SOLICITUD PRIVADA DE OFERTAS 2015-142

"ADQUISICIÓN DE HARDWARE Y SOFTWARE PARA LA PERSONERÍA DE MEDELLÍN"

ADENDA 3

Mediante la presente Adenda se modifica el siguiente aspecto:

ANEXO 3. ESPECIFICACIONES TÉCNICAS FORTIGATE

ITEM 1. HARWARE Y SOFWARE (UTM) PARA LA PROTECCION DE LA RED:

ITEM 1.1 CARACTERÍSTICAS TÉCNICAS DEL DISPOSITIVO

DENOMINACIÓN TÉCNICA DEL BIEN	**CARACTERÍSTICAS TÉCNICAS DEL DISPOSITIVO**
CARACTERÍSTICAS TECNICAS DEL DISPOSITIVO	
ESPECIFICACIONES TÉCNICAS	**CARACTERÍSTICAS MÍNIMAS EXIGIDAS**
Descripción	
Número de Interfaces Requeridas	42 10/100/1000 (RJ-45) 2 GE SFP DMZ Interfaces
Throughput de Firewall	4 Gbps para paquetes UDP de 1518/512/64 bytes
Throughput de VPN IPSec	1,3 Gbps para paquetes de 512 bytes
Throughput de Antivirus	600 Mbps
Throughput de IPS	2.1 Gbps
Tuneles dedicados	2.000 site to site, 5.000 client to site
Tuneles SSL	300 concurrentes
Throughput VPN SSL	400 Mbps
Sesiones Concurrentes (tcp)	3,2 Milliones
Nuevas sesiones / segundo	77.000 TCP
Politicas	10.000
Número de Instancias virtuales	10
AC Power	100–240V AC, 50–60 Hz
Consumo de poder promedio	66 / 99 W

ITEM 1.2 CARACTERÍSTICAS GENERALES DEL SISTEMA

CARACTERÍSTICAS MÍNIMAS EXIGIDAS POR LA PERSONERIA DE MEDELLÍN	CARACTERÍSTICAS DEL PRODUCTO OFRECIDO POR EL PROVEEDOR

CARACTERISTICAS GENERALES DEL SISTEMA

*** Generalidades**

- Formato tipo appliance (dispositivo de propósito específico)
- Basado en tecnología ASIC y que sea capaz de brindar una solución de "Complete Content Protection". Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux.
- Interface de administración gráfica (GUI) vía Web (http y HTTPS)
- Interface de administración vía CLI (Línea de comando) vía telnet, ssh y consola serial.
- Debe tener la posibilidad de definir administradores para la solución, de modo que pueda segmentarse la responsabilidad de los administradores por tareas operativas
- Debe tener la capacidad de poder integrar dispositivos tipo UTM para que le reporten, y establecer comunicaciones seguras con dichos dispositivos. Soportando todos los modelos.
- Debe tener la capacidad de asignar cuotas de espacio en disco por dispositivo, de modo que un solo dispositivo no consuma la totalidad del disco de la solución
- Debe consolidar en el dispositivo.
- Capacidad de incrementar el rendimiento de VPN a través de soluciones en hardware dentro del mismo dispositivo (mediante el uso de un ASIC).
- Capacidad de reensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC).
- El equipo deberá poder ser configurado en modo gateway o en modo transparente en la red.
- En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.
- El sistema operativo debe incluir un servidor de DNS que permita resolver de forma local ciertas consultas de acuerdo a la configuración del administrador.

*** Análisis Forense y Correlación**

- Debe ser capaz de hacer correlación de la información almacenada. Esto es, identificar patrones y/o tendencias en la información almacenada. Una visión general de información detallada, como actividad de la red programas de mensajería instantánea y correo electrónico.
- Debe de ser capaz de hacer búsquedas por username o dirección IP, para que toda la información almacenada de dicho username o dirección IP sea mostrada en un reporte donde pueda darse seguimiento a su actividad.

