MIBS	•	•	•	•	•	•
	Registro del sistema y NTP	•	•	•	•	•	•
	Monitoreo del uso	•	•	•	•	•	•
	Reversión de configuración	•	•	•	•	•	•
	Gestión centralizada	–	–	–	•	•	•
	Emisión de informes centralizados	–	–	–	•	•	•
	API REST de gestión	–	–	–	•	•	•
	API REST de autenticación	–	–	–	•	•	•
	Contabilidad RADIUS	–	–	–	•	•	•
	Tareas programadas	–	–	–	•	•	•
	Licencias de sesión centralizadas	–	–	–	•	•	•
	Auditoría guiada por eventos	–	–	–	•	•	•
Redes	IPv6	•	•	•	•	•	•
	Equilibrio de carga global	–	–	–	•	•	•
	Equilibrio de carga de servidor	•	•	•	–	–	–
	Replicación del estado de TCP	•	•	•	•	•	•
	Conmutación por error de la agrupación (clúster)	–	–	–	•	•	•
	Alta disponibilidad activa/pasiva	–	•	•	•	•	•
	Alta disponibilidad activa/activa	–	–	–	•	•	•
	Escalabilidad horizontal	–	–	–	•	•	•
	FQDN individuales o múltiples	–	–	–	•	•	•
	Proxy de túnel inteligente L3-7	•	•	•	•	•	•
	Proxy de aplicación L7	•	•	•	•	•	•
Integración	Soporte para 2FA TOTP	•	•	•	•	•	•
	Compatibilidad con productos de EMM y MDM	–	–	–	•	•	•
	Compatibilidad con productos de SIEM	–	–	–	•	•	•
	Bóveda de contraseñas de TPAM	–	–	–	•	•	•
	Compatibilidad con hipervisor ESX	–	–	•	–	–	•
	Compatibilidad con hipervisor Hyper-V	–	–	•	–	–	•
Opciones de licencia	Licencia basada en la suscripción	–	–	–	•	•	•
	Licencia perpetua con soporte	•	•	•	•	•	•
	Firewall de Aplicaciones Web (WAF)	•	•	•	–	–	–
	Concesión de licencias Spike	•	•	•	•	•	•
	Concesión escalonada de licencias	–	–	–	•	•	•
	Asistencia virtual	•	•	•	–	–	–

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

SONICWALL®

Beneficios de la actualización a dispositivos de alta gama

Mayor desempeño | Mayor rendimiento | Funciones avanzadas | Mejor escalabilidad

Especificaciones del dispositivo

Elija entre una variedad de dispositivos construidos especialmente para un acceso móvil seguro (SMA). Obtenga opciones de implementación flexibles con dispositivos virtuales y físicos.

Especificaciones del dispositivo físico

Desempeño	SMA 210	SMA 410	SMA 6210	SMA 7210
Sesiones concurrentes/Usuarios	Hasta 200	Hasta 400	Hasta 2.000	Hasta 10.000
Rendimiento SSL VPN* (con CCU máx.)	560 Mbps	844 Mbps	Hasta 800 Mbps	Hasta 5,0 Gbps
Factor de forma	1U	1U	1U	1U
Dimensiones	16,92 x 10,23 x 1,75 pulgadas (43 x 26 x 4,5 cm)	16,92 x 10,23 x 1,75 pulgadas (43 x 26 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 (43 x 41,5 x 4,5 cm)
Peso del dispositivo	11 libras (5 kg)	11 libras (5 kg)	17,7 libras (8 kg)	18,3 libras (8,3 kg)
Aceleración de datos de cifrado (AES-NI)	NO	NO	SÍ	SÍ
Puerto de gestión especial	NO	NO	SÍ	SÍ
Aceleración SSL	NO	NO	SÍ	SÍ
Almacenamiento	4 GB (memoria flash)	4 GB (memoria flash)	2 x 1 TB SATA; RAID 1	2 x 1 TB SATA; RAID 1
Interfaces	(2) GB Ethernet, (2) USB, (1) consola	(4) GB Ethernet, (2) USB, (1) consola	1GE con (6) puertos, (2) USB, (1) consola	1GE con (6) puertos, 10 Gb con (2) puertos SFP+, (2) USB, (1) consola
Memoria	4 GB	8 GB	8 GB DDR4	16 GB DDR4
chip TPM	NO	NO	SÍ	SÍ
Procesador	4 núcleos	8 núcleos	4 núcleos	4 núcleos
MTBF (a 25 °C o 77 °F) en horas	61.815	60.151	70.127	129.601
Operaciones y cumplimiento	**SMA 210**	**SMA 410**	**SMA 6210**	**SMA 7210**
Alimentación	Fuente de alimentación fija	Fuente de alimentación fija	Fuente de alimentación fija	Dos fuentes de alimentación, intercambiables en caliente
Potencia de entrada	100-240 VCA, 50-60 MHz	100-240 VCA, 50-60 MHz	100-240 VCA, 1,1 A	100-240 VCA, 1,79 A
Consumo de energía	26,9 W	31,9 W	77 W	114 W
Disipación de calor total	92 BTU	109 BTU	264 BTU	389 BTU
Entorno	WEEE, EU RoHS, China RoHS			
Choque no operativo	110 g, 2 ms			
Emisiones	FCC, ICES, CE, C-Tick, VCCI; MIC			
Seguridad	TUV/GS, UL, CE PSB, CCC, BSMI, esquema CB			
Temperatura de funcionamiento	0 °C a 40 °C (32 °F a 104 °F)			
Certificación FIPS	NO	NO	FIPS 140-2 Nivel 2 con protección antimanipulación	

