EL SISTEMA DE GESTIÓN GLOBAL DE SONICWALL

Funciones completas de gestión de la seguridad, monitorización, informes y análisis

Una estrategia de gestión de la seguridad eficaz requiere un conocimiento profundo del entorno de seguridad que permita fomentar una mejor coordinación de las políticas, así como la toma de decisiones más acertadas. Sin una visión del sistema de seguridad de toda la empresa, las organizaciones a menudo corren el riesgo de sufrir ataques cibernéticos y de caer en incumplimientos normativos que podrían haberse evitado. El uso de numerosas herramientas basadas en plataformas diferentes, así como de diferentes formatos de datos, hace que los análisis e informes de seguridad resulten ineficientes a nivel operativo. Ello reduce aún más la capacidad de las organizaciones de reconocer los riesgos de seguridad y de reaccionar rápidamente. Las organizaciones deben establecer un enfoque sistemático para controlar el entorno de seguridad de red con el fin de superar estos retos.

Es aquí donde entra en juego el Sistema de gestión global (GMS) de SonicWall. GMS integra funciones de gestión, monitorización, análisis, pruebas forenses e informes de auditorías. Esto constituye la base de una estrategia de control de la seguridad, cumplimiento normativo y gestión de riesgos. La plataforma GMS, rica en prestaciones, proporciona a empresas distribuidas, proveedores de servicios y otras organizaciones un enfoque holístico y fluido para unificar todos los aspectos operativos de su entorno de seguridad. Con GMS, los equipos de seguridad pueden gestionar fácilmente las soluciones de firewall, los puntos de acceso inalámbricos, la seguridad del correo electrónico y el acceso móvil seguro de SonicWall, así como las soluciones de switches de red de otros proveedores. Todo esto se hace a través de un proceso de flujo de trabajo controlado y auditable para mantener las redes eficaces, seguras y conformes a la normativa. GMS incluye funciones centralizadas de gestión y refuerzo de políticas, monitorización de eventos en tiempo real, análisis e informes de datos granulares, seguimiento, etc., en una plataforma de gestión unificada.

Ventajas:

- Establece un programa unificado de control de la seguridad, cumplimiento normativo y gestión de riesgos
- Adopta un enfoque coherente y auditable para orquestar la seguridad, realizar pruebas forenses y elaborar análisis e informes
- Reduce el riesgo y proporciona una respuesta rápida ante eventos de seguridad
- Proporciona una visión del ecosistema de seguridad de toda la empresa
- Automatiza los flujos de trabajo y garantiza el cumplimiento de las normas de seguridad en las operaciones
- Operacionalice los firewalls en oficinas remotas y sucursales siguiendo la opción de implementación automática (sin necesidad de intervención) en cuatro sencillos pasos
- Permite aprovisionar, gestionar y monitorizar la implementación, la conectividad y el rendimiento de SD-WAN de forma centralizada
- Elabora informes sobre las leyes HIPAA, SOX y las normas de la PCI para auditores internos y externos
- Implementación rápida y sencilla con opciones de software, dispositivo virtual o implementación en la nube — todo ello con un coste reducido

CONTROL CENTRALIZADO

- Establezca una ruta sencilla para la gestión completa de la seguridad, la elaboración de informes de análisis y el cumplimiento normativo a fin de unificar su programa de defensa de seguridad de red
- Automatice y correlacione los flujos de trabajo para formar una estrategia totalmente coordinada de control de la seguridad, cumplimiento normativo y gestión de riesgos

CUMPLIMIENTO NORMATIVO

- Ayuda a mantener satisfechos a los organismos reguladores y a los auditores con informes de seguridad automáticos sobre las normas PCI, HIPAA y SOX
- Personalice cualquier combinación de datos de seguridad auditables para avanzar en el cumplimiento de normas específicas

GESTIÓN DE RIESGOS

- Actúe rápidamente e impulse la colaboración, la comunicación y el conocimiento de todo el framework de seguridad compartido
- Tome decisiones informadas sobre las políticas de seguridad en base a información consolidada y crítica en el tiempo sobre las amenazas para aumentar el nivel de eficiencia de la seguridad

GMS proporciona un enfoque holístico de control de la seguridad, cumplimiento normativo y gestión de riesgos

Automatización de flujos de trabajo

Utilizando la automatización nativa de flujos de trabajo, GMS ayuda a que las operaciones de seguridad cumplan los requisitos de gestión y auditoría de los cambios de políticas de firewall de varias normas legales, como PCI, HIPPA y el RGPD. Permite realizar cambios de políticas al aplicar una serie de procedimientos rigurosos para configurar, comparar, validar, revisar y aprobar políticas de firewall antes de su implementación. Los grupos de aprobación son flexibles para cumplir los cambiantes procedimientos de autorización y auditoría desde diferentes tipos de organizaciones. La automatización de flujos de trabajo implementa mediante programación políticas de seguridad autorizadas para mejorar la eficiencia de las operaciones, mitigar riesgos y eliminar errores.

