Descripción Tecnológica

SPAMINA EMAIL FIREWALL

SPAMINA EMAIL SERVICE FIREWALL

V.3.1.1

Tecnología

SOLUCIÓN DE FIREWALL DE CORREO

Este producto propone una solución de seguridad, ofrecida en 2 modos según sus necesidades, "in house" **SPAMINA EMAIL FIREWALL** o "SaaS" **SPAMINA EMAIL SERVICE FIREWALL**, que integra las plataformas hardware más reconocidas del mercado con el software de SPAMINA, de manera que conjuntamente proporciona una forma de protección extremadamente eficaz y eficiente para las cuentas de correo electrónico de las empresas.

Nuestra solución se basa en un sistema multicapa dinámico que combina distintos filtros y mecanismos de protección. Estos filtros son continuamente analizados, monitorizados y modificados cuidadosamente para utilizar los que tienen un comportamiento óptimo en cada momento. El objetivo de SPAMINA no es otro que el de conseguir el mejor filtrado posible minimizando la pérdida de tiempo que supone el spam para administradores y usuarios. Para ello se usan tanto tecnologías propias (listas de confianza, alta por promoción,...) como tecnologías estándar (RBLs, redes de Bayes, listas blancas y negras, greylisting, traffic shaping,…). Para conseguir nuestro objetivo, colaboramos con algunos de los mejores proveedores de tecnología antispam en el mundo y su sistema de reputación de IPs, asegurando de esta manera la máxima efectividad en todo momento.

Gracias a la combinación de las mejores tecnologías del mercado SPAMINA permite disminuir la carga del servidor de correo electrónico del cliente ya que elimina el spam, virus y phishing de manera que el servidor final pueda dedicarse únicamente al correo productivo que normalmente es menor al 10% del total de correo recibido.

Accediendo través de paneles de administración con diversos perfiles disponibles, se podrán controlar y consultar la solución en conjunto o de cada uno de sus dominios por separado. Existe la posibilidad de que los usuarios finales dispongan de acceso a parte de esta configuración así como a sus respectivos buzones de correo válido y spam a través de web o de un pequeño notificador instalable en su propio ordenador. Todos estos paneles de manera segura mediante SSL.

Filtros utilizados por SPAMINA:

SPAMINA dispone de diversos métodos de filtrado que dependiendo del resultado obtenido rechazarán o marcarán el correo electrónico como spam para la posterior validación del usuario si así lo desea. Estos criterios se aplican minimizando los recursos necesarios para obtener toda la información relativa a cada prueba para su evaluación durante el filtraje en el momento más adecuado. Aquellos métodos que sea posible deshabilitar desde la interfaz web de administración se indicarán en la descripción que se muestra a continuación:

- **Listas blancas/negras**: A diferencia de otros sistemas antispam, SPAMINA puede aplicar las listas blancas / negras de IP antes que cualquier otro filtro. De esta manera se asegura que el cliente, pueda recibir correo de servidores concretos aunque estos hayan sido etiquetados como servidores de mala reputación. Existen diversos niveles de aplicación de las listas, siendo el más restrictivo el aplicado a nivel de IP por el administrador de empresa desde su panel web. En este caso cualquier IP que esté en LN o LB se rechaza o acepta (no pasando el resto de filtros de conexión).
- **Reputación de ips**: La segunda capa de filtrado es la de la reputación de IP y RBLs. En ella se comprueba la reputación del servidor origen de manera que mediante el estudio de su comportamiento, tanto histórico como actual, se puede categorizar su correo y llegar a eliminar más de un 90% del spam. No sólo se consigue reducir de manera drástica la cantidad de spam sino que se hace de la manera más eficiente posible al cerrar la conexión con el spammer incluso antes de recibir el correo. El spammer detecta que no se le acepta correo y lo tiene en cuenta en el momento de decidir los dominios menos protegidos a los que dirigirá los siguientes ataques. Para conseguir que la cantidad de falsos positivos sea prácticamente nula SPAMINA no descarta ningún correo que no esté, como mínimo, en 2 de las 6 RBLs consultadas. En el caso de coincidir en menos de 3 RBLs, se aplicará el criterio de marcado del correo como spam.