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

Especificaciones del dispositivo virtual

Especificaciones	SMA 500v (ESX/ESXi/Hyper-V)	SMA 8200v (ESX/ESXi/Hyper-V)
Sesiones concurrentes	Hasta 250 usuarios	Hasta 5000
Rendimiento SSL-VPN* (en CCU máx.)	Hasta 186 Mbps	Hasta 1,58 Gbps
Memoria asignada	2 GB	8 GB
Procesador	1 núcleo	4 núcleos
Aceleración SSL	NO	SÍ
Tamaño del disco aplicado	2 GB	64 GB (por defecto)
Sistema operativo instalado	Linux	Linux reforzado
Puerto de gestión especial	NO	SÍ

** El rendimiento puede variar según la implementación y la conectividad. Los números publicados se basan en las condiciones de laboratorio internas. SMA 8200v en escalas Hyper-V de hasta 5000 sesiones concurrentes y proporciona un rendimiento SSL-VPN de hasta 1,58 Gbps al ejecutar el SO de SMA 12.1 con Windows Server 2016*

Información sobre pedidos

SKU	DISPOSITIVO CON ACCESO MÓVIL SEGURO (SMA) DE SONICWALL
02-SSC-2800	SMA 210 con 5 licencias de usuario
02-SSC-2801	SMA 410 con 25 licencias de usuario
01-SSC-8469	SMA 500v con 5 licencias de usuario
02-SSC-0978	SMA 7210 con licencia de prueba de administrador
02-SSC-0976	SMA 6210 con licencia de prueba de administrador
01-SSC-8468	SMA 8200v (dispositivo virtual)
SKU	**LICENCIAS DE USUARIO DE SMA SONICWALL**
01-SSC-9182	SMA 500V añadir 5 usuarios (También disponible para SMA 210)
01-SSC-2414	SMA 500V añadir 100 usuarios (También disponible para SMA 410)
01-SSC-7856	SMA 5 licencias de usuario - apilable para 6210, 7210, 8200v
01-SSC-7860	SMA 100 licencias de usuario - apilable para 6210, 7210, 8200v
01-SSC-7865	SMA 5000 licencias de usuario - apilable para 7210, 8200v
SKU	**CONTRATO DE SOPORTE DE SMA DE SONICWALL**
01-SSC-9191	Soporte 24x7 para SMA 500V, hasta 25 usuarios, 1 año (también disponible para SMA 210 y 410)
01-SSC-2326	Soporte 24x7 para SMA 6210, 100 usuarios, 1 año - apilable
01-SSC-2350	Soporte 24x7 para SMA 7210, 500 usuarios, 1 año - apilable
01-SSC-8434	Soporte 24x7 para SMA 8200V, 5 usuarios, 1 año - apilable (También disponible para SMA 6210, 7210)
01-SSC-8446	Soporte 24x7 para SMA 8200V, 100 usuarios, 1 año - apilable (También disponible para SMA 6210, 7210)
01-SSC-7913	Soporte 24x7 para SMA 8200V, 5000 usuarios, 1 año - apilable (También disponible para SMA 6210, 7210)
SKU	**GESTIÓN CENTRAL PARA 6210, 7210, 8200V**
Licencia de dispositivo CMS	
01-SSC-8535	Base CMS + 3 licencias de dispositivos (sin cargo - para pruebas y uso con licencias de usuario y suscripción)
01-SSC-8536	CMS, 100 licencias de dispositivos, 1 año (para uso con licencias de usuario y suscripción)
01-SSC-3369	Base CMS + 3 dispositivos (sin cargo - para usar con licencias de usuario perpetuas)
01-SSC-3402	CMS, 100 licencias de dispositivos, 1 año (para uso con licencias de usuario perpetuas)
Licencias de usuario centrales (suscripción)	
01-SSC-2298	CMS, licencia agrupada de 10 usuarios, 1 año
01-SSC-8539	CMS, licencia agrupada de 1000 usuarios, 1 año
01-SSC-5339	CMS, licencia agrupada de 50.000 usuarios, 1 año
Licencias de usuario centrales (perpetuas)	
01-SSC-2053	CMS, licencia perpetua para 10 usuarios
01-SSC-2058	CMS, licencia perpetua para 1000 usuarios
01-SSC-2063	CMS, licencia perpetua para 50.000 usuarios
Soporte para licencias de usuario centrales (perpetuas)	
01-SSC-2065	Soporte 24x7, CMS, 1 año, 10 usuarios
01-SSC-2070	Soporte 24x7, CMS, 1 año, 1000 usuarios
01-SSC-2075	Soporte 24x7, CMS, 1 año, 50.000 usuarios
Licencias de ActiveSync centrales (suscripción)	
01-SSC-2088	CMS, licencia agrupada de correo electrónico, 10 usuarios, 1 año
01-SSC-2093	CMS, licencia agrupada de correo electrónico, 1000 usuarios, 1 año
01-SSC-2087	CMS, licencia agrupada de correo electrónico, 50.000 usuarios, 1 año