GMS proporciona un enfoque holístico de control de la seguridad, cumplimiento normativo y gestión de riesgos.

1. CONFIGURACIÓN Y COMPARACIÓN

GMS configura las **órdenes de cambios** de políticas y marca las diferencias con **códigos de colores** para poder hacer comparaciones claras

2. VALIDACIÓN

GMS **valida la integridad de la lógica de la política**

3. REVISIÓN Y APROBACIÓN

GMS envía e-mails a los revisores y realiza un **seguimiento (aprobación/ desaprobación)** de la política

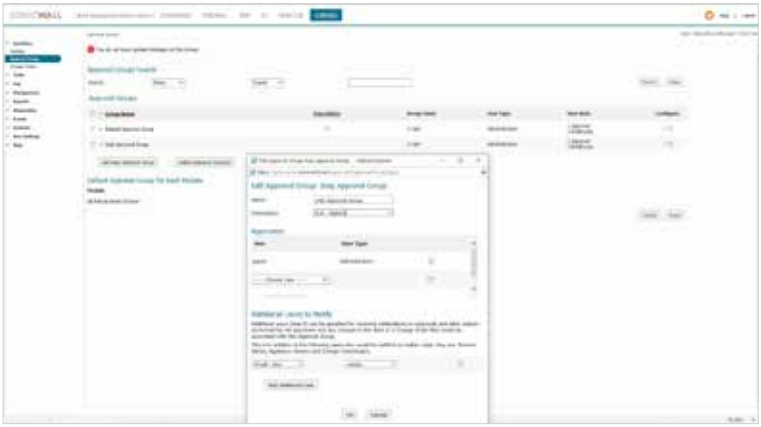
4. IMPLEMENTACIÓN

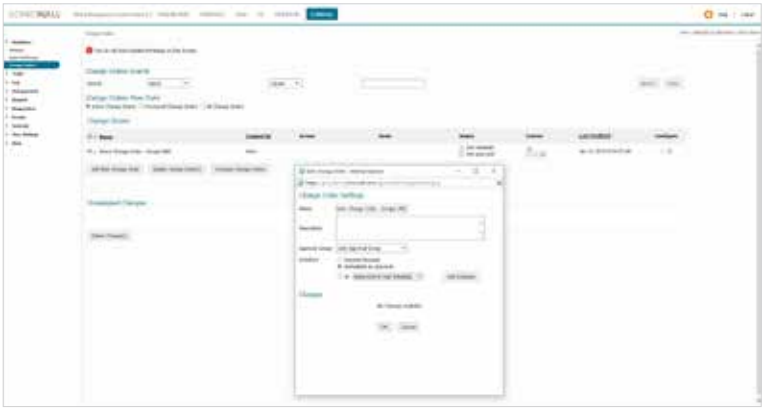
GMS implementa los cambios de políticas inmediatamente o **de forma planificada**

5. AUDITORÍA

Los registros de cambios permiten **auditar** las políticas con precisión y obtener datos exactos sobre el **cumplimiento normativo**

Automatización de flujos de trabajo de GMS: Cinco pasos para una gestión de políticas libre de errores





Partner Enabled Services

¿Necesita ayuda para planificar, implementar u optimizar su solución SonicWall? Los Partners de servicios avanzados de SonicWall están cualificados para proporcionarle servicios profesionales de clase mundial. Si desea obtener más información, visite www.sonicwall.com/PES.

Implementación sin necesidad de intervención

Integrado en GMS, el servicio de Implementación automática (sin necesidad de intervención) simplifica y acelera el proceso de aprovisionamiento para los firewalls de SonicWall en ubicaciones de oficinas remotas y sucursales. El proceso requiere una intervención mínima por parte del usuario y operacionaliza de forma completamente automatizada los firewalls a escala en cuatro sencillos pasos. Esto reduce considerablemente el tiempo, el coste y la complejidad asociados a la instalación y la configuración, mientras que la seguridad y la conectividad se producen de forma instantánea y automática.

