ANEXO TÉCNICO 1

1		SUMINISTRO DE HARDWARE DE SEGURIDAD PERIMETRAL
1.1	Generalidades	La entidad requiere de la renovación o adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red.
		La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7.
		Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listado ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado. Debe cubrir cinco años de vida útil para el servicio en la Entidad.
		Los equipos NGFW deberán tener soporte vigente de fabrica durante la fecha de contrato del servicio, el soporte del fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware.
		Se deberá proporcionar una cuenta de acceso al portal oficial de soporte del fabricante, donde la Entidad tendrá la potestad de dar seguimiento a los casos abiertos por el oferente.
		Se deberá proporcionar una cuenta de acceso al portal oficial de educación del fabricante, donde la Entidad tendrá la potestad de acceder, de manera gratuita y a demanda y de manera autónoma, a cursos en línea sobre las diversas tecnologías del fabricante.
		La solución ofrecida debe tener un módulo en la nube que permita enriquecer la comprensión de la implementación del firewall. Dentro de las características principales debe: - Evaluar la configuración del firewall e identificar áreas de mejora (políticas de seguridad) - Proporcionar un acceso fácil a los datos de telemetría históricos y en tiempo real del firewall - Detectar problemas del sistema, estado de salud del firewall - Contar con un panel de Adopción que muestre el porcentaje de utilización de las funciones de seguridad adquiridas en el firewall
		Dicha herramienta deberá contemplar la adopción de buenas prácticas en materia de configuración de los diferentes módulos de seguridad de la solución, como mínimo: Control de Aplicaciones, Antivirus/Antimalware, Antispyware/Antibot, IPS, Sandboxing, Filtro Web, DNS Security y Gestión de Logs.
		La herramienta de evaluación de buenas prácticas deberá ser específica para la configuración de los Next Generation Firewall implementados, no se aceptarán portales con guías de usuarios genéricas.
		El oferente deberá ejecutar la evaluación de buenas prácticas de forma periódica por lo menos dos veces durante la vigencia del contrato, con el objetivo de proporcionar un servicio de mejora continua sobre las configuraciones del Next Generation Firewall. La Entidad deberá poder realizar la evaluación de buenas prácticas a libre demanda y de manera autónoma.
		Throughput de Next Generation Firewall de 8.5 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño). En el caso que el fabricante tenga mediciones con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes, deberá garantizar este Throughput con el máximo nivel de inspección del fabricante.
		Throughput de Prevención de Amenazas de 4.5 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, control de amenazas avanzadas de día cero (Sandboxing), DNS Security, Filtro de Archivos, y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar un throughput mínimo medido con el nivel o modo más alto de inspección. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido por la Entidad cuando se vayan habilitando los módulos de seguridad indicados en el modo más alto de inspección.
		No se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, se deberá comprobar el requerimiento de throughput con documentación pública del fabricante adjuntando el link que lo respalde.
		La plataforma de hardware debe soportar mínimo 900,000 sesiones simultaneas y mínimo 100,000 sesiones por segundo nuevas.
		Capacidad de Descifrado de sesiones SSL de al menos 51,000 sesiones concurrentes
		Fuente de energia redundante
		Fuente de energia tipo Hot Swappable
		Flujo de la ventilación de datacenter del estilo “Front-to-back”
		Disco (de estado sólido) interno de 120 GB o superior
		Mínimo 8 interfaces de red 10/100/1000 en cobre, formato RJ45 para tráfico de datos de la red
		Mínimo 6 interfaces de red 1 Gbps en formato SFP para el tráfico de datos de la red
		Mínimo 4 interfaces de red 1/10 Gbps en formato SFP/SFP+ para el tráfico de datos de la red.
		1 (una) interfaz de red tipo RJ45 de 1 Gbps dedicada para administración tipo Fuera de banda (Out of band)
		1 (una) interfaz de tipo consola
		1 Puerto de consola Micro-USB tipo A

		2 puertos control 1 Gbps de alta disponibilidad en formato RJ45 para tráfico de administración
		1 puerto control 10 Gbps de alta disponibilidad en formato SFP/SFP+ para el tráfico de administración.
