ANEXO TÉCNICO

Especificaciones Técnicas Detalladas Solución de Seguridad (NGFW)

DESCRIPCION	
1. FIREWALL DE NUEVA GENERACIÓN,	**CUMPLE SI/NO**
1. Generalidades.	
Dispositivo de seguridad informática perimetral de propósito específico con sistema operativo propietario del fabricante tipo Firewall de Nueva Generación.	
Capacidad de soportar alta disponibilidad.	
Contar con tecnología ASIC para permitir acelerar procesos.	
Pertenecer al cuadrante de líder de gartner para Network Firewall	
La solución deberá estar calificada como recomendada en el SVM de firewall de NSS LABS	
2. Rendimiento (mímimo)	
• Firewall 78 Gbps	
• IPS 12 Gbps	
• NGFW (FW + IPS + Control de Aplicaciones) 9,5 Gbps	
• Proteccion de amenazas (FW + IPS + Control de Aplicaciones + AntiMalware) 7 Gbps	
• IPSec VPN 45 Gbps	
• Soporte de 8 Millones sesiones concurrentes	
• Inspección SSL 10 Gbps	
• Soporte de 10000 usuarios VPN SSL	
• Rendimiento de VPN SSL 8 Gbps	
3. Conectividad (mínimo las siguientes interfaces de conexión)	
• 18 interfaces de 1 GE RJ45	
• 8 interfaces de 1 GE SFP	
• 4 interfaces de 10 GE SFP+	
• 4 interfaces de 25 GE SFP28	
• 2 interfaces de 40 GE QSFP+	
4. Aprovisionamiento transceiver para el equipo	
• 8 Módulos de transceiver de 1 GE SFP	
• 8 Módulos de transceiver de 10 GE SFP+	
• 2 Módulos de transceiver de 40 GE QSFP+	
5. Address Traslation (soportar lo siguiente tipos de traducción de direcciones)	
• NAT y PAT	
• NAT estático	
• NAT: destino, origen	
• NAT, NAT64 persistente	
6. Funciones básicas de Firewall	
Analisis por reglas de firewall de las conexiones que pasen por el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.	
Integración con directorio activo y soportar políticas de seguridad basadas en identidad de acuerdo al grupo de pertenencia de los usuarios.	

	Capacidad de generar advertencias sobre configuración de políticas duplicadas	
	Capacidad de integración 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	
	Soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface) como por GUI (Graphical User Interface).	
	Soporte de captura de paquetes por política de seguridad implementada y exportación en formato PCAP	
	Ser capaz de crear e integrar políticas contra ataques DoS (Denial of service) por interface.	
	Ser capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico.	
	Tener la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis.	
7.	**Conectividad y Enrutamiento**	
	Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.	
	Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.	
	Soporte a ruteo dinámico RIP V1, V2, OSPF y BGP	
	Capacidad de habilitar políticas de ruteo en IPv6	
	Capacidad de habilitar ruteo estático para cada interfaz en IPv6.	
	Soporte de balanceado de enlaces WAN inteligente (SD-WAN Seguro) basado en: Aplicaciones cloud, SLA y Mejor calidad de enlace basado en (Jitter, latencia, ancho de banda, perdida de paquetes)	
8.	**VPN IPSEC**	
	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	
	Soporte de longitudes de llave para AES de 128, 192 y 256 bits	
9.	**VPN SSL**	
	Capacidad de realizar SSL VPNs por usuarios.	
	Soporte a certificados PKI X.509 para construcción de VPNs SSL.	
	Soporte de autenticación de dos factores, por certificado digital y contraseña para acceso al portal de VPN.	
10.	**Autenticación**	
	Soporte de autenticación local y remota integrándose con Servidores de Autenticación RADIUS ,LDAP o TACACS+.	
	Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticación transparente bajo “Single-Sign-On”.	
	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.	
	Capacidad de soportar autenticación de acceso de usuario a través de 802.1x y portal cautivo.	
11.	**Manejo de tráfico y calidad de servicio.**	
	Capacidad de poder asignar parámetros de traffic shapping atreves de reglas de manera independiente	

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 y categoría URL de las mismas para la regla en general.	
Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en Kilobits por segundo	
12. Antimalware	
Capacidad de análisis, control de acceso, detención de ataques y antivirus en tiempo real por lo menos de los protocolos: HTTP, SMTP, IMAP, POP3, FTP, MAPI	
Módulo antimalware y firmas propietarias y desarrolladas por el fabricante de la solución no por concesión de terceros por medio de licencias	
Inspección de mínimo las siguientes extensiones de archivos comprimidos: GZIP,RAR,LZH,IHA,CAB,ARJ,ZIP	
Antivirus integrable de forma nativa con una solución sandbox del fabricante de la solución	
13. Filtrado WEB	
Control de sitios de navegación por medio de categorias	
Mínimo 78 categorías de filtros de URLs	
Base de datos de al menos 47 millones de registros clasificados.	
Capacidad de categorización de contenido Web requerido mediante IPv6.	
Posibilidad de exceptuar la inspección de HTTPS por categoría.	
Capacidad de bloquear contenido de youtube usando el Channel ID	
El filtrado debe ser sobre tráfico http y https.	
14. Protección contra intrusos (IPS)	
El sistema de detección y prevención de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror.	
Definición de políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores.	
Capacidad de detección de más de 7000 ataques.	
El sistema de detección y prevención de intrusos y la interfaz de administración debe estar integrado dentro de la solución ofrecida sin necesidad de instalar un servidor o dispositivo externo.	
Permitir el servicio de detección y prevención de intrusos por medio de política de control de accesos.	
Almacenamiento de información sobre el paquete de red que detonó la detección del ataque y al menos cinco paquetes sucesivos con visualización en formato PCAP	
15. Control de Aplicaciones	
Capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.	
La identificación de la aplicación independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.	
Contar con un listado de al menos 3000 aplicaciones ya definidas por el fabricante.	
Permitir, bloquear, registrar en log y resetear conexión para aplicaciones identificadas	
Inspeccionar aplicaciones tipo Cloud como dropbox, icloud entre otras entregando información como login de usuarios y transferencia de archivos.	
16. Inspección de Contenido SSL/SSH	