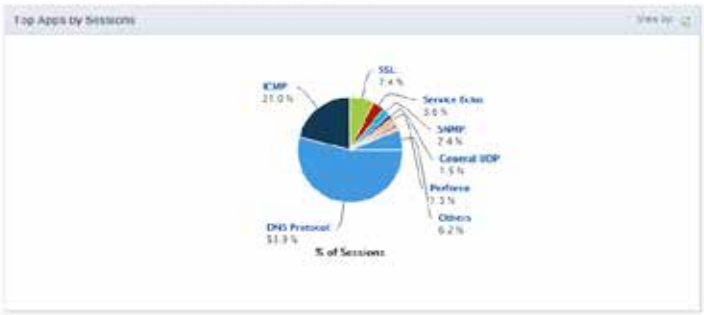
PASO 1	**REGISTRE EL FIREWALL** Registre el nuevo firewall en MySonicWall utilizando el número de serie asignado y el código de autenticación.
PASO 2	**CONECTE EL FIREWALL** Conecte el firewall a la red utilizando el cable Ethernet que vino con la unidad.
PASO 3	**ENCIENDA EL FIREWALL** Encienda el firewall tras conectar el cable de alimentación y enchufarlo a una toma de corriente de pared estándar. A las unidades se les asigna automáticamente una IP WAN utilizando un servidor DHCP. Una vez establecida la conectividad, se descubre, autentica y añade automáticamente la unidad a Capture Security Center con todas las licencias y las configuraciones sincronizadas con MySonicWall y el Administrador de licencias.
PASO 4	**GESTIONE EL FIREWALL** La unidad ya está operativa y se gestiona a través de la consola de gestión central basada en la nube de Capture Security Center (actualizaciones de firmware, parches de seguridad y cambios de configuración a nivel de grupo).

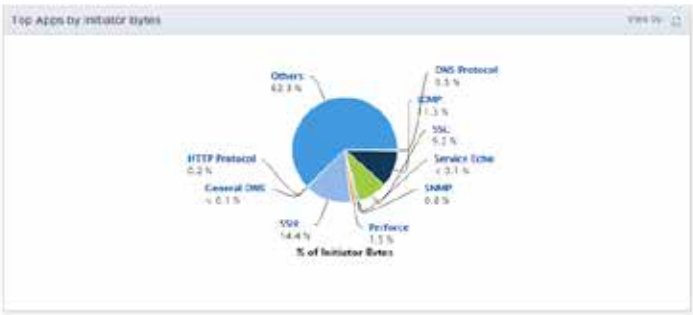
Implementación sin necesidad de intervención: Operacionalice el firewall en cuatro sencillos pasos

