ANEXO No. 11
ANEXO TÉCNICO
ESPECIFICACIONES TÉCNICAS

Las especificaciones técnicas mínimas de obligatorio cumplimiento para ADQUISICIÓN DE UN DISPOSITIVO NGFW, CON SU RESPECTIVO LICENCIAMIENTO, SOPORTE ESPECIALIZADO PARA PUESTA EN FUNCIONAMIENTO, ACTUALIZACIONES Y SOPORTE TÉCNICO DE FABRICA PARA EL INSTITUTO DE CASAS FISCALES DEL EJÉRCITO y que deberá comprometerse a cumplir el proponente con su oferta, las cuales de definen a continuación:

Se requiere que el Instituto de Casas Fiscales del Ejército contrate con una persona natural o jurídica que esté en la capacidad de brindar los servicios para la "ADQUISICIÓN DE UN DISPOSITIVO NGFW, CON SU RESPECTIVO LICENCIAMIENTO, SOPORTE ESPECIALIZADO PARA PUESTA EN FUNCIONAMIENTO, ACTUALIZACIONES Y SOPORTE TÉCNICO DE FABRICA PARA EL INSTITUTO DE CASAS FISCALES DEL EJÉRCITO"**.**

CARACTERÍSTICAS DEL DISPOSITIVO.

NOTA: Los proponentes deben manifestar en la carta de presentación de la oferta su aceptación y compromiso con el cumplimiento de todas y cada de las características del servicio indicadas a continuación y denominadas **Servicios mínimos requeridos.**

5.2.1 SOLUCIÓN FIREWALL NGFW
2.1.1.1 Descripción General de la solución: Adquisición de una solución Firewall de protección de redes, superior a UTM y con características de Next Generation Firewall (NGFW) para la seguridad de la red de la Entidad. La solución se requiere con capacidad de operación en alta disponibilidad, se entiende por alta disponibilidad, poder contar con por lo menos 2 (dos) appliances con las mismas características mínimas mencionadas en estas especificaciones; aunque, en este proceso de adquisición solo se comprará un único equipo appliance, la capacidad de alta disponibilidad se exige, en caso de que a futuro la entidad requiera adquirir un segundo dispositivo. El fabricante debe pertenecer al cuadrante de líderes de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales" en los últimos 5 reportes. El fabricante deberá tener una efectividad de seguridad mayor o igual al 97% según el último reporte de NSS Labs para Next Generation Firewall.

El fabricante debe estar certificado por USGv6 para trabajar IPv6 tanto en Firewall como en IPS.

La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7.

Para efectos de la propuesta, ninguno de los modelos ofertados podrán estar listados ni anunciados 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.

El equipo NGFW deberá tener soporte vigente de fábrica mínimo por tres años a partir la fecha de su instalación, 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. Asimismo, el soporte del fabricante deberá brindar herramientas de evaluación de configuraciones del NGFW alineadas a las buenas prácticas de la industria y propuestas por el fabricante.

Se deberá proporcionar a la Entidad una cuenta de acceso al portal oficial de soporte del fabricante, donde esta tendrá la potestad de dar seguimiento a los casos abiertos por el Oferente, sobre requerimientos de servicio para el dispositivo.

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, a cursos en línea sobre las diversas tecnologías del fabricante.

El servicio deberá incluir al menos una evaluación de buenas prácticas de implementación, la cual deberá ser dirigida por un personal /empleado propio del fabricante de la solución NGFW. Esta evaluación deberá validar el nivel de adopción de buenas prácticas de configuración del NGFW implementado en la Entidad; se deberá entregar un informe con las recomendaciones técnicas para mejorar la configuración del equipo NGFW. Esta evaluación se deberá realizar antes de la finalización del contrato y posteriormente a la implementación del NGFW y previa coordinación entre la Entidad y el Oferente**.**

El proponente debe contar con un software de mesa de ayuda (helpdesk) licenciado, en el cual se reportarán todos los eventos o requerimientos por parte de la entidad y así llevar

trazabilidad y control del tiempo utilizado en la solución de los problemas para garantizar oportunidad en el servicio, en razón a los acuerdos de nivel de servicio acordados.

