Comprehensive Anti-Spam Service

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 80%. Este tráfico no solo es peligroso, sino 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 firewall 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 que requiere tan solo 10 minutos. CASS proporciona protección y prestaciones antispam, antiphishing y antimalware completas para el tráfico entrante, SonicWall Capture Threat Network, reputación de IP, gestión avanzada de contenidos, prevención de ataques por denegación de servicio, cuarentena completa e informes de correo basura personalizables a nivel de usuario. Asimismo, CASS supera el filtrado RBL ofreciendo una eficacia de más del 99% contra el spam y una tasa de detección de más del 80% del spam en la pasarela. CASS utiliza tecnologías antispam avanzadas como el filtrado Adversarial Bayesian™ con técnicas avanzadas de detección y de aprendizaje automático.

Prestaciones y ventajas

Detenga los ataques de spam, phishing y virus utilizando múltiples tecnologías probadas y patentadas*, como p.ej. la comprobación de la reputación. Esta prestación no solo evalúa la reputación de la dirección IP del remitente, sino también la del contenido, la estructura, los enlaces, las imágenes y los archivos adjuntos del mismo. Asimismo, utiliza técnicas avanzadas para analizar el contenido del correo electrónico, como filtrado Adversarial Bayesian, análisis de imágenes y detección de mensajes ininteligibles para detectar amenazas conocidas ocultas y amenazas nuevas. El diseño basado en nube utiliza estas técnicas antispam avanzadas sin repercusión en el procesamiento del firewall ni en el rendimiento global de la red.

Información sobre las amenazas en tiempo real a través de la red SonicWall Capture Threat Network, que recopila y analiza información basándose en listas de amenazas de la industria. Cada día realiza pruebas y evaluaciones rigurosas de millones de e-mails, puntuando la reputación de los remitentes y del contenido e identificando amenazas nuevas en tiempo real con el fin de proporcionar la protección más potente y actual contra nuevos ataques de spam mientras garantiza la entrega de los mensajes de correo electrónico inofensivos.

SonicWall Capture Cloud utiliza la tecnología de la red Capture Threat Network de SonicWall para ofrecer protección antivirus y antispyware basada en la nube.

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

Ventajas:

- Detiene los ataques de spam
- Información sobre amenazas en tiempo real con la red Capture Threat Network de SonicWall
- Capture Cloud
- Bandeja de correo basura de usuario opcional
- Listas integradas de permitir y bloquear
- Protocolización y elaboración de informes integradas
- Integración de LDAP
- Soporte de sistemas de seguridad de correo electrónico postconectados

Patentes EEUU: 7,814,545; 7,343,624; 7,665,140; 7,653,698; 7,546,348

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.

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. Los administradores de TI también pueden añadir un control granular con listas de permitir y bloquear a nivel de personas, empresas y listas. CASS soporta por completo esta prestación, que no requiere configuración ni formación adicionales.

Funciones integradas de protocolización y elaboración de informes, incorporadas en el firewall de SonicWall. El estado y las estadísticas de servicio se pueden visualizar con un solo clic y se pueden consultar las entradas de los archivos de registro por nombre del servicio. El estado de servicio muestra la disponibilidad de CASS, de las bandejas de correo basura y del servidor de correo electrónico postconectado.

Integración LDAP. Permite una gestión robusta, sencilla y segura de los usuarios y ofrece flexibilidad adicional a través del soporte de integración LDAP.

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.

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

Gracias a CASS, las empresas más pequeñas que desean aprovechar su inversión en un firewall 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 firewall. 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 firewalls 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:

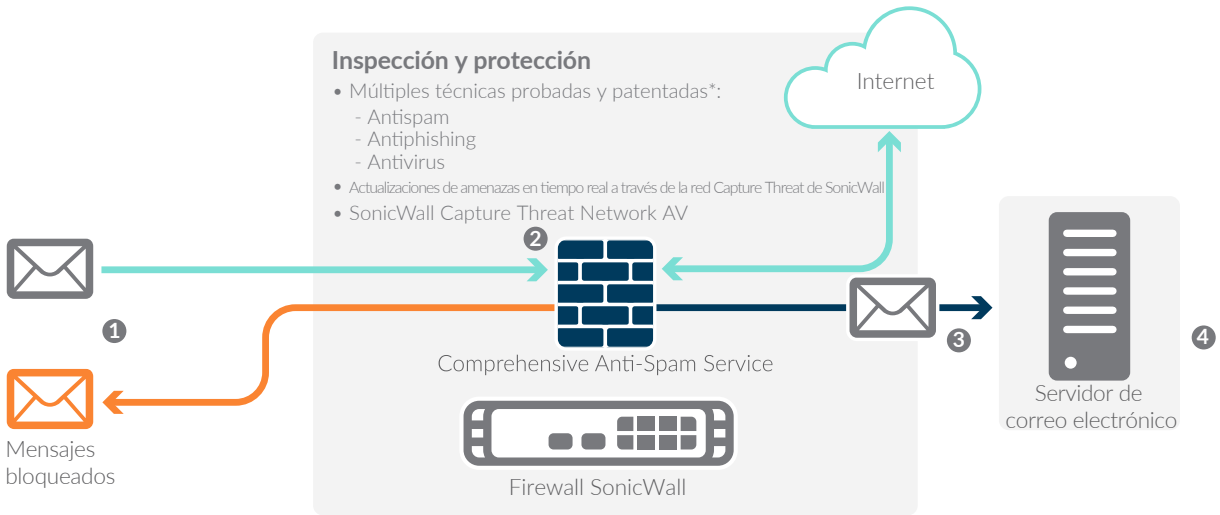
- Todos los firewalls de las series SonicWall TZ y Network Security appliance (NSa)* con SonicOS 5.6.3 o superior
- No se soportan las plataformas y/o versiones de SonicOS que no figuran aquí

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 2008 o Windows Server 2012.

Funcionamiento de SonicWall Comprehensive Anti-Spam Service



1 El tráfico SMTP llega al firewall de SonicWall.

2 Comprehensive Anti-Spam Service comprueba la reputación del servidor IP remitente en tiempo real. SonicWall Capture Threat Network 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 firewall. El resto del correo electrónico se procesa utilizando la red SonicWall Capture Threat Network basada en la nube, que aplica las técnicas probadas de detección de spam de SonicWall.

3 El correo legítimo se entrega al servidor de correo electrónico.

4 Opcionalmente, el correo no deseado puede depositarse en las bandejas de correo basura de SonicWall en el servidor de correo electrónico, pudiéndose enviar a cada usuario un informe de correo basura en forma de mensajes de correo electrónico.

Comprehensive Anti-Spam Service

01-SSC-0682 Serie SOHO (1 año)

01-SSC-0632 Serie TZ300 (1 año)

01-SSC-0561 Serie TZ400 (1 año)

01-SSC-0482 Serie TZ500 (1 año)

01-SSC-0252 Serie TZ600 (1 año)

01-SSC-2001 NS*a* 2650 (1 año)

01-SSC-4030 NS*a* 3650 (1 año)

01-SSC-4062 NS*a* 4650 (1 año)

01-SSC-4068 NS*a* 5650 (1 año)

01-SSC-9131 NS*a* 6600 (1 año)

** Excluidos NSa 9250-9650*

Hay disponibles números SKU de varios años. Visítenos en www.sonicwall.com

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

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.

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

DataSheet-CompAntiSpamService-US-VG-MKTG4092