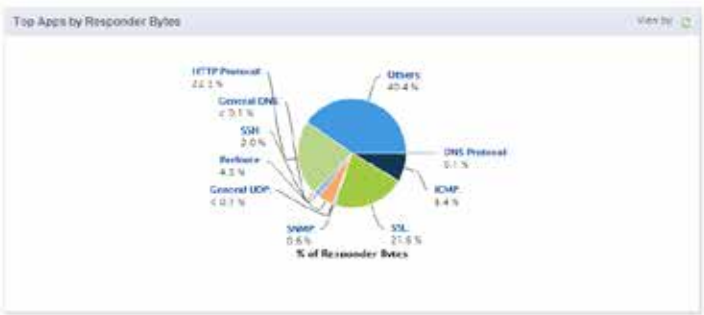
Informes

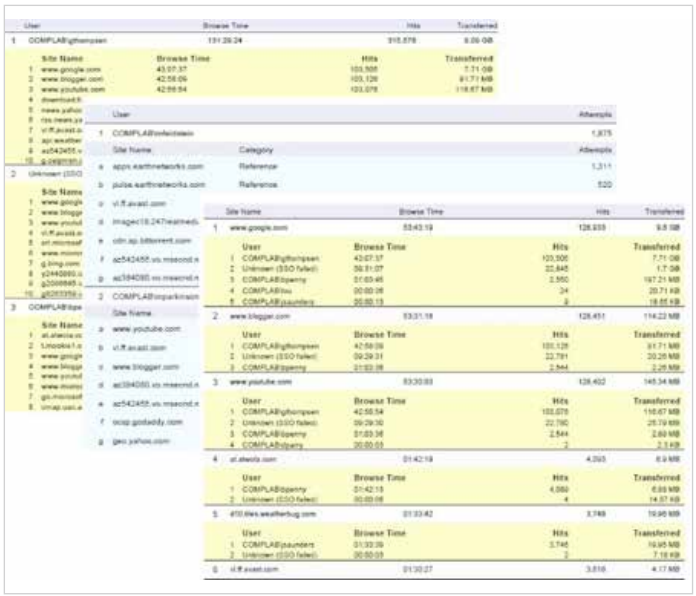
Capture Security Center ofrece más de 140 informes predefinidos, así como la flexibilidad necesaria para crear informes personalizados utilizando cualquier combinación de datos auditables con el fin de aplicarlos a diferentes casos de uso. Los resultados incluyen información global y detallada de los eventos de la red, las actividades de los usuarios, las amenazas, los problemas operacionales y de rendimiento, la eficacia de la seguridad, la preparación para el cumplimiento normativo e incluso análisis post-mortem. Todos los informes están diseñados con información colectiva de muchos años de colaboraciones de clientes y partners de SonicWall. Esto proporciona la granularidad profunda, el alcance y los conocimientos de datos syslog e IPFIX/NetFlow necesarios para seguir, medir y gestionar una operación efectiva tanto de la red como de la seguridad.

Los informes gráficos intuitivos simplifican la monitorización de los dispositivos gestionados. Los administradores pueden identificar anomalías del tráfico fácilmente basándose en los datos de utilización para determinados intervalos de tiempo, iniciadores, respondedores o servicios. Asimismo, pueden exportar los informes a una hoja de cálculo de Microsoft® Excel®, un archivo PDF (formato de documento portátil) o directamente a una impresora para las revisiones rutinarias del negocio.