Información sobre pedidos (continuación)

SKU	GESTIÓN CENTRAL PARA 6210, 7210, 8200V
Licencias Spike centrales	
01-SSC-2111	CMS Spike de 1000 usuarios, 5 días
01-SSC-2115	CMS Spike de 50.000 usuarios, 5 días
Complemento de captura (suscripción)	
Póngase en contacto con su revendedor ** Las licencias de suscripción cuentan con soporte 24x7 incluido*	
SKU	**COMPLEMENTOS PARA SMA DE SONICWALL**
01-SSC-2406	Complemento FIPS para SMA 7210
01-SSC-2405	Complemento FIPS para SMA 6210
01-SSC-9185	Firewall de aplicaciones web 1 año para SMA 500V (También disponible para SMA 210 y 410)
SKU	**ACTUALIZACIÓN SEGURA DE SMA DE SONICWALL**
02-SSC-2794	SMA 210 Secure Upgrade Plus, paquete de 5 usuarios con soporte 24X7 hasta 25 usuarios por 1 año
02-SSC-2795	SMA 210 Secure Upgrade Plus, paquete de 5 usuarios con soporte 24X7 hasta 25 usuarios por 3 años
02-SSC-2798	SMA 410 Secure Upgrade Plus, paquete de 25 usuarios con soporte 24X7 hasta 100 usuarios por 1 año
02-SSC-2799	SMA 410 Secure Upgrade Plus, paquete de 25 usuarios con soporte 24X7 hasta 100 usuarios por 3 años
02-SSC-2893	SMA 6210 Secure Upgrade Plus, soporte 24X7 hasta 100 usuarios por 1 año
02-SSC-2894	SMA 6210 Secure Upgrade Plus, soporte 24X7 hasta 100 usuarios por 3 años
02-SSC-2895	SMA 7210 Secure Upgrade Plus, soporte 24X7 hasta 250 usuarios por 1 año
02-SSC-2896	SMA 7210 Secure Upgrade Plus, soporte 24X7 hasta 250 usuarios por 3 años
02-SSC-0860	SMA 8200 V Secure Upgrade Plus, soporte 24X7 hasta 100 usuarios por 1 año
02-SSC-0862	SMA 8200 V Secure Upgrade Plus, soporte 24X7 hasta 100 usuarios por 3 años
02-SSC-2807	SMA 500V Secure Upgrade Plus, soporte 24X7 hasta 100 usuarios por 1 año
02-SSC-2808	SMA 500V Secure Upgrade Plus, soporte 24X7 hasta 100 usuarios por 3 años
SKU	**LICENCIA SPIKE PARA SMA (INCREMENTO NECESARIO PARA ALCANZAR LA CAPACIDAD)**
01-SSC-2240	SMA 210 licencias Spike de 10 días para 50 usuarios (También disponible para SMA 410 y 500v)
01-SSC-7873	SMA 8200v licencias Spike de 10 días para 5-2500 usuarios (También disponible para SMA 6210, 7210)
02-SSC-4490	SMA 500 V LICENCIA SPIKE DE 30 DÍAS PARA 250 USUARIOS
02-SSC-4489	SMA 500 V LICENCIA SPIKE DE 60 DÍAS PARA 250 USUARIOS
02-SSC-4488	SMA 200/210 LICENCIA SPIKE DE 30 DÍAS PARA 50 USUARIOS
02-SSC-4487	SMA 200/210 LICENCIA SPIKE DE 60 DÍAS PARA 50 USUARIOS
02-SSC-4486	SMA 400/410 LICENCIA SPIKE DE 30 DÍAS PARA 250 USUARIOS
02-SSC-4485	SMA 400/410 LICENCIA SPIKE DE 60 DÍAS PARA 250 USUARIOS
02-SSC-4471	SMA CMS LICENCIA SPIKE ADICIONAL DE 30 DÍAS PARA 100 USUARIOS
02-SSC-4473	SMA CMS LICENCIA SPIKE ADICIONAL DE 30 DÍAS PARA 500 USUARIOS
02-SSC-4475	MA CMS LICENCIA SPIKE ADICIONAL DE 30 DÍAS PARA 1.000 USUARIOS
02-SSC-4477	SMA CMS LICENCIA SPIKE ADICIONAL DE 30 DÍAS PARA 5.000 USUARIOS
02-SSC-4479	SMA CMS LICENCIA SPIKE ADICIONAL DE 30 DÍAS PARA 10.000 USUARIOS
02-SSC-4481	MA CMS LICENCIA SPIKE ADICIONAL DE 30 DÍAS PARA 25.000 USUARIOS
02-SSC-4483	SMA CMS LICENCIA SPIKE ADICIONAL DE 30 DÍAS PARA 50.000 USUARIOS
02-SSC-4472	SMA CMS LICENCIA SPIKE ADICIONAL DE 60 DÍAS PARA 100 USUARIOS
02-SSC-4474	SMA CMS LICENCIA SPIKE ADICIONAL DE 60 DÍAS PARA 500 USUARIOS
02-SSC-4476	SMA CMS LICENCIA SPIKE ADICIONAL DE 60 DÍAS PARA 1.000 USUARIOS