Como parte de la oferta, el oferente debe responsabilizarse del proceso de migración de la máquina que actualmente posee el Instituto, y garantizar el correcto funcionamiento de todas las reglas y aplicaciones, realizando pruebas a los servicios para validar su puesta en marcha.

2.1.1.2 Especificaciones Técnicas Mínimas:

ITEM	DESCRIPCIÓN	ESPECIFICACIONES TÉCNICAS
01	**Dispositivo NGFW**	• Throughput de Next Generation Firewall de 2.9 Gbps medido con tráfico real (transacciones http 64KB o transacciones usando tráfico mixto de aplicaciones similar a un tráfico empresarial). No se aceptarán mediciones hechas con tráfico UDP o bajo el marco de RFCs no actualizados como los 3511, 2544, 2647 o 1242, o empleando tráfico mixto que no especifique tamaño de transacciones o paquetes. • "Throughput de Threat Prevention de 1.6 Gbps medido con tráfico de real (transacciones http 64KB o transacciones usando tráfico mixto de aplicaciones similar a un tráfico empresarial), con las siguientes funcionalidades habilitadas simultáneamente: Firewall con clasificación y control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Anti-malware de red, Antispyware (o AntiBot), control de amenazas avanzadas de día cero (Sandboxing), control de archivos y logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el nivel o modo más alto de inspección. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o empleando tráfico mixto que no especifique tamaño de transacciones o paquetes. • 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 hasta 300.000 sesiones simultaneas y 51.000 sesiones por segundo • Capacidad de descifrado de sesiones SSL de al menos 38.400 sesiones concurrentes • Fuente de energía redundante • Disco interno de 128 GB • El equipo debe permitir ser configurado en modo gateway o en modo transparente en la red.

		• Para la solución, NO se aceptan sistemas de propósito general (PCs o servidores) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux. • Todos los componentes del sistema: procesador, tarjeta principal y en general el conjunto electrónico debe ser de propósito específico. • Este hardware debe contar con una garantía mínima de (3) tres años por parte del fabricante. Rendimiento • firewall throughput 2.9 Gbps. • Rendimiento de Threat Prevention 1.6 Gbps • Rendimiento IPSec 2.2 Gbps. • Túneles IPSec VPN Gateway-to-Gateway 2.800. • Túneles IPSec VPN Client-to-Gateway 2.800. • Soporte de 51.000 sesiones nuevas por segundos concurrentes. • Soporte a mínimo 200 usuarios VPN SSL. Conectividad • Mínimo 8 interfaces 10/100/1000 (RJ-45). Estas interfaces deben poderse configurar a elección como interfaces WAN. • 1 (una) interfaz de tipo consola • 1 Puerto de consola Micro-USB tipo A • Capacidad mínima de 5 instancias de footing virtuales • Capacidad mínima de 100 zonas de seguridad • Capacidad de etiquetas VLAN 802.1Q por equipo/interfaz: 4,094/4,094 • El equipo debe contar de manera nativa con interfaz gráfica web (GUI), Línea de comandos (CLI) e Interfaz de programación de aplicaciones (Rest API) Características Generales • 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 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. • Soportar túneles GRE como punto inicio o finalización del túnel. • 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 permitir el bloqueo de ataques de Denegación de Servicio (DoS), definiendo un umbral máximo de conexiones por segundo por tipo de paquete (SYN, ICMP, UDP). • 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. Manejo de tráfico y calidad de servicio • 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 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. • Soportar túneles GRE como punto inicio o finalización del túnel. • 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 permitir el bloqueo de ataques de Denegación de Servicio (DoS), definiendo un umbral máximo de

		conexiones por segundo por tipo de paquete (SYN, ICMP, UDP). • 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. Funciones básicas del 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. • Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método. • Permitir añadir un comentario de auditoria cada vez que se haga un cambio o se edite la política de seguridad. Cada comentario deberá estar asociado a la versión de la política editada. • Al crear o editar políticas de seguridad, se debe poder forzar el uso de una descripción, tag o comentario de auditoria. 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 contar con mecanismos que faciliten la optimización de reglas de seguridad: • - Mostrar la primera y última vez que se utilizó una regla de seguridad • - Mostrar a través de un filtro, las reglas de seguridad que no han tenido uso desde un período definido. VPN • La solución debe estar en capacidad de establecer hasta doscientos (200) túneles de VPN SSL • Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL. • La VPN IPSec debe soportar como mínimo: o DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard) o Autenticación MD5, SHA-1, SHA-2; o Diffie-Hellman Group 1, Group 2, Group 5 y Group 14; o Algoritmo Internet Key Exchange (IKEv1 & IKEv2);