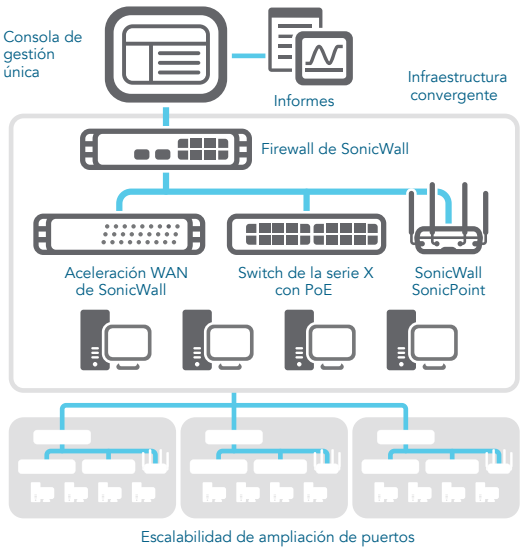
SONICWALL®

Prestaciones de gestión y monitorización de la seguridad	
Prestación	Descripción
Gestión centralizada de la seguridad y de la red	Ayuda a los administradores a implementar, gestionar y supervisar un entorno de seguridad de red distribuido.
Configuración federada de políticas	Establece políticas fácilmente desde una ubicación central para miles de firewalls, puntos de acceso inalámbricos, dispositivos de seguridad de correo electrónico, acceso remoto seguro y switches de SonicWall.
Gestión y flujo de trabajo de las solicitudes de cambio	Esta prestación garantiza la corrección y el cumplimiento de las modificaciones de políticas reforzando un proceso riguroso para la configuración, comparación, validación, revisión y aprobación de políticas antes de la implementación. Los grupos de aprobación son configurables por los usuarios para cumplir la política de seguridad de la empresa. Todos los cambios de las políticas se registran de forma auditable, garantizándose así que el firewall cumpla la normativa vigente. Todos los detalles granulares de cualquier cambio realizado se archivan de forma histórica para facilitar el cumplimiento normativo, el seguimiento y la resolución de problemas.
Implementación sin necesidad de intervención	Simplifica y acelera la implementación y el aprovisionamiento de los firewalls de SonicWall que utilizan la nube de forma remota. Transfiere políticas automáticamente, realiza actualizaciones de firmware y sincroniza licencias.
Aprovisionamiento de SD-WAN	Aprovisione, gestione y monitorice de forma centralizada y sencilla la implementación y conectividad de SD-WAN en un entorno empresarial distribuido.
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 del firmware en dispositivos gestionados para minimizar las interrupciones del servicio.
Gestión de licencias optimizada	Simplifica la gestión de dispositivos mediante una consola unificada, así como la gestión de la seguridad y de las suscripciones de licencias de soporte.
Dashboard universal	Incluye widgets personalizables, mapas geográficos e informes centrados en el usuario.
Monitorización activa de dispositivos y alertas	Proporciona alertas en tiempo real con prestaciones de monitorización 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 el Protocolo de control de transmisiones/Protocolo Internet (TCP/IP) y SNMP, facilitando enormemente los esfuerzos de resolución de problemas para identificar los eventos críticos de la red y reaccionar ante ellos.
Visualización e inteligencia de aplicaciones	Ofrece informes históricos y en tiempo real sobre las aplicaciones que se están utilizando y los usuarios que las utilizan. Los informes son completamente personalizables mediante prestaciones intuitivas de filtrado y desglose.
Múltiples opciones de integración	Incluyen una interfaz de programación de aplicaciones (API) para servicios Web, soporte de interfaz de línea de comandos (CLI) para la mayoría de las funciones, así como soporte de trap SNMP para proveedores de servicios y empresas.
Gestión de switches de la serie Dell Networking X	Ahora, los switches de la serie X de Dell pueden gestionarse fácilmente desde los firewalls de las series TZ, NSA y SuperMassive para ofrecer una única consola desde la cual gestionar toda la infraestructura de seguridad de red.
Soporte de redes cerradas	Implemente GMS en entornos cerrados, como redes gubernamentales altamente protegidas. Todos los conjuntos de claves de licencias y archivos de definiciones de los servicios de backend de SonicWall se empaquetan, cifran y transfieren de forma segura al sistema de archivos local, donde GMS puede acceder a las actualizaciones requeridas, cargarlas y transferirlas a todos los dispositivos de seguridad gestionados.
Informes y análisis de seguridad	
Prestación	Descripción
Informe botnet	Incluye cuatro tipos de informes: Intentos, objetivos, iniciadores e intervalos de tiempo, que incluyen contexto de vectores de ataque, como ID de botnet, direcciones IP, países, hosts, puertos, interfaces, iniciador/objetivo, origen/destino y usuario.
