INFORME DE VERIFICACION TECNICA DEFINITIVA
7 DE FEBRERO DE 2022

SOLICITUD SIMPLE DE OFERTAS 003.S.S.O.2022

PROPUESTA NO. 1			
PROPONENTE: SIGNOS EDUCACION Y TECNOLOGIA SAS			
REQUISITOS A VERIFICAR	**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
FG-200F: Firewall de Nueva Generación, 18 x GE RJ45 (incluyendo 1 x MGMT port, 1 X HA port, 16 x puertos), 8 x GE SFP slots, 4 ranuras x 10GE SFP+, acelerado por hardware NP6XLite y CP9. Rendimiento de Firewall 27 Gbps, Rendimiento de IPS 5 Gbps, Rendimiento de NGFW (FW + IPS + Control de Aplicaciones) 3.5 Gbps, Rendimiento Protección de amenazas (FW + IPS + Control de Aplicaciones + AntiMalware) 3 Gbps, Rendimiento IPSec VPN 13 Gbps, Soporte de 3 Millones sesiones concurrentes, Rendimiento de Inspección SSL 4 Gbps, Soporte de 500 usuarios VPN SSL, • Rendimiento de VPN SSL 2 Gbps Licenciamiento por 3 años (Antimalware, Sandbox cloud, Filtrado Web, Control de aplicaciones, Sistema de protección contra intrusos), con soporte por 3 años 7/24 con el fabricante. Garantía de 3 años sobre equipos. CANTIDAD: 2	**X**		
FN-TRAN-SX : 1GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots. CANTIDAD: 9	**X**		
FN-TRAN-SFP+SR : 10GE SFP+ transceiver module, short range for	**X**		

all systems with SFP+ and SFP/SFP+ slots. CANTIDAD: 21			
FS-548D-FPOE : Switch tipo Core, capa 3 compatible con controlador desde Firewall perimetral, incluye 48 Puertos PoE+ switch con puertos (48 x GE RJ45, 4 x 10 GE SFP+ and 2 x 40 GE QSFP+), límite de potencia máxima 750W POE . Garantía de tres años sobre equipos. CANTIDAD:2	X		
FS-424E-POE : Switch tipo Distribución, capa 3 compatible con controlador desde Firewall perimetral, incluye 24 Puertos PoE+ switch con puertos (24 x GE RJ45, 4 x 10 GE SFP+), límite de potencia máxima 250W POE. Garantía de tres años sobre equipos. CANTIDAD: 7	X		
Patchcord de FO Multimodo 50/125 m duplex conector LC/PC-LC/PC 3.0 mm de diámetro 3.0 metros de longitud OM3 10 Gbps bota recta corta chaqueta aqua en PVC para uso interior. CANTIDAD: 13	X		
Servicios de integración y configuración de la solución perimetral y actualización de red para cumplimiento de mejores prácticas de configuración y seguridad, incluye configuración de los switch para remplazo de los switch existentes.	X		
Revisión y reconfiguración de la red inalámbrica del Hospital Universitario Departamental de Nariño para el correcto aprovechamiento de las capacidades de la base instalada actualmente.	X		

Instalación 130 metros de fibra óptica 4 hilos (Incluye materiales y mano de obra) Rack principal a rack nutrición.	X		
3 Años de soporte técnico Remoto 7x24 en la ciudad de Pasto, para solución de seguridad perimetral Firewall (NGFW) junto la solución de Switch ofertada	X		
1. Generalidades.			
Adquisición de dos (2) sistema de seguridad informática perimetral e interna que sea del tipo Firewall de Nueva Generación, donde se deberán ofrecer ya incluidas y listas para ser utilizadas, las funcionalidades que se detallan en el presente documento.	X		
La solución debe estar en la capacidad de soportar alta disponibilidad.	X		
El dispositivo debe ser un equipo de propósito específico.	X		
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 trafico	X		
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.	X		
Los firewalls de nueva generación deberán ser la controladora de los switches solicitados en este mismo proceso	X		

	El equipo deberá poder ser configurado en modo Gateway o en modo transparente en la red.	X		
	El equipo debe entregar en tiempo real estadísticas de usuarios, aplicaciones, seguridad. Presentar preferiblemente en formato de drilldown este tipo de información donde sea posible por usuario verificar que aplicaciones, sitios, categorías y amenazas de seguridad se han tenido en un tiempo de 24 horas.	X		
	La plataforma debe tener la capacidad de poder permitir observar el consumo de ancho de banda en tiempo real por usuario, fuente IP, aplicación y páginas web. Con el fin de detectar algún tipo de problema referente a consumos altos de ancho de banda.	X		
	Debe tener la capacidad de generar un widget de visualización, una vez se realiza el filtro de algún tipo de búsqueda especifica	X		
	La solución deberá pertenecer al cuadrante de líder de Gartner para Network Firewalls	X		
	La solución deberá estar calificada como recomendada en el SVM de firewall de NSS LABS	X		
	Los dos dispositivos deben contar con licenciamiento y soporte directo con fabrica por al menos un (1) año	X		
2.	**Rendimiento**			
	El equipo deberá cumplir con las siguientes características mínimas de desempeño ya activas y funcionales:	X		
	• Rendimiento de Firewall 27 Gbps	X		
	• Rendimiento de IPS 5 Gbps	X		
	• Rendimiento de NGFW (FW + IPS + Control de Aplicaciones) 3.5 Gbps	X		
	• Rendimiento Protección de amenazas (FW + IPS +	X		

Control de Aplicaciones + AntiMalware) 3 Gbps			
• Rendimiento IPSec VPN 13 Gbps	X		
• Soporte de 3 Millones sesiones concurrentes	X		
• Rendimiento de Inspección SSL 4 Gbps	X		
• Soporte de 500 usuarios VPN SSL	X		
• Rendimiento de VPN SSL 2 Gbps	X		
3. Conectividad			
Cada equipo deberá contar con las siguientes interfaces de conexión:	X		
• 16 interfaces de 1 Gbps RJ45	X		
• 8 interfaces de 1 Gbps SFP	X		
• 2 interfaces de 10 Gbps SFP+	X		
Aprovisionamiento transceiver:	X		
• 4 Módulos de transceiver de 10 GE SFP+. • 2 Módulos de transceiver de 1 GE SFP	X		
4. Address Traslation			
La plataforma debe soportar lo siguiente tipos de traducción de direcciones:	X		
• NAT y PAT	X		
• NAT estático	X		
• NAT: destino, origen	X		
• NAT, NAT64 persistente	X		
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.	X		
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.	X		
La solución soportará políticas basadas en dispositivo. Esto Significa que podrán definirse políticas de seguridad de acuerdo al dispositivo	X		

	(móvil, laptop) que tenga el usuario. Esta característica no deberá incurrir en ningún tipo de licenciamiento adicional que ocasiones costos adicionales para la entidad.			
	Debe ser posible hacer políticas basados en usuarios, grupos de usuarios y dispositivos sobre una misma política, y ser lo más granular posible en la definición de políticas.	**X**		
	Debe contar con una herramienta de búsqueda de políticas por medio del GUI (Graphical User Interface). que determine cual política procesara un flujo de datos dado (Resaltando la política que coincide), usando distintos parámetros como IP de origen, destino, servicio, protocolo, interface de fuente entre otros	**X**		
	Debe tener la capacidad de generar una advertencia al administrador cuando este configure una política duplicada	**X**		
	Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén predefinidos.	**X**		
	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 la instancias desplegadas en la nube y estas ser usadas como objetos de reglas o políticas de firewall	**X**		
	Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface) como por GUI (Graphical User Interface).	**X**		
	La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP	**X**		
	El dispositivo será capaz de crear e integrar políticas contra ataques DoS	**X**		

