



SonicWALL Comprehensive Anti-Spam Service

GESTIÓN UNIFICADA DE AMENAZAS

Protección antispam inmediata en la pasarela

Hoy en día, la tasa de mensajes de correo electrónico no deseados (correos spam, phishing y mensajes infectados por virus) asciende casi al 94%. Este tráfico, no solo es peligroso, si no que además distrae a los empleados, paraliza las comunicaciones corporativas y frena la productividad de la organización. Si este correo basura se elimina ya en la pasarela, es posible mejorar la eficiencia de la red y aumentar la productividad de la plantilla y del correo electrónico.

SonicWALL® Comprehensive Anti-Spam Service (CASS) ofrece protección completa antispam y antivirus para pymes y puede implementarse de forma instantánea en cualquier cortafuegos SonicWALL. CASS agiliza la implementación, simplifica la administración y reduce la complejidad de la infraestructura informática al consolidar soluciones y ofrecer un servicio antispam de un solo clic y una configuración avanzada de tan solo 10 minutos. CASS proporciona antispam, antiphishing y antimalware completo para el tráfico entrante, reputación IP combinada con SonicWALL Global Response Intelligent Defense (GRID), gestión avanzada de contenidos, prevención de Denial of Service, cuarentena completa e informes de correo basura personalizables a nivel de usuario. Asimismo, CASS supera el filtrado RBL ofreciendo una eficacia de más del 98% contra spam y una tasa de detección de más del 80% del spam en la pasarela. Para procesar el correo restante, CASS utiliza tecnologías antispam avanzadas como el filtrado Adversarial Bayesian™.

Prestaciones y ventajas

Gestión avanzada de reputación (ARM). Esta prestación utiliza la reputación IP del remitente para bloquear los mensajes basura a nivel de conexión (p.ej., spam, phishing y virus adjuntos). Mediante la red GRID de SonicWALL se evalúa la reputación en tiempo real para identificar y bloquear los correos no deseados procedentes de direcciones sospechosas. La gestión avanzada de la reputación permite prescindir de los servicios de lista negra en tiempo real poco efectivos, lentos y propensos a errores.

Gestión avanzada de contenido basada en nube (ACM). Elimina el correo basura restante aplicando las probadas técnicas antispam de SonicWALL (p.ej., análisis Adversarial Bayesian, datos de la red GRID de SonicWALL, motor de inferencia de imágenes, detección de mensajes ininteligibles y análisis bayesiano antiphishing). El diseño basado en nube utiliza estas técnicas antispam avanzadas sin impactar en el procesamiento del cortafuegos ni y el rendimiento global de la red.

Enrutamiento flexible del correo no deseado. Clasifica el correo basura según las categorías spam, spam probable, phishing, phishing probable, virus y virus probable. Para garantizar el control adecuado y el cumplimiento de las normas corporativas y legales, los mensajes de cada categoría pueden rechazarse, marcarse y entregarse, enviarse a la bandeja de correo basura del usuario o borrarse.

Bandeja de correo basura de usuario opcional. Permite configurar rápidamente para todos los usuarios bandejas de correo basura en las que se guardan los correos no deseados. Los usuarios pueden recibir informes de bandeja de spam por correo electrónico para ver los correos (como texto) y reclasificarlos en su caso como mensajes legítimos. El departamento de TI mantiene el control sobre las categorías mostradas, los plazos y la retención de los informes de bandeja de spam.

SonicWALL **GRID antivirus** entra en acción automáticamente junto con SonicWALL CASS para detectar correos

basados en SMTP con virus y reenviarlos en la pasarela según lo haya definido el administrador (p.ej., rechazarlos o borrarlos). Si se adquieren por separado, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service y SonicWALL Enforced Client Anti-Virus and Anti-Spyware Service ofrecen una protección antivirus multicapa completa.

Listas integradas de permitir y bloquear. Estas listas están incorporadas en los dispositivos de seguridad de red de SonicWALL. Las direcciones IP pueden permitirse o bloquearse en la pasarela. También puede añadirse un control granular con listas de permitir y bloquear a nivel de personas, empresas y listas. Esta prestación es soportada por completo por CASS y no requiere ni configuración ni entrenamiento adicional.

Protocolización y elaboración de informes integradas. Esta prestación incorporada en los dispositivos de seguridad de red de SonicWALL permite visualizar fácilmente el estado y las estadísticas del servicio con un solo clic y consultar las entradas de los archivos de registro según nombre del servicio. El estado del servicio muestra la disponibilidad de SonicWALL Comprehensive Anti-Spam Service, de las bandejas de correo basura y del servidor de correo electrónico postconectado.

Integración flexible de LDAP. Permite una gestión robusta, sencilla y segura de los usuarios y ofrece flexibilidad adicional soportando la integración de múltiples servidores LDAP.

En caso de utilizarse, SonicWALL Comprehensive Anti-Spam Service **soporta los sistemas de seguridad de correo electrónico postconectados**. Por ejemplo, SonicWALL Email Security puede proporcionar prestaciones avanzadas como políticas de gobierno corporativo o de cumplimiento de normas, políticas y preferencias por usuario, informes avanzados y también otras funciones requeridas.