		• 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. • 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). • 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 soportar 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: o Antes del usuario se autentique en la estación; o Después de la autenticación del usuario en la estación usando Single Sign On (SSO); o 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. Autenticación • 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 poder monitorear eventos de login y logout del Active Directory utilizando el protocolo WinRM. • Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive

		Portal). Adicionalmente se podrá añadir un segundo factor de autenticación. • Debe permitir la definición de grupos dinámicos de usuarios. • Debe soportar la identificación de múltiples usuarios conectados en una misma dirección IP en ambientes Citrix y Microsoft Terminal Server. • 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. Filtrado Web • 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 60 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. • 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.

		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. • La medida de defensa contra ataques Flood deberán basarse en mecanismos de early drop o random early detection. • 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). • La protección contra ataques Flood deberá permitir definir al menos 3 tipos de umbrales, el primero para generar una alerta al administrador, el segundo para activar la protección y el tercero para restringir el acceso en su totalidad en base a dicha política de DoS. • 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 alertar el ataque, activar la protección bloqueando la IP que supera el umbral definido y adicionalmente definir un tiempo de bloqueo. • 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 proteger contra ataques basados en protocolos No-IP en interfaces Layer 2 (como Appletalks, Banyan, VINES, Novell, SCADA y otros), la solución deberá soportar la definición de protocolos a ser aceptados en base al formato Ethertype (Hex). • 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 y grupo de usuario origen, 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 Control de Aplicaciones • Reconocer por lo menos 3000 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 a través de expresiones regulares firmas de aplicaciones conocidas por los fabricantes independiente del puerto y protocolo. 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 poder permitir acceder por ejemplo a Office365, Google G Suites para dominios manejados por la organización y no otras cuentas de SaaS dentro de esas nubes. • Aplicaciones que usen técnicas evasivas, utilizadas por malware, como transferencia de archivos y/o uso excesivo de ancho de banda. • Las políticas de seguridad tienen que poder ser creadas en base a las aplicaciones y no en base a puertos TCP/UDP. • La aplicación de seguridad tiene que ser 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación, ejemplo si 2 aplicaciones utilizan el mismo

