Señores
AUDITORÍA GENERAL DE LA REPÚBLICA
Bogotá

Asunto: Respuesta a la solicitud de Cotización

En atención a la invitación a presentar oferta para el estudio de mercado, nos permitimos presentar nuestra propuesta:

DESCRIPCION	
1. SOLUCIÓN DE FIREWALL DE NUEVA GENERACIÓN	**CUMPLE SI/NO**
MARCA: FORTINET	
MODELO: FG-120G	
1. Generalidades.	
Adquisición de dos (2) appliance de seguridad informática perimetral con sistema operativo propietario del fabricante, del tipo Firewall de Nueva Generación, en los que se deberán ofrecer, ya incluidas y listas para su uso, las funcionalidades que se detallan en el presente documento.	SI
La solución debe contar con una arquitectura que permita alta disponibilidad.	SI
Los dispositivos deben ser equipos de propósito específico.	SI
No es aceptable un servidor de propósito genérico. Los equipos deben ser nuevos, no se aceptarán equipos remanufacturados o OEM.	SI
Para garantizar la protección de inversión, alineación con las tendencias tecnológicas de la industria, soporte y vigencia tecnológica y estar preparados para los requerimientos futuros, los equipos ofertados deben corresponder a un único fabricante que figure como líder en el Cuadrante mágico™ de Gartner® de 2025 para firewall de malla híbrida	SI
El dispositivo debe contar con tecnología ASIC para permitir acelerar los procesos (no solo por CPU) y de esta manera permita mejorar el rendimiento del procesamiento de tráfico	SI
2. Rendimiento	
El equipo deberá cumplir con las siguientes características mínimas de desempeño ya activas y funcionales:	SI
• Rendimiento de Firewall: mínimo 39 Gbps	SI
• Rendimiento de IPS: mínimo 5 Gbps	SI
• Rendimiento de NGFW: mínimo 3 Gbps	SI
• Rendimiento protección de amenazas: mínimo 2 Gbps	SI
• Rendimiento IPSec VPN: 35 Gbps	SI
• Sesiones concurrentes: mínimo 3.000.000	SI
• Rendimiento de Inspección SSL 3 Gbps	SI
• Latencia >= a 3 µs	SI
• Rendimiento de VPN SSL: mínimo 1 Gbps	SI

3. Conectividad	
El equipo deberá contar con las siguientes interfaces de conexión:	SI
• Mínimo 16 puertos de 1 GE RJ45	SI
• 8 interfaces SFP de 1 GE	SI
• 4 interfaces de 10 GE SFP+	SI
4. Traducción de direcciones	
La plataforma debe soportar los siguientes tipos de traducción de direcciones:	SI
• NAT y PAT	SI
• NAT estático	SI
• NAT destino, origen	SI
• NAT, NAT64 persistente	SI
5. Funciones básicas de Firewall	
Las reglas de firewall deben analizar las conexiones que pasen por el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.	SI
La solución debe integrarse con el directorio activo y soportar políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.	SI
Debe tener la capacidad de generar una advertencia al administrador cuando este configure una política duplicada	SI
Debe estar en la capacidad de integrase con plataforma Cloud IaaS como: AWS,Azure,Google etc. Con el fin de generar y actualizar objetos de direcciones de manera automática basado en los parámetros de red (IP,TAG etc) de las instancias desplegadas en la nube y estas ser usadas como objetos de reglas o políticas de firewall	SI
Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface) como por GUI (Graphical User Interface).	SI
La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP	SI
El dispositivo será capaz de crear e integrar políticas contra ataques DoS (Denial of service) las cuales se deben poder aplicar por interfaces	SI
El dispositivo será capaz de ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico.	SI
Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis.	SI
6. Conectividad y Enrutamiento	
Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.	SI
Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.	SI
Soporte a ruteo dinámico RIP V1, V2, OSPF y BGP	SI
La solución podrá habilitar políticas de ruteo en IPv6	SI
La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6.	SI

	La Solución deberá soportar balanceado de enlaces WAN inteligente (SD-WAN Seguro) sin licencia adicional basado en: Aplicaciones cloud, SLA y Mejor calidad de enlace basado en (Jitter, latencia, ancho de banda, perdida de paquetes)	SI
7.	**VPN IPSEC**	
	El equipo deberá soportar las siguientes características:	SI
	Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).	SI
	Soporte para IKEv2 y IKE Configuration Method.	SI
	Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES	SI
	Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits	SI
8.	**VPN SSL**	
	Capacidad de realizar SSL VPNs por usuarios sin incurrir en costos adicionales.	SI
	Soporte a certificados PKI X.509 para construcción de VPNs SSL.	SI
	Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.	SI
9.	**Autenticación**	
	El dispositivo deberá manejar los siguientes tipos de autenticación:	SI
	Capacidad de soporta autenticación local y remota integrándose con Servidores de Autenticación RADIUS ,LDAP o TACACS+.	SI
	Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es aprovechar las credenciales del dominio de Windows bajo un concepto “Single-Sign-On”.	SI
	Soporte de Token Físicos o Mobile sobre Smartphone basado en IOS o Android, token de SMS, email o con plataformas de terceros como RSA SecurID.	SI
	Capacidad de soportar autenticación de acceso de usuario a través de 802.1x y portal cautivo.	SI
10.	**Manejo de tráfico y calidad de servicio.**	
	Capacidad de poder asignar parámetros de traffic shapping atreves de reglas de manera independiente	SI
	Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión	SI
	Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación y categoría URL de las mismas para la regla en general.	SI
	Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en Kilobits por segundo	SI
11.	**Antimalware**	

Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.MAPI	SI
El módulo de antimalware debe haber sido desarrollado por el mismo fabricante de la solución de firewall, así como las firmas deberán ser de su propiedad y no por medio de licenciamiento o concesiones de un tercero, esto con el fin de garantizar la idoneidad de la protección, así como los tiempos de respuesta del soporte de la misma.	SI
Debe soportar la inspección de archivos comprimidos como los son: GZIP,RAR,LZH,IHA,CAB,ARJ;ZIP entre otros con el fin de proteger contra estas técnicas de evasión.	SI
El Antivirus deberá integrarse de forma nativa con una solución sandbox del mismo fabricante, de tal manera que envíen muestras de archivos a dicho dispositivo para su análisis.	SI
12. Filtrado WEB	
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 78 categorías y por lo menos 47 millones de sitios web en la base de datos.	SI
Debe poder categorizar contenido Web requerido mediante IPv6.	SI
Será posible exceptuar la inspección de HTTPS por categoría.	SI
Debe contar con la capacidad de bloquear contenido de youtube usando el Channel ID	SI
El filtrado debe ser sobre tráfico http y https.	SI
13. Protección contra intrusos (IPS)	
El sistema de detección y prevención de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror.	SI
Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores.	SI
Capacidad de detección de más de 7000 ataques.	SI
El sistema de detección y prevención de intrusos deberá estar integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, La interfaz de administración del sistema de detección y prevención de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso.	SI
Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes	SI

sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP.	
14. Control de Aplicaciones	
La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.	SI
La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.	SI
La solución debe tener un listado de al menos 3000 aplicaciones ya definidas por el fabricante.	SI
Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log y resetear conexión	SI
Debe ser posible inspeccionar aplicaciones tipo Cloud como dropbox, icloud entre otras entregando información como login de usuarios y transferencia de archivos.	SI
15. Inspección de Contenido SSL/SSH	
La solución debe soportar inspeccionar tráfico que esté siendo encriptado mediante SSL al menos para los siguientes protocolos: HTTP, IMAP, SMTP, POP3 y FTP en su versión segura	SI
Debe ser posible definir perfiles de inspección SSL donde se definan los protocolos a inspeccionar y el certificado usado, estos perfiles deben poder ser escogidos una vez se defina la política de seguridad.	SI
La inspección deberá realizarse: mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle) para una inspección completa o solo inspeccionando el certificado sin necesidad de hacer full inspection.	SI
16. Alta Disponibilidad	
El dispositivo deberá soportar *alta disponibilidad* transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6	SI
Alta Disponibilidad en modo Activo-Activo de forma automática sin requerir hacer políticas de enrutamiento basado en orígenes y destino para poder hacer la distribución del tráfico.	SI
La solución debe soportar hasta 2 equipos en esquema de HA.	SI
17. Visibilidad	
La solución debe estar en la capacidad de visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real, esto deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional.	SI
Deber tener la capacidad de poder validar con qué política la sesión se está coincidiendo y un link hacia la misma.	SI
De las aplicaciones Cloud como Dropbox que permiten compartir archivos, debe ser posible ver que archivos fueron subidos y descargados por los usuarios.	SI

18. Características de Administración	
Interface gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interface debe soportar SSL sobre HTTP (HTTPS)	SI
Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos	SI
Debe tener la capacidad de gestionar todas las políticas de seguridad, además de poder gestionar Switches y APs dentro de una única consola de gestión Debe estar en capacidad de administrar switches y Access point para generar una red SD-LAN administrada y gestionada desde el mismo Firewall.	SI
19. Virtualización	
El dispositivo deberá poder virtualizar los servicios de seguridad mediante “Virtual Systems”, “Virtual Firewalls” o “Virtual Domains”	SI
Debe soportar e incluir la licencia para al menos 10 (diez) instancias virtuales dentro de la solución a proveer.	SI
Cada instancia virtual debe poder tener un administrador independiente	SI
20. Licenciamiento y actualizaciones	
El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, VPNs equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.	SI
La vigencia de las actualizaciones para los servicios de IPS, AI-based Inline Malware Prevention, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, debe proveerse por al menos dos (2) años.	SI
La plataforma es requerida por un periodo de dos (2) años en un esquema de soporte 7x24 ante el fabricante.	SI
21. Accesorios	
Modulo 1 GE SFP transceiver, short range 500m, LC connector, MMF, 850nm, -20°C to 85°C, for systems with SFP slots	SI
Modulo 10GE SFP+ transceiver, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots	SI

FORMATO ECONÓMICO

ítem	Elemento	Cantidad	Valor unitario	IVA	Valor total
1	FIREWALL DE NUEVA GENERACIÓN	2	$ 46.049.000,00	$ 8.749.310,00	$ 109.596.620,00
2	EQUIPO DE TRABAJO	1	$ 24.540.077,00	$ 4.662.615,00	$ 29.202.692,00
				Valor Total Iva Incluido	**$ 138.799.312,00**

El valor cotizado asciende a la suma de CIENTO TREINTA Y OCHO MILLONES SETECIENTOS NOVENTA Y NUEVE MIL TRECIENTOS DOCE PESOS M/CTE ($138.799.312)

Cordialmente,

Juan Castro

_____

JUAN FERNANDO CASTRO SIERRA
LAN SECURITY NETWORKS
Móvil: (57) 3013914651
Correo: Juan.castro@lsn.com.co
Barranquilla – Colombia