Información sobre pedidos (continuación)

SKU	LICENCIA SPIKE PARA SMA (INCREMENTO NECESARIO PARA ALCANZAR LA CAPACIDAD)
02-SSC-4478	SMA CMS LICENCIA SPIKE ADICIONAL DE 60 DÍAS PARA 5.000 USUARIOS
02-SSC-4480	SMA CMS LICENCIA SPIKE ADICIONAL DE 60 DÍAS PARA 10.000 USUARIOS
02-SSC-4482	SMA CMS LICENCIA SPIKE ADICIONAL DE 60 DÍAS PARA 25.000 USUARIOS
02-SSC-4484	SMA CMS LICENCIA SPIKE ADICIONAL DE 60 DÍAS PARA 50.000 USUARIOS

** También hay disponibles contratos de soporte y SKU para varios años. Para obtener una lista completa de SKU, comuníquese con su revendedor o vendedor.*

Servicios habilitados por *partners*

¿Necesita ayuda para planificar, desplegar u optimizar su solución de SonicWall? Los *partners* de servicios avanzados de SonicWall están formados para prestarle servicios profesionales de primera clase. Obtenga más información en www.sonicwall.com/PES.

Acerca de SonicWall

SonicWall ofrece Boundless Cybersecurity para la era hiperdistribuida en una realidad laboral en la que todo el mundo usa tecnología móvil, a distancia y poco segura. SonicWall protege a las organizaciones que se movilizan por su nueva normalidad empresarial con una protección sin fisuras que detiene los ciberataques más evasivos en puntos de exposición ilimitados y una plantilla laboral cada vez más remota, móvil y con acceso a la nube. Al conocer lo desconocido, proporcionar visibilidad en tiempo real y posibilitar una economía revolucionaria, SonicWall cierra la brecha comercial en materia de ciberseguridad para empresas, gobiernos y pymes de todo el mundo. Si desea más información visite www.sonicwall.com o síganos en Twitter, LinkedIn, Facebook e Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Encontrará más información en nuestro sitio web.
www.sonicwall.com

Datasheet-SecureMobileAccess-US-COG-2726