INFORME N°052-14-GG/ODIS-OSITRAN

A	:	**JESUS LEÓN LAMAS** Jefe de la Oficinas de Desarrollo Institucional y Sistemas
DE	:	**EVERTH GOMEZ BACILIO** Analista de Redes y Telecomunicaciones.
ASUNTO:		INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOLUCIÓN ANTISPAM.
REFERENCIA	:	MEMORANDO N° 003-2014-GG/ODIS-OSITRAN
FECHA :		07 de Abril de 2014

I. ANTECEDENTES:

Se remite a la ODIS el 25/03/14 el documento al que se hace referencia, en el cual se solicita realizar una investigación y evaluación técnica antes de realizar las especificaciones técnicas o términos de referencia, a fin de que estos respondan a por lo menos 2 marcas.

En referencia a lo solicitado, se ha realizado la siguiente evaluación técnica con respecto a la necesidad de adquirir una solución Antispam Para OSITRAN:

1. **JUSTIFICACION:**
   El Spam hoy en día es un problema, se estima que el 70% del tráfico internacional de email es SPAM, el correo basura involucra un costo de dinero para las empresas, tanto en el tiempo que se pierde examinándolo, como por los recursos de hardware y software necesarios para manejarlo.

2. **ALTERNATIVAS DE SOLUCION:**
   Actualmente existen 2 tecnologías de solución en el mercado; ***Solución basada en Hardware y Solución Basada en Software.*** A continuación, detallo las ventajas que tenemos al elegir una Solución Basada en Hardware:

2.1 Complejidad de Instalación:

Solución basada en Hardware:

- Sistema Operativo y software de aplicación pre cargado y configurado.
- Reducción del tiempo en la Implementación y funcionamiento.
- Administración centralizada en una sola interface web.
- Conocimiento informáticos mínimos requerido por el usuario.
- Preparado para instalación en redes de producción y DMZ.

Solución basada en Software:

- Requiere conocimientos informáticos avanzados para instalar y configurar la solución.
- Puede requerir bibliotecas de terceros, una versión más reciente del sistema operativo y los Service Packs más recientes, para poner en funcionamiento.
- Requiere la instalación de un servidor y un sistema operativo, involucrando costo adicional.
- Requiere la instalación de un servidor web y un servidor de base de datos.
- Requiere la instalación del software antispam.

2.2 Administración:

Solución basada en Hardware:

- Interfaz independiente del Sistema Operativo.
- Fácil Asistentes de configuración.
- Acceso a la interface web de cuarentana Spam para los usuarios.

Solución basada en Software:

- No todas las soluciones en software tienen una interface de administración.
- Requiere interactuar con otro software.

2.3 Capacidad:

Solución basada en Hardware:

- Diseñado especialmente para funcionar en el hardware con que viene.
- Compatible con la mayoría de plataformas de software.
- Interfaz independiente del Sistema Operativo.

Solución basada en Software:

- Frecuentes problemas de operatividad entre hardware y software.
- Requiere una versión especial del software para su sistema operativo específico.

2.4 Costo de Mantenimiento:

Solución basada en Hardware:

- Las actualizaciones se aplican automáticamente sin intervención del usuario.

Solución basada en Software:

- Las actualizaciones de software pueden causar alteraciones en el sistema operativo.
- Requiere la actualización del sistema operativo servidor con los últimos parches, así como el seguimiento y la identificación de todos los parches.

2.5 Estabilidad:

Solución basada en Hardware:

- Sistema Operativo estable, garantiza menos tiempo de inactividad.
- El hardware del dispositivo se ha diseñado para el uso de la solución anti spam.
- -Alta Fiabilidad.

Solución basada en Software:

- El software de la solución no puede trabajar con los recursos necesarios, porque el hardware no se ha probado y diseñado para el software anti spam.

2.6 Performance:

Solución basada en Hardware:

- El software de dispositivo de servidor está configurado para trabajar bien con el hardware suministrado ya que se trata del mismo fabricante.

Solución basada en Hardware:

- Menos calidad y desempeño, pues el software no aprovecha el hardware suministrado al no estar diseñado para que trabajen entre sí.

3.- CARACTERISTICAS DEL EQUIPO ANTISPAM.