Actualmente se revisan la siguientes RBLs aunque están en constante revisión y actualización de estas listas:

- sbl.spamhaus.org
- bl.spamcop.net
- cbl.abuseat.org
- dnsbl.sorbs.net
- xbl.spamhaus.org
- dnsbl.njabl.org

- **Greylisting**: Los correos se categorizan según la probabilidad de que sean válidos. Cuando la puntuación que reciben no permite asegurar que los correos sean válidos, se puede aplicar la técnica del greylisting que consiste en dar un error temporal al servidor remitente. Si el servidor está mandando spam, normalmente no reintentará, mientras que si el correo es válido, el servidor tiene la obligación (si está bien configurado) de reintentar el envío al cabo de cierto tiempo. Es una prueba iniciales que se aplica por defecto durante el filtraje.

- **Listas blancas/negras por dominio o dirección de correo**: Tanto el administrador de empresa, el de un dominio o el propio usuario desde el panel web de control de cada uno, pueden introducir direcciones y dominios conocidos para asegurarse que no serán filtrados creando falsos positivos

- **Listas de confianza:** Las listas de confianza se forman de manera automática con las direcciones válidas de correos que asiduamente recibe cada usuario. Esta lista es personal y se genera de forma automática, siguiendo un algoritmo propio de SPAMINA que asegura la confiabilidad de las cuentas. Gracias a las listas de confianza se evitan falsos positivos sin que el usuario tenga que intervenir en ningún momento. Desde el panel de administración se podrán consultar y eliminar las direcciones de correo que se hayan incluido a nivel de dominio y de cada usuario.

- **SPF**: Usando Sender Policy Framework, se consigue asegurar que los servidores desde los que SPAMINA recibe el correo están autorizados para mandar correo de unos dominios determinados. Con esta técnica que se aplica por defecto a todos los correos, se evita el email spoofing, es decir, la suplantación de identidad. Para poder usar SPF, éste debe estar correctamente configurado en los servidores de origen. En este caso, si están definidos los registros en el DNS emisor y la ip a comprar no existe, se rechaza el correo.

- **Validación de dominio remitente (SenderDomval)**: Se comprueba la existencia de registros MX en los dominios emisores para garantizar la entrega de correo, si no existe no podrá recibir correo y por lo tanto tampoco debe poder enviar. Esta prueba eliminar el spam que se envía desde dominios inexistentes.

- **Validación de remitente (Sendercallout)**: Se comprueba la existencia del remitente para eliminar el spam que se envía desde cuentas inexistentes.

- **Delay**: Los correos se categorizan según la probabilidad de que sean válidos. Cuando la puntuación que reciben no permite asegurar que los correos sean válidos, se puede aplicar un cierto retardo en la conexión que penaliza el servidor remitente. Si es un servidor de spam no le interesará perder tiempo y cortará la conexión para intentarlo con otros servidores.

- **Antivirus**: El análisis de virus se aplica a la totalidad de los correos que entran en el sistema, independientemente de si se considera como válido o spam. Actualmente SPAMINA aplica

ClamAV como antivirus por defecto pero es posible realizar un filtrado multicapa con otros antivirus si así se solicita durante la instalación al servicio técnico. El antivirus se actualiza constantemente de manera automática. Existe la posibilidad de desactivar el filtrado antivirus desde la interfaz web de administración para todos los dominios o para algunos de ellos.

- **SPAMINA Footprinting**: Detecta si un mensaje es enviado por SPAMINA mediante el uso de una firma especial que se agrega dentro del correo electrónico.

Una vez el correo ha sido validado por los filtros de conexión y ha sido filtrado por el antivirus, el correo pasa a un módulo independiente que dependerá de la opción escogida previamente por el administrador o el usuario desde la administración.

Módulo de Filtrado Automático

Se usa tecnología basada en sistemas OpenSource (SpamAssassin y Bogofilter) que usan desde filtros bayesianos hasta pruebas basadas en DNS o consultas en Bases de Datos externas. Se utilizan más de 600 reglas para asegurar la máxima eficacia.

Las reglas y pruebas de estos dos sistemas se ajustan constantemente para conseguir un rendimiento óptimo según el tipo de spam, de manera que se adapta a las necesidades del usuario, maximizando la eficiencia del sistema antispam y evitando los falsos positivos, sin necesidad de que el usuario intervenga en la mejora del mismo.