Informe de Geo IP	Contiene información sobre el tráfico bloqueado en base al país de origen o destino del tráfico. Incluye cuatro tipos de informes: Intentos, objetivos, iniciadores e intervalos de tiempo, que incluyen contexto de vectores de ataque, como ID de botnet, direcciones IP, países, hosts, puertos, interfaces, iniciador/objetivo, origen/destino y usuario.

Informes y análisis de seguridad (cont.)	
Prestación	Descripción
Informe de direcciones MAC	Muestra la dirección MAC (Media Access Control) en la página de informes. Incluye información específica de los dispositivos (MAC del iniciador y MAC del respondedor) en cinco tipos de informes: • Uso de datos > Iniciadores • Uso de datos > Respondedores • Uso de datos > Detalles • Actividad de usuarios > Detalles • Actividad Web > Iniciadores
Informe de Capture ATP	Muestra información detallada sobre el comportamiento de las amenazas para responder a una amenaza o infección.
Informes sobre las normas HIPPA, PCI y SOX	Incluye plantillas predefinidas de informes sobre las normas PCI, HIPAA y SOX para las auditorías de cumplimiento de la normativa de seguridad vigente.
Informes de puntos de acceso inalámbricos no autorizados	Muestra todos los dispositivos inalámbricos que se están utilizando, así como el comportamiento no autorizado de las interconexiones punto a punto ad hoc entre hosts y asociaciones accidentales de usuarios que se conectan a redes vecinas no autorizadas.
Análisis e informes de flujos	Proporcionan un agente de informes de flujos para el análisis del tráfico de las aplicaciones y datos sobre el uso mediante protocolos IPFIX o NetFlow para ofrecer una monitorización en tiempo real e histórica. Ofrecen a los administradores una interfaz efectiva y eficiente para monitorizar visualmente su red en tiempo real. De esta forma, pueden identificar aplicaciones y páginas Web con gran demanda de ancho de banda, visualizar el uso de las aplicaciones por usuarios y anticiparse a ataques y amenazas en la red. • Un visor en tiempo real personalizable mediante funciones de arrastrar y soltar • Una pantalla de informes en tiempo real con filtrado de un solo clic • Un cuadro de mando de Flujos principales con botones de «Ver por» de un solo clic • Una pantalla de informes de flujos con cinco pestañas de atributos de flujos adicionales • Una pantalla de análisis de flujos con potentes funciones de correlación y rotación • Un visor de sesiones para el desglose profundo de sesiones individuales y paquetes.
Informes inteligentes y visualización de actividades	Proporciona informes de gestión e informes gráficos completos para los firewalls y los dispositivos de seguridad del correo electrónico y de acceso móvil seguro de SonicWall. Ofrece una visión más amplia de las tendencias de uso y los eventos de seguridad, al tiempo que permite la adaptación al diseño corporativo de 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 una revolucionaria mejora de la arquitectura, optimiza el lento proceso de resumen, lo cual permite elaborar informes casi en tiempo real sobre los mensajes syslog entrantes. También ofrece la posibilidad de desglosar los datos y personalizar ampliamente los informes.
Informes programados universales	Planifica informes que se crean automáticamente y se envían a través de múltiples dispositivos de diversos tipos a los destinatarios autorizados.
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 de análisis forenses y resolución de problemas.
Seguridad de la autenticación	
Prestación	Descripción
Bloqueo de cuentas	La política de bloqueo de cuentas desactiva las cuentas de usuario de GMS en el caso de que se realice un determinado número de intentos con contraseñas incorrectas durante un determinado periodo. Esto ayuda a impedir que los perpetradores de ataques adivinen las contraseñas de los usuarios y a reducir la probabilidad de que se produzcan ataques con éxito y los criminales accedan sin autorización a los recursos y datos protegidos de la red.
Complejidad de la contraseña	La política de complejidad de la contraseña establece las directrices mínimas consideradas importantes para contar con una contraseña fuerte de inicio de sesión y acceso al sistema GMS.
Acceso de administrador a un intervalo de direcciones específico	Los clientes podrán controlar el acceso de administrador a intervalos de direcciones IP específicos.