*** Análisis de vulnerabilidades**

- Debe poseer (integrado o por separado) la capacidad de hacer análisis de vulnerabilidades en la red, mediante plug-ins de ataques actualizables, y generar un reporte de cuáles vulnerabilidades fueron encontradas en la red.

*** Cuarentenas**

- Debe de poder recibir archivos de dispositivos o mecanismos antivirus compatibles con la finalidad de usar el espacio en disco como espacio para cuarentena.
- Debe de poder recibir archivos de dispositivos o mecanismos antispam compatibles con la finalidad de usar el espacio en disco como espacio para cuarentena.

*** Almacenamiento de Contenido**

- Debe ser capaz de recibir bitácoras de los protocolos http, SMTP y messengers (Yahoo, MSN) para poder almacenar los mensajes que han fluído en la red a través de dichos protocolos, para su posterior visualización
- Los mensajes deberán poder ser almacenados completamente, o solo un "resumen" de la conexión. El mensaje completo exhibirá el contenido completo, mientras que el resumen solo mostrará fuente y destino de la comunicación, así como su duración.
- Debe de ser capaz de hacer búsquedas sobre los mensajes almacenados

Características Técnicas

Número de Interfaces Requeridas	42 10/100/1000 (RJ-45) 2 GE SFP DMZ Interfaces
Throughput de Firewall	4 Gbps para paquetes UDP de 1518/512/64 bytes
Throughput de VPN IPSec	1.3 Gbps para paquetes de 512 bytes
Throughput de Antivirus	600 Mbps
Throughput de IPS	2.1 Gbps
Tuneles dedicados	2.000 site to site, 5.000 client to site
Tuneles SSL	300 concurrentes
Throughput VPN SSL	400 Mbps
Sesiones Concurrentes	3.2 Million TCP
Nuevas sesiones / segundo	77.000 TCP
Políticas	10.000
Número de Instancias virtuales	10
AC Power	100–240V AC, 50–60 Hz
Consumo de poder promedio (Promedio/Máximo)	66 / 99 W
Instalación y configuración	El proponente deberá configurar, instalar, poner en funcionamiento el equipo en la personería de Medellin para lo cual deberá contar con ingenieria

		vinculada laboralmente certificada por el fabricante en nivel profesional	
	Soporte	El proponente deberá suministrar soporte presencial 7x24 durante la vigencia del licenciamiento en la personería de Medellin el tiempo máximo de atención después de reportado un incidente será de 3 horas. Deberá contar así mismo con plataforma web para sistema de tickets suministrando un usuario y contraseña.	
	Informes	El proponente deberá entregar licencia Forticlaud para reportes mensuales de consumo de internet lo cual será verificado por el interventor del contrato. Así mismo, deberá presentar mensualmente informe del soporte ofrecido a la Personería de Medellin.	
	Ficha técnica	El proponente deberá entregar ficha técnica original y certificado de distribuidor autorizado expedido por el fabricante	
	Pruebas de seguridad	El proponente deberá realizar pruebas de vulnerabilidad (Caja Negra externa) para lo cual deberá contar con personal vinculado laboralmente en Hacking Ético	

ITEM 1.3 LICENCIAMIENTO Y GARANTÍA

CARACTERÍSTICAS MÍNIMAS EXIGIDAS	**CARACTERÍSTICAS DEL PRODUCTO OFRECIDO POR EL PROVEEDOR**
LICENCIAMIENTO Y GARANTÍA	
El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, cajas de correo, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS y URL Filtering debe proveerse por al menos UN (1) año para la unidad de UTM en modalidad 8x5. El proponente deberá presentar licenciamiento de la solución donde se exprese la garantía del equipo (Hardware) durante el tiempo solicitado.	

ITEM 1.4 INSTALACIÓN CONFIGURACIÓN Y ENTRENAMIENTO EN LAS SOLUCIONES PROPUESTAS.