- **Content Filter**: Se permite personalizar el filtrado al administrador y a los usuarios individuales la posibilidad de crear sus propios filtros. Estos filtros pueden crearse por empresa o usuario y funcionan analizando las palabras del correo y actuando según la configuración correspondiente desde la interfaz web.

- **Bogofilter y SpamAssassin**: Dos de los módulos que se usan en SPAMINA son Bogofilter y SpamAssassin.

  Éstos se basan en distintas técnicas antispam que van desde los filtros bayesianos hasta pruebas basadas en DNS o consultas en Bases de Datos. Las reglas y pruebas incluidas en estos dos sistemas se ajustan constantemente para conseguir un rendimiento óptimo según el tipo de spam. Dependiendo de la puntuación obtenida al ejecutar ambos algoritmos sobre cada correo, este será rechazado si se determina con un grado muy alto de certeza que el correo es spam. El correo será únicamente marcado como spam si cumple con un umbral configurable por el propio usuario desde su interfaz de administración (por defecto será un umbral alto). La aplicación de estas pruebas, puede ser deshabilitada por el administrador a nivel general o por dominios desde la interfaz web de administración.

  - Algunas de las pruebas que se realizan son:

    - **Inspección de "Headers"**: Los "Headers" o cabeceras de mensaje contienen información importante acerca del mismo .

    - **Análisis del Mensaje**: El cuerpo y titulo del mensaje son leídos por SpamAssassin, realizando búsquedas por palabras claves o estructuras que conforman un correo spam.

    - **Análisis probabilísticos / bayesianos**: Una vez definidas las reglas iniciales para la detección, se realizan análisis probabilísticos para determinar similitudes entre mensajes entrantes y aquellos ya detectados como SPAM anteriormente.

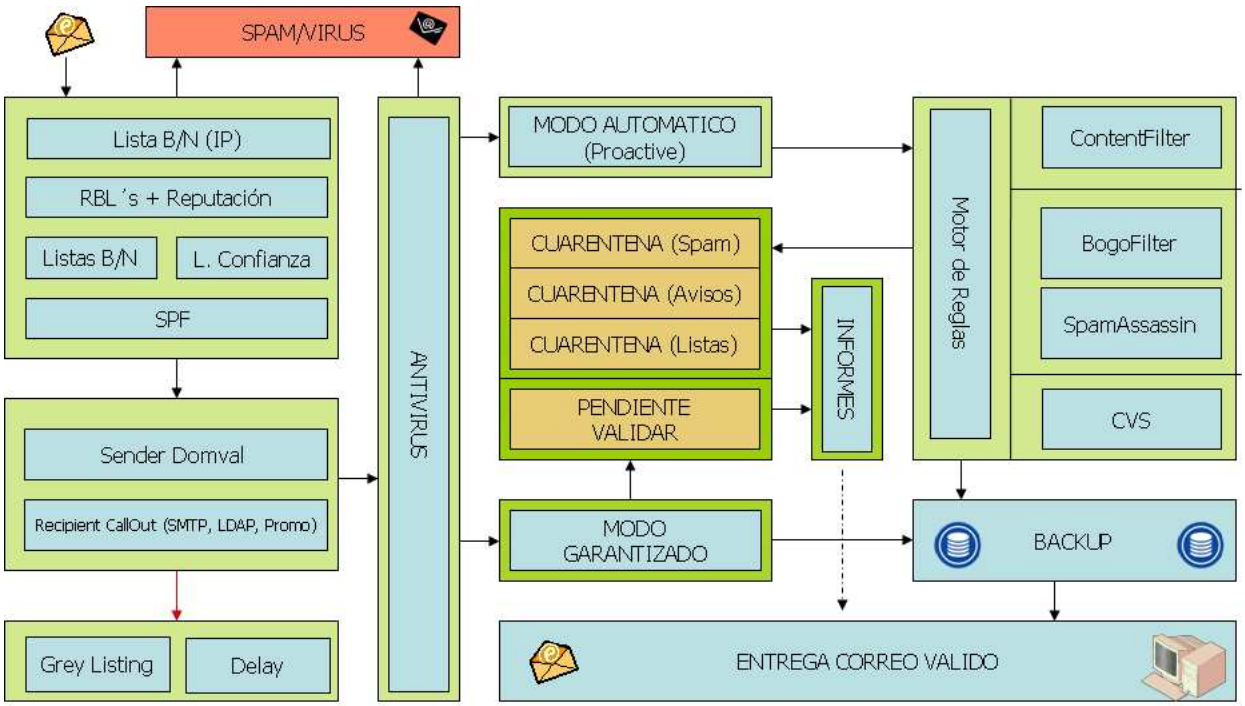
- **Listas "Hash" / Firmas de Correo**: Debido a que un correo SPAM suele ser enviado a miles de personas a la vez, la estructura de cada mensaje es idéntica en todas sus instancias, así produciendo un "Hash" inequívoco. SpamAssasisn consulta listas de "Hashes" sobre mensajes conocidos.

