ANEXO TECNICO

Descripción técnica:

Ítem	Requerimiento Técnico Mínimo (de obligatorio cumplimiento)
1	**Generalidades** **ADQUISICION FORTIGATE 600C NUEVO** (FortiGate-600C Hardware plus 8x5 FortiCare and FortiGuard Bundle Hardware plus 2 year 8x5 Forticare and FortiGuard UTM Bundle) **REALIZAR LA RENOVACION** (UTM Bundle 8x5 FortiCare plus NGFW, AV, Web Filtering and Antispam Services) La entidad actualmente tiene un firewall Fortinet FG600C3973804136 y el objetivo es comprar uno de igual características para ponerlos en alta disponibilidad, soporte y licencia de 2 años. Para nuestro Fortinet FG600C3973804136 se requiere comprar la licencia y soporte por 2 años ya que se encuentra vencida. El nuevo firewall Fortinet debe tener doble fuente redundante y se adquiere una nueva fuente para el que se encuentra en la Entidad. Con la adquisición de nuevo firewall se debe realizar la instalación, configuración y puesta en funcionamiento de los 2 firewall en alta disponibilidad, lo cual requiere que se haga un afinamiento de todas las políticas, reglas, zonas, DMZ, NAT, VPN, redes e interfaces y las demás que se requieran.
2	**Rendimiento** El equipo deberá cumplir con las mismas características firewall Fortinet FG600C3973804136 para poder formar la alta disponibilidad, el nuevo firewall debe traer todos sus conectores y demás cables que se requieran para poderlos interconectar.
3	**Conectividad** El equipo deberá contar con las siguientes interfaces electrónicas de conexión: • Interfaces 10/100/1000 cobre • Interfaces de fibra con sus respectivos transceiver.
4	**Protocolos soportados** • IPv4 e IPv6 • DHCP cliente, servidor, relay
5	**Certificaciones y estándares soportados.** El sistema completo deberá estar certificado en: • FIPS NIVEL 2 • ICSA LABS Firewall and VPN • ICSA LABS IPS • ICSA LABS Gateway AV • IPv6 Ready Logo Phase 2

6	**Address Traslation** • NAT y PAT • NAT estático • NAT: destino, origen • NAT, NAT64 persistente
7	**Manejo de tráfico y calidad de servicio** • Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall • Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión • Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general. • Capacidad de poder definir ancho de banda garantizado en Kilobytes por segundo • Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en Kilobytes por segundo • Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia
8	**Funciones básicas de Firewall** • Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. • Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos. • Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario). • La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP. • La solución será capaz de habilitar o deshabilitar el paso de tráfico a través de procesadores de propósito específico, si el dispositivo cuenta con estos procesadores integrados dentro del mismo. • El dispositivo será capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico • Tendrá la capacidad de hacer escaneo a profundidad de trafico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis

	• La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios. • La solución soportará políticas basadas en dispositivo. Esto significa que podrán definirse políticas de seguridad de acuerdo al dispositivo (móvil, laptop) que tenga el usuario.
9	**Conectividad y Enrutamiento** • Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP. • Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs. • Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas. • Soporte a políticas de ruteo (policy routing) • Soporte a ruteo dinámico RIP V1, V2, OSPF y BGP • Soporte a ruteo dinámico RIPng, OSPFv3 • La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes. • Soporte de ECMP (Equal Cost Multi-Path) • Soporte a ruteo de multicast • La solución permitirá la integración con analizadores de tráfico mediante los protocolos Flow. • La solución podrá habilitar políticas de ruteo en IPv6 • La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6
10	**VPN IPSEC** El equipo deberá soportar las siguientes características: • Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site) • Soporte para IKEv2 y IKE Configuration Method • Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES • Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits • Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14. • Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256. • Posibilidad de crear VPN's entre gateways y clientes con IPSec. Estoes, VPNs IPSeC site-to- site y VPNs IPSec client-to-site. • La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN).