	(Denial of service) las cuales se deben poder aplicar por interfaces			
	El dispositivo será capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico.	X		
	Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis.	X		
	Tener la capacidad de utilizar objetos de direcciones para ser utilizados en el enrutamiento con el fin de facilitar la administración y la visibilidad.	X		
	Debe estar en la capacidad de dar estadísticas de uso por políticas como: Ancho de banda actual, Sesiones activas, Ultimo vez usada.	X		
6.	**Conectividad y Enrutamiento**			
	Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.	X		
	Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs.	X		
	Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.	X		
	Soporte a políticas de ruteo (policy routing)	X		
	Soporte a ruteo dinámico RIP V1, V2, OSPF y BGP	X		
	Soporte a ruteo dinámico RIPng, OSPFv3.	X		
	Soporte de ECMP (Equal Cost Multi-Path) o balanceo de enlaces WAN por medio de lo siguiente métodos.	X		
	Sesiones	X		
	IP Fuente	X		
	Volumen	X		
	Spillover	X		
	Soporte de reglas que permitan dirigir un tráfico especifico a través	X		

	de un enlace WAN, ya sea por destino, aplicación (adobe,Facebook,youtube), servicio o fuentes (IP, Usuario)			
	Soporte a ruteo de multicast PIM SM y PIM DM.	X		
	La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow o Netflow.	X		
	La solución podrá habilitar políticas de ruteo en IPv6	X		
	La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6.	X		
	La solución debe contar con una herramienta de búsqueda de rutas por medio del GUI (Graphical User Interface) sobre la tabla de enrutamiento, con el fin facilitar la lectura y control de la tabla de enrutamiento usando parámetros de destino ya sea IP o FQDN	X		
	La Solución deberá soportar balanceado de enlaces WAN inteligente (SD-WAN Seguro) sin licencia adicional basado en:	X		
	Aplicaciones cloud	X		
	SLA	X		
	Mejor calidad de enlace basado en (Jitter, latencia, ancho de banda, perdida de paquetes)	X		
	Integrar en una única interface lógica distintos tipos de enlaces WAN físicos para permitir balanceo de los mismos	X		
7.	**VPN IPSEC**			
	El equipo deberá soportar las siguientes características:	X		
	Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).	X		
	Soporte para IKEv2 y IKE Configuration Method.	X		

	Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES	X		
	Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits	X		
	Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.	X		
	Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.	X		
	Posibilidad de crear VPN's entre gateways y clientes con IPSec. VPNs IPSeC site-to-site y VPNs IPSec client-to-site.	X		
	La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN).	X		
	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.	X		
	Deberá tener la capacidad de crear conexiones VPNs por demanda (ADVPN), con el fin de permitir la fácil gestion de topologías Hub-Spoke y estas puedan convertirse en full-mesh al momento de comunicaciones directas entre Spokes.	X		
8.	**VPN SSL**			
	Capacidad de realizar SSL VPNs por usuarios sin incurrir en costos adicionales.	X		
	Soporte a certificados PKI X.509 para construcción de VPNs SSL.	X		
	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.	X		
	Soporte de autenticación de dos factores con token, la solución debe estar en la capacidad de suplir o	X		

	integrarse con tokens físicos, basados en software, SMS o correo			
	Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.	**X**		
	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.	**X**		
	La VPN SSL integrada deberá soportar a través de algún plug-in ActiveX y/o Java, la capacidad de poner dentro del túnel SSL tráfico que no sea HTTP/HTTPS	**X**		
	Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL	**X**		
	Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente.	**X**		
	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	**X**		
	Los portales personalizados deberán soportar al menos la definición de:	**X**		
	Widgets a mostrar	**X**		
	Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC	**X**		
	Soporte para Escritorio Virtual	**X**		
	Política de verificación de la estación de trabajo	**X**		
	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.	**X**		
9.	**Autenticación**			

	El dispositivo deberá manejar los siguientes tipos de autenticación:	**X**		
	Capacidad de soporta autenticación local y remota integrándose con Servidores de Autenticación RADIUS ,LDAP o TACACS+.	**X**		
	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”.	**X**		
	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.	**X**		
	Soporte autenticación de usuario a través de PKI y certificados.	**X**		
	Capacidad de soportar autenticación de acceso de usuario a través de 802.1x y portal cautivo	**X**		
10.	**Manejo de tráfico y calidad de servicio.**			
	Capacidad de poder asignar parámetros de traffic shapping atreves de reglas de manera independiente	**X**		
	Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión	**X**		
	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.	**X**		
	Capacidad de poder definir ancho de banda garantizado en Kilobits por segundo	**X**		

	Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en Kilobits por segundo	**X**		
11.	**Antimalware**	**X**		
	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	**X**		
	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.	**X**		
	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.	**X**		
	El Antivirus deberá poder configurarse de forma que los archivos que pasan sean totalmente capturados y analizados, permitiendo hacer análisis sobre archivos que tengan varios niveles de compresión.	**X**		
	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.	**X**		
	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.	**X**		

	El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.	**X**		
	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.	**X**		
	El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging).	**X**		
	La solución debe incluir mecanismos para detectar y detener conexiones a redes Botnet y servidores C&C.	**X**		
12.	**Filtrado WEB**	**X**		
	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.	**X**		
	Debe poder categorizar contenido Web requerido mediante IPv6.	**X**		
	La solución debe permitir realizar el filtrado de contenido, tanto realizando reconstrucción de toda la sesión como realizando inspección paquete a paquete sin realizar reconstrucción de la comunicación.	**X**		
	Capacidad de filtrado de scripts en páginas web (JAVA/Active X).	**X**		
	La solución de Filtrado 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	**X**		

funcionalidad se soportará al menos para Google, Yahoo! y Bing.			
Será posible exceptuar la inspección de HTTPS por categoría.	X		
Debe contar con la capacidad de restringir contenido de youtube usando restricción strict o Moderate por medio del perfil de Filtro de Contenido para trafico HTTP, garantizando de manera centralizada, que todas las sesiones aceptadas por una política de seguridad con este perfil, van a poder acceder solamente a contenido Youtube configurado por el administrador de la cuenta, bloqueando cualquier tipo de contenido distinto al permitido	X		
Debe contar con la capacidad de bloquear contenido de youtube usando el Channel ID	X		
La solución debe permitir controlar el acceso a sitios web por medio de palabras o patrones que se encuentren dentro de su contenido.	X		
El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido.	X		
El sistema de filtrado URL debe incluir la capacidad de no solo poner una entrada URL de manera simple si no que también por medio de metacaracteres (Wildcards o regular expressions)	X		
La solución debe poder aplicar distintos perfiles de navegación de acuerdo al usuario que se esté autenticando. Estos perfiles deben poder ser aplicados a usuarios o grupos de usuarios.	X		
La solución debe estar en la capacidad de filtrar el acceso a cuentas de google, permitiendo acceso solo a cuentas corporativas de google.	X		

	El filtrado debe ser sobre tráfico http y https.	X		
13	**Protección contra intrusos (IPS)**	X		
	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.	X		
	Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores.	X		
	Capacidad de detección de más de 7000 ataques.	X		
	Capacidad de actualización automática de firmas IPS mediante tecnología de tipo “Push” (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo “pull” (Consultar los centros de actualización por versiones nuevas)	X		
	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.	X		
	El sistema de detección y prevención de intrusos deberá soportar captar ataques por variaciones de	X		

protocolo y por firmas de ataques conocidos (signature based / Rate base). 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	**X**		
El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios.	**X**		
Métodos de notificación:	**X**		
Alarmas presentadas en la consola de administración del appliance.	**X**		
Alertas vía correo electrónico.	**X**		
Debe tener la capacidad de cuarentena, prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado.	**X**		
La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma “indefinida”, hasta que un administrador tome una acción al respecto.	**X**		
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.	**X**		
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.	**X**		
	La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.	**X**		
	La solución debe tener un listado de al menos 3000 aplicaciones ya definidas por el fabricante.	**X**		
	El listado de aplicaciones debe actualizarse periódicamente.	**X**		
	Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log y resetear conexión	**X**		
	Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.	**X**		
	Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping.	**X**		
	Preferentemente deben soportar mayor granularidad en las acciones.	**X**		
	Debe ser posible inspeccionar aplicaciones tipo Cloud como dropbox, icloud entre otras entregando información como login de usuarios y transferencia de archivos.	**X**		
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	**X**		
	Debe ser posible definir perfiles de inspección SSL donde se definan los protocolos a inspeccionar y el certificado usado, estos perfiles	**X**		

	deben poder ser escogidos una vez se defina la política de seguridad.			
	Debe ser posible definir si la inspección se realiza desde múltiples clientes conectando a servidores (es decir usuarios que navegan a servicios externos con SSL) o protegiendo un servidor interno de la entidad.	**X**		
	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.	**X**		
	Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado.	**X**		
	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	**X**		
	Debe ser posible inspeccionar tráfico SSH funcionalidades como Port-Fortward o X11.	**X**		
16.	**Alta Disponibilidad**	**X**		
	Los dispositivos deberán soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6	**X**		
	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.	**X**		
	Posibilidad de definir al menos dos interfaces para sincronía	**X**		