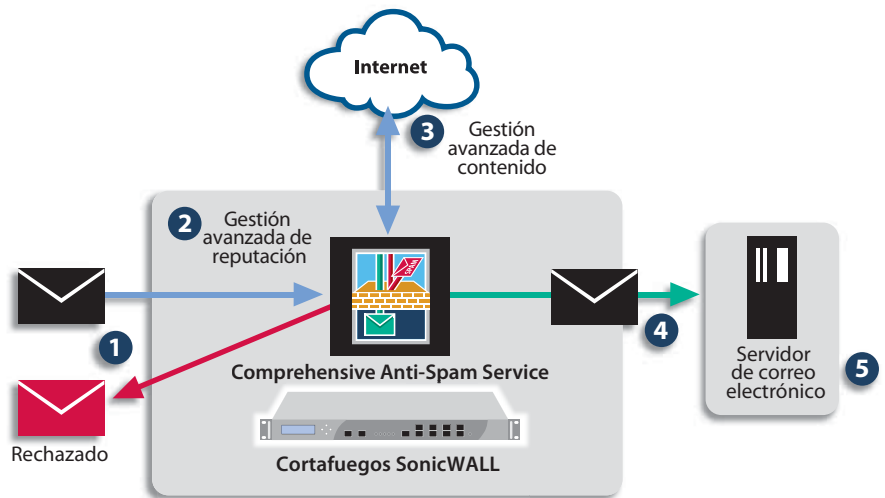
- **Gestión avanzada de reputación (ARM)**
- **Gestión avanzada de contenido basada en nube (ACM)**
- **Enrutamiento flexible del correo no deseado**
- **Bandeja de correo basura de usuario opcional**
- **GRID antivirus**
- **Listas integradas de permitir y bloquear**
- **Protocolización y elaboración de informes integradas**
- **Integración flexible de LDAP**
- **Soporte de sistemas de seguridad de correo electrónico postconectados**

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Especificaciones

Funcionamiento de SonicWALL Comprehensive Anti-Spam Service



- 1 El tráfico SMTP llega al cortafuegos de SonicWALL
- 2 SonicWALL Comprehensive Anti-Spam Service comprueba la reputación del servidor IP remitente en tiempo real mediante el servicio avanzado de gestión de reputación (Advanced Reputation Management, ARM). ARM recibe información en tiempo real de más de 4 millones de puntos terminales en todo el mundo para evaluar la reputación de los servidores que envían correo electrónico. Más del 80% del correo no deseado puede bloquearse a nivel de conexión, lo cual reduce la carga de procesamiento del cortafuegos.
- 3 Los correos restantes se procesan mediante el servicio de gestión avanzada de contenido (Advanced Content Management, ACM) basado en nube. El servicio ACM utiliza las probadas técnicas de detección de spam de SonicWALL.
- 4 El correo legítimo se entrega al servidor de correo electrónico.
- 5 Opcionalmente, el correo no deseado puede depositarse en las bandejas de correo basura de SonicWALL del servidor de correo electrónico, pudiéndose enviar a cada usuario un informe de correo basura en forma de mensajes de correo electrónico.

¿Para quién está pensado SonicWALL Comprehensive Anti-Spam Service?

Gracias a CASS, las empresas más pequeñas que desean aprovechar la inversión en un cortafuegos SonicWALL pueden garantizar rápidamente que solo llegue a su servidor de correo electrónico el correo legítimo. Los administradores pueden gestionar CASS mediante una interfaz integrada en el mismo cortafuegos. Por otro lado, las empresas más grandes pueden añadir una capa adicional a su protección antispam conectando CASS antes de una solución SonicWALL Email Security. De esta forma pueden bloquear más del 80% del correo basura a nivel de conexión y reducir así el procesamiento subsiguiente en los sistemas postconectados. Las empresas distribuidas que reciben correo en múltiples emplazamientos pueden implementar CASS en diferentes cortafuegos SonicWALL remotos para reducir el tráfico spam de la red. Además pueden utilizar SonicWALL Email Security para centralizar los servicios de protección del correo electrónico.

Plataformas y servidores de correo electrónico soportados

SonicWALL Comprehensive Anti-Spam Service está disponible como servicio de suscripción en los siguientes productos SonicWALL:

- Series TZ 100, TZ 200 y TZ 210 con SonicOS 5.6.3 o superior
- Todas las series SonicWALL Network Security Appliance (NSA) y SonicWALL E-Class NSA con SonicOS 5.6.3 o superior
- No se soportan las plataformas y/o versiones de SonicOS que no figuran aquí

SonicWALL Comprehensive Anti-Spam Service funciona con cualquier servidor de correo electrónico que acepte mensajes SMTP entrantes.

Opciones de SonicWALL Comprehensive Anti-Spam Service

La opción de **bandeja de correo basura de usuario** requiere que la aplicación de almacenamiento de correo basura (suministrada como parte del servicio) se instale en un servidor (normalmente el servidor de correo electrónico del cliente) con Windows Server 2003 o Windows Server 2008.

Línea de productos de protección completa de SonicWALL



SEGURIDAD DE RED



ACCESO REMOTO SEGURO



SEGURIDAD DE WEB Y EMAIL



BACKUP Y RECUPERACIÓN



POLÍTICAS Y GESTIÓN

SONICWALL

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™



Comprehensive Anti-Spam Service

Comprehensive Anti-Spam Service para la serie TZ 100 (1 año)
01-SSC-8985

Comprehensive Anti-Spam Service para la serie TZ 200 (1 año)
01-SSC-8988

Comprehensive Anti-Spam Service para la serie TZ 210 (1 año)
01-SSC-8991

Comprehensive Anti-Spam Service para NSA 240 (1 año)
01-SSC-8994

Comprehensive Anti-Spam Service para NSA 2400 (1 año)
01-SSC-8997

Comprehensive Anti-Spam Service para NSA 3500 (1 año)
01-SSC-9000

También hay disponibles números de producto para suscripciones de varios años. Visite www.sonicwall.com.

Comprehensive Anti-Spam Service soporta un número de usuarios ilimitado. No obstante, se recomienda utilizarlo para 250 usuarios o menos.

SonicWALL Iberia
T + 34 653 948 287
Spain@sonicwall.com

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