		Debe poder soportar un mínimo de 5 dominios o sistemas virtuales
		El equipo debe contar de manera nativa con interfaz gráfica web (GUI), Línea de comandos (CLI) e Interfaz de programación de aplicaciones (Rest API)
1.3	Características de red	Capacidad de etiquetas VLAN 802.1Q por equipo/interfaz: 4,094/4,094.
		El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.
		Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).
		Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Descifrado SSL/TLS y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), OSPFv3, QoS, DHCPv6 Relay, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones.
		Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP.
		Permitir NAT de destino basado en dominio en lugar de IP. El equipo deberá ser capaz de balancear el tráfico entrante por esa regla de NAT de destino.
		Soportar DNS Dinámico en las interfaces de red del equipo de seguridad.
		Capacidad de inspeccionar el contenido en túneles GRE, GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el equipo de seguridad sea el punto final del túnel.
		Soportar IPv6 en modos de alta disponibilidad, tanto Activo/Activo como Activo/Pasivo.
		Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas sin necesidad de tener que hacer uso de contextos o dominios virtuales.
1.5	Funcionalidades de Firewall	Control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones.
		Permitir el agendamiento de las políticas de seguridad.
		Debe ser posible especificar en las reglas de seguridad un grupo de objetos basados en IP y/o URL que se alimenten dinámicamente de una fuente externa.
		Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método.
		Permitir añadir un comentario de auditoría cada vez que se cree o se edite la política de seguridad. Cada comentario deberá estar asociado a la versión de la política editada. Esto con el fin de garantizar buenas prácticas de documentación, organización y auditoria.
		Debe permitir realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules).
		Debe mostrar la primera y última vez que se utilizó una regla de seguridad.
		Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.
		Debe mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red.
1.6	Descifrado de tráfico SSL/TLS	Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos.
		Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall.
		Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido
		Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido o emisor no confiable, a pesar de no aplicar descifrado al tráfico SSL/TLS
		Debe soportar certificados que utilice Subject Alternative Name (SAN) y Server Name Indication (SNI).
		Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado, identificados por dominios y wildcards.
		Debe permitir reenviar el tráfico descifrado por una interfaz Port Mirror o Sniffer a un equipo externo al Firewall, como por ejemplo un DLP.
		Capacidad de poder hacer decifrado a por lo menos TLS v1.1, v1.2 y v1.3
		Para los certificados almacenados localmente en el firewall, tiene que ser posible bloquear la posibilidad de exportar de las claves privadas, para evitar un uso indebido por parte de los adminsitradores.
		Debe contar con un dashboard de reportes y logs dedicados a monitorear el tráfico de descifrado SSL/TLS, este dashboard deberá estar disponible en la interfaz gráfica, con el objetivo de identificar rápidamente problemas relacionados con las técnicas de descifrado de tráfico, el mismo debe tener varios estados de troubleshooting y proveer de las herramientas a los administradores para encontrar rápidamente las causas por las cuales se puede producir una falla en el descifrado del tráfico (por ejemplo, informar sobre certificados expirados, claves de cifrado débiles, certificados revocados, cierre de la conexión por parte del cliente, entre otros).

1.7	Identificación y control de aplicaciones	Reconocer por lo menos 4860 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email.
		Debe procesar e inspeccionar aplicaciones que utilicen HTTP/2
		Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de expresiones regulares, firmas u otro mecanismo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389.
		Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado.
		Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.
		Permitir nativamente la creación de firmas personalizadas basadas en expresiones regulares de aplicaciones propietarias desde la interfaz de gestión, sin la necesidad de acción por parte del fabricante.
		Permitir la inserción o modificación de valores en la cabecera HTTP del tráfico de aplicaciones SaaS que pasen por el equipo de seguridad. Con el objetivo de permitir acceder por ejemplo a Office365, Google G Suites para dominios manejados por la organizacion y no otras cuentas de SaaS dentro de esas nubes.
		Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en características de las aplicaciones como: • Tecnología utilizada en las aplicaciones (Client-Server, Browser Based, Network Protocol). • Nivel de riesgo de las aplicaciones. • Categoría y sub-categoría de aplicaciones.
		Aplicaciones que usen técnicas evasivas, utilizadas por malware, como transferencia de archivos y/o uso excesivo de ancho de banda.