Módulo de filtrado Garantizado

Se verifica la existencia del remitente en la lista blanca del receptor, entregándose el correo inmediatamente si la verificación es positiva. En caso contrario se envía un correo al remitente explicando que se está usando un servicio antispam y que para verificar el remitente debe hacer clic en un link. Una vez el remitente se ha validado el correo se entrega al destinatario así como todos los futuros correos del mismo remitente.

En caso que el remitente no se valide se permite al destinatario validarlo manualmente para evitar la pérdida de cualquier correo. SPAMINA sigue las recomendaciones de la RFC 3834 a fin de evitar la generación del Spam Colateral.

Arquitectura de filtrado



OTRAS FUNCIONALIDADES

Filtrado saliente

SPAMINA permite filtrar en modo in house, no sólo el correo entrante sino también el saliente mediante filtros de contenido y antivirus. Se incluye la posibilidad de configurar a través de la interfaz de administración web por usuario, dominio o empresa, un número máximo de destinatarios a partir del cual no se permitirá le envío de correo.

Alta disponibilidad

Ofrecemos una solución de alta disponibilidad basada en clúster de nodos en modo activo-activo. Éste sistema, a diferencia de otros fabricantes, nos permite, no sólo soportar **puntas de tráfico de prácticamente el doble** que un servidor standalone sino que además **no se pierde información alguna en caso de caída de uno de los nodos**. La información se replica en tiempo real entre como mínimo dos nodos, teniendo también la posibilidad de usar almacenamiento externo. Además esta propuesta aporta otra diferencia importante que es el **balanceo de carga interno** con lo que el balanceo de carga es real y no necesita de HW externo. Tampoco es necesario tener un servidor dedicado al control del clúster con lo que el coste se limita al HW que realmente se usa.

Email continuity

En caso de caída del servidor de correo final, SPAMINA seguirá recibiendo el correo externo y almacenándolo para entregarlo en cuanto el servidor del cliente se recupere. De esta manera en caso de caída no se rechaza ningún correo y los usuarios, a través de webmail o del panel de control, pueden acceder y trabajar con el correo hasta que su servidor se recupere.

Modos de modo de alta

Existen 4 modos distintos de alta de usuarios para dar la mayor flexibilidad posible al cliente.

- **Alta Manual**: El administrador es el encargado de dar de alta cada una de las cuentas de los usuarios manualmente. Esta opción se recomienda únicamente en el caso de querer añadir un número reducido de usuarios.
- **Alta Automática por SMTP call out o LDAP**: SPAMINA permite dar de alta los usuarios de forma automática a medida que empiecen a recibir correo. Para ello comprueba que las direcciones de correo de los destinatarios existan en el servidor final. Estas comprobaciones se pueden realizar directamente contra el servidor SMTP o contra un servidor LDAP corporativo (compatible con OpenLDAP, Active Directory y Domino), creando el usuario en SPAMINA si éste existe o rechazando el correo si no existe. Este modo de alta también permite trabajar en varias de las opciones de configuración del panel de administración a nivel de grupos definidos en cada LDAP.
- **Alta por promoción**: El Modo de Alta por Promoción es un mecanismo diseñado por SPAMINA para el modo “in house” que permite al usuario final decidir si desea proteger su cuenta de correo electrónico. El mecanismo de promoción se activa cuando llega un correo electrónico para un usuario no dado de alta pero perteneciente a un dominio protegido por SPAMINA. En ese momento se entrega al destinatario el correo recibido y paralelamente se envía una invitación para que el usuario final decida si quiere ser protegido contra el Spam.

