**ESPECIFICACIONES TÉCNICAS**

| **ITEM:**  **1.1** | **DENOMINACIÓN DEL EQUIPO:**  **Firewall de Ultima Generación para Perímetro Empresarial** | **ESPECIFICACIONES TÉCNICAS REQUERIDAS** | **ESPECIFICACIONES TECNICAS DEL BIEN OFERTADO** | **MODELO Y/O MARCA** | **PAÍS DE ORIGEN** |
| --- | --- | --- | --- | --- | --- |
| **Lote I: Infraestructura de Firewall de Ultima Generación (NGFW)**  **Nota: Colocar en el recuadro especificaciones técnicas del bien ofertado, el detalle del requerimiento ofertado junto al número de página dentro de la oferta o manual del fabricando donde se encuentra o especifica dicha información.** | | | | | |
|  |  | Se requieren **dos (2) Firewalls de última generación** o NGFW, ambos instalados en el perímetro de la red empresarial del Ministerio e instalados bajo el esquema de alta disponibilidad (Modos: activo/activo, activo/pasivo). |  |  |  |
| El NGFW de contar con un motor de ML para prevención de amenazas desconocidas en tiempo real 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. |  |  |  |
| La solución debe permitir la detección de amenazas de día cero complejas a través de una integración con una plataforma Sandboxing. Al mismo tiempo, el dispositivo debe poder acceder y descargar protecciones generadas por el Sandbox contra malware de día 0 en tiempo real. |  |  |  |
| Se debe contar con un módulo de optimización de políticas integrado directamente en el NGFW (sin necesidad de añadir componentes adicionales), 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. Con el fin de facilitar la migración de la política de Capa 4 a Capa 7. |  |  |  |
| Incorporar la capacidad de reconocer las aplicaciones que operan en la red, sin importar el puerto utilizado, el protocolo empleado, las técnicas de evasión aplicadas o el tipo de cifrado, ya sea TLS o SSL. |  |  |  |
| Al crear políticas basadas en aplicaciones, si las mismas dependen de otras aplicaciones para su funcionamiento correcto, la interfaz gráfica debe mostrar y permitir agregar las aplicaciones necesarias. |  |  |  |
| Integrar la capacidad de inspeccionar completamente la carga útil de las aplicaciones, incluyendo archivos y patrones de datos, con el objetivo de detectar y bloquear contenido malicioso, así como impedir intentos de exfiltración de datos |  |  |  |
| La solución debe ser capaz de identificar cuando un usuario ingrese credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de phishing. |  |  |  |
| Habilitar la visibilidad de la actividad vinculada a usuarios y grupos específicos, más allá de direcciones IP individuales, permitiendo la aplicación de políticas de seguridad, la generación de informes detallados y la realización de análisis forenses sobre dichas entidades |  |  |  |
| 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 definir multiples grupos de usuarios dinámicos para tomar medidas de seguridad temporales sin esperar a que se aplique ningún cambio a los directorios de usuarios. |  |  |  |
| 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 debe ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador. |  |  |  |
| Implementar mecanismos de seguridad adaptativos que respondan al comportamiento de los usuarios, permitiendo aplicar restricciones específicas a aquellos identificados como potencialmente sospechosos o maliciosos. |  |  |  |
| Contar con la capacidad de inspeccionar y aplicar políticas de seguridad al tráfico cifrado mediante TLS/SSL, tanto en dirección entrante como saliente, incluyendo comunicaciones que utilicen los protocolos TLS 1.3 y HTTP/2 |  |  |  |
| Ofrecer visibilidad completa del tráfico cifrado mediante el protocolo TLS, permitiendo identificar el volumen de datos cifrados, así como las versiones de TLS/SSL y los conjuntos de cifrado utilizados, sin necesidad de realizar descifrado del contenido. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el Gartner Magic Quadrant for Network Firewalls en el ultimo informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el The Forrester Wave: Enterprise Firewalls en el ultimo informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el The Forrester Wave: Zero Trust Platform Providers en el último informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el Gartner Magic Quadrant for SD-WAN en el último informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el Gartner Magic Quadrant for Security Service Edge en el último informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el The Forrester Wave: Security Service Edge en el último informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el Gartner Magic Quadrant for Single-Vendor SASE en el último informe publicado. |  |  |  |
| La solución propuesta por el fabricante debe contar con certificación USGv6 para trabajar IPv6 tanto en Firewall como en IPS. |  |  |  |
| Disponer de mecanismos que permitan gestionar el uso de versiones obsoletas del protocolo TLS, algoritmos de cifrado inseguros y certificados mal configurados, con el fin de reforzar la postura de seguridad. |  |  |  |
| Facilitar la activación o desactivación del descifrado de tráfico de forma granular, en función de criterios como la categoría de la URL, el origen y destino, la dirección IP, el usuario, el grupo de usuarios, el tipo de dispositivo y el puerto utilizado. |  |  |  |
| Disponer de mecanismos automáticos de prevención contra malware conocido, desconocido y altamente evasivo, mediante tecnologías avanzadas de detección. |  |  |  |
| Contar con capacidades basadas en inteligencia artificial para la detección de exploits y actividades de comando y control, tanto conocidas como desconocidas. |  |  |  |