	El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red.	X		
	Debe ser posible definir interfaces de gestión independientes para cada miembro en un clúster.	X		
	Debe ser posible definir que Firewall Virtual estará activo sobre un miembro del Cluster para hacer una distribución de carga en caso de ser necesario.	X		
	El equipo debe soportar hasta 4 equipos en esquema de HA.	X		
17.	**Visibilidad**	X		
	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.	X		
	Menú tipo dropdown para navegar por la información.	X		
	Visualización de las sesiones top 100	X		
	Mostrar los orígenes del tráfico o usuarios que lo generan.	X		
	Mostrar las aplicaciones y su categorización según riesgo.	X		
	Visibilidad de aplicaciones Cloud usadas por el usuario.	X		
	Visibilidad de Destinos del tráfico.	X		
	Visibilidad de los sitios web más consultados por los usuarios.	X		
	Visibilidad de las amenazas o incidentes que han ocurrido o estén ocurriendo en la red	X		
	En la información de sources, aplicaciones, navegación debe ser posible con un doble-click filtrar la información para ser más específica la búsqueda.	X		
	Se debe ver aplicaciones, sitios, amenazas por cada usuario.	X		
	Se debe ver el ancho de banda que se está consumiendo en tiempo real por cada fuente, destino, sitio web,	X		

	aplicación etc. Con el fin de tener una clara visión del consumo.			
	Deber tener la capacidad de poder validar con que política la sesión se está coincidiendo y un link hacia la misma.	X		
	De las aplicaciones Cloud como Dropbox que permiten compartir archivos, debe ser posible ver que archivos fueron subidos y descargados por los usuarios.	X		
	De aplicaciones de contenido como youtube debe ser posible ver que videos fueron vistos por los usuarios.	X		
	Debe tener la capacidad de generar un diagrama de conexión lógicas. En el cual se visualice la plataforma y los equipos conectados a ella (por medio del tráfico que los mismos generan)	X		
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)	X		
	Interface basada en línea de comando (CLI) para administración de la solución.	X		
	Puerto de consola dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto.	X		
	Comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interface gráfica de usuario como la consola de administración de línea de comandos (SSH)	X		
	El administrador del sistema podrá tener las opciones incluidas de	X		

autenticarse vía usuario/contraseña y vía certificados digitales.			
El equipo ofrecerá la flexibilidad para especificar que los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet, Http o Https.	**X**		
El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.	**X**		
Soporte de SNMP versión 2	**X**		
Soporte de SNMP versión 3	**X**		
Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos	**X**		
Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.	**X**		
Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.	**X**		
Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión.	**X**		
Permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica.	**X**		
Contar con facilidades de administración a través de la interfaz	**X**		

	gráfica como ayudantes de configuración (setup wizard).			
	Contar con la posibilidad de agregar una barra superior (Top Bar) cuando los usuarios estén navegando con información como el ID de usuario, cuota de navegación utilizada, y aplicaciones que vayan en contra de las políticas de la empresa.	**X**		
	Contar con herramientas gráficas para visualizar fácilmente las sesiones en el equipo, incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.	**X**		
19.	**Virtualización**	**X**		
	El dispositivo deberá poder virtualizar los servicios de seguridad mediante “Virtual Systems”, “Virtual Firewalls” o “Virtual Domains”	**X**		
	La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS.	**X**		
	Se debe incluir la licencia para al menos 10 (diez) instancias virtuales dentro de la solución a proveer, de los cuales se deberán configurar como mínimo tres acorde a los requerimientos de la entidad.	**X**		
	Cada instancia virtual debe poder tener un administrador independiente	**X**		
	La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales.	**X**		
	Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red	**X**		
	Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual	**X**		

	Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual.	**X**		
	Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual.	**X**		
	Debe ser posible definir enlaces de comunicación entre los sistemas virtuales sin que el trafico deba salir de la solución por medio de enlaces o conexiones virtuales, y estas conexiones deben poder realizarse incluso entre instancias virtuales en modo NAT y en modo Transparente	**X**		
	Se debe poder ver el consumo de CPU y memoria de cada instancia virtual.	**X**		
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.	**X**		
	La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering debe proveerse por al menos 3 años.	**X**		
	La plataforma es requerida por un periodo de un (3) año en un esquema 7x24 ante el fabricante.	**X**		
	Funcionalidades de Administración • El switch deberá poder aceptar actualizaciones de firmware • Los switches con PoE deberán tener la capacidad de habilitar o deshabilitar la funcion de PoE • Deberá soportar detección y notificación de conflictos de direcciones IP • Deberá soportar administración por IPv4 e IPv6	**X**		

• Deberá soportar Telnet / SSH para acceso a la consola • Deberá soportar HTTP / HTTPS • Deberá soportar SNMP v1/v2c/v3 • Deberá poder configurar su reloj mediante un NTP Server • Deberá contar con una línea de comandos estándar y con interface para configurar via Web • Los switches deben tener la capacidad de ser administrados desde el Next Generation Firewall con el que cuenta la entidad actualmente y con el ofertado en el proceso, con el fin de poder brindar un alto nivel de seguridad. • Deberá soportar actualizaciones de Software por: TFTP/FTP/GUI • Deberá soportar HTTP REST APIs para Configuracion y monitoreo			
Funcionalidades de Alta Disponibilidad • Deberá soportar Multi-Chassis LAG (MCLAG) • Deberá soportar STP sobre Multi-Chassis LAG (MCLAG) **Funcionalidades de Calidad de Servicio** • Deberá soportar priorización de tráfico basada en 802.1p • Deberá soportar priorización de tráfico basada en IP TOS/DSCP • Deberá soportar marcado de tráfico con 802.1p y/o IP TOS/DSCP **Otras Funcionalidades Requeridas** • Deberá soportar Syslog	**X**		

• Los Switches deberán integrarse de forma nativa con la solución de Logs y Reportes con la que cuenta actualmente la entidad. • Debe contar con un sensor de temperatura interno • Debe permitir monitorear la temperatura del dispositivo • Debe soportar QSFP+ low-power mode • Debe soportar Energy-Efficient Ethernet (EEE)			
Funcionalidades específicas de la solución Los switches deberán soportar las siguientes funcionalidades capa 2: ▪ Auto descubrimiento de multiples switches ▪ Stack virtual ▪ Gestión centralizada desde plataforma de gestión o software de gestión para configuración de VLANs, PoE, Link aggregation, spanning tree, LLDP/MED, IGMP Snooping y actualización de software. ▪ Soporte de autenticacion 802.1x. ▪ Soporte de DHCP Snooping, detección de dispositivos, listas negras y blancas de direcciones MAC y control de políticas de usuarios y dispositivos. ▪ Soporte de Sticky MAC, MAC Limit, inspección ARP dinámica, 802.1p, TOS/DSCP. ▪ Gestión a través de SSH, HTTP, HTTPS, SNMP y CLI. ▪ Deberá soportar Link Aggregation estático ▪ Deberá soportar LACP ▪ Deberá soportar Spanning Tree ▪ Deberá soportar Jumbo Frames	**X**		