		La aplicación de políticas de seguridad debe tener la posibilidad de aplicar reglas específicas a cada aplicación, ejemplo si 2 aplicaciones utilizan el mismo puerto de comunicaciones, se tienen que poder crear 2 políticas de seguridad en las cuales se apliquen controles de seguridad diferentes a cada aplicación.
		Al crear politicas basadas en aplicaciones, si las mismas dependen de otras aplicaciones, la interfaz grafica debe sugerir y permitir agregar las politicas dependientes de la seleccionada, para poder permitir el uso correcto de la aplicacion.
		Debe contar con la posibilidad de un módulo de optimización de políticas, que identifique las aplicaciones que han pasado sobre políticas basadas en puertos o de Capa 4, indicando consumo en Bytes, Hits y Fechas de visualización. Este módulo deberá facilitar la migración de la política de Capa 4 a una política de Capa 7 a través de un wizard.
1.8	Protección ante ataques de denegación de servicio (DoS)	Debe ser posible definir un umbral conexiones por segundo en base para proteger ante diversos tipos de Ataques Flood como SYN Flood, UDP Flood, ICMP Flood, ICMPv6 Flood y Otros ataques basados en Floods de IP
		Para el caso de los SYN Flood debe ser posible utilizar SYN Cookies como medidas de defensa
		La protección contra ataques Flood deberán poder ser aplicadas a una interfaz del Next Generation Firewall o individualmente a uno o más equipos protegidos (por ejemplo, un servidor)
		Deberá permitir configurar límites o umbrales que permitan proteger contra ataques de denegación de servicios como syn flood, escaneo de puertos, inundación udp, inundación icmp, entre otros.
		Debe identificar y bloquear ataques de escaneo de puertos TCP, UDP y Host Sweep, asimismo, debe ser posible definir un umbral definido en eventos por segundo para estos tipos de escaneo
		La protección contra ataques de escaneo deberá permitir definir una lista de excepciones basadas en direcciones IP, a los cuales no se le aplicarán la protección (por ejemplo, en caso de una herramienta de escaneo legítimo)
		Debe proteger contra ataques basado en paquetes IP, como mínimo IP Spoofing, Paquetes Fragmentados, Strict Source Routing, Loose Source Routing, Record Route
		Debe proteger contra ataques basado en paquetes TCP, como mínimo Split Handshake, paquetes TCP SYN y TCP SYN/ACK con datos contenidos durante el handshake, Validación del Three Handshake.
		Debe proteger contra ataques basado en paquetes ICMP, como mínimo paquetes con Ping ID 0, paquetes ICMP fragmentados, paquetes ICMP extensos
		Debe proteger contra ataques basado en paquetes IPv6 e ICMPv6
		Debe contar con un mecanismo que proteja contra la saturación del buffer de paquetes por cada interfaz de datos de la solución
		Debe permitir limitar un número máximo de sesiones que podrán ser generadas hacia un equipo destino, con la finalidad de evitar la saturación de sesiones hacia un equipo protegido.
		Debe permitir reglas de prevención contra ataques DoS de tal forma que se pueda definir la IP, la IP destino, Puertos y regla de protección DoS.
		Se debe poder definir un horario para que automáticamente se aplique la regla de prevención contra ataques DoS
		Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus (Antimalware de red), Antispyware/Antibot
		Capacidad de realizar DNS Sinkhole para la identificación de equipos comprometidos por Spyware en entornos corporativos

1.9	Prevención de amenazas	El Firewall deberá contar con la capacidad de generar firmas de protección de malware generadas en segundos, generadas a partir del análisis de machine learning en linea. De esta manera, se deben poder detener y prevenir los ataques de día cero en línea en tiempo real.
		La solución debe ser capaz de identificar decenas de millones de dominios maliciosos con análisis en tiempo real sin depender de firmas estáticas.
		La solución debe ser capaz de predecir y detener dominios maliciosos de malware basados en algoritmos de generación de dominio (DGA).
		Debe poder clasificar los dominios maliciosos en categorias como: malware, DGA, DNS tunneling, Comando y Control, DNS dinamicos, phising o dominios recientemente registrados.