		puerto de comunicaciones, se tienen que poder crear 2 politicas de seguridad en las cuales se apliquen controles de seguridad diferentes a cada aplicación. • Debe poder identificar y crear políticas de aplicaciones de redes industriales (Redes OT), como ser Scada, modbus, dnp3, iccp, opc, siemens, etc • Debe poder permitirse granularidad de aplicaciones de redes industriales, es decir, en las aplicaciones de este tipo de redes poder identificar acciones como lectura, escritura, apertura, llamadas, etc • Al crear políticas basadas en aplicaciones, si las mismas dependen de otras aplicaciones, la interfaz gráfica debe sugerir y permitir agregar las políticas dependientes de la seleccionada, para poder permitir el uso correcto de la aplicación. • Debe contar con 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. Inspección de contenido SSL • 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 permitir los algoritmos de cifrado para negociar la conexión SSL/TLS, deberá soportar como mínimo los siguientes: RSA, DHE, ECDHE, 3DES, AES-128-GCM, AES-128-CBC, AES-256-GCM, AES-256-CBC, CHACHA20-POLY1305, MD5, SHA1, SHA256, SHA384. • Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido. • Debe poder bloquear las sesiones cuyo certificado no es válido o el emisor no es confiable a pesar de no aplicar descifrado al tráfico SSL/TLS • Debe soportar certificados que utilice Subject Alternative Name (SAN). • 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 Snnifer a un equipo externo al Firewall, como por ejemplo un DLP. • Debe permitir cifrar la comunicación entre dos Firewall de HA durante la sincronización de las configuraciones. • Capacidad de poder hacer descifrado 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 las claves privadas, para evitar un uso indebido por parte de los administradores. • La solución tiene que 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 tiene que tener varios estados de trobleshooting y proveer de las herramientas a los administradores para encontrar rápidamente las causas por las cuales se puede producir una falla en la descifrado del tráfico (ej.: informar sobre certificados expirados, claves de cifrado débiles, certificados revocados, cierre de la conexión por parte del cliente, entre otros). Prevención de amenazas • Para seguridad del ambiente contra ataques, el dispositivo de seguridad debe poseer módulo de IPS (Intrusión Prevention System), Antivirus (Antimalware de red), Anti-Spyware (o Antibot) • Capacidad de realizar DNS Sinkhole para la identificación de equipos comprometidos por Spyware en entornos corporativos • Las funcionalidades de IPS, Antivirus y Anti-Spyware 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, 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. • Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, 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. • Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto. • Capacidad de inspeccionar malware que se distribuye por SMB v3 en IPv6. • 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 permitir ver las aplicaciones en su red y aprender cómo funcionan, sus características de comportamiento y su riesgo relativo. Las aplicaciones y las funciones de la aplicación se identifican a través de múltiples técnicas, incluidas las firmas de la aplicación, el descifrado (si es necesario), protocolo de decodificación y heurística. • 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 deben incluir tanto la detección de anomalías como la coincidencia de firmas, utilizando la coincidencia de patrones con 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). • Debe detectar patrones en el cuerpo del archivo que se pueden usar para identificar variaciones futuras de los archivos, incluso si el contenido se ha modificado ligeramente (polimorfo). Alta disponibilidad • Soporte a configuración de alta disponibilidad Activo/Pasivo y Activo/Activo, con despliegues de los equipos tanto en modo transparente como en modo capa 3 (L3). • La configuración en alta disponibilidad debe sincronizar: Sesiones; Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QoS y objetos de red; Certificados de descifrado. • El HA (modo de Alta-Disponibilidad) debe posibilitar monitoreo de fallo de enlaces. • Para la funcionalidad de HA y Clustering no debe requerirse de dispositivos o software externos a los NGFW. • Se debe poder crear clusters de más de dos dispositivos para la sincronización de sesiones. Esta funcionalidad no debe requerir licenciamiento.

		• La funcionalidad de clustering debe permitir incorporar al mismo tiempo dispositivos independientes, así como dispositivos configurados en HA. Consola de administración y monitoreo • Debe ser administrado por una consola web que pueda trabajar en varios idiomas, como mínimo inglés y español. • La administración del equipo, gestión de reportes y gestión de logs deben contar con recursos dedicados de CPU, Memoria RAM y Disco Duro, ya sea integrado dentro del mismo appliance u otro appliance independiente del mismo fabricante. • Permitir exportar las reglas de seguridad en formato CSV y PDF. • Debe contar con un dashboard que permita monitorear las sesiones y CPU del equipo Firewall, estado de las interfaces, versión de firmware y última fecha de actualización de la base de datos de las firmas de seguridad. • Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad de los usuarios VPN. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad. • Debe contar con un dashboard interactivo y gráfico que permita monitorear el tráfico asociado a amenazas de seguridad como malware, spyware, exploits, análisis de malware de día cero, acceso a dominios maliciosos, aplicaciones que no utilizan puerto estándar. Esta información podrá ser filtrada en base a un rango de tiempo, IP, usuario, país y regla de seguridad. • Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. 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 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. Análisis de malware de día cero • El dispositivo de seguridad debe ser capaz de enviar archivos transferidos de forma automática para análisis en una plataforma de tipo sandbox, la cual podrá ser en versión nube o appliance on-premise. • 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 . • El dispositivo debe contar con un motor de machine learning para contener malware de día 0, sin depender de firmas. • La plataforma de Sandboxing deberá tener capacidades robustas para entornos de altos requerimientos de