▪ Deberá soportar Auto-negociacion para la velocidad de los puertos y para Duplex ▪ Deberá soportar el estandar IEEE 802.1D MAC Bridging/STP ▪ Deberá soportar el estandar IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) ▪ Deberá soportar el estandar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) ▪ Deberá soportar la funcionalidad STP Root Guard ▪ Deberá soportar STP BPDU Guard ▪ Deberá soportar Edge Port / Port Fast ▪ Deberá soportar el estandar IEEE 802.1Q VLAN Tagging ▪ Deberá soportar Private VLAN ▪ Deberá soportar el estandar IEEE 802.3ad Link Aggregation con LACP ▪ Deberá poder balancear trafico Unicast/Multicast sobre un puerto trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac) ▪ Deberá soportar el estandar IEEE 802.1AX Link Aggregation ▪ Deberá soportar instancias de Spanning Tree (MSTP/CST) ▪ Deberá soportar el estandar IEEE 802.3x Flow Control con Back-pressure ▪ Deberá soportar el estandar IEEE 802.3 10Base-T ▪ Deberá soportar el estandar IEEE 802.3u 100Base-TX ▪ Deberá soportar el estandar IEEE 802.3z 1000Base-SX/LX ▪ Deberá soportar el estandar IEEE 802.3ab 1000Base-T ▪ Deberá soportar el estandar IEEE 802.3ae 10 Gigabit Ethernet ▪ Deberá soportar el estandar IEEE 802.3 CSMA/CD como			

metodo de acceso y las especificaciones de la capa fisica ▪ Deberá contar con la funcionalidad de Control de Tormentas (Storm Control) ▪ Deberá soportar la creacion de VLANs por MAC, IP y Ethertype-based ▪ Deberá soportar la funcionalidad de Virtual-Wire ▪ Deberá soportar Split Port (QSFP+ breakout to 4xSFP+) ▪ Deberá soportar Time-Domain Reflectometer (TDR) ▪ Deberá soportar 4094 VLANs simultáneas ▪ Deberá soportar IGMP Snooping ▪ Deberá soportar IGMP proxy y querier ▪ Deberá soportar emgency location identifier numbers (ELINs) en LLDP-MED ▪ Deberá permitir la negociación de POE en LLDP-MED ▪ Deberá permitir limitar la cantidad de MACs aprendidas por puerto ▪ Deberá permitir un mínimo de 15 instancias de MSTP ▪ Deberá permitir controlar tormentas de broadcast independientemente en cada puerto ▪ Deberá soportar un mecanismo de detección y prevención de loops ▪ Deberá soportar VLAN Stacking (QinQ) ▪ Deberá soportar SPAN ▪ Deberá soportar RSPAN y ERSPAN Los switches deberán soportar las siguientes funcionalidades capa 3: • Deberá soportar ruteo estático • Deberá soportar RIP v2 • Deberá soportar OSPF v2 • Deberá soportar VRRP			

• Deberá soportar IS-IS • Deberá soportar BGP • Deberá soportar protocolos de ruteo multicast • Deberá soportar Equal Cost Multipath Routing (ECMP) • Deberá soportar Bidirectional Forwarding Detection (BFD) • Deberá soportar DHCP Relay • Deberá soportar DHCP Server			
RFCs Soportados • Deberá soportar el RFC 2571 Architecture for Describing SNMP • Deberá soportar DHCP Client • Deberá soportar el RFC 854 Telnet Server • Deberá soportar el RFC 2865 RADIUS • Deberá soportar el RFC 1643 Ethernet-like Interface MIB • Deberá soportar el RFC 1213 MIB-II • Deberá soportar el RFC 1354 IP Forwarding Table MIB • Deberá soportar el RFC 2572 SNMP Message Processing and Dispatching • Deberá soportar el RFC 1573 SNMP MIB II • Deberá soportar el RFC 1157 SNMPv1/v2c • Deberá soportar el RFC 2030 SNTP	**X**		
Funcionalidades de Seguridad y Visibilidad • Deberá soportar Port Mirroring • Deberá soportar Admin Authentication Via RFC 2865 RADIUS	**X**		

• Deberá soportar el estándar IEEE 802.1x authentication Port-based • Deberá soportar el estándar IEEE 802.1x Authentication MAC-based • Deberá soportar el estándar IEEE 802.1x Guest and Fallback VLAN • Deberá soportar el estándar IEEE 802.1x MAC Access Bypass (MAB) • Deberá soportar el estándar IEEE 802.1x Dynamic VLAN Assignment • Deberá soportar Radius CoA (Change of Authority) • Deberá soportar el estándar IEEE 802.1ab Link Layer Discovery Protocol (LLDP) • Deberá soportar el estándar IEEE 802.1ab LLDP-MED • Deberá soportar Radius Accounting • Deberá soportar EAP pass-through • Deberá soportar detección de dispositivos • Deberá soportar MAC-IP binding • Deberá soportar sFlow • Deberá soportar Flow Export • Deberá soportar ACLs • Deberá soportar múltiples ACLs de ingreso • Deberá soportar scheduling de ACLs • Deberá soportar DHCP Snooping • Deberá soportar listas de servidores DHCP permitidos • Deberá soportar bloqueo de DHCP			

• Deberá permitir Dynamic ARP Inspection (DAI) • Deberá permitir Access VLANs • Deberá permitir tagging de tráfico con VLAN ID mediante ACLs			
1. SERVICIOS PROFESIONALES Y DE SOPORTE Generalidades:			
El oferente deberá entregar todas las soluciones / equipos en los sitios/sedes indicados por la entidad.	**X**		
Instalación, Implementación, configuración y puesta en marcha de las soluciones de seguridad y conectividad ofertadas.	**X**		
El oferente deberá realizar la instalación y configuración de los equipos con personal certificado por el fabricante con el cual se esté presentando.		**X**	No anexa certificado técnico emitido por el fabricante sobre el personal que realizará la implementación
Todas las plataformas deberán ser de propósito específico, no se aceptan soluciones genéricas.	**X**		
El oferente deberá presentar certificación de distribuidor autorizado del fabricante para este proceso. Lo anterior con el fin de garantizar la experiencia en la implementación de las soluciones que requiere la entidad.		**X**	No anexa certificado como proveedor autorizado por el fabricante
2. Implementación y puesta en marcha solución de seguridad	**X**		
El proponente seleccionado deberá entregar implementada y funcionando las soluciones completas, de acuerdo a los requerimientos y políticas.	**X**		
La implementación deberá contemplar: • Planeación de cada una de las actividades, validadas en conjunto con el HOSPITAL DEPARTAMENTAL DE NARIÑO • Configuración y alistamiento del software y firmware del	**X**		

• hardware a la última versión estable aprobada por el fabricante para todas las plataformas. • Afinamiento y estabilización de las plataformas. • Pruebas de Servicio de las plataformas. Entrega de las plataformas a satisfacción del HOSPITAL DEPARTAMENTAL DE NARIÑO			
La entidad requiere que se realicen pruebas / muestras de las plataformas donde se evidencie la correcta configuración y afinamiento de cada plataforma.	**X**		
Equipo Mínimo de Trabajo.			
El oferente debe contar con un equipo mínimo de trabajo para la ejecución del proyecto, el cual debe estar conformado como mínimo por:			
Gerente del Proyecto Profesionales Ingeniero de Sistemas, Electrónico o de Telecomunicaciones con experiencia mínima de 2 años a partir de la emisión de la Tarjeta Profesional y para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986: Cédula de Ciudadanía Tarjeta Profesional Postgrado en Redes de computación o Seguridad de la Información o afines		**X**	No anexa título profesional con experiencia. No anexa tarjeta profesional. No anexa título de postgrado en redes de computación o seguridad de la información.
Ingeniero Implementador Profesionales Ingeniero de Sistemas, Electrónico o de Telecomunicaciones con experiencia mínima de 2 años a partir de la emisión de la Tarjeta Profesional y para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986: Cédula de Ciudadanía Tarjeta Profesional		**X**	No anexa título profesional con experiencia. No anexa tarjeta profesional. No anexa título de postgrado en redes de computación o seguridad de la información.

Postgrado en Redes de computación o Seguridad de la Información o afines. Certificación técnica como Arquitecto de seguridad de redes emitida por el fabricante.			No anexa certificación técnica como arquitecto de seguridad de redes emitida por fabricante

PROPUESTA NO. 2			
PROPONENTE: INGENIERIA TELEMATICA SAS			
REQUISITOS A VERIFICAR	**CUMPLE**	**NO CUMPLE**	**OBSERVACIONES**
FG-200F: Firewall de Nueva Generación, 18 x GE RJ45 (incluyendo 1 x MGMT port, 1 X HA port, 16 x puertos), 8 x GE SFP slots, 4 ranuras x 10GE SFP+, acelerado por hardware NP6XLite y CP9. Rendimiento de Firewall 27 Gbps, Rendimiento de IPS 5 Gbps, Rendimiento de NGFW (FW + IPS + Control de Aplicaciones) 3.5 Gbps, Rendimiento Protección de amenazas (FW + IPS + Control de Aplicaciones + AntiMalware) 3 Gbps, Rendimiento IPSec VPN 13 Gbps, Soporte de 3 Millones sesiones concurrentes, Rendimiento de Inspección SSL 4 Gbps, Soporte de 500 usuarios VPN SSL, • Rendimiento de VPN SSL 2 Gbps Licenciamiento por 3 años (Antimalware, Sandbox cloud, Filtrado Web, Control de aplicaciones, Sistema de protección contra intrusos), con soporte por 3 años 7/24 con el fabricante. Garantía de 3 años sobre equipos. CANTIDAD: 2	**X**		
FN-TRAN-SX : 1GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots. CANTIDAD: 9	**X**		

FN-TRAN-SFP+SR : 10GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots. CANTIDAD: 21	x		
FS-548D-FPOE : Switch tipo Core, capa 3 compatible con controlador desde Firewall perimetral, incluye 48 Puertos PoE+ switch con puertos (48 x GE RJ45, 4 x 10 GE SFP+ and 2 x 40 GE QSFP+), límite de potencia máxima 750W POE . Garantía de tres años sobre equipos. CANTIDAD:2	x		
FS-424E-POE : Switch tipo Distribución, capa 3 compatible con controlador desde Firewall perimetral, incluye 24 Puertos PoE+ switch con puertos (24 x GE RJ45, 4 x 10 GE SFP+), límite de potencia máxima 250W POE. Garantía de tres años sobre equipos. CANTIDAD: 7	x		
Patchcord de FO Multimodo 50/125 m duplex conector LC/PC-LC/PC 3.0 mm de diámetro 3.0 metros de longitud OM3 10 Gbps bota recta corta chaqueta aqua en PVC para uso interior. CANTIDAD: 13	x		
Servicios de integración y configuración de la solución perimetral y actualización de red para cumplimiento de mejores prácticas de configuración y seguridad, incluye configuración de los switch para remplazo de los switch existentes.	x		
Revisión y reconfiguración de la red inalámbrica del Hospital Universitario Departamental de Nariño para el correcto aprovechamiento de las	x		

capacidades de la base instalada actualmente.			
Instalación 130 metros de fibra óptica 4 hilos (Incluye materiales y mano de obra) Rack principal a rack nutrición.	X		
3 Años de soporte técnico Remoto 7x24 en la ciudad de Pasto, para solución de seguridad perimetral Firewall (NGFW) junto la solución de Switch ofertada	X		
21. Generalidades.			
Adquisición de dos (2) sistema de seguridad informática perimetral e interna que sea del tipo Firewall de Nueva Generación, donde se deberán ofrecer ya incluidas y listas para ser utilizadas, las funcionalidades que se detallan en el presente documento.	X		
La solución debe estar en la capacidad de soportar alta disponibilidad.	X		
El dispositivo debe ser un equipo de propósito específico.	X		
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 trafico	X		
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.	X		

	Los firewalls de nueva generación deberán ser la controladora de los switches solicitados en este mismo proceso	X		
	El equipo deberá poder ser configurado en modo Gateway o en modo transparente en la red.	X		
	El equipo debe entregar en tiempo real estadísticas de usuarios, aplicaciones, seguridad. Presentar preferiblemente en formato de drilldown este tipo de información donde sea posible por usuario verificar que aplicaciones, sitios, categorías y amenazas de seguridad se han tenido en un tiempo de 24 horas.	X		
	La plataforma debe tener la capacidad de poder permitir observar el consumo de ancho de banda en tiempo real por usuario, fuente IP, aplicación y páginas web. Con el fin de detectar algún tipo de problema referente a consumos altos de ancho de banda.	X		
	Debe tener la capacidad de generar un widget de visualización, una vez se realiza el filtro de algún tipo de búsqueda especifica	X		
	La solución deberá pertenecer al cuadrante de líder de Gartner para Network Firewalls	X		
	La solución deberá estar calificada como recomendada en el SVM de firewall de NSS LABS	X		
	Los dos dispositivos deben contar con licenciamiento y soporte directo con fabrica por al menos un (1) año	X		
22.	**Rendimiento**			
	El equipo deberá cumplir con las siguientes características mínimas de desempeño ya activas y funcionales:	X		
	• Rendimiento de Firewall 27 Gbps	X		
	• Rendimiento de IPS 5 Gbps	X		

• Rendimiento de NGFW (FW + IPS + Control de Aplicaciones) 3.5 Gbps	X		
• Rendimiento Protección de amenazas (FW + IPS + Control de Aplicaciones + AntiMalware) 3 Gbps	X		
• Rendimiento IPSec VPN 13 Gbps	X		
• Soporte de 3 Millones sesiones concurrentes	X		
• Rendimiento de Inspección SSL 4 Gbps	X		
• Soporte de 500 usuarios VPN SSL	X		
• Rendimiento de VPN SSL 2 Gbps	X		
23. Conectividad			
Cada equipo deberá contar con las siguientes interfaces de conexión:	X		
• 16 interfaces de 1 Gbps RJ45	X		
• 8 interfaces de 1 Gbps SFP	X		
• 2 interfaces de 10 Gbps SFP+	X		
Aprovisionamiento transceiver:	X		
• 4 Módulos de transceiver de 10 GE SFP+. • 2 Módulos de transceiver de 1 GE SFP	X		
24. Address Traslation			
La plataforma debe soportar lo siguiente tipos de traducción de direcciones:	X		
• NAT y PAT	X		
• NAT estático	X		
• NAT: destino, origen	X		
• NAT, NAT64 persistente	X		
25. 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.	X		
La solución debe integrarse con el directorio activo y soportar políticas basadas en identidad. Esto significa que podrán definirse políticas de	X		

	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. Esta característica no deberá incurrir en ningún tipo de licenciamiento adicional que ocasiones costos adicionales para la entidad.	**X**		
	Debe ser posible hacer políticas basados en usuarios, grupos de usuarios y dispositivos sobre una misma política, y ser lo más granular posible en la definición de políticas.	**X**		
	Debe contar con una herramienta de búsqueda de políticas por medio del GUI (Graphical User Interface). que determine cual política procesara un flujo de datos dado (Resaltando la política que coincide), usando distintos parámetros como IP de origen, destino, servicio, protocolo, interface de fuente entre otros	**X**		
	Debe tener la capacidad de generar una advertencia al administrador cuando este configure una política duplicada	**X**		
	Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén predefinidos.	**X**		
	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 la instancias desplegadas en la nube y estas ser usadas como objetos de reglas o políticas de firewall	**X**		
	Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface) como por GUI (Graphical User Interface).	**X**		
	La solución tendrá la capacidad de hacer captura de paquetes por	**X**		

	política de seguridad implementada para luego ser exportado en formato PCAP			
	El dispositivo será capaz de crear e integrar políticas contra ataques DoS (Denial of service) las cuales se deben poder aplicar por interfaces	X		
	El dispositivo será capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico.	X		
	Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis.	X		
	Tener la capacidad de utilizar objetos de direcciones para ser utilizados en el enrutamiento con el fin de facilitar la administración y la visibilidad.	X		
	Debe estar en la capacidad de dar estadísticas de uso por políticas como: Ancho de banda actual, Sesiones activas, Ultimo vez usada.	X		
26.	**Conectividad y Enrutamiento**			
	Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.	X		
	Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs.	X		
	Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.	X		
	Soporte a políticas de ruteo (policy routing)	X		
	Soporte a ruteo dinámico RIP V1, V2, OSPF y BGP	X		
	Soporte a ruteo dinámico RIPng, OSPFv3.	X		
	Soporte de ECMP (Equal Cost Multi-Path) o balanceo de enlaces WAN por medio de lo siguiente métodos.	X		
	Sesiones	X		