		Las funcionalidades de IPS, Antivirus y Antispyware/Antibot deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones debido a caducidad de soporte con el fabricante.
		Cuando se utilicen las funciones de IPS, Antivirus y Antispyware/Antibot, el equipamiento debe entregar el mismo performance (no degradar) entre tener 1 única firma de IPS habilitada o tener todas las firmas de IPS, Antivirus y Antispyware habilitadas simultáneamente.
		El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.
		Las firmas deberán estar basadas en patrones del malware y no únicamente en hashes, con el objetivo de detectar malware polimórfico que pertenezca a una misma familia.
		Debe soportar granularidad en las políticas de IPS, Antivirus y Antispyware/Antibot, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de todos esos ítems.
		Debe permitir capturar el paquete de red (en formato PCAP) asociada a la alerta de seguridad.
		Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.
		Permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, HTTP/2, HTTPS, FTP, SMB (versiones 1,2 y 3), SMTP, IMAP y POP3. Deberá tener cobertura tanto en IPv4 como en IPv6 para los protocolos en mención
		Previene ataques utilizando Inteligencia de amenazas global
		Protección contra cargas ocultas en tipos de archivos comunes, como documentos de Microsoft® Office y PDF.
		Debe combinar un motor de prevención de amenazas en tiempo real con una base de datos URL completa y elementos de identificación de aplicaciones para limitar la transferencia no autorizada de datos y archivos y detectar y bloquear una amplia gama de exploits, malware, navegación web peligrosa y objetivos y amenazas desconocidas.
		Debe admitir la conversión de firmas de snort configuradas correctamente. Snort Intrusion Prevention System (IPS) y firmas del Sistema de nombres de dominio (DNS) se puede convertir en listas dinámicas externas.
		Las protecciones IPS incluyen tanto la detección de anomalías como la comparación de firmas, utilizando la coincidencia de patrones con reconocimiento de estado para comprender el orden y la secuencia de llegada de los paquetes.
		Debe proteger la red de amenazas comunes y amenazas persistentes avanzadas (APT)
1.10	Análisis de malware de día cero (Sandboxing)	La solución debe contar con un mecanismo interno basado en ML que permita detectar el malware de día cero que se propaga por la red en tiempo real y sin depender de firmas de antivirus.
		Adicionalmente, la solución propuesta debe incluir la detección de amenazas de día cero complejas a través de una integración con una plataforma Sandboxing.
		El dispositivo debe poder acceder y descargar protecciones contra malware de día 0 en tiempo real.
		En caso se trate de sandbox cloud, deberá ser una nube gestionada en su totalidad por el fabricante y deberá contar con certificación de seguridad y privacidad de datos, como mínimo SOC Tipo 2 o FedRAMP
		La plataforma de Sandboxing podrá ser ofrecido en Nube (Cloud), On-premise o ambos. Como mínimo se requiere que el Sandbox propuesto pueda detectar el malware de día cero en un tiempo no mayor a 5 minutos utilizando la emulación completa de malware en entornos Windows, Linux, Android y Mac.
		Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows 8, Windows 10, Mac OS X, Linux y Android.
		Debe analizar Links/URLs para determinar si es o no malicioso, a pesar de no estar categorizada dentro de la Base de Datos del fabricante.
		Debe proveer información forense sobre las acciones realizadas por el malware y generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware.
		Deberá soportar el análisis de archivos ejecutables (EXE), DLLs, ELF (Linux), archivos comprimidos (ZIP, 7ZIP, RAR) archivos office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), archivos de tipos script (.vbs, .ps1, .js), email link, flash, archivos de MacOSX (mach-o, dmg, pkg) y Android APKs en el ambiente controlado.
		El Next Generation Firewall debe ser capaz de enviar al sandbox de manera automática los archivos sospechosos que se propaguen por los protocolos HTTP, HTTPS, HTTP/2, FTP, SMTP, POP3, IMAP y SMB (versiones 1, 2 y 3). Tanto en IPv4 como en IPv6.
		Debe permitir al administrador la descarga del archivo original analizado por el Sandbox.
		Debe permitir reportar al fabricante eventos que son falso-positivo y falsonegativo en el análisis de malware de día cero a partir de la propia consola de administración.