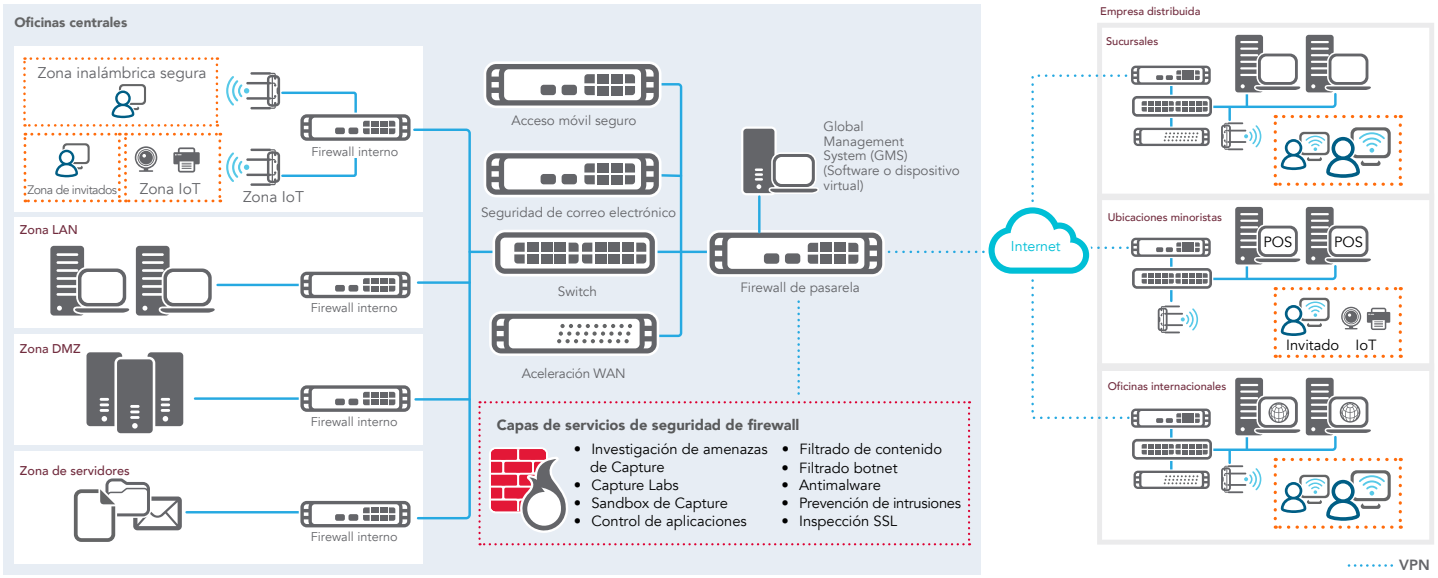
Arquitectura distribuida escalable

GMS es una solución local, implementable como dispositivo de software o virtual. GMS se basa en una arquitectura distribuida que simplifica la disponibilidad y la escalabilidad ilimitadas del sistema. Una sola instancia de GMS puede añadir visibilidad y control sobre miles de dispositivos de seguridad de red gestionados, independientemente de su ubicación. A nivel de interacción con el cliente, sus cuadros de mando universales altamente interactivos, cargados con datos de monitorización, informes y análisis en tiempo real, ayudan a tomar decisiones inteligentes en materia de políticas de seguridad y fomentan la colaboración, la comunicación y el conocimiento en todo el marco de seguridad compartido. Gracias a la visión del entorno de seguridad de toda la empresa y a la inteligencia de seguridad en tiempo real, puesta a disposición de los miembros adecuados de la organización, se pueden emprender acciones acertadas relacionadas con las políticas y los controles de seguridad, dirigidas a lograr una seguridad adaptativa y reforzada.



SonicWall Global Management System (GMS)

GMS local proporciona una plataforma completa y escalable de gestión de la seguridad, análisis e informes para empresas distribuidas y centros de datos.



Entornos de SonicWall Global Management System locales

Visión de conjunto de las prestaciones

Informes

- Conjunto completo de informes gráficos
- Informes sobre el cumplimiento de normas
- Informes personalizables con funciones de desglose
- Protocolización centralizada
- Informes sobre amenazas múltiples
- Informes centrados en el usuario
- Informes del uso de las aplicaciones
- Informes de servicios granulares
- Nuevas funciones de inteligencia de ataques
- Informe de ancho de banda y servicios por interfaz
- Informes para dispositivos de firewall de SonicWall
- Informes para dispositivos SonicWall SRA SSL VPN
- Informes programados universales
- Informes Syslog e IPFIX de próxima generación
- Informes flexibles y granulares casi en tiempo real
- Informes del ancho de banda por usuario
- Informes de actividad de VPN cliente
- Resumen detallado de los servicios a través de un informe VPN
- Informes de puntos de acceso inalámbricos no autorizados
- Informes de Web Application Firewall (WAF) de SRA para pymes

Gestión

- Acceso desde cualquier lugar
- Alertas y notificaciones
- Herramientas de diagnóstico
- Múltiples sesiones de usuarios simultáneas
- Gestión y planificación offline
- Gestión de las políticas de firewall de seguridad
- Gestión de las políticas de seguridad de VPN
- Gestión de las políticas de seguridad del correo electrónico
- Gestión de las políticas de Acceso remoto seguro/SSL VPN
- Gestión de los servicios de seguridad de valor añadido
- Definición de plantillas de políticas a nivel de grupo
- Replicación de políticas desde un dispositivo a un grupo de dispositivos
- Replicación desde el nivel de grupo a un dispositivo individual
- Redundancia y alta disponibilidad
- Gestión del aprovisionamiento
- Arquitectura escalable y distribuida
- Vistas de gestión dinámicas
- Administrador unificado de licencias
- Interfaz de línea de comandos (CLI)
- Interfaz de programación (API) de aplicaciones de servicios Web
- Gestión basada en roles (usuarios, grupos)
- Dashboard universal
- Backup de archivos preferentes para dispositivos de firewall
- SD-WAN
- Implementación sin necesidad de intervención
- Soporte de redes cerradas
- Soporte de sándwiches de firewalls

Monitorización

Flujos de datos IPFIX en tiempo real

Soporte SNMP

Supervisión activa de dispositivos y alertas

Gestión del relé SNMP

Monitorización del estado de la VPN y el firewall

Supervisión en vivo y alertas Syslog

Seguridad de la autenticación

Bloqueo de cuentas

Complejidad de la contraseña

Acceso de administrador a un intervalo de direcciones específico

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 2016
- Windows Server 2012 Standard 64 bits
- Windows Server 2012 R2 Standard 64 bits (Versiones en inglés y japonés)
- Windows Server 2012 R2 Datacenter

Requisitos de hardware

- Utilice la calculadora de capacidad de GMS para determinar los requisitos de hardware para su implementación.

Requisitos de dispositivo virtual

- Hipervisor: ESXi 6.5, 6.0 ó 5.5
- Utilice la calculadora de capacidad de GMS para determinar los requisitos de hardware para su implementación.