	IP Fuente	X		
	Volumen	X		
	Spillover	X		
	Soporte de reglas que permitan dirigir un tráfico especifico a través de un enlace WAN, ya sea por destino, aplicación (adobe,Facebook,youtube), servicio o fuentes (IP, Usuario)	X		
	Soporte a ruteo de multicast PIM SM y PIM DM.	X		
	La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow o Netflow.	X		
	La solución podrá habilitar políticas de ruteo en IPv6	X		
	La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6.	X		
	La solución debe contar con una herramienta de búsqueda de rutas por medio del GUI (Graphical User Interface) sobre la tabla de enrutamiento, con el fin facilitar la lectura y control de la tabla de enrutamiento usando parámetros de destino ya sea IP o FQDN	X		
	La Solución deberá soportar balanceado de enlaces WAN inteligente (SD-WAN Seguro) sin licencia adicional basado en:	X		
	Aplicaciones cloud	X		
	SLA	X		
	Mejor calidad de enlace basado en (Jitter, latencia, ancho de banda, perdida de paquetes)	X		
	Integrar en una única interface lógica distintos tipos de enlaces WAN físicos para permitir balanceo de los mismos	X		
27.	**VPN IPSEC**			
	El equipo deberá soportar las siguientes características:	X		

	Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).	**X**		
	Soporte para IKEv2 y IKE Configuration Method.	**X**		
	Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES	**X**		
	Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits	**X**		
	Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.	**X**		
	Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.	**X**		
	Posibilidad de crear VPN's entre gateways y clientes con IPSec. VPNs IPSeC site-to-site y VPNs IPSec client-to-site.	**X**		
	La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN).	**X**		
	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.	**X**		
	Deberá tener la capacidad de crear conexiones VPNs por demanda (ADVPN), con el fin de permitir la fácil gestion de topologías Hub-Spoke y estas puedan convertirse en full-mesh al momento de comunicaciones directas entre Spokes.	**X**		
28.	**VPN SSL**			
	Capacidad de realizar SSL VPNs por usuarios sin incurrir en costos adicionales.	**X**		
	Soporte a certificados PKI X.509 para construcción de VPNs SSL.	**X**		
	Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado	**X**		

digital además de una contraseña para lograr acceso al portal de VPN.			
Soporte de autenticación de dos factores con token, la solución debe estar en la capacidad de suplir o integrarse con tokens físicos, basados en software, SMS o correo	X		
Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.	X		
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.	X		
La VPN SSL integrada deberá soportar a través de algún plug-in ActiveX y/o Java, la capacidad de poner dentro del túnel SSL tráfico que no sea HTTP/HTTPS	X		
Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL	X		
Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente.	X		
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	X		
Los portales personalizados deberán soportar al menos la definición de:	X		
Widgets a mostrar	X		
Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC	X		
Soporte para Escritorio Virtual	X		
Política de verificación de la estación de trabajo	X		
La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que	X		

	previene contra ciertos ataques además de evitar la divulgación de información.			
29.	**Autenticación**			
	El dispositivo deberá manejar los siguientes tipos de autenticación:	**X**		
	Capacidad de soporta autenticación local y remota integrándose con Servidores de Autenticación RADIUS ,LDAP o TACACS+.	**X**		
	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".	**X**		
	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.	**X**		
	Soporte autenticación de usuario a través de PKI y certificados.	**X**		
	Capacidad de soportar autenticación de acceso de usuario a través de 802.1x y portal cautivo	**X**		
30.	**Manejo de tráfico y calidad de servicio.**			
	Capacidad de poder asignar parámetros de traffic shapping atreves de reglas de manera independiente	**X**		
	Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión	**X**		
	Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la	**X**		

	aplicación y categoría URL de las mismas para la regla en general.			
	Capacidad de poder definir ancho de banda garantizado en Kilobits por segundo	X		
	Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en Kilobits por segundo	X		
31.	**Antimalware**	X		
	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	X		
	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.	X		
	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.	X		
	El Antivirus deberá poder configurarse de forma que los archivos que pasan sean totalmente capturados y analizados, permitiendo hacer análisis sobre archivos que tengan varios niveles de compresión.	X		
	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.	X		
	Antivirus en tiempo real, integrado a la plataforma de seguridad “appliance”. Sin necesidad de	X		

	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.	**X**		
	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.	**X**		
	El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging).	**X**		
	La solución debe incluir mecanismos para detectar y detener conexiones a redes Botnet y servidores C&C.	**X**		
32.	**Filtrado WEB**	**X**		
	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.	**X**		
	Debe poder categorizar contenido Web requerido mediante IPv6.	**X**		
	La solución debe permitir realizar el filtrado de contenido, tanto realizando reconstrucción de toda la sesión como realizando inspección paquete a paquete sin realizar reconstrucción de la comunicación.	**X**		
	Capacidad de filtrado de scripts en páginas web (JAVA/Active X).	**X**		
	La solución de Filtrado de Contenido debe soportar el forzamiento de “Safe Search” o “Búsqueda Segura” independientemente de la	**X**		

	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.			
	Será posible exceptuar la inspección de HTTPS por categoría.	**X**		
	Debe contar con la capacidad de restringir contenido de youtube usando restricción strict o Moderate por medio del perfil de Filtro de Contenido para trafico HTTP, garantizando de manera centralizada, que todas las sesiones aceptadas por una política de seguridad con este perfil, van a poder acceder solamente a contenido Youtube configurado por el administrador de la cuenta, bloqueando cualquier tipo de contenido distinto al permitido	**X**		
	Debe contar con la capacidad de bloquear contenido de youtube usando el Channel ID	**X**		
	La solución debe permitir controlar el acceso a sitios web por medio de palabras o patrones que se encuentren dentro de su contenido.	**X**		
	El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido.	**X**		
	El sistema de filtrado URL debe incluir la capacidad de no solo poner una entrada URL de manera simple si no que también por medio de metacaracteres (Wildcards o regular expressions)	**X**		
	La solución debe poder aplicar distintos perfiles de navegación de acuerdo al usuario que se esté autenticando. Estos perfiles deben poder ser aplicados a usuarios o grupos de usuarios.	**X**		
	La solución debe estar en la capacidad de filtrar el acceso a	**X**		

	cuentas de google, permitiendo acceso solo a cuentas corporativas de google.			
	El filtrado debe ser sobre tráfico http y https.	X		
33.	**Protección contra intrusos (IPS)**	X		
	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.	X		
	Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores.	X		
	Capacidad de detección de más de 7000 ataques.	X		
	Capacidad de actualización automática de firmas IPS mediante tecnología de tipo “Push” (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo “pull” (Consultar los centros de actualización por versiones nuevas)	X		
	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.	X		

El sistema de detección y prevención de intrusos deberá soportar captar ataques por variaciones de protocolo y por firmas de ataques conocidos (signature based / Rate base). Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo.	**X**		
Actualización automática de firmas para el detector de intrusos	**X**		
El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios.	**X**		
Métodos de notificación:	**X**		
Alarmas presentadas en la consola de administración del appliance.	**X**		
Alertas vía correo electrónico.	**X**		
Debe tener la capacidad de cuarentena, prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado.	**X**		
La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma “indefinida”, hasta que un administrador tome una acción al respecto.	**X**		
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.	**X**		

34.	**Control de Aplicaciones**			
	La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.	**X**		
	La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.	**X**		
	La solución debe tener un listado de al menos 3000 aplicaciones ya definidas por el fabricante.	**X**		
	El listado de aplicaciones debe actualizarse periódicamente.	**X**		
	Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log y resetear conexión	**X**		
	Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.	**X**		
	Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping.	**X**		
	Preferentemente deben soportar mayor granularidad en las acciones.	**X**		
	Debe ser posible inspeccionar aplicaciones tipo Cloud como dropbox, icloud entre otras entregando información como login de usuarios y transferencia de archivos.	**X**		
35.	**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	**X**		
	Debe ser posible definir perfiles de inspección SSL donde se definan los protocolos a inspeccionar y el certificado usado, estos perfiles	**X**		

	deben poder ser escogidos una vez se defina la política de seguridad.			
	Debe ser posible definir si la inspección se realiza desde múltiples clientes conectando a servidores (es decir usuarios que navegan a servicios externos con SSL) o protegiendo un servidor interno de la entidad.	**X**		
	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.	**X**		
	Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado.	**X**		
	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	**X**		
	Debe ser posible inspeccionar tráfico SSH funcionalidades como Port-Fortward o X11.	**X**		
36.	**Alta Disponibilidad**	**X**		
	Los dispositivos deberán soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6	**X**		
	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.	**X**		
	Posibilidad de definir al menos dos interfaces para sincronía	**X**		