		ciberseguridad. 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. • En caso de tratarse de Sandbox Cloud, el NGFW deberá tener la capacidad de enviar como mínimo 75 archivos desconocidos por minuto para ser analizados en nube. El Sandbox OnCloud deberá emular los archivos sospechosos en entornos Windows, Linux, Android y Mac sin estar limitado a una capacidad de hardware ni VMs (Virtual Machines). • Debe soportar la inspección de archivos que viajen por los protocolos HTTP, HTTP/2, HTTPS, FTP, SMTP, POP3, IMAP y SMB (versiones 1, 2 y 3). Deberá tener cobertura tanto en IPv4 como en IPv6 • Debe proveer información forense sobre las acciones realizadas por el malware y generar automáticamente las firmas de Antivirus y bloquear el acceso a las URLs maliciosas utilizadas por el malware. • Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración. • 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. • Capacidad de poder aplicar técnicas de aprendizaje de maquina (Machine Learning) localmente sobre los NGFW para poder identificar amenazas desconocidas y bloquear la mismas durante la descarga de los archivos por parte de los usuarios. Filtro de datos • Los archivos deben ser identificados por extensión y firmas. • Permite identificar y opcionalmente prevenir la transferencia (subida o bajada) de varios tipos de archivos (incluidos MS Office, PDF, PE, APK, Flash, DLL, BAT, CAB, PIF, REG, archivos comprimidos en RAR, ZIP u otro) identificados sobre aplicaciones. • Permitir identificar y opcionalmente prevenir la transferencia de información sensible basados en el contenido del archivo, incluyendo, más no limitando al número de tarjetas de crédito; y permitiendo la creación de nuevos tipos de datos vía expresión regular. Calidad de servicio (QOS) • Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube o Netflix por ejemplo), se requiere que la solución tenga la capacidad

		de controlarlas por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones. • Soportar la creación de políticas de QoS por: dirección de origen y destino, por usuario y grupo de LDAP/AD, por aplicaciones, por puerto. • El QoS debe permitir la definición de clases por: ancho de banda garantizado, ancho de banda máximo, prioridad. • Soportar marcación de paquetes DSCP, inclusive por aplicaciones; • Permitir el monitoreo en tiempo real del tráfico gestionado por el QoS.
2	**Subscripción de licenciamiento con el fabricante**	• Se requiere una subscripción de licenciamiento equivalente a: Enterprise Subscription Bundle (Advanced Threat Prevention, Advanced URL Filtering, Wildfire, DNS Security, SD-WAN, IOT Security and SaaS Security Inline), **por un término de 3 años (36 meses).**
3	**Subscripción de Soporte con el fabricante**	• Se requiere una subscripción de soporte con el fabricante equivalente a Partner enabled premium support, **por el termino de 3 años (36 meses).**

REQUISITOS DE GESTIÓN AMBIENTAL (para la ejecución)

No	REQUISITO	SOPORTES
1	Recolectar los residuos generados durante los trabajos de instalación y/o mantenimiento, y entregarlos al ICFE por intermedio del supervisor o administrador del conjunto, para que se haga la respectiva disposición final.	Acta de entrega de residuos (Formato ICFE)

2.1.2 REQUISITOS HABILITANTES	
2.1.2.1	El proponente debe presentar para el proceso de evaluación, las certificaciones de experiencia correspondientes a la prestación de servicios de **SUMINISTRO Y SOPORTE TECNICO DE EQUIPOS DE SEGURIDAD FIREWALL, UTM y/o NGFW**.
2.1.2.2	El proponente debe contar con un software de mesa de ayuda (helpdesk) licenciado, en el cual se reportarán todos los eventos o requerimientos por parte de la entidad y así llevar trazabilidad y control del tiempo utilizado en la solución de los problemas para garantizar oportunidad en el servicio, en razón a los acuerdos de nivel de servicio acordados.

2.1.2.3	El proponente debe presentar para el proceso de evaluación, una certificación como Partner Autorizado por parte del fabricante del equipo ofrecido en la solución ofertada al ICFE.
2.1.2.4	El proponente debe presentar las siguientes certificaciones del fabricante del dispositivo NGFW: 1. Evidencia de que el fabricante pertenece al cuadrante de líderes de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales" en los últimos 5 reportes. 2. Evidencia de que el fabricante tiene una efectividad de seguridad mayor o igual al 97% según el último reporte de NSS Labs para Next Generation Firewall. 3. Evidencia de que el fabricante está certificado por USGv6 para trabajar IPv6 tanto en Firewall como en IPS.

El oferente con la firma se compromete a cumplir con las especificaciones técnicas establecida en el presente Anexo.

_____

Firma Proponente
Nombre:
Documento Identidad: