



- **Gestión centralizada de la seguridad y de la red**
- **Políticas fáciles de establecer**
- **Despliegue y configuración VPN eficientes**
- **Gestión fuera de línea**
- **Gestión de licencias optimizada**
- **Dashboard universal**
- **Supervisión activa de dispositivos y alertas**
- **Soporte SNMP**
- **Informes inteligentes y visualización de actividades**
- **Protocolización centralizada**
- **Informes syslog de próxima generación en tiempo real e históricos**
- **Análisis del tráfico de aplicaciones**
- **Amplio soporte de plataformas diferentes**
- **Opciones de implementación flexibles**
- **Múltiples opciones de integración**

Las tareas de gestión, supervisión e informes para las actuales redes distribuidas en continuo crecimiento son cada vez más complejas y costosas. No obstante, las empresas deben garantizar la continuidad del negocio y el cumplimiento de las más estrictas normativas con un presupuesto limitado. Los proveedores de servicios deben cumplir los acuerdos de nivel de servicio (SLAs) para una creciente cantidad de dispositivos de clientes dotados de modelos de licencias cada vez más complejos. Al mismo tiempo, deben alcanzar los objetivos de rendimiento de la inversión (ROI). La empresas que no utilizan herramientas de próxima generación para el análisis del tráfico de aplicaciones o funciones de informes syslog no obtienen información detallada sobre el uso del ancho de banda, el tráfico de aplicaciones ni la productividad de los empleados. Las organizaciones necesitan herramientas de gestión sencillas, asequibles y escalables, capaces de soportar miles de dispositivos y políticas de seguridad.

El Sistema de gestión global de SonicWALL (GMS®) proporciona a las organizaciones, a las empresas distribuidas y a los proveedores de servicios una herramienta potente e intuitiva para gestionar e implementar de forma rápida y centralizada las soluciones SonicWALL de cortafuegos, antispam, backup y recuperación y acceso remoto seguro. GMS también ofrece supervisión centralizada en tiempo real, así como informes exhaustivos sobre las políticas y el cumplimiento de normas. Para los clientes de empresas grandes, GMS optimiza la gestión de las políticas de seguridad y la implementación de dispositivos, minimizando al mismo tiempo los costes de administración. Para los proveedores de servicios, GMS simplifica la gestión de la seguridad de múltiples clientes y crea oportunidades de ingresos adicionales. Los administradores pueden agrupar soluciones GMS para ofrecer un mayor nivel de redundancia y escalabilidad. GMS de SonicWALL ofrece una gran flexibilidad de implementación, ya que está disponible como software, como hardware y como dispositivo virtual.

Prestaciones y ventajas

Gestión centralizada de la seguridad y de la red.

Ayuda a los administradores a implementar, gestionar y supervisar un entorno de red distribuido.

Políticas fáciles de establecer desde una ubicación central para miles de dispositivos SonicWALL, ya sean cortafuegos, dispositivos antispam, de backup y recuperación o de acceso remoto seguro.

Despliegue y configuración VPN eficientes. Permiten habilitar la conectividad VPN de forma sencilla y consolidar miles de políticas de seguridad.

Gestión fuera de línea. Permite programar actualizaciones de la configuración y/o del firmware en dispositivos gestionados para minimizar las interrupciones del servicio.

Gestión de licencias optimizada. Simplifica la gestión de las suscripciones a licencias de seguridad y de soporte de los dispositivos SonicWALL a través de una única consola unificada.

Dashboard universal. Incluye widgets personalizables, mapas geográficos e informes centrados en el usuario.

Supervisión activa de dispositivos y alertas. Proporciona alertas en tiempo real con prestaciones de supervisión integradas. Simplifica la resolución de problemas, ya que permite a los administradores tomar medidas de precaución y aplicar medidas correctivas de forma inmediata.

Soporte SNMP. Proporciona traps eficaces en tiempo real para todos los dispositivos y aplicaciones que soportan TCP/IP y SNMP, facilitando enormemente los esfuerzos de resolución de problemas para identificar los eventos críticos de la red y reaccionar ante ellos.

Informes inteligentes y visualización de actividades. Facilita informes gráficos y de gestión sobre los dispositivos de cortafuegos, antispam, backup y recuperación y acceso remoto seguro de SonicWALL, proporcionando una visión más amplia de las tendencias de uso y de los eventos de

seguridad, así como un diseño corporativo coherente para los proveedores de servicios.

Protocolización centralizada. Proporciona un punto central para consolidar los eventos de seguridad y protocolos de miles de dispositivos, permitiendo realizar los análisis forenses de la red desde un único punto.

Informes syslog de próxima generación en tiempo real e históricos. Gracias a las mejoras revolucionarias realizadas en la arquitectura, esta prestación agiliza el lento proceso de sumariación de datos, permitiendo crear informes casi en tiempo real sobre los mensajes syslog entrantes. Asimismo permite personalizar ampliamente los informes y desglosar los datos para obtener una visión más detallada.

Análisis del tráfico de aplicaciones. Ofrece a las organizaciones una visión transparente del tráfico de aplicaciones, del uso del ancho de banda y de las amenazas de seguridad, así como potentes prestaciones forenses y de resolución de problemas.

Amplio soporte de plataformas diferentes para las plataformas SonicWALL de cortafuegos, antispam, backup y recuperación y acceso remoto seguro, de modo que quedan cubiertos todos los productos SonicWALL de la red.

Opciones flexibles de implementación. Con el fin de optimizar la utilización, facilitar la migración y reducir los costes de capital, esta solución está disponible como software, como dispositivo reforzado de alto rendimiento y como dispositivo virtual.

Múltiples opciones de integración. Incluyen una interfaz de programación de aplicaciones (API) para servicios Web, soporte CLI para la mayoría de las funciones, así como soporte de trap SNMP para proveedores de servicios e empresas.

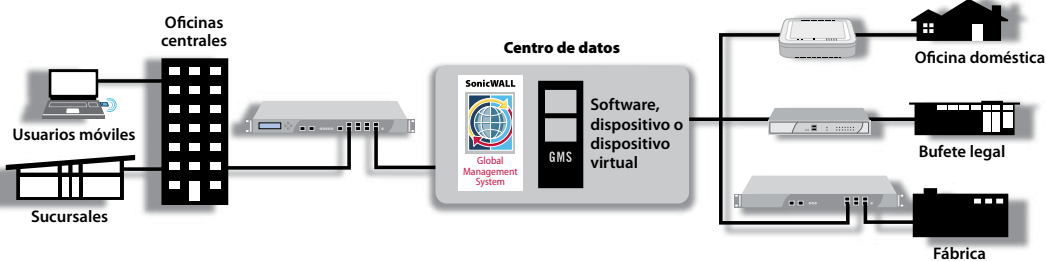
SONICWALL®

Especificaciones técnicas



Global Management System de SonicWALL

GMS proporciona una completa solución de gestión de seguridad para empresas y proveedores de servicios.



SonicWALL GMS Standard Edition

Licencia de software SonicWALL GMS para 5 nodos
01-SSC-7680

Licencia de software SonicWALL GMS para 10 nodos
01-SSC-3363

Licencia de software SonicWALL GMS para 25 nodos
01-SSC-3311

Ampliación de software SonicWALL GMS para 1 nodo
01-SSC-7662

Ampliación de software SonicWALL GMS para 5 nodos
01-SSC-3350

Ampliación de software SonicWALL GMS para 10 nodos
01-SSC-7664

Ampliación de software SonicWALL GMS para 25 nodos
01-SSC-3301

Ampliación de software SonicWALL GMS para 100 nodos
01-SSC-3303

Ampliación de software SonicWALL GMS para 250 nodos
01-SSC-3304

Ampliación de software SonicWALL GMS para 1.000 nodos
01-SSC-3306

Visite www.sonicwall.com/us/products/6030.html para obtener una visión general de los números de producto para servicios de soporte.



Los dashboards contextuales ofrecen diversos widgets informativos, como mapas geográficos, informes syslog, resúmenes del uso del ancho de banda, páginas web más visitadas o la información que resulte más relevante para cada usuario.



Con los informes gráficos intuitivos, la supervisión de dispositivos SonicWALL gestionados es un juego de niños. Analyzer permite identificar anomalías del tráfico basándose en los datos de utilización para determinados intervalos de tiempo, iniciadores, contestadores o servicios. Los informes pueden exportarse a MS Excel o PDF o pueden imprimirse directamente.

Requisitos mínimos del sistema

A continuación se especifican los requisitos mínimos de SonicWALL GMS con respecto a sistemas operativos, bases de datos, controladores, hardware y dispositivos soportados por SonicWALL:

Sistema operativo

Windows Server 2003 64 bits (SP2), Windows Server 64 bits (SP2), Windows Server 2008 SBS 64 bits (R2), Windows Server 2008 Standard 64 bits (R2).

En todos los casos, SonicWALL GMS se ejecuta como aplicación de 32 bits.

Hardware para instalación simple

Entorno x86: servidor con procesador dual-core CPU de Intel de 3 GHz como mínimo, 4 GB de memoria RAM y 300 GB de espacio libre en disco.