	El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red	X		
	Debe ser posible definir interfaces de gestión independientes para cada miembro en un clúster.	X		
	Debe ser posible definir que Firewall Virtual estará activo sobre un miembro del Cluster para hacer una distribución de carga en caso de ser necesario.	X		
	El equipo debe soportar hasta 4 equipos en esquema de HA.	X		
37.	**Visibilidad**	X		
	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.	X		
	Menú tipo dropdown para navegar por la información.	X		
	Visualización de las sesiones top 100	X		
	Mostrar los orígenes del tráfico o usuarios que lo generan.	X		
	Mostrar las aplicaciones y su categorización según riesgo.	X		
	Visibilidad de aplicaciones Cloud usadas por el usuario.	X		
	Visibilidad de Destinos del tráfico.	X		
	Visibilidad de los sitios web más consultados por los usuarios.	X		
	Visibilidad de las amenazas o incidentes que han ocurrido o estén ocurriendo en la red	X		
	En la información de sources, aplicaciones, navegación debe ser posible con un doble-click filtrar la información para ser más específica la búsqueda.	X		
	Se debe ver aplicaciones, sitios, amenazas por cada usuario.	X		
	Se debe ver el ancho de banda que se está consumiendo en tiempo real por cada fuente, destino, sitio web,	X		

	aplicación etc. Con el fin de tener una clara visión del consumo.			
	Deber tener la capacidad de poder validar con que política la sesión se está coincidiendo y un link hacia la misma.	X		
	De las aplicaciones Cloud como Dropbox que permiten compartir archivos, debe ser posible ver que archivos fueron subidos y descargados por los usuarios.	X		
	De aplicaciones de contenido como youtube debe ser posible ver que videos fueron vistos por los usuarios.	X		
	Debe tener la capacidad de generar un diagrama de conexión lógicas. En el cual se visualice la plataforma y los equipos conectados a ella (por medio del tráfico que los mismos generan)	X		
38.	**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)	X		
	Interface basada en línea de comando (CLI) para administración de la solución.	X		
	Puerto de consola dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto.	X		
	Comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interface gráfica de usuario como la consola de administración de línea de comandos (SSH)	X		
	El administrador del sistema podrá tener las opciones incluidas de	X		

autenticarse vía usuario/contraseña y vía certificados digitales.			
El equipo ofrecerá la flexibilidad para especificar que los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet, Http o Https.	X		
El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.	X		
Soporte de SNMP versión 2	X		
Soporte de SNMP versión 3	X		
Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos	X		
Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.	X		
Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.	X		
Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión.	X		
Permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica.	X		
Contar con facilidades de administración a través de la interfaz	X		

	gráfica como ayudantes de configuración (setup wizard).			
	Contar con la posibilidad de agregar una barra superior (Top Bar) cuando los usuarios estén navegando con información como el ID de usuario, cuota de navegación utilizada, y aplicaciones que vayan en contra de las políticas de la empresa.	**X**		
	Contar con herramientas gráficas para visualizar fácilmente las sesiones en el equipo, incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.	**X**		
39.	**Virtualización**	**X**		
	El dispositivo deberá poder virtualizar los servicios de seguridad mediante “Virtual Systems”, “Virtual Firewalls” o “Virtual Domains”	**X**		
	La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS.	**X**		
	Se debe incluir la licencia para al menos 10 (diez) instancias virtuales dentro de la solución a proveer, de los cuales se deberán configurar como mínimo tres acorde a los requerimientos de la entidad.	**X**		
	Cada instancia virtual debe poder tener un administrador independiente	**X**		
	La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales.	**X**		
	Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red	**X**		
	Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual	**X**		

	Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual.	**X**		
	Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual.	**X**		
	Debe ser posible definir enlaces de comunicación entre los sistemas virtuales sin que el trafico deba salir de la solución por medio de enlaces o conexiones virtuales, y estas conexiones deben poder realizarse incluso entre instancias virtuales en modo NAT y en modo Transparente	**X**		
	Se debe poder ver el consumo de CPU y memoria de cada instancia virtual.	**X**		
40.	**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.	**X**		
	La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering debe proveerse por al menos 3 años.	**X**		
	La plataforma es requerida por un periodo de un (3) año en un esquema 7x24 ante el fabricante.	**X**		
	Funcionalidades de Administración • El switch deberá poder aceptar actualizaciones de firmware • Los switches con PoE deberán tener la capacidad de habilitar o deshabilitar la funcion de PoE • Deberá soportar detección y notificación de conflictos de direcciones IP • Deberá soportar administración por IPv4 e IPv6	**X**		

• Deberá soportar Telnet / SSH para acceso a la consola • Deberá soportar HTTP / HTTPS • Deberá soportar SNMP v1/v2c/v3 • Deberá poder configurar su reloj mediante un NTP Server • Deberá contar con una línea de comandos estándar y con interface para configurar via Web • Los switches deben tener la capacidad de ser administrados desde el Next Generation Firewall con el que cuenta la entidad actualmente y con el ofertado en el proceso, con el fin de poder brindar un alto nivel de seguridad. • Deberá soportar actualizaciones de Software por: TFTP/FTP/GUI • Deberá soportar HTTP REST APIs para Configuracion y monitoreo			
Funcionalidades de Alta Disponibilidad • Deberá soportar Multi-Chassis LAG (MCLAG) • Deberá soportar STP sobre Multi-Chassis LAG (MCLAG) **Funcionalidades de Calidad de Servicio** • Deberá soportar priorización de tráfico basada en 802.1p • Deberá soportar priorización de tráfico basada en IP TOS/DSCP • Deberá soportar marcado de tráfico con 802.1p y/o IP TOS/DSCP **Otras Funcionalidades Requeridas** • Deberá soportar Syslog	**X**		

• Los Switches deberán integrarse de forma nativa con la solución de Logs y Reportes con la que cuenta actualmente la entidad. • Debe contar con un sensor de temperatura interno • Debe permitir monitorear la temperatura del dispositivo • Debe soportar QSFP+ low-power mode • Debe soportar Energy-Efficient Ethernet (EEE)			
Funcionalidades específicas de la solución Los switches deberán soportar las siguientes funcionalidades capa 2: ▪ Auto descubrimiento de multiples switches ▪ Stack virtual ▪ Gestión centralizada desde plataforma de gestión o software de gestión para configuración de VLANs, PoE, Link aggregation, spanning tree, LLDP/MED, IGMP Snooping y actualización de software. ▪ Soporte de autenticacion 802.1x. ▪ Soporte de DHCP Snooping, detección de dispositivos, listas negras y blancas de direcciones MAC y control de políticas de usuarios y dispositivos. ▪ Soporte de Sticky MAC, MAC Limit, inspección ARP dinámica, 802.1p, TOS/DSCP. ▪ Gestión a través de SSH, HTTP, HTTPS, SNMP y CLI. ▪ Deberá soportar Link Aggregation estático ▪ Deberá soportar LACP ▪ Deberá soportar Spanning Tree ▪ Deberá soportar Jumbo Frames	**X**		

▪ Deberá soportar Auto-negociacion para la velocidad de los puertos y para Duplex ▪ Deberá soportar el estandar IEEE 802.1D MAC Bridging/STP ▪ Deberá soportar el estandar IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) ▪ Deberá soportar el estandar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) ▪ Deberá soportar la funcionalidad STP Root Guard ▪ Deberá soportar STP BPDU Guard ▪ Deberá soportar Edge Port / Port Fast ▪ Deberá soportar el estandar IEEE 802.1Q VLAN Tagging ▪ Deberá soportar Private VLAN ▪ Deberá soportar el estandar IEEE 802.3ad Link Aggregation con LACP ▪ Deberá poder balancear trafico Unicast/Multicast sobre un puerto trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac) ▪ Deberá soportar el estandar IEEE 802.1AX Link Aggregation ▪ Deberá soportar instancias de Spanning Tree (MSTP/CST) ▪ Deberá soportar el estandar IEEE 802.3x Flow Control con Back-pressure ▪ Deberá soportar el estandar IEEE 802.3 10Base-T ▪ Deberá soportar el estandar IEEE 802.3u 100Base-TX ▪ Deberá soportar el estandar IEEE 802.3z 1000Base-SX/LX ▪ Deberá soportar el estandar IEEE 802.3ab 1000Base-T ▪ Deberá soportar el estandar IEEE 802.3ae 10 Gigabit Ethernet ▪ Deberá soportar el estandar IEEE 802.3 CSMA/CD como			

metodo de acceso y las especificaciones de la capa fisica ▪ Deberá contar con la funcionalidad de Control de Tormentas (Storm Control) ▪ Deberá soportar la creacion de VLANs por MAC, IP y Ethertype-based ▪ Deberá soportar la funcionalidad de Virtual-Wire ▪ Deberá soportar Split Port (QSFP+ breakout to 4xSFP+) ▪ Deberá soportar Time-Domain Reflectometer (TDR) ▪ Deberá soportar 4094 VLANs simultáneas ▪ Deberá soportar IGMP Snooping ▪ Deberá soportar IGMP proxy y querier ▪ Deberá soportar emgency location identifier numbers (ELINs) en LLDP-MED ▪ Deberá permitir la negociación de POE en LLDP-MED ▪ Deberá permitir limitar la cantidad de MACs aprendidas por puerto ▪ Deberá permitir un mínimo de 15 instancias de MSTP ▪ Deberá permitir controlar tormentas de broadcast independientemente en cada puerto ▪ Deberá soportar un mecanismo de detección y prevención de loops ▪ Deberá soportar VLAN Stacking (QinQ) ▪ Deberá soportar SPAN ▪ Deberá soportar RSPAN y ERSPAN Los switches deberán soportar las siguientes funcionalidades capa 3: • Deberá soportar ruteo estático • Deberá soportar RIP v2 • Deberá soportar OSPF v2 • Deberá soportar VRRP			

• Deberá soportar IS-IS • Deberá soportar BGP • Deberá soportar protocolos de ruteo multicast • Deberá soportar Equal Cost Multipath Routing (ECMP) • Deberá soportar Bidirectional Forwarding Detection (BFD) • Deberá soportar DHCP Relay • Deberá soportar DHCP Server			
RFCs Soportados • Deberá soportar el RFC 2571 Architecture for Describing SNMP • Deberá soportar DHCP Client • Deberá soportar el RFC 854 Telnet Server • Deberá soportar el RFC 2865 RADIUS • Deberá soportar el RFC 1643 Ethernet-like Interface MIB • Deberá soportar el RFC 1213 MIB-II • Deberá soportar el RFC 1354 IP Forwarding Table MIB • Deberá soportar el RFC 2572 SNMP Message Processing and Dispatching • Deberá soportar el RFC 1573 SNMP MIB II • Deberá soportar el RFC 1157 SNMPv1/v2c • Deberá soportar el RFC 2030 SNTP	**X**		
Funcionalidades de Seguridad y Visibilidad • Deberá soportar Port Mirroring • Deberá soportar Admin Authentication Via RFC 2865 RADIUS	**X**		

• Deberá soportar el estándar IEEE 802.1x authentication Port-based • Deberá soportar el estándar IEEE 802.1x Authentication MAC-based • Deberá soportar el estándar IEEE 802.1x Guest and Fallback VLAN • Deberá soportar el estándar IEEE 802.1x MAC Access Bypass (MAB) • Deberá soportar el estándar IEEE 802.1x Dynamic VLAN Assignment • Deberá soportar Radius CoA (Change of Authority) • Deberá soportar el estándar IEEE 802.1ab Link Layer Discovery Protocol (LLDP) • Deberá soportar el estándar IEEE 802.1ab LLDP-MED • Deberá soportar Radius Accounting • Deberá soportar EAP pass-through • Deberá soportar detección de dispositivos • Deberá soportar MAC-IP binding • Deberá soportar sFlow • Deberá soportar Flow Export • Deberá soportar ACLs • Deberá soportar múltiples ACLs de ingreso • Deberá soportar scheduling de ACLs • Deberá soportar DHCP Snooping • Deberá soportar listas de servidores DHCP permitidos • Deberá soportar bloqueo de DHCP			

• Deberá permitir Dynamic ARP Inspection (DAI) • Deberá permitir Access VLANs • Deberá permitir tagging de tráfico con VLAN ID mediante ACLs			
3. SERVICIOS PROFESIONALES Y DE SOPORTE Generalidades:			
El oferente deberá entregar todas las soluciones / equipos en los sitios/sedes indicados por la entidad.	**X**		
Instalación, Implementación, configuración y puesta en marcha de las soluciones de seguridad y conectividad ofertadas.	**X**		
El oferente deberá realizar la instalación y configuración de los equipos con personal certificado por el fabricante con el cual se esté presentando.	**X**		
Todas las plataformas deberán ser de propósito específico, no se aceptan soluciones genéricas.	**X**		
El oferente deberá presentar certificación de distribuidor autorizado del fabricante para este proceso. Lo anterior con el fin de garantizar la experiencia en la implementación de las soluciones que requiere la entidad.	**X**		
4. Implementación y puesta en marcha solución de seguridad	**X**		
El proponente seleccionado deberá entregar implementada y funcionando las soluciones completas, de acuerdo a los requerimientos y políticas.	**X**		
La implementación deberá contemplar: • Planeación de cada una de las actividades, validadas en conjunto con el HOSPITAL DEPARTAMENTAL DE NARIÑO • Configuración y alistamiento del software y firmware del hardware a la última versión	**X**		

estable aprobada por el fabricante para todas las plataformas. • Afinamiento y estabilización de las plataformas. • Pruebas de Servicio de las plataformas. Entrega de las plataformas a satisfacción del HOSPITAL DEPARTAMENTAL DE NARIÑO			
La entidad requiere que se realicen pruebas / muestras de las plataformas donde se evidencie la correcta configuración y afinamiento de cada plataforma.	**X**		
Equipo Mínimo de Trabajo.			
El oferente debe contar con un equipo mínimo de trabajo para la ejecución del proyecto, el cual debe estar conformado como mínimo por:			
Gerente del Proyecto Profesionales Ingeniero de Sistemas, Electrónico o de Telecomunicaciones con experiencia mínima de 2 años a partir de la emisión de la Tarjeta Profesional y para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986: Cédula de Ciudadanía Tarjeta Profesional Postgrado en Redes de computación o Seguridad de la Información o afines	**X**		
Ingeniero Implementador Profesionales Ingeniero de Sistemas, Electrónico o de Telecomunicaciones con experiencia mínima de 2 años a partir de la emisión de la Tarjeta Profesional y para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986: Cédula de Ciudadanía Tarjeta Profesional	**X**		

Postgrado en Redes de computación o Seguridad de la Información o afines. Certificación técnica como Arquitecto de seguridad de redes emitida por el fabricante.			

CONSOLIDADO EVALUACION REQUISITOS HABILITANTES (CAPACIDAD TECNICA)

No.	**NOMBRES**	**RESULTADO VERIFICACION REQUISITOS HABILITANTES (CAPACIDAD TECNICA)**
01	**SIGNOS EDUCACION Y TECNOLOGIA SAS**	**NO HABILITADO**
OBSERVACIONES:	El Oferente SIGNOS Y EDUACION TECNOLOGIA SAS : -No anexa certificado técnico emitido por el fabricante sobre el personal que realizará la implementación -No anexa certificado como proveedor autorizado por el fabricante -No anexa título profesional con experiencia. -No anexa tarjeta profesional. No anexa título de postgrado en redes de computación o seguridad de la información. -No anexa título profesional con experiencia. -No anexa tarjeta profesional. No anexa título de postgrado en redes de computación o seguridad de la información. -No anexa certificación técnica como arquitecto de seguridad de redes emitida por fabricante	
02	**INGENIERIA TELEMATICA SAS**	**HABILITADO**

Pasto (N), 7 de Febrero de dos mil veintidós (2022)

HENRY LUIS RODRIGUEZ CARDENAS

Profesional Especializado Gestión de la Información

Evaluación Técnica