		Deberá soportar el análisis de archivos ejecutables (EXE), DLLs, ELF (Linux), archivos comprimidos (ZIP, 7ZIP, RAR) archivos office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), archivos de tipos script (.vbs, .ps1, .js), email link, flash, archivos de MacOS (mach-o, dmg, pkg) y Android APKs en el ambiente controlado.
		Permitir la subida de archivos al sandbox de forma manual y vía API.
		Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (no debe usar hypervisores comerciales), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.
		La solución debe realizar el análisis en un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales.
		La capacidad mínima de archivos por minuto que debe poder enviarse a análisis debe ser de 70 archivos.
		La solución debe realizar el análisis en un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales.
1.11	Filtro de contenido Web	Capacidad de poder aplicar técnicas de aprendizaje de maquina (Machine Learning) localmente sobre los NGFW para poder identificar nuevos sitios de phishing, con la capacidad de poder bloquear los mismos.
		Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora)
		Deberá incluir la capacidad de creación de políticas basadas en la visibilidad e identificar el usuario que accede a una URL a través de la integración con servicios de directorio, autenticación vía LDAP, Active Directory, e-Directory y base de datos local.
		Debe soportar un cache local de URLs en el appliance, evitando el delay de comunicación/validación de las URLs
		Debe poseer al menos 78 categorías de URLs, incluyendo las de malware y phishing.
		Debe permitir la creación de categorías personalizadas.
		Debe contar con multi categorías de URL, que permita que un sitio web pertenezca a dos categorías distintas.
		Debe identificar y categorizar los dominios nuevos, menores a 30 días de antigüedad.
		Debe permitir la customización de la página de bloqueo.
		Debe permitir notificar al usuario, mostrándole solo una página de alerta, pero permitiéndole continuar la navegación al site.
		Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de phishing.
1.12	Identificación de usuarios	Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de autenticación vía LDAP, Active Directory, E- Novell directory, Exchange y base de datos local.
		Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente.
		Debe soportar la recepción de eventos de autenticación de controladoras Wireless, dispositivos 802.1x, soluciones NAC, soluciones proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API, así como la lectura mediante WMI a equipos Windows para la identificación de direcciones IP y usuarios.
		Debe permitir la definición de grupos dinámicos de usuarios.
		Debe de permitir la identificación de los usuarios de la red utilizando una variedad de métodos de acceso y sistemas operativos, incluidos Microsoft Windows, Apple iOS, Mac OS, Android y Linux / UNIX.
		Debe de poder leer las direcciones IPv4 o IPv6 de los usuarios desde el encabezado X-Forwarded-For (XFF) en las solicitudes del cliente HTTP cuando el firewall se implementa entre Internet y un servidor proxy que de otro modo ocultaría las direcciones IP del usuario.
		Debe de tener un API para actualizar ID de usuario, así como la capacidad de analizar syslogs para mapeos de ID de usuario.
1,13	Conexiones remotas seguras	Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL.
		La VPN IPSec debe soportar como mínimo: • DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard). • Autenticación MD5, SHA-1, SHA-2. • Diffie-Hellman Group 1, Group 2, Group 5 y Group 14. • Algoritmo Internet Key Exchange (IKEv1 & IKEv2);
		Las VPN deben debera estar en la capacidad o tener disponible en futuras actualizaciones la capacidad de configurar PPK poscuánticas en IKEv2 y se deben basar en el estándar RFC 8784.
		Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.
		Las VPN client-to-site deben poder operar usando el protocolo IPSec o SSL y permitir la conexión por medio de agente instalado en el sistema operativo y soportar una cantidad mínima de 1400 usuarios concurrentes (Para el NGFW del DataCenter Principal).
		Debe permitir crear políticas de control de aplicaciones, IPS, Antivirus, Antispyware para tráfico de los clientes remotos conectados en la VPN client-to-site.
		Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA).

	(VPN)	Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.
		Debe soportat Split Tunel, de tal forma que el tráfico hacia internet no se enrute por la VPN
		Debe permitir los siguientes tipos de conexión del cliente al túnel VPN: • Antes del usuario se autentique en la estación. • Después de la autenticación del usuario en la estación usando Single Sign On (SSO). • Bajo demanda del usuario.