  El usuario puede escoger las siguientes opciones cuando reciba la invitación:

  - Activar: se protege la cuenta de correo contra spam, virus y phishing.

- Rechazar: la cuenta se da de alta como usuario con filtrado básico (filtros por conexión) y no tendrá cuarentena, ni filtros por contenido.

Acceso al contenido del correo

SPAMINA permite al administrador del modo “in house” poder acceder al contenido de todos los correos que pasen por el sistema de filtrado desde la interfaz de administración web mediante logs de correo. Esta opción es configurada por los técnicos de SPAMINA de manera que en caso de renunciar a ella es imposible que el administrador tenga acceso al correo de los usuarios. Estos logs son accesibles en el modo SaaS desde el sistema si así es requerido por el cliente.

Colas de entrega y almacenamiento independientes

SPAMINA trabaja con dos colas que permiten entregar y guardar el correo de manera totalmente independiente. De esta manera, si existiera un inconveniente en el almacenamiento de SPAMINA, este no afectará a la entrega del correo del servidor del cliente, y viceversa, ofreciendo de esta manera dos caminos para que el usuario tenga acceso a sus correos.

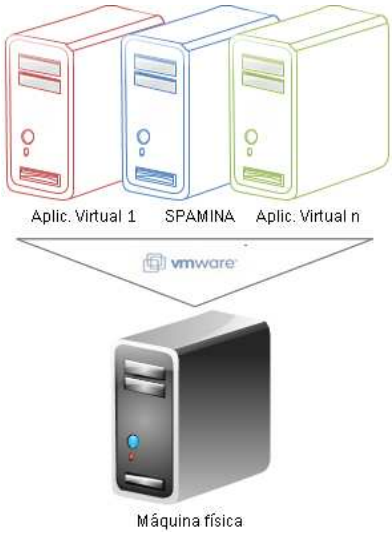
INTEGRACIÓN y ADAPTACIÓN TOTAL

SPAMINA, tanto en modo SaaS como en modo “in house”, es independiente del servidor de correo usado por nuestros clientes pudiendo acceder a su correo filtrado tanto desde los tradicionales clientes de correo como MS Outlook® como desde Blackberry®.

Existen diferentes posibilidades que serán evaluadas durante el estudio previo a la instalación del producto ajustándose a las necesidades de cada cliente. Desde instalaciones standalone para cubrir las necesidades básicas de pequeñas empresas hasta instalaciones multicapa virtuales en varios servidores (físicos o no) combinados con nuestros clusters, se ofrecen una amplia gama de posibilidades para cada tipo de cliente y cada nivel de seguridad, escalado y alta disponibilidad. Siempre contando con el apoyo de hardware homologado por los principales fabricantes (HP, IBM, SUN y VISA).

Tecnología

VIRTUALIZACIÓN



VMware consiste en un sistema virtual por software, es decir, un programa que simula un sistema físico (un ordenador, un hardware) con las características de un hardware determinado. Cuando se ejecuta el programa (ej. SPAMINA EMAIL FIREWALL), proporciona un ambiente de ejecución similar a todos los efectos a un ordenador físico.

Nuestra experiencia y colaboración con VMware, nos permite ofrecer nuestra solución modo “in house” sobre plataformas virtualizadas proporcionando los beneficios de ambos productos a nuestros clientes. El principal de estos beneficios es la reducción de costes proporcionando la flexibilidad, robustez y portabilidad de este pool de recursos lógicos.

Mientras que en los sistemas tradicionales, es necesario focalizar los esfuerzos por separado, en este nuevo enfoque, el administrador podrá realizar una administración centralizada (mantenimiento, back-up o planes de contingencia) de los recursos separando el sistema operativo base del dedicado a nuestro producto u otras aplicaciones que pueden ejecutarse simultáneamente. Además, un fallo o detención en cualquiera de las ejecuciones virtuales no afecta a las demás, de forma que su ejecución es totalmente segura.

La monitorización será de un único sistema físico asignando la carga y configuración necesaria a cada máquina virtual de forma dinámica sin penalizaciones de coste. Hay que tener en cuenta que la escalabilidad de esta arquitectura permite fácilmente ampliar los recursos dedicados sin necesidad de cambios en hardware.