

PROPUESTAS

MailSecure CCOTTA Appliance de Optenet: gestión eficaz y precisa del spam en la empresa

MailSecure CCOTTA Appliance de Optenet es una solución rápida, efectiva y robusta contra el spam en organizaciones que manejan diferentes volúmenes de tráfico email para la gestión de sus comunicaciones. Rápida, por su algoritmo inteligente que coordina y ejecuta acciones precisas de seguridad en tiempo real; efectiva, por la interacción de múltiples técnicas de análisis que detectan, clasifican y tratan el correo basura y las amenazas ligadas a él (spyware, virus, phishing y código malicioso); y robusta, por su sistema de compensación de colas de tráfico, que multiplica el rendimiento de la herramienta, evitando saturaciones en la infraestructura del correo electrónico.

Máxima precisión en tiempo real

Debido a la naturaleza de misión crítica del correo-e en la empresa, mantener una baja tasa de falsos positivos es uno de los factores más importantes a la hora de seleccionar una solución anti-spam. Optenet MailSecure CCOTTA Appliance es una herramienta anti-spam de alto rendimiento que gestiona con eficacia el correo basura y evita la eliminación de correo útil por error en las organizaciones. El cerebro de la plataforma es el Optenet Intelligent Greylisting Algorithm, un algoritmo inteligente que ejecuta acciones precisas de seguridad contra amenazas de correo, a partir del contraste de los resultados de múltiples métodos de análisis que interactúan de forma complementaria en la detección de spam. Ello dota a la solución de una rapidez inigualable, ya que es capaz de discernir en tiempo real qué tratamiento es el más adecuado para cada mensaje.

Análisis inteligente para la detección de spam

La efectividad en el proceso de detección, clasificación y tratamiento de spam de MailSecure CCOTTA Appliance de Optenet viene dada por la combinación de una serie de técnicas de análisis inteligentes que interactúan entre sí agrupadas en dos frentes:

1ª línea de defensa: análisis del tráfico email. La primera línea de defensa analiza el tráfico e-mail a partir de filtros basados en reputación (histórica, contextual y externa) que calculan la probabilidad de que un mensaje que proviene de una determinada dirección IP sea spam. Dichos filtros pueden bloquear gran cantidad de correo basura, incluso antes de que éste entre en la red interna de la compañía, ahorrando así un valioso ancho de banda a la organización. Asimismo, la solución utiliza métodos de contraste de remitentes con comportamiento de spammers; de verificación de remitentes a través de Sender Policy Framework (SPF), y de comprobación de orígenes sospechosos a partir de consultas DNSBL. Dichas técnicas verifican el correo entrante y reaccionan en función de las características de su comportamiento. Si el origen del correo es dañino se bloquea, y si es benigno pasa a la siguiente línea de defensa.

2ª línea de defensa: análisis del contenido del mensaje. La segunda línea de defensa estudia toda la información y los atributos que contiene el correo desde el punto de vista semántico: el cuerpo del mensaje, los hipervínculos que incluye, el destino y los contenidos de los hipervínculos, el contenido de los archivos adjuntos... y lo complementa con tecnología de anti-virus de Kaspersky Labs y de comprobación de firmas digitales como DKIM, promovida en la actualidad por empresas tan populares como Google, Ebay o PayPal. Al examinar todo el contexto del mensaje, Optenet MailSecure identifica con gran precisión los correos basura sin bloquear mensajes legítimos.

Alto rendimiento ante picos de transmisiones

El rendimiento es importante para la mayoría de los clientes ya que determina el número de sistemas que deben utilizarse para manejar el volumen de correo-e de una organización. Cuanto mayor sea el desempeño del motor de búsqueda de una herramienta anti-spam, menor será el número de sistemas requeridos para manejar el volumen de correo-e actual y sus incrementos futuros. Esto significa que cualquier incremento en el rendimiento del motor de búsqueda anti-spam se

traducirá en un incremento en el rendimiento general del sistema. Optenet MailSecure CCOTTA Appliance incorpora una arquitectura optimizada para compensar las colas de tráfico y evitar que la infraestructura se sature, incluso durante los más feroces ataques masivos de virus o spam, todo mientras se ahorra dinero en hardware, espacio, energía y tiempo de administración. Dicha arquitectura permite tratar hasta 65.000 conexiones TCP simultáneas, manteniendo un flujo constante y limitado de conexiones hacia el servidor de correo. De esta manera el sistema es capaz de actuar de amortiguador entre Internet y la red privada ante picos de transmisiones.

