MINISTERIO DE RELACIONES EXTERIORES

INFORME DE EVALUACIÓN DE SOFTWARE DGG Nº 011-2008

"Licenciamiento de Filtros de Contenido y Antispam"

1. Nombre del Área

El área encargada de la evaluación técnica para la renovación de licencias de software de filtro antispam y de contenido para correo electrónico y filtro de contenido web por Internet es el Departamento de Comunicaciones de la Dirección General de Gestión Informática (DGG).

2. Nombre y Cargo del Responsable de la Evaluación

Jorge Armas Orbegozo, Jefe del Departamento de Comunicaciones

3. Fecha

30 de Setiembre del 2008

4. Justificación

Los Funcionarios del Ministerio de Relaciones Exteriores utilizan el correo electrónico para realizar las siguientes funciones:

- Intercambio de mensajería electrónica entre Cancillería y sus misiones en el exterior, como lo son las embajadas, consulados, representaciones y oficinas descentralizadas
- Intercambio de mensajería electrónica entre Cancillería y las misiones de otros países
- Intercambio de mensajería electrónica entre Cancillería y organismos internacionales
- Otras mensajerías electrónicas necesarias para cumplir sus objetivos institucionales

Además utilizan la navegación en web para consultar información publicada en la Internet sobre ámbitos de su competencia, como lo son la política exterior, la gestión consular, la promoción comercial, la gestión administrativa, etc.

En este sentido, con la finalidad de reforzar la seguridad perimetral de la red y reducir los problemas ocasionados por las amenazas existentes, la Cancillería cuenta en la actualidad con sistemas de filtro antispam y contenido de correo electrónico (sistema antispam) y sistemas de filtrado de contenido Web.

Las soluciones implementadas por la Cancillería son los productos Surfcontrol webfilter y Surfcontrol e-mail filter. Dichos productos aseguran la privacidad de la información y la continuidad de los servicios de correo electrónico, Internet y de los servidores de la Cancillería, minimizando la vulnerabilidad de los sistemas y de la información contenida en ellos.

JORGE ARMAS ORBEGOZO
Jefe de Comunicaciones

Dirección General de Gestión Informática

Por motivo del vencimiento de las licencias adquiridas y debido a que los productos Surfcontrol quedarán sin vigencia en el mercado esto a razón que la empresa fue adquirida por la empresa Websense a inicios del presente año, se hace necesario adquirir productos con características similares o superiores, a fin de que los servicios de seguridad implementados no sean interrumpidos.

5. Alternativas

Para la formulación y análisis de alternativas, se debe considerar que al haber sido comprada la empresa Surfcontrol por Websense, los productos Surfcontrol quedaran descontinuados del mercado, y ya que la empresa Websense tiene costos de renovación equivalentes al 100% del costo de venta sólo se tiene una única alternativa que es la de adquirir una nueva solución de filtros de contenido.

Los productos analizados son los siguientes

Filtro antispam y de contenido de correo electrónico:

- Websense E-mail Security
- Ironport E-Mail security

Filtro de contenido web

- Websense Web Filter
- Ironport Web Security

En el mercado existen soluciones para filtros de contenido del tipo Network Appliance y del tipo software.

Las soluciones de software requieren de un servidor adicional y de licencias de sistema operativo lo cual puede incrementar los costos de propiedad (TCO) en aproximadamente unos $8000 por filtro como costo escondido.

Actualmente las soluciones del tipo Network Appliance han tomado mayor aceptación por ser soluciones que incluyen el equipo y licencias del sistema operativo especializado todo en el mismo equipo y por el mismo costo, teniendo un menor costo de TCO.

Se han establecido las especificaciones técnicas que servirán para la posterior evaluación de las propuestas, razón por la cual no se realizará en el presente informe una comparación de productos de filtro de contenido disponibles en el mercado.

