MEMORANDUM D.E.T.A. N° 309/2016

A	:	***OSVALDO FERRAS,*** Jefe. Dpto. Evaluaciones Técnicas y Administrativo.
DE	:	***LIC. MIGUEL CALDERON,*** Jefe. División Investigación Tecnológica.
FECHA	:	17 de noviembre de 2016.
REFERENCIA	:	Remitir Evaluación Técnica.

Me dirijo a Usted y por su intermedio a quien corresponda, a fin de remitirle la Evaluación Técnica de las ofertas pertenecientes al **Llamado M.O.P.C. LCO N° 56/2016 "ADQUISICIÓN DE WEB FILTER" con ID N° 312.174.**

Se Adjunta:

- Planilla de Evaluación Técnica.

Sin otro particular aprovecho la oportunidad para saludarlo Atentamente.

Sr. Osvaldo Ferras.
Jefe
Dpto. Evaluaciones Técnicas y Administrativa.

Al Señor Director, con el Vto. Bo. de este Departamento.

Lic. Luis M. Andrada D.
Director.
Dirección de Informática.

A la Dirección de Bienes y Suministros, para su conocimiento.

MINISTERIO DE OBRAS PÚBLICAS Y COMUNICACIONES

TETÃ REKUÁI GOBIERNO NACIONAL
Jajapo ñande rapera ko'ãga guive
Construyendo el futuro hoy

MOPC - Gabinete - Dirección de Informática - Dpto. de Evaluaciones Técnicas y Administrativo - Div. Investigación Tecnológica / Evaluación Técnica - ADQUISICIÓN DE WEB FILTER ID: 312.174

Características Técnicas		Especificaciones técnicas mínimas requeridas	CGTEC .S.A.
REQUERIMIENTOS GENERALES			
Modo de cotizar No se acepta por respuesta "cumple". Los oferentes deberán especificar claramente como el equipo cotizado cumple con lo exigido.			
Modelo	Indicar exactamente el modelo del equipo a fin de cotejar en la Web	Exigido	DELL SONICWALL
Garantía	Garantía de (3) tres años del fabricante (on site) con provisión de partes originales sin cargo alguno para la institución durante el periodo de la garantía con respaldo del oferente.	Exigido	CUMPLE
Servicio Técnico	El oferente deberá contar con una autorización escrita del fabricante o el distribuidor en Paraguay para presentar la oferta, a su vez, el oferente deberá estar debidamente autorizado por el fabricante para prestar servicio técnico y contar con técnicos certificados, o en su defecto, indicar el Centro Autorizado de Servicios en el Paraguay donde se deberá realizar el reclamo de garantía correspondiente.	Exigido	CUMPLE
Adicionales	Presentar autorización del fabricante o distribuidor de la marca ofertada. Para los distribuidores será de carácter sustancial carta de autorización del fabricante dirigida a la convocante.	Exigido	CUMPLE
	El oferente deberá incluir los accesorios, cables, drivers, interfaces, manuales y conectores para el optimo funcionamiento del equipo, por mas que estos no sean expresamente solicitados.	Exigido	CUMPLE
La Solución propuesta deberá incorporar un cluster de dos equipos (Alta disponibilidad Activo –Pasivo; o Activo - Activo) con las siguientes funcionalidades mínimamente:		Exigido	CUMPLE