		Debe asignar una IP a cada cliente que se conecte a la VPN en formato IPv4 e IPv6, de forma automática mediante un pool de IP.
		Debe contar con un dashboard gráfico que permita monitorear a los usuarios conectados por VPN.
		El agente de VPN client-to-site debe ser compatible al menos con: Windows 10, Windows 11, MacOS X 10.15 o superior.
		La capacidad de establecer VPN's cliente a sitio con agente debe permanecer funcional para equipos windows y Mac aún con el vencimiento del licenciamiento y soporte.
		Los algoritmos de cifrado capaces de resistir ataques Post-Cuanticos en las VPNs sitio a sitio.
1,14	Administracion	Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta de terceros. La captura de paquetes deberá poder ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino)
		Debe permitir la visualización de los logs del tráfico de red, tráfico malicioso, envíos de archivos al sandbox, filtro web, eventos de sistema
		Debe permitir la visualización de los logs de con información del Usuario y Dirección IP asignada, esto deberá ser visible en la interfaz gráfica
		Debe permitir la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizo, su IP y el horario de la alteración
		Debe ser capaz de enviar los logs vía SNMP Trap, Correo Electrónico, Syslog y HTTP (vía API)
		Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.
		Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables.
		La autenticación deberá estar disponible localmente o integrado con plataformas SAML, Kerberos, RADIUS, TACACS+ y LDAP
		Ante escenarios donde existan dos o más administradores logueados en el Next Generation Firewall, y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.
		Contar con un módulo que permita comparar y que indique específicamente que cambio se hizo a una política de seguridad respecto a una versión anterior de dicha política.
		Debe ser capaz de detectar errores humanos de configuración de reglas de seguridad donde se sobrepongan reglas generales sobre reglas específicas (shadowing rules).
		Debe permitir el almacenamiento de diferentes versiones de archivos de respaldo de configuración (backup).
		Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada.
		Debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema.
		La plataforma de seguridad debe permitir realizar tareas de gestión a través del API basado en XML.
1,15	Proteccion avanzada de DNS	La solución debe ser alimentada por un servicio de inteligencia global capaz de identificar decenas de millones de dominios maliciosos con análisis en tiempo real sin depender de firmas estáticas.
		El servicio de protección de DNS debe poder habilitarse sin modificar la configuracion de DNS de la red local o desviar el trafico DNS a servidores externos.
		la solucion debe ser un servicio que funcione integrado en la platforma de NGFW, sin requerir adicionar hardware adicional y sin impactar el rendimiento del NGFW.
		El servicio de protección de DNS debe alimentarse de telemetría provista por clientes a nivel mundial y más de 30 fuentes de inteligencia de amenazas de terceros.
		La solución debe ser capaz de predecir y detener dominios maliciosos de malware basados en algoritmos de generación de dominio (DGA).
		Debe utilizar machine learning y/o inteligencia artificial para detectar nuevos dominios nunca antes vistos autogenerados por algoritmos DGA
		Debe poseer políticas para bloquear dominios DGA o interrumpir las consultar de DNS a dichos dominios.
		Debe detectar e interrumpir robo de datos ocultos o tunelizados en tráfico DNS
		Debe analizar las consultas de DNS, incluyendo las tasas de consultas y patrones, entropía y frecuencia de n-grams para detectar posibles intentos de tunelización.

		Debe permitir como accion ante peticiones DNS maliciosas: alertar, bloquear las conexiones y ademas responder a la peticion con IP sumidero (sinkhole) con el fin de identificar al usuario/equipo realizando consultas DNS maliciosas.
		Debe poder clasificar los dominios maliciosos en categorias como: malware, DGA, DNS tunneling, Comando y Control, DNS dinamicos, phising o dominios recientemente registrados.
		Debe perimir la accion a tomar dependiendo de la categoria a la que pertenezca el dominio, pudiendo tomar acciones diferentes para cada tipo de categoría.
		La solucion debe brindar el contexto de cada dominio incluyendo historial completo para informar el origen y reputacion de cada dominio.
		Debe brindar analitica de cada consulta DNS: frecuencia de visita, marca de tiempo, informacion del DNS pasiva, WHOIS y cualquier etiqueta de malware asociada.