	• En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall.
11	**VPN SSL** • Capacidad de realizar SSL VPNs. • Soporte a certificados PKI X.509 para construcción de VPNs SSL. • 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. • Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet. • Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL. • Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning) • La VPN SSL integrada deberá soportar a través de algún plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS • Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL • Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente • Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios. • Los portales personalizados deberán soportar al menos la definición de: Widgets a mostrar: Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC o Soporte para Escritorio Virtual o Política de verificación de la estación de trabajo. • La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información.
12	**Autenticación**

	El dispositivo deberá manejar los siguiente tipos de autenticación: • Capacidad de integrarse con Servidores de Autenticación RADIUS. • •Capacidad incluida, al integrarse con Microsoft Windows Active Directory, de autenticar transparentemente usuarios sin preguntarles username o password, aprovechando las credenciales del dominio de Windows bajo un concepto "Single-Sign-On" • Soporte de doble Factor de autenticación para reglas de firewall o VPN. • Soporte de Token Físicos o Mobile sobre Smartphone basado en IOS o Android.
13	**Módulos de Seguridad**
13.1	**Antivirus** • 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. • El Antivirus deberá poder configurarse en modo Proxy como en modo de Flujo. En el primer caso, los archivos serán totalmente reconstruidos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente. • Antivirus 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. • El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6. • La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo appliance, que permita la aplicación de esta protección por política de control de acceso. • El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging). • Se debe incluir protección contra amenazas avanzadas y persistentes (Advanced Persistent Threats). Dentro de estos controles se debe incluir: 1. Protección contra botnets: Se deben bloquear intentos de conexión a servidores de Botnets, para ello se debe contar con una lista de los servidores de Botnet más utilizado. Dicha lista debe actualizarse de forma periódica por el fabricante

	2. Sandboxing: La funcionalidad de Sandbox hace que el archivo sea ejecutado en un ambiente seguro para analizar su comportamiento y, a base del mismo, tomar una acción sobre el mismo.
13.2	**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 75 categorías y por lo menos 54 millones de sitios web en la base de datos. • Debe poder categorizar contenido Web requerido mediante IPv6. • La solución debe permitir realizar el filtrado de contenido, tanto realizando reconstrucción de toda la sesión (modo proxy) como realizando inspección paquete a paquete sin realizar reconstrucción de la comunicación (modo flujo). • Capacidad de filtrado de scripts en páginas web (JAVA/Active X). • La solución de Filtraje de Contenido debe soportar el forzamiento de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta • Funcionalidad se soportará al menos para Google, Yahoo! y Bing.
13.3	**Protección contra Intrusos IPS** • El Detector y preventor 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 spam o mirror. • Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. • Capacidad de detección de más de 4000 ataques. • El detector y preventor de intrusos deberá soportar captar ataques por variaciones de protocolo y además por firmas de ataques conocidos (signature based / misuse detection). • Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo. • Actualización automática de firmas para el detector de intrusos • 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 sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP.

13.4	**Control de Aplicaciones** • Lo solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo. • La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico. • La solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante. • El listado de aplicaciones debe actualizarse periódicamente. • Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: • Permitir, bloquear, registrar en log. • Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log. • Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de trafficshaping. • Preferentemente deben soportar mayor granularidad en las acciones.
13.5	**Inspección de Contenido SSL** • La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S. • La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle). • El equipo debe ser capaz de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS **lisis de Vulnerabilidades:** • La solución deberá Permitir hacer análisis de vulnerabilidades y generar un reporte de cuáles vulnerabilidades fueron encontradas. No deberá tener límite de equipos a analizar.
14	**Alta disponibilidad** • El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que uno falle tanto para IPV4 como para IPV6 • Debe soportar Alta Disponibilidad en modo Activo-Pasivo

	• Debe soportar Alta Disponibilidad en modo Activo-Activo • Debe soportar Posibilidad de definir al menos dos interfaces para sincronía • El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red. • Deberá Ser posible definir interfaces de gestión independientes para cada miembro en un clúster.
15	**Virtualización** • La solución ofertada deberá tener como mínimo 10 firewalls virtuales incluidos. • El dispositivo deberá poder virtual izar los servicios de seguridad mediante “Virtual Systems”, “Virtual Firewalls” o “Virtual Domains” • Cada instancia virtual deberá poder estar en modo Gateway o en modo transparente a la red. • Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual.
16	**Cliente de VPN** • Se debe suministrar el software de cliente para VPN. • La solución debe estar licenciada para cinco mil (5000) usuarios de VPN SSL dinámicos, externos o móviles. • El cliente debe permitir la autenticación por dos factores.
17	**Licencia** • El nuevo fortiGate 600 C debe traer Licencia y soporte por dos Años • El fortiGate 600 C - FG600C3973804136 se le debe adquirir licencia y Soporte de 2 años.
18	**Fuente de energía** • El nuevo fortiGate 600 C debe traer doble fuente redundante. • El fortiGate 600 C - FG600C3973804136 se le debe adquirir una nueva fuente para que quede con doble fuente redundante
19	**Conectores y cables** • El proponente debe entregar todos los cables y conectores que se requieren para interconectar los dos firewall y crear la alta disponibilidad.
20	**Banco de horas** • 100 horas de soporte en sitio especializadas en firewall para hacer ajustes, afinamientos, reglas y políticas que requiera la Entidad, que

	sean consumibles en 2 años. Esta bolsa de horas debe ser diferente a la de soporte y garantía que se incluyen con la adquisición. Banco de 100 horas para asesorías y/o nuevas configuraciones, en horario 5x8. Ciudad de prestación del servicio: Bogotá, Vigencia 2 años.
21	**Servicio de Instalación** • Servicio de implementación de un Appliance FortiGate-600C a configurarse en cluster, alta disponibilidad con un equipo FortiGate-600 ya instalado (armado de cluster) • Incluye adicionalmente la configuración del balanceo de carga para 2 enlaces de Internet y la instalación de las fuentes redundantes para los dos equipos.
22	**Capacitación** • Capacitación presencial en la Entidad a dos funcionarios de TI de la ANI, donde explique la configuración y manejo del Firewall, políticas, reglas, VPN, Objetos, administración general. Se estima que esta capacitación tenga una duración de 8 horas. • Dos Vouchers de capacitación presencial y examen de certificación (Curso 301 – Duración de 3 días y manejo de funcionalidades avanzadas), para funcionarios de la Entidad del área TI a implementar, administrar y brindar soporte a la infraestructura comprada. Este curso se debe dictar en un centro de entrenamiento Fortinet desarrollado por expertos para realizar los respectivos laboratorios.

CONDICIONES MÍNIMAS GENERALES

El contratista deberá ejecutar el objeto del contrato cumpliendo cada una de las especificaciones técnicas y requerimientos mínimos de los ítems anteriores.

Se debe instalar, configurar y dejar en correcto funcionamiento la solución brindada.

La garantía y soporte de los equipos deberá ser por un periodo mínimo de 24 Meses.

El contratista se compromete con la Entidad, a suministrar todos los equipos certificados y garantizados de fábrica, cumpliendo las Normas técnicas vigentes nacionales e internacionales.

El contratista debe comprometerse a entregar los reportes de los mantenimientos o reparaciones técnicas realizadas en el equipo o equipos en el periodo de garantía.

El contratista deberá explicar claramente la metodología que se debe seguir para solicitar y prestar el servicio.

El personal propuesto debe estar certificado por el fabricante de la marca ofrecida en nivel NSE-4, para lo cual deberán adjuntar, junto con la oferta, los respectivos certificados del fabricante, con fecha de expedición menor a 2 años a partir de la presentación de la oferta, con el fin de garantizar que se encuentran vigentes.

Uno de los ingenieros del equipo de trabajo, que participarán en el proyecto, debe estar certificado como NSE-5, para lo cual deberá presentar el respectivo certificado del fabricante, con expedición menor a 2 años, a partir de la presentación de la oferta, con el fin de garantizar que el personal tiene los conocimientos sobre las últimas versiones liberadas por el fabricante.