• Firewall tipo Stateful inspection.			CUMPLE
• VPN IPSec .			CUMPLE
• VPN SSL.			CUMPLE
• Antivirus y Antispyware de perímetro.			CUMPLE
• Sistema de Prevención de intrusos.			CUMPLE
• Sistema de filtrado de navegación Web.			CUMPLE
• Administración de ancho de banda.			CUMPLE
La solución deberá ser tipo appliance, una plataforma específica para hacer labores de Next Generation Firewall.		Exigido	CUMPLE
La solución deberá tener sistema operativo específicos para seguridad, sistemas operativos basados en Linux o Windows no serán aceptadas.		Exigido	CUMPLE
El dispositivo tiene que tener una arquitectura basada en procesadores de propósito específico multinúcleo, NO se aceptan procesadores de propósitos generales como ser XEON o OPTERON etc..		Exigido	CUMPLE
Tecnología de procesamiento multinúcleo.		Exigido	CUMPLE
Puertos 10/100/1000 en cobre.		10 como mínimo.	CUMPLE
Puertos 10/100/1000 SFP.		4 como mínimo.	CUMPLE
Puerto 10/100/1000 en cobre independiente para la consola de gestión (out-of-band management).		1 como mínimo.	CUMPLE
Interfaces SFP+ para conexión en Fibra o Cobre a 10 Gbps		2 como mínimo.	CUMPLE
Ventiladores Redundantes.		Exigido	CUMPLE
Sin límites a nivel lógico de la cantidad de usuarios.		Exigido	CUMPLE
El sistema permitirá el uso failover de puertos, es decir si una interface falla automáticamente opere otra.		Exigido	CUMPLE
El proponente deberá entregar 2 (equipos) armando un cluster de 2 nodos cada uno en alta disponibilidad mínimamente en activo/pasivo cada cluster.		Exigido	CUMPLE
El sistema soportará enrutamiento basado en políticas para que el tráfico sea enrutado a las diferentes interfaces basado en el servicio, la direcciones IP de origen o de destino.		Exigido	CUMPLE
El sistema deberá Permitir enrutamiento: BGP, OSPF, RIPv1/v2, rutas estáticas, Multicast.		Exigido	CUMPLE
El sistema deberá tener capacidad de soportar NAT 1:1, 1:muchos, muchos:1, muchos:muchos, flexible NAT, PAT, y modo transparente.		Exigido	CUMPLE
El sistema deberá soportar Jumbo Frames.		Exigido	CUMPLE
El sistema deberá soportar hacer Port Mirroring.		Exigido	CUMPLE
CARACTERISTICAS DE FIREWALL			
El sistema podrá ser implementado como Router, Layer 2 bridge, Wire mode (Sin hacer bridge capa 2) o como un network tap escuchando el tráfico.		Exigido	CUMPLE
Rendimiento de Firewall usando la metodología de medición basada en el RFC 2544.		8 Gbps como mínimo.	CUMPLE
Rendimiento de Firewall usando la metodología de medición basada en IMIX.		2.2 Gbps como mínimo.	CUMPLE
Cantidad máxima de conexiones en modo firewall.		562.000 como minimo.	CUMPLE
Cantidad máxima de conexiones con los módulos de IPS, Antivirus, Antispyware y Control de Aplicaciones activados (DPI).		350.000 como mínimo.	CUMPLE