6. Análisis Comparativo Técnico

Las especificaciones técnicas son las siguientes:

CARACTERÍSTICAS TÉCNICAS FILTRO DE CONTENIDO WEB

- Ejecución en appliance (hardware y software de propósito específico), el cual será incluido con la solución.
- Interfase de usuario multilenguaje, incluyendo los idiomas inglés y español.
- Debe permitir desplegarse de dos maneras:
  - Solución independientemente.
  - Solución integrada con otros sistemas proxy
- Debe limitar los sitios de Internet que los usuarios pueden visitar basado en Url's categorizados contenidos en la base datos de la aplicación.
- Debe contar por lo menos con 50 categorías (pornografía, violencia, racismo, religión, etc) y soportar categorización multilenguaje de Internet.
- Appliance para la seguridad de navegación web que opere como Proxy Caché y URL Filter.
- Inspección profunda de contenido de las aplicaciones y monitor de tráfico Layer 4.
- Aplicación Proxy con capacidad de monitor de tráfico L4.
- Capacidad de administrar y hacer reportes con varios modos de despliegue
- Reportes robustos en tiempo real e históricos.
- Interface Gráfica de fácil uso.
- Políticas flexibles que permitan a los administradores permitir o bloquear basado en la fuente o destino, añadir URLs, dominios, direcciones IP específicas o CIDRs.
- Autenticación integrada a través de los directorios tales como LDAP o Active Directory y capacidad de ejecutar múltiples esquemas de autenticación como NTLM o Básica.
- Debe contar con una consola o monitor en tiempo real que registre el tráfico de navegación de los usuarios. Esta consola debe incluir información tipo usuario conectado, la página web visitada y categoría a la que pertenece en la aplicación, tiempo de conexión, dirección IP del host remoto.
- Debe proveer herramientas para respaldar y restaurar la configuración de la aplicación.
- Debe incluir opciones para automatizar el mantenimiento del sistema como por ejemplo purgar o compactar la base de datos.
- Debe efectuar actualizaciones automatizadas diarias de los componentes de la solución.
- Debe soportar administración remota basada en Web o en Consola.
- Soporte de SYSLOG

JORGE ARMANDO ORTEGOZO
Jefe de Comunicaciones

CARACTERÍSTICAS TÉCNICAS FILTRO DE CONTENIDO SMTP

- El equipo deberá estar licenciado para 300 usuarios y deberá poder escalar hasta 1,500 usuarios de correo electrónico
- Ejecución en appliance (hardware y software de propósito específico), el cual será incluido con la solución.
- Interfase de usuario multilenguaje, incluyendo los idiomas inglés y español.
- Protección contra correo no deseado y no solicitado (Sistema antispam).
- Protección contra phishing (estafas electrónicas) y contra spyware (software espía).
- Generación de listas blancas y negras según políticas establecidas por el administrador.
- Enrutamiento del spam según niveles, de manera selectiva, de acuerdo a calificación (puntuación del correo no deseado).
- Bloqueo de spammers conocidos por dominio o dirección IP.
- Separación de políticas de filtrado de contenido del tráfico entrante y saliente.
- Realizar excepciones a las reglas de filtrado para usuarios determinados.
- Bloqueo de archivos adjuntos de acuerdo al asunto del mensaje (subject), texto del mensaje, extensión nombre de archivo y al usuario de destino.
- Funcionamiento en modo antirelay.
- Integración con LDAP con Microsoft Active Directory y Lotus Notes
- Soporte para enmascaramiento de dominio por LDAP en el correo saliente.
- Tecnología de Gateway Virtual para configurar más de una dirección IP sobre una interfase ethernet para el envío o recepción de correos electrónicos
- Sistema de filtrado antispam RBL.
- Servicio de base de datos de filtrado por reputación
- Contar con una cuarentena a la que se puedan dirigir los correos electrónicos dudosos, para su futura revisión.
- Período de almacenamiento en cuarentena configurable.
- Envío de un correo electrónico con resumen del contenido de las casillas de correo individuales para cuarentena a todos los usuarios finales, con mensajes en cuarentena, y al administrador del sistema. El envío será automático y en forma diaria.
- Proporcionar acceso vía Web a los usuarios hacia sus respectivas casillas de cuarentena.
- Herramienta de monitoreo incorporada.
- Administración centralizada e integral del sistema, permitiendo al administrador configurar y ejecutar políticas, y monitorear la efectividad de la protección de filtrado. Dichas políticas comprenderán reglas para usuarios individuales o para grupos de usuarios.
- Incluir una interfase administrativa vía Web.
- Consola de administración accesible remotamente y con validación mediante usuario y contraseña.
- Generación de registros e informes multinivel y de auditoria, en forma gráfico y en modo detallado.
- Generar informes y reportes configurables y personalizables (incluyendo destinatarios de correo no deseado más frecuentes, emisores de correo no deseados más frecuentes, entre otros) en tiempo real.
- Los reportes deberán ser exportables a distintos formatos (HTML, PDF, CSV, texto, etc.)