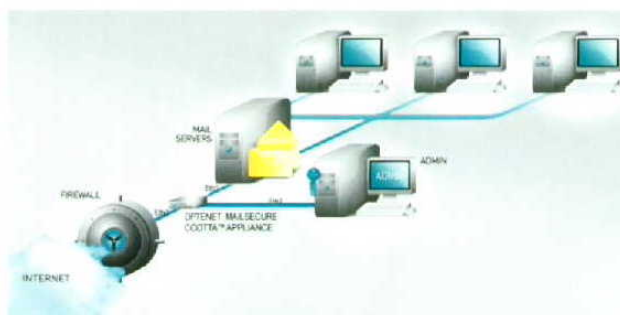
Gestión centralizada via web

Optenet MailSecure CCOTTA Appliance posee una potente consola centralizada via web que permite fijar de forma sencilla, intuitiva y flexible, políticas de filtrado ilimitadas, ajustadas a las necesidades de cada empresa. Desde ella, el administrador puede determinar valores de configuración básicos que afectan al servicio de anti-spam, pero también ofrece lo necesario para tener un control completo sobre su funcionamiento (la posibilidad de establecer límites máximos de tamaño de correo, número de mensajes por sesión, etcétera).

La solución viene configurada por defecto de forma optimizada para maximizar la detección de spam y reducir virtualmente a cero la tasa de falsos positivos. No obstante, existen opciones avanzadas que dejan realizar hasta los más mínimos ajustes para lograr una perfecta integración en la organización. La consola permite comprobar el estado de la solución en tiempo real y los mensajes que están siendo monitorizados por la solución, y personalizar las actualizaciones del sistema a medida del cliente. Asimismo, dispone de uno de los sistemas más rápidos de monitorización y generación de informes especializados en tiempo real que analizan el tráfico de correo dentro de la organización desde diferentes perspectivas, por usuarios o grupos de usuarios.

Facilidad de despliegue gracias a la tecnología CCOTTA

Toda la familia de productos para empresas de Optenet incorpora el Carrier Class Optenet Transparent Traffic Analyzer (CCOTTA), exclusivo de Optenet. En MailSecure CCOTTA es un módulo que administra de forma inteligente el despliegue de la solución en la infraestructura de red del cliente, ya que su comportamiento es totalmente transparente. Así, tras la instalación inicial, no es necesario cambiar la configuración de red de los dispositivos protegidos, ni las reglas de aplicaciones ya desplegadas. ■



Despliegue de MailSecure CCOTTA Appliance

El despliegue de MailSecure CCOTTA Appliance en la red se realiza a través de tres interfaces (eth0, eth1 y eth2).

- (1) La interfaz eth0 del appliance, en el segmento que conecta hacia Internet.
- (2) La interfaz eth1 del appliance, en el segmento que conecta con el servidor de correo.
- (3) La interfaz eth2, para administrar la solución.

Las interfaces eth0 y eth1 interceptan el tráfico entrante y saliente de la organización, aplicando de esta manera el filtrado del correo. Gracias a la Tecnología CCOTTA estas interfaces actúan en modo transparente en nivel 2 del modelo OSI, y por lo tanto no necesitan direccionamiento IP. Para los elementos interconectados el comportamiento de este appliance es igual al de un cable, sin ser necesario alterar la configuración IP de los elementos protegidos.

La interfaz eth2 se emplea para proporcionar acceso seguro a la consola de administración, pudiendo ser conectada al segmento DMZ de la organización o a una zona separada, si los administradores así lo desean.