De acuerdo a lo evaluado anteriormente y de acuerdo a la actual infraestructura de OSITRAN, se eligieron los siguientes productos, líderes en el mercado de tecnologías Antispam.

- Cisco Ironport
- Fortimail
- Symantec Mail Security

La solución antispam a adquirir debe cumplir las siguientes características Técnicas:

- Appliance Antispam (hardware y software) de propósito específico.
- Proveer un mínimo de 10,000 conexiones concurrentes.
- Debe Soportar 250 buzones de correo electrónico, con un crecimiento mínimo de hasta 1,000 buzones.
- Sistema de cuarentena para el almacenamiento de SPAM y mensajes sospechosos con acceso desde la interface del usuario.
- El sistema de almacenamiento de espacio y por tiempo de cuarentena debe de ser configurable.
- Función de notificación por correo de manera automática a los usuarios con resumen del contenido de la casilla de correos en cuarentena.
- Sistema modular con soporte de protección antivirus.
- Integración con los sistemas LDAP y Active Directory.
- Proveer un sistema de customizacion de reglas de filtrado usando algún lenguaje de programación.
- Soporte de protocolos de correo SMTP /ESMTP sobre TLS.
- Soporte de protocolo de transferencia de archivos scp y ftp.
- Uso de algoritmos de criptografía AES y RC4.
- Capacidad de generar políticas al tráfico entrante y al tráfico saliente de forma independiente.
- Uso de tecnología Heurística para la detección del Spam.
- Capacidad para detectar el idioma del correo (7 idiomas como mínimo).
- Creación de políticas, por dominio, por usuario o por grupo.
- Notificación automática a los usuarios indicando los correos SPAM que tiene almacenado para que ellos puedan gestionar su contenido.
- Poseer una base de datos para el bloqueo de direcciones IP y de base de datos por reputación, desarrollada y mantenida por el fabricante.
- Detección preventiva del SPAM y bloqueo de mensajes a nivel de conexión TCP.
- Soporte de agregación de encabezados con mensajes propios de la entidad para notificación a los usuarios por evento que se requieran informar.
- La solución Antispam debe garantizar la confidencialidad de la información a través de las políticas implementadas por la entidad.

- Debe proveer integración con la solución de correo electrónico de la entidad (Active Directory y Microsoft Exchange 2007 y superior).
- La solución debe poseer un sistema de actualización automática con nuevas formas de ataques.
- La herramienta debe tener la capacidad de configurar clasificación y categorización remitentes permitidos, opción con la cual se pueda especificar a qué mensajes de correo no deben aplicarse la comprobación de Antispam. Estos remitentes pueden ser por redes y dominios determinados.
- Separación de políticas de filtrado de contenido del trafico entrante y saliente.
- Realizar excepciones a las reglas de filtrado para usuarios determinados.
- Bloqueo de archivos adjuntos de acuerdo al asunto del mensaje (subjet), texto del mensaje, extensión nombre de archivo y al usuario de destino.
- Posibilidad de configurar filtros con capacidad de análisis de encabezado, asunto y contenido.
- Configuración del límite de la cantidad de mensajes por sesión de SMTP.
- Configuración del límite de los attachments (Tamaño en KB o MB) a nivel de TCP.
- Debe poseer capacidad de identificación y bloqueo de SPAM en distintos idiomas.
- Capacidad de marcado de mensajes en el sujeto o encabezado y posterior envío a buzón alternativa de usuario.
- La solución debe manejar sistema agente de transporte de mensaje MTA.
- La herramienta debe de notificar al administrador de la solución sobre eventos, cuarentenas, reportes de mensajes procesados, de forma automática vía e-mail.
- Enrutamiento del spam según niveles de forma selectiva de acuerdo a puntuación de correo no deseado.
- Generación de listas blancas y negras según políticas establecidas por la organización.
- Reglas de filtrado por destino, remitente, copia carbón, encabezado de correo, cuerpo, tamaño, archivos adjuntos, contenido malicioso, bloqueo de archivos cabecera MIME.
- Opciones de configuración ANTI-RELAY.
- Múltiples opciones de respuesta: eliminar adjunto, eliminar mensajes, entrega normal, enviar a cuarentena.
- Configuración de archivos basados en estándar XML.
- Soporte para envío y recepción de correo encriptado SSL/TLS.
- Deberá poseer al menos 2 instancias de filtros configurables la primera a nivel de sesión SMTP y la restante como análisis de contenido.
- Soportar el manejo de colas de envío y recepción de correo paralelo (por destino), por dominio o dirección IP.
- Deberá soportar SPF (Sender Policy Framework Verification) and SIDF (Sender ID Framework)
- Soporte para ruteo de mensajes por dominio, tabla de alias y LDAP.
- Soporte para enmascaramiento de dominio, por LDAP en el correo saliente.
- La autenticación por LDAP se podrá aplicar durante la conversación SMTP o durante el procesamiento de los mensajes.
- Soporte para configurar más de una IP, mínimo 4 en el mismo equipo, para el envío/recepción de correo.