Guía de compatibilidad de hardware de VMware:

www.vmware.com/resources/compatibility/search.php

Bases de datos soportadas

- Bases de datos externas: Microsoft SQL Server 2012 y 2014
- En paquete con la aplicación GMS: MySQL

Navegadores de Internet

- Microsoft® Internet Explorer 11.0 o superior (no utilizar modo de compatibilidad)
- Mozilla Firefox 37.0 o superior
- Google Chrome 42.0 o superior
- Safari (última versión)

Dispositivos SonicWall soportados para gestión GMS

- Dispositivos SonicWall de seguridad de red: Dispositivos de las series SuperMassive E10000 y 9000, E-Class NSA, NSa y TZ
- Dispositivos virtuales de seguridad de red de SonicWall: Serie NSv
- Dispositivos SonicWall Secure Mobile Access (SMA): Series SMA y E-Class SRA
- Dispositivos Email Security de SonicWall
- Todos los dispositivos y aplicaciones con capacidad TCP/IP y SNMP para supervisión activa

Información de pedido para el Sistema de gestión global (GMS)	
Producto	SKU
LICENCIA DE SOFTWARE PARA SONICWALL GMS DE 5 NODOS	01-SSC-3311
LICENCIA DE SOFTWARE PARA SONICWALL GMS DE 10 NODOS	01-SSC-7662
LICENCIA DE SOFTWARE PARA SONICWALL GMS DE 25 NODOS	01-SSC-3350
AMPLIACIÓN DEL SOFTWARE SONICWALL GMS, 1 NODO	01-SSC-7664
AMPLIACIÓN DEL SOFTWARE SONICWALL GMS, 5 NODOS	01-SSC-3301
AMPLIACIÓN DEL SOFTWARE SONICWALL GMS, 10 NODOS	01-SSC-3303
AMPLIACIÓN DEL SOFTWARE SONICWALL GMS, 25 NODOS	01-SSC-3304
AMPLIACIÓN DEL SOFTWARE SONICWALL GMS, 100 NODOS	01-SSC-3306
AMPLIACIÓN DEL SOFTWARE SONICWALL GMS, 250 NODOS	01-SSC-0424
AMPLIACIÓN DEL SOFTWARE SONICWALL GMS, 1000 NODOS	01-SSC-7675
SONICWALL GMS DE GESTIÓN DE CAMBIOS Y FLUJOS DE TRABAJO	01-SSC-6524
SOPORTE DE SONICWALL GMS E-CLASS 24X7,1 NODO, 1 AÑO	01-SSC-6514
SOPORTE DE SONICWALL GMS E-CLASS 24X7,1 NODO, 5 AÑOS	01-SSC-3334
SOPORTE DE SONICWALL GMS E-CLASS 24X7,1 NODO, 10 AÑOS	01-SSC-3336
SOPORTE DE SONICWALL GMS E-CLASS 24X7,1 NODO, 25 AÑOS	01-SSC-3337
SOPORTE DE SONICWALL GMS E-CLASS 24X7,1 NODO, 100 AÑOS	01-SSC-3338
SOPORTE DE SONICWALL GMS E-CLASS 24X7,1 NODO, 250 AÑOS	01-SSC-6524
SOPORTE DE SONICWALL GMS E-CLASS 24X7,1 NODO, 1000 AÑOS	01-SSC-6514
SOPORTE DE SONICWALL GMS E-CLASS 24X7,1 NODO, 25 AÑOS	01-SSC-3334
SOPORTE DE SONICWALL GMS E-CLASS 24X7,1 NODO, 100 AÑOS	01-SSC-3336
SOPORTE DE SONICWALL GMS E-CLASS 24X7,1 NODO, 250 AÑOS	01-SSC-3337
SOPORTE DE SONICWALL GMS E-CLASS 24X7,1 NODO, 1000 AÑOS	01-SSC-3338

Acerca de nosotros

SonicWall lleva más de 27 años combatiendo la industria del crimen cibernético y defendiendo a las empresas pequeñas, medianas y grandes de todo el mundo. Nuestra combinación de productos y partners nos ha permitido crear una solución automatizada de detección y prevención de brechas en tiempo real adaptada a las necesidades específicas de más de 500.000 organizaciones en más de 215 países y territorios, para que usted pueda centrarse por completo en su negocio sin tener que preocuparse por las amenazas. Para más información, visite **www.sonicwall.com** o síganos en Twitter, LinkedIn, Facebook e Instagram.

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

DataSheet-SonicWallGlobalManagementSystem-US-VG-MKTG4042