CARACTERÍSTICAS MÍNIMAS EXIGIDAS POR LA PERSONERIA DE MEDELLÍN	CARACTERÍSTICAS DEL PRODUCTO OFRECIDO POR EL PROVEEDOR
Implementación y Entrenamiento en las Soluciones Propuestas	
Características Básicas	
El proponente deberá configurar, instalar y poner en marcha la solución de seguridad perimetral UTM en la Personería de Medellin, para lo cual, deberá contar con mínimo un ingeniero de sistemas certificado por el fabricante de la solución de seguridad presentada Un (1) entrenamiento para tres (3) administradores/agentes de soporte, con una duración mínimo de 1 día.	
El programa de entrenamiento incluirá los siguientes temas: - Generalidades y configuración del sistema - Políticas y directivas de Firewall – Filtrado web – Control de APP – IPS - Fortivew - Mantenimiento - Recomendaciones - Listas blancas y negras - Cuarentena - Filtrado de contenido - Informes - VPN - En General todo el soporte y nuevas configuraciones que se requieran durante la vigencia del Licenciamiento .	

ITEM 1.5 SOPORTE TÉCNICO LOCAL.

CARACTERÍSTICAS MÍNIMAS EXIGIDAS POR LA PERSONERIA DE MEDELLÍN	CARACTERÍSTICAS DEL PRODUCTO OFRECIDO POR EL PROVEEDOR
SOPORTE TÉCNICO LOCAL	
Mantenimiento Correctivo y Soporte	
Características Básicas	
Atención y solución de incidentes en tercer nivel, teniendo en cuenta lo siguiente: - Se deberá comunicar al personal de sistemas (Administrador del Sistema) de la Personería de Medellín con uno(s) profesional(es) de soporte técnico, tan rápidamente como sea posible en concordancia con el nivel de prioridad de la	

solicitud. Deberá cumplir los términos acordados en los convenios de soporte mutuamente establecidos: Tiempo de respuesta a soporte presencial deberá ser máximo de tres horas con atención inmediata a correo electrónica y telefónica. Los reportes deberán presentarse dentro de los 5 días de cada mes y durante un año, los soportes entregados deberán evidenciar el uso de los recursos de internet, eventuales ataques informáticos y el soporte mensual ofrecido a la personería de Medellin - Para garantizar el optimó funcionamiento de las soluciones implementadas y/o soportadas, los profesionales de soporte deberán poseer un alto nivel de conocimiento y experiencia. Por lo tanto el proponente debera adjuntar certificaciones del personal en soluciones instaladas y soportadas cuyo objeto sea igual al del presente proceso
Alcance
Características Básicas
Soporte presencial en modalidad 7x24 atendido por Ingeniero especialista del producto durante 1 año. Las actividades presenciales se brindarán en la ciudad de Medellín en horario de atención 7x24 Atención telefónica, correo electrónico y web.
Cubrimiento
- Solución a consultas técnicas de instalación, administración y configuración de los productos cubiertos por el soporte. - Solución a problemas reportados en el funcionamiento u operación de los productos cubiertos por el soporte. - Solución a consultas técnicas avanzadas. - Escalamiento al fabricante para definir soluciones a problemas reportados, en caso de ser necesario. - Revisión y análisis de registros de eventos enviados por el cliente para efectuar por parte del proveedor, diagnósticos para la generación de soluciones. - Monitoreo de la aplicación de las soluciones por parte del cliente. - Entrega de un reporte mensual de casos abiertos. - Informe de cada visita con diagnóstico del incidente, solución(es) aplicada(s) y recomendaciones.

Las demás condiciones que no han sido objeto de modificación o aclaración siguen vigentes.

La presente Adenda hace parte integral de los Términos y Condiciones de la Solicitud Privada de Ofertas SPVA 2015-142.

Medellín, Noviembre 17 de 2015