- Incluir actualizaciones periódicas o inmediatas, de nuevas reglas y algoritmos de correo no deseado.
- El fabricante proveerá actualizaciones en modo online, sin requerir corte reinicio o apagado del sistema.

ADMINISTRACION

- Debe poseer una interfaz de administración vía browser sobre protocolo HTTPS.
- Sistema de reporte exportable a HTML, PDF, CSV y por tareas automáticas programables en fechas y horas por periodos diarios, semanales, mensuales, etc.
- Proveer un sistema de reportes estadísticos por virus, SPAM, ataques, IP origen, IP destino, IP destino. Dominio de redes detallando los propietarios de las redes.
- Debe poseer un sistema seguimiento de mensajes (messages Traking) desde la misma consola web de administración.
- Factibilidad de generación de solicitudes de soporte con el fabricante desde la consola de administración.
- Debe permitir la creación de múltiples usuarios administradores con distintos niveles de permiso de acceso.
- Soporte de backup y restore de toda la configuración realizada.
- Soporte el monitoreo por SNMP v1, v2c, V3, y MIB-II.
- Reporte automático de alertas y/o alarmas a través de correo electrónico.

FUNCIONALIDADES DEL MODULO ANTIVIRUS

- Debe proveer una solución antivirus embebida en el sistema sin instalar software o hardware adicionales.
- Debe soportar al menos dos (02) motores de antivirus embebidos en el sistema para análisis y detección de virus y licenciado al menos uno de los motores.
- Debe detectar virus, malware y otros tipos de software indeseados por medio de secuencia de códigos específicos que se encuentran en los virus.
- Debe tener análisis heurístico para garantizar que se detengan las variantes de virus con la mínima información disponible sobre los patrones de los códigos del virus.
- Facultad de manejo de múltiples opciones para el manejo de mensajes en caso estén infectados, encriptadas no pudieron ser escaneados.
- Debe contar con un sistema de cuarentena.
- Debe permitir colocar etiquetas a los mensajes infectados, limpiados, encriptadas y los que no se han podido escanear.

SOBRE EL APPLIANCE

- 500 GB mínimo de disco con tecnología SATA (2*250) RAID 1, software.
- 2 puertos Ethernet 10/100/1000 tx.
- 1 Puerto Serial RS232, para la consola de administración local.
- Memoria mínima de 4 GB.

SERVICIOS

- Instalación y configuración del equipo en la sede de OSITRAN.
- Taller de Capacitación para 3 personas, 03 (tres) sesiones de 04 (cuatro) horas cada una.

4.- CONCLUSIONES:

Las conclusiones de la evaluación realizada son las siguientes:

- OSITRAN obtendrá mayor calidad en el nivel de servicios de red al reducir el ancho de banda.
- El servicio de correo es crítico y de alta importancia para las labores diarias de los usuarios, por lo que se requiere contar con una solución Antispam, acorde con las tecnologías y amenazas actuales existentes, que asegure a su vez el correcto funcionamiento del sistema de correo de OSITRAN.
- Por las razones expuestas anteriormente, se recomienda adquirir e implementar las soluciones propuestas a fin de mejorar el nivel de seguridad de información de OSITRAN.
- En ese sentido, adjunto los Términos de Referencia para su revisión y aprobación.

Atentamente,

OSITRAN V°B° EVERTH GOMEZ

Everth Gómez Bacilo
Analista de Redes y Telecomunicaciones

Reg. Sal GG/ ODIS N° 12212- 2014