Soporte de inspección de tráfico que esté siendo encriptado mediante SSL al menos para los siguientes protocolos: HTTP, IMAP, SMTP, POP3 y FTP en su versión segura	
Definición de perfiles de inspección SSL con definición de los protocolos a inspeccionar y el certificado usado.	
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.	
17. Alta Disponibilidad	
Soportar Alta Disponibilidad transparente, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6	
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.	
El equipo debe soportar hasta 4 equipos en esquema de HA.	
18. Visibilidad	
La solución debe estar en la capacidad de visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real en la consola de administración.	
Capacidad de validar con que política la sesión se está coincidiendo y un link hacia la misma.	
De las aplicaciones Cloud como Dropbox que permiten compartir archivos, debe ser posible ver que archivos fueron subidos y descargados por los usuarios.	
19. 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.	
Soporte de al menos 3 servidores de registros de sistema (Syslog) para poder enviar bitácoras a servidores de registro remotos	
Debe tener la capacidad de gestionar todas las políticas de seguridad, además de poder gestionar Switches y APs dentro de una única consola de gestion	
20. Virtualización	
El dispositivo deberá poder virtualizar los servicios de seguridad mediante sistemas virtuales, firewalls virtuales o dominios virtuales	
Soportar hasta 250 instancias virtuales, e incluir la licencia para al menos 10 (diez) instancias virtuales dentro de la solución.	
Cada instancia virtual debe poder tener un administrador independiente	
21. 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.	
La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering debe proveerse por al menos cinco (5) años.	
La plataforma es requerida por un periodo de cinco (5) años en un esquema de soporte 7x24 ante el fabricante.	
Se debe incluir cambio de partes (RMA) con un tiempo máximo de un (1) día para los tiempos de entrega de las partes a cambiar.	

2. PLATAFORMA DE GESTION DE LOGS Y REPORTES.	**CUMPLE**
1. Generalidades	

Dispositivo físico que permita registrar cada transacción de la plataforma de seguridad perimetral de la entidad	
Recolección, preparación y emisión de reporte de eventos, actividades y tendencias ocurridas en la plataforma de seguridad perimetral ofertada.	
Contar con licenciamiento y soporte directo con fabrica por al menos cinco (5) años	
2. Desempeño (mínimo)	
▪ Capacidad de recepción de hasta 100 GB de logs diarios.	
▪ Capacidad de Almacenamiento de 8 Terabytes	
▪ Capacidad de soportar una tasa sostenida de analítica de 2000 logs por segundo.	
▪ 4 interfaces de red de 1 GE de RJ45 o Cobre	
▪ Capacidad de recibir logs hasta de 180 equipos	
3. Funciones Generales	
Visor de tráfico en tiempo real.	
Visor de tráfico histórico.	
Visor personalizado de log de tráfico	
Permitir acceso simultáneo de administración,	
Permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.	
Autenticación de usuarios de acceso a la plataforma via LDAP, Radius y TACACS+	
Contar con la capacidad de crear informes en formato HTML, PDF, XML y CSV	
Capacidad de personalizar la portada de los reportes obtenidos.	
Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.	
Dashboard para operaciones SOC de monitoreo de amenazas de seguridad en la red	
Dashboard para operaciones SOC de monitoreo de comprometimiento de usuarios y uso sospechoso de la web en la red de datos.	
Dashboard para operaciones SOC que monitorea el tráfico en la red de datos.	
Dashboard para operaciones SOC que monitorea el tráfico de aplicaciones y sitios web en la red de datos	
Dashboard para operaciones SOC que monitorea detecciones de amenazas de día cero en la red de datos.	
Dashboard para operaciones SOC que monitorea actividad de endpoints en la red de datos.	
Dashboard para operaciones SOC que monitorea actividad VPN en la red de datos.	
Dashboard para operaciones SOC que monitorea puntos de acceso WiFi y SSIDs	
Soporte de configuración de alta disponibilidad Master/Slave en la capa 3	
Permitir crear incidentes a partir de alertas de eventos para endpoint	
Permitir la integración al sistema de tickets ServiceNow, Amazon S3 y Microsoft Azure	
Permitir respaldar logs en nube publica de Google Cloud	
Soporte de estándar SAML para autenticación de usuarios administradores	
3 Reportes de Next Generation firewall	
Cumplimiento de PCI DSS	
Utilización de aplicaciones SaaS	
Prevención de perdida de datos (DLP)	
VPN	
Sistema de prevención de intrusos (IPS)	
Reputación de cliente	
Análisis de seguridad de usuario	
Análisis de amenaza cibernética	

Diario de eventos e incidentes de seguridad	
Tráfico DNS	
Tráfico de correo electrónico	
Top 10 de Aplicaciones utilizadas en la red	
Top 10 de Websites utilizadas en la red	
Uso de redes sociales	