Hardware para instalación con servidores distribuidos

Servidor GMS Entorno x86: servidor con procesador dual-core CPU de Intel de 3 GHz como mínimo, 4 GB de memoria RAM y 300 GB de espacio libre en disco.

Dispositivo virtual

Hipervisor: VMware ESX y ESXi

Sistema operativo instalado: SonicLinux reforzado

Tamaño del dispositivo: 250 GB, 950 GB

Memoria asignada: 4 GB

Guía de compatibilidad de hardware de VMware: <http://www.vmware.com/resources/compatibility/search.php>

Bases de datos soportadas

Bases de datos externas: Microsoft SQL 2005 64 bits (SP2), Microsoft SQL 2008 64 bits (R2)

En paquete con la aplicación GMS: MySQL

Navegadores de Internet

Microsoft® Internet Explorer 8.0 o superior

Mozilla Firefox 6.0 o superior

Google Chrome 13.0 y superior

Soportados únicamente en plataformas Microsoft Windows

Java

Java SE Runtime Environment 1.6 o posterior

Pasarela GMS

Cortafuegos de las series SonicWALL SuperMassive™ E10000, E-Class Network Security Appliance (NSA), NSA o PRO con firmware mínimo y cortafuegos¹ SonicWALL basados en VPN

Dispositivos SonicWALL soportados para gestión GMS

Dispositivos de seguridad de red SonicWALL: Dispositivos³ de las series SuperMassive E10000, E-Class NSA, NSA, PRO, TZ

Dispositivos Continuous Data Protection de SonicWALL

Dispositivos Content Security Manager (CSM) de SonicWALL

Dispositivos Secure Remote Access de SonicWALL E-Class SRA y SRA para pymes

Dispositivos Email Security de SonicWALL

Todos los dispositivos y aplicaciones con capacidad TCP/IP y SNMP para una supervisión activa

Firmware soportado

Serie SonicWALL SuperMassive E10000: SonicOS Enhanced 5.0 o superior

SonicWALL E-Class NSA y NSA: SonicOS Enhanced 5.0 o superior

Serie SonicWALL NSA: SonicOS Enhanced 3.2 o superior

Serie SonicWALL TZ: SonicOS Standard 3.1 o superior, y SonicOS Enhanced 3.2 o superior

SonicWALL CDP: Mozilla Firefox 2.3 o superior

SonicWALL CSM: Enhanced 2.0 o superior

SonicWALL SRA para pymes: Enhanced 2.0 o superior

SonicWALL Aventail E-Class SRA: Enhanced 9.0 o superior⁴

SonicWALL Email Security: Firmware SonicWALL Email Security 7.0

¹ En todos los casos, SonicWALL GMS se ejecuta como aplicación de 32 bits. Las bases de datos incluidas en el paquete se ejecutarán en modo de 64 bits en Windows OS 64 bits.

² Si se utiliza la opción de gestión de túneles VPN para una comunicación segura entre el servidor SonicWALL GMS y las aplicaciones gestionadas utilizando túneles VPN, se requiere una pasarela GMS. La pasarela GMS debería ser, como mínimo, un dispositivo SonicWALL NSA con firmware mínimo SonicOS Enhanced 5.0, o un dispositivo SonicWALL PRO 2040 con firmware mínimo SonicOS Enhanced 3.2. Si se utilizan túneles VPN existentes o HTTPS como método de gestión, no se requiere ninguna pasarela GMS. ³ No se soportan los modelos antiguos SonicWALL XPRS/XPRS2, SonicWALL SOHO2, SonicWALL Tele2 ni SonicWALL Pro/Pro-VX. ⁴ Solo dispositivos Aventail E-Class SSL VPN de reciente fabricación con números de serie hexadecimales de 12 caracteres.



UMA EM5000 GMS Mobile es una aplicación gratuita para el iPhone® de Apple® (actualmente disponible como software beta) que los administradores de GMS pueden utilizar desde cualquier lugar para iniciar sesión de forma remota en su sistema GMS y obtener una visión general de todos los dispositivos gestionados, comprobar el estado de los dispositivos y gestionar las alertas GMS que van llegando.



Línea de soluciones de seguridad dinámica de SonicWALL



SEGURIDAD DE RED



ACCESO REMOTO SEGURO



SEGURIDAD DE WEB Y EMAIL



BACKUP Y RECUPERACIÓN



POLÍTICAS Y GESTIÓN

SonicWALL Iberia
T + 34 935 041 694
Spain@sonicwall.com

Contactos de soporte SonicWALL
www.sonicwall.com/emea/4724.html



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™