- Notificación de eventos vía SNMP y SMTP.
- Archivado y limpieza de datos históricos de las bases de datos, durante horas de reducida actividad (de modo programable).
- Funcionamiento con múltiples servidores de correo electrónico y múltiples dominios.
- Soporte de los protocolos de correo electrónico SMTP y ESMTP.
- Configuración a través de puerto de administración por consola.
- Incluir actualizaciones periódicas o inmediatas, de nuevas reglas y algoritmos de correo no deseado.
- Distribución diaria de las actualizaciones, incluyendo la actualización gratuita, continua y automática contra firmas de ataques.
- El fabricante proveerá actualizaciones en modo online, sin requerir corte reinicio o apagado del sistema.
- Soportar el manejo de colas de envío y recepción de correo en paralelo (por destino), por dominio o dirección IP.
- Soportar manejo de máximas conexiones concurrentes desde una sola IP configurable por dominio o IP origen.
- Soportar manejo de máximos mensajes por conexión configurable por dominio o IP origen.
- Soportar manejo de límite de máximo destinatarios por mensaje configurable por dominio o IP origen.
- Soportar manejo de límite de recepción de correo (rate limit) configurable por dominio o dirección IP origen.

7. Análisis Comparativo de Costo – Beneficio

- **Costos**

Para realizar el estudio de mercado se evaluaron los siguientes productos para identificar montos referenciales

Filtro antispam y de contenido de correo electrónico:

Producto	Licencias	Costo Unitario US$	Costo Total US$	Costo Renovación unitario US$
Websense E-mail Security	300	26.6	7980	7980
Ironport E-Mail security	300	31.1	9332	6532

Filtro de contenido web

Producto	Licencias	Costo Unitario US$	Costo Total US$	Costo Renovación unitario US$
Websense Web Filter	500	35	17500	17500
Ironport Web Security	500	32.66	16331	11431

- **Beneficios**

Este tipo de productos garantizará la seguridad de la red Cancillería, asegurando la continuidad de las labores cotidianas del Ministerio de Relaciones Exteriores.

- **Hardware Necesario**

El Ministerio de Relaciones Exteriores cuenta con el hardware necesario para implantar el producto

8. Conclusiones

Las conclusiones del presente informe son las siguientes:

- Debido a la caducidad de la licencia de los productos de filtro de contenido que tiene la Cancillería y debido a que los productos Surfcontrol serían descontinuados por su actual dueño Websense se hace necesario adquirir una nueva solución de productos de filtros de contenido
- Ya que en la actualidad se utiliza una solución por software que utiliza 3 servidores para su operación; escoger una nueva solución de software significaría disponer de la misma cantidad de equipos adicionales para poder hacer una migración sin necesidad de parar las operaciones.
- En este sentido, se recomienda adquirir una solución de filtros de contenido del tipo Network Appliance que facilite la migración del actual sistema al nuevo sistema además de disminuir los costos de propiedad al no requerir ni servidores ni sistemas operativos adicionales manteniendo los niveles de seguridad con los que actualmente se cuentan además de liberar 3 servidores para que puedan ser utilizados por otros servicios.

JORGE ARMAS ORBEGOZO
Jefe del Departamento de Comunicaciones

Dirección General de Gestión Informática