Osvaldo R. Moreno R.
Técnico Verificador
Div. I.T. - D.E.T.A.

Lic. Miguel A. Calderón F.

Osvaldo L. Ferras P.
Jefe Dpto. Evaluaciones
Técnicas y Administrativo

Permitir administración por Zonas (grupos lógicos de interfaces).	Exigido	CUMPLE
En cada zona se debe permitir activar ciertos filtros y otros no.	Exigido	CUMPLE
Las reglas de firewall deben analizar las conexiones que atraviesen el equipo, entre interfaces, grupos de interfaces (o Zonas)	Exigido	CUMPLE
Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto fuente y destino (o zonas).	Exigido	CUMPLE
Las reglas del firewall deberán tomar en cuenta dirección IP fuente (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando.	Exigido	CUMPLE
Las acciones de las reglas deberán contener al menos el aceptar, o rechazar la comunicación.	Exigido	CUMPLE
Las reglas de firewall se deben poder aplicar en un horario determinado.	Exigido	CUMPLE
Calidad de servicio (QoS): Prioridad de ancho de banda, ancho de banda máximo, ancho de banda garantizado, marcado DSCP, 802.1p por cada regla de firewall.	Exigido	CUMPLE
El producto debe contar con la certificación ICSA Labs para Firewall corporativo o superior.	Exigido	CUMPLE
El producto debe contar con la certificación "Recommended" NSS labs para Next Generation Firewall del año 2014 o superior.	Exigido	CUMPLE
CARACTERISTICAS DE VPN		
Cantidad de túneles VPN Site to Site.	2.000 como mínimo.	CUMPLE
Mínimo Rendimiento 3DES/AES usando la metodología de medición basada en el RFC 2544.	4 Gbps	CUMPLE
Licencias cliente VPN para acceso remoto:	Soportado 1.500 como mínimo y 100 suministrado	CUMPLE
Para intercambio de claves, soportar mínimo: IKE, IKEv2, clave manual, PKI (X.509), L2TP a través de IPSec.	SI, IKE, IKEv2, clave manual, PKI (X.509), L2TP a través de IPSec	CUMPLE
Soportar DHCP sobre VPNs.	Exigido	CUMPLE
Para VPNs, descontaminar el tráfico en tiempo real antes de que llegue a la red corporativa y sin necesidad de que intervenga el usuario. De este modo se neutralizan a tiempo las vulnerabilidades y el código malicioso.	Exigido	CUMPLE
Filtrado de URLs (URL Filtering) con licencias incluidas		
Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 50 categorías y debe actualizarse automáticamente.	Exigido	CUMPLE
Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.	Exigido	CUMPLE
Soporte a YouTube for Schools para hacer filtrado selectivo de contenido de videos.	Exigido	CUMPLE
Configurable directamente desde la interfaz de administración del dispositivo appliance.	Exigido	CUMPLE
Permitir crear perfiles para filtro de contenido y que sean aplicados a usuarios locales o de LDAP/Active directory, Grupos o Direcciones IP.	Exigido	CUMPLE
El mensaje entregado al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables.	Exigido	CUMPLE
El filtrado se podrá hacer por horarios.	Exigido	CUMPLE
Rastreo por HTTP URL, HTTPS IP, palabra clave y contenido, bloqueo de ActiveX, Java Applet, y cookies, gestión del ancho de banda según categorías de clasificación, listas de admitidos/bloqueados personalizadas.	Exigido	CUMPLE
El sistema deberá soportar de mecanismos de Autenticación: RADIUS, Active Directory, LDAP, base de datos interna, Reconocimiento transparente de usuario del LDAP, reconocimiento de usuarios presentes en Terminal services (Windows y Citrix) y usuarios locales.	Exigido	CUMPLE
El sistema podrá hacer reconocimiento transparente (sin validación adicional) de los usuarios ya autenticados a través de un RADIUS server usando información de RADIUS accounting.	Exigido	CUMPLE
El sistema podrá hacer filtrado de páginas web sobre usuarios que no estén dentro de la red a través de un cliente de filtrado web.	Exigido	CUMPLE
CARACTERISTICAS DE INSPECCION PROFUNDA DE PAQUETES con licencias incluidas		
La solución deberá contar con un Sistema de Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention Service y Application Firewall.	Exigido	CUMPLE
Inspección de virus, spyware, prevención de intrusos (IPS). Deberá ser granular, permitir entrar en el detalle de cada una de las firmas de posibles ataques.	Exigido	CUMPLE
El sistema de inspección profunda de paquetes deberá funcionar bidireccionalmente.	Exigido	CUMPLE
El sistema de inspección profunda de paquetes deberá operar sin proxies para evitar problemas de latencia.	Exigido	CUMPLE
Sistema de Prevención de Intrusos IPS con licencias incluidas		
Rendimiento mínimo en IPS según RFC 2544.	2.5 Gbps como mínimo.	CUMPLE
El sistema IPS contará con al menos 4.800 firmas de ataques.	Exigido	CUMPLE
El sistema deberá contar con protección de ataques de inundación (flood) a nivel de UDP, ICMP y el conocido SYN Flood.	Exigido	CUMPLE

Osvaldo R. Moreno R.
Técnico Verificador
Div. I.T. - D.E.T.A.

Lic. Miguel A. Calderón F.
Jefe Div. Investigación Tecnológica

Osvaldo L. Ferras P.
Jefe Dpto. Evaluaciones
Técnicas y Administrativo
Dirección Informática - MOPC.

El sistema deberá permitir al administrador ejecutar acciones sobre los eventos de IPS como bloquear el tráfico, registrar o capturar el tráfico generado por el ataque.	Exigido	CUMPLE
El IPS podrá inspeccionar el tráfico entre las zonas internas de la red.	Exigido	CUMPLE
Creación personalizable de reglas de IPS.	Exigido	CUMPLE
El sistema de IPS deberá detectar anomalías en los protocolos.	Exigido	CUMPLE
Prevención de ataques de ataques DoS, DDoS y de escaneo.	Exigido	CUMPLE
Deberá contar con mecanismos de anti-evasión.	Exigido	CUMPLE
Para VoIP: Total compatibilidad con H.323v1-5, SIP, Gatekeeper, gestión de ancho de banda saliente, VoIP sobre WLAN, seguridad de inspección profunda, total Interoperabilidad con la mayoría de los dispositivos VoIP de pasarela y comunicaciones.	Exigido	CUMPLE
Sistema de control de aplicaciones con licencias Incluidas		
Rendimiento de la inspección en profundidad de las aplicaciones.	2.5 Gbps como mínimo.	CUMPLE
El sistema deberá identificar, categorizar y controlar y visualizar tráfico de más de 4300 aplicaciones agrupadas en al menos 25 Categorías.	Exigido	CUMPLE
Las aplicaciones se deben identificar independientemente del Stack o del puerto(TCP, UDP, etc.) que usen.	Exigido	CUMPLE
El sistema podrá detectar aplicaciones propias, definidas por el usuarios.	Exigido	CUMPLE
Las políticas de control de aplicaciones se podrán hacer granular por dirección IP, usuario, grupos de usuarios locales o de LDAP/Active Directory y basado en horarios.	Exigido	CUMPLE
El sistema deberá permitir la creación de reglas de control de ancho de banda de las aplicaciones soportadas.	Exigido	CUMPLE
El sistema deberá reportar en tiempo real cuales de las aplicaciones soportadas están siendo usadas, que usuario o dirección IP lo está haciendo y cuánto tráfico está cursando.	Exigido	CUMPLE
Antivirus de Perímetro con licencias Incluidas		
El sistema deberá acreditar un rendimiento de Gateway Antivirus en el modo de operación que brinda mayor seguridad.	1.5 Gbps como mínimo.	CUMPLE
Debe ser capaz de analizar, tráfico entrante y saliente mínimo de los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP, CIFS/NETBIOS, y esta debe estar completamente integrada a la administración del dispositivo appliance.	Exigido	CUMPLE
Permitir escaneo de virus o spyware sobre protocolos basados en stream TCP, como Mensajería Instantánea y P2P.	Exigido	CUMPLE
El sistema deberá realizar análisis antivirus sin limitación del tamaño del archivo transferido.	Exigido	CUMPLE
No se permitirán tecnologías basadas en redireccionar el tráfico hacia un dispositivo externos para examinar los paquetes de datos.	Exigido	CUMPLE
Control granular de firmas de virus y spyware.	Exigido	CUMPLE
Actualizaciones automáticas con un intervalo mínimo de búsqueda de actualizaciones de 1hora.	Exigido	CUMPLE
Inspección de tráfico cifrado con licencias Incluidas		
El sistema deberá hacer inspección de Aplicaciones, IPS, antivirus y filtrado de páginas web sobre comunicaciones cifradas por TLS (Transport Layer Security) tales como HTTPS.	Exigido	CUMPLE
Rendimiento en Inspección SSL (DPI SSL).	500 Mbps	CUMPLE
Servicios de Seguridad en la nube con licencias Incluidas		
EL sistema contará con un servicio online de detección de virus en la nube con capacidad de reconocimiento de más de 10 millones de amenazas el cual se puedan enviar muestras resumidas del tráfico para detectar códigos maliciosos.	SI	CUMPLE
El sistema contará con filtrado de conexiones a centros de control de Botnets basado en reputación de direcciones IP.	SI	CUMPLE
El sistema contará con controles de localización geográfica basados en la dirección IP de origen para hacer reglas de conexión por país bien sea de manera general o por reglas de firewall.	SI	CUMPLE
Soporte a IPV6 con al menos las siguientes funcionalidades		
Reglas de firewall.	Exigido	CUMPLE
Administración de ancho de banda.	Exigido	CUMPLE
Filtrado de páginas web.	Exigido	CUMPLE
IPS.	Exigido	CUMPLE
VPN Site to site IPSec y SSL.	Exigido	CUMPLE
VPN SSL.	Exigido	CUMPLE
Antispyware, Antivirus.	Exigido	CUMPLE
Control de aplicaciones sobre IPV6.	Exigido	CUMPLE
Visualización en tiempo real de aplicaciones.	Exigido	CUMPLE
Soporte a VLANs en IPV6.	Exigido	CUMPLE
Soporte a DHCP y servidor de DHCP.	Exigido	CUMPLE
Soporte a IPV4 e IPV6 Dual Stack.	Exigido	CUMPLE
Soporte a NAT en IPV6.	Exigido	CUMPLE
Soporte a Neighbor Discovery Protocol.	Exigido	CUMPLE
Soporte a FTPv6 con EPRT y EPSV en transferencias FTP IPV6.	Exigido	CUMPLE
Protección a Syn Floods de IPV6.	Exigido	CUMPLE
Soporte a ICMP V6.	Exigido	CUMPLE
Soporte a Políticas de enrutamiento en IPV6, RIPng OSPFv3 y BGP4.	Exigido	CUMPLE
Soporte a SNMP sobre IPV6.	Exigido	CUMPLE
Soporte a ISATAP.	Exigido	CUMPLE
Soporte a IPv4 to IPv6 tunneling.	Exigido	CUMPLE

Osvaldo R. Moreno R.
Técnico Verificador
Div. I.T. - D.E.T.A.

Lic. Miguel A. Calderón F.
Jefe Div. Investigación Tecnológica

Osvaldo L. Ferras P.
Jefe Dpto. S... Técnicas y ...

Soporte a IPv6 to IPv4 tunneling.	Exigido	CUMPLE
Soporte a IPV6 Rapid Deployment.	Exigido	CUMPLE
Soporte a Multicast Listener Discovery.	Exigido	CUMPLE
Sobre una máquina (física o virtual) a ser provista por la convocante, el oferente deberá instalar un gestor reportes centralizados.		
Software de administración de logs y eventos, vía web.	Exigido	CUMPLE
Interfaz de Administración vía web y CLI.	CLI, SSH, GUI, GMS	CUMPLE
Interfaz gráfica Web (HTTP, HTTPS), línea de comandos (SSH, consola), SNMP v2 o v3.	Exigido	CUMPLE
El sistema operará como un receptor de logs de todos los Next-Generation Firewalls instalados de la solución.	Exigido	CUMPLE
El sistema de reportes deberá permitir monitoreo en tiempo real del tráfico registrado.	Exigido	CUMPLE
El sistema deberá una capacidad de manejo de logs, auditoria, gestión de backups y almacenamiento necesario para manejo de reportes de por lo menos 3 TB de modo a almacenar los eventos por el máximo tiempo posible.	Exigido	CUMPLE
El sistema permitirá la generación de reportes detallados sobre cada uno de los equipos instalados en la solución.	Exigido	CUMPLE
Los reportes como mínimo deberán incluir:		
• Ancho de banda utilizado.		CUMPLE
• Usuarios que más emplean ancho de banda.		CUMPLE
• Servicios más usados.		CUMPLE
• Páginas web más visitadas.		CUMPLE
• Usuarios que más tiempo emplean navegando.		CUMPLE
• Reporte de páginas web empleadas por usuario.		CUMPLE
• Páginas web más filtradas.		CUMPLE
• Usuarios más filtrados.		CUMPLE
• Categorías más filtradas.		CUMPLE
• Uso del FTP y de Correo.		CUMPLE
• Uso de las VPNs.		CUMPLE
• Virus más encontrados.		CUMPLE
• Spyware más encontrados.		CUMPLE
• Eventos de IPS más encontrados.		CUMPLE
• Obtención de los ítems arriba mencionados con posibilidad de agruparlos de manera diaria, semanal mensual o entre un rango de fechas personalizado.		CUMPLE
LICENCIAS		
Las licencias proveídas con los equipos para alta disponibilidad, clustering, y reportes solicitados deben ser por 3 años.	Exigido	CUMPLE
El servicio de soporte 24x7 del fabricante debe ser por 3 años.	Exigido	CUMPLE
El servicio de actualización de las firmas de los servicios de seguridad que requieran actualizaciones frecuentes debe ser licenciado por 3 años.	Exigido	CUMPLE
Se debe incluir en la oferta una carta de autorización del fabricante, representante o distribuidor para presentar la oferta de los bienes solicitados. En los casos de Distribuidores o Representantes, estos deberán contar con la carta del Fabricante dirigida al Representante Regional o Distribuidor Autorizado que le extendió la carta, a fin de demostrar la cadena de autorizaciones que debe ser originada y partir necesariamente del Fabricante.	Exigido	CUMPLE
Para demostrar la capacidad Técnica el oferente deberá presentar al menos un técnico con antigüedad mínima de 6 meses en la empresa oferente, certificado por el fabricante de la marca ofrecida donde la Certificación deberá ser mínimamente del tipo Professional de Seguridad o Administrador Avanzado de Seguridad de Red o del tipo Especialista de Seguridad de Red con experiencia mayor a un año según conste en el certificado. (no serán aceptables Certificados técnicos del tipo Pre venta).	Exigido	CUMPLE
INSTALACIÓN		
Instalación — El servicio contemplará todos los suministros, actividades de montaje, instalación en general, configuración y puesta en funcionamiento del equipo.	Exigido	CUMPLE
CAPACITACIÓN		
Capacitación — Curso Básico de 30 horas incluida la prueba de certificación (cantidad: 3 alumnos como mínimo)	Exigido	CUMPLE

Osvaldo R. Moreno R.
Técnico Verificador
Div. I.T. - D.E.T.A.
Dirección de Informática - MOPC

Lic. Miguel A. Calderón F.
Jefe Div. Investigación Tecnológica
Dirección Informática-MOPC

Osvaldo L. Ferras P.
Jefe Dpto. Evaluaciones
Técnicas y Administrativo
Dirección Informática - MOPC.