| Incluir capacidad de analizar los envíos de nombres de usuario y contraseñas a sitios web por usuarios internos del Ministerio y compararlos con credenciales corporativas válidas. |  |  |  |
| Incluir capacidad de SD-WAN con funcionalidad de cálculo de calidad de la ruta (vibración, pérdida de paquetes y latencia), selección de ruta inicial y cambio dinámico de la ruta |  |  |  |
| Incorporar funcionalidades que permitan la identificación y el control granular de aplicaciones dentro del entorno de red. |  |  |  |
| Para garantizar la seguridad del entorno frente a ataques, el sistema debe integrar un módulo de prevención de intrusiones (IPS), protección antimalware a nivel de red (antivirus) y capacidades antispyware/antibot. |  |  |  |
| Debe permitir capturar el paquete de red (en formato PCAP) asociada a la alerta de seguridad. |  |  |  |
| Debe permitir el bloqueo de virus y software espía en al menos los siguientes protocolos: HTTP, HTTP/2, HTTPS, FTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3, asegurando cobertura tanto para tráfico IPv4 como IPv6 en todos los protocolos mencionados. |  |  |  |
| Implementar mecanismos de protección contra cargas maliciosas ocultas en archivos comunes, como documentos de Microsoft Office y archivos PDF |  |  |  |
| Debe admitir el análisis en entorno controlado de archivos ejecutables (EXE), bibliotecas dinámicas (DLL), archivos ELF (Linux), archivos comprimidos (ZIP, 7ZIP, RAR), documentos de Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos Java (.jar y .class), scripts (.vbs, .ps1, .js), enlaces de correo electrónico, contenido Flash, archivos de MacOSX (mach-o, dmg, pkg) y paquetes APK de Android. |  |  |  |
| Contar con la capacidad de aplicar técnicas de aprendizaje automático (Machine Learning) de forma local en los NGFW, con el fin de identificar proactivamente nuevos sitios de phishing o amenazas de dia ceros para bloquearla en tiempo real (preveniendo el paciente cero) y bloquear su acceso o ejecución en tiempo real. |  |  |  |
| Debe contar con un sistema de categorización de URLs que permita asignar múltiples categorías a un mismo sitio web, facilitando una clasificación más precisa y flexible para la aplicación de políticas de seguridad. |  |  |  |
| Debe incorporar la capacidad de definir políticas basadas en la visibilidad y el control de usuarios y/o grupos de usuarios, mediante la integración con servicios de autenticación como LDAP, Active Directory, Novell eDirectory, Microsoft Exchange y bases de datos locales. |  |  |  |
| La solución debe estar respaldada por un servicio de inteligencia global que permita la detección de decenas de millones de dominios maliciosos mediante análisis en tiempo real, sin depender exclusivamente de firmas estáticas. |  |  |  |
| Debe contar con capacidades para detectar e interrumpir intentos de exfiltración de datos ocultos o tunelizados a través del tráfico DNS. |  |  |  |
| La solución debe ofrecer un rendimiento de firewall de próxima generación (NGFW) igual o superior a 19 Gb/s 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. |  |  |  |
| La solución debe ofrecer un rendimiento de Prevención de Amenazas de 10 Gb/s 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), 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 cuando se vayan habilitando los módulos de seguridad indicados en el modo más alto de inspección. |  |  |  |
| El equipo debe soportar como mínimo 220,000 sesiones simultaneas, medido con paquetes en capa de Aplicación (por ejemplo HTTP) |  |  |  |
| La plataforma de hardware debe soportar 220,000 sesiones por segundo, medidos con paquetes HTTP de 1 byte |  |  |  |
| Debe ser compatible, como mínimo, con los modos de operación de interfaz L2, L3, TAP y modo transparente (cable virtual) |  |  |  |
| Debe ofrecer soporte, como mínimo, para los siguientes protocolos y funcionalidades de enrutamiento: OSPF v2/v3 con capacidad de reinicio sin interrupciones, BGP con reinicio sin pérdida de estado, RIP, enrutamiento estático, reenvío basado en políticas (PBR) y detección de fallos mediante BFD. |  |  |  |
| Debe ser compatible con el protocolo punto a punto sobre Ethernet (PPPoE), permitiendo su implementación en entornos que requieran autenticación y encapsulamiento de tráfico sobre enlaces Ethernet |  |  |  |
| Debe ofrecer soporte para protocolos de multidifusión, incluyendo PIM-SM, PIM-SSM y las versiones 1, 2 y 3 de IGMP |  |  |  |
| Debe admitir funcionalidades de traducción de direcciones de red (NAT) en modos IPv4, incluyendo NAT con IP estática, IP dinámica, traducción dinámica de IP y puertos (PAT), así como soporte para NAT64 y NPTv6 |  |  |  |
| Plano de Datos y Planos de gestión independientes cada un hardware dedicado para su función |  |  |  |
| Debe ser de 1 RU |  |  |  |
| El equipo debe contar con un mínimo de 12 interfaces Ethernet multigigabit con soporte para velocidades de 1G, 2.5G, 5G y 10G; al menos 10 puertos SFP/SFP+ compatibles con velocidades de 1G y 10G; y 4 puertos SFP28 con capacidad de transmisión de hasta 25G. |  |  |  |
| El dispositivo debe disponer de al menos un puerto de gestión fuera de banda con soporte para velocidades 10/100/1000 Mbps, un puerto de consola tipo RJ-45, un puerto USB estándar y un puerto de consola adicional tipo micro-USB. |  |  |  |
| La solución propuesta no debe estar clasificada ni publicada en el sitio web oficial del fabricante como producto en estado de fin de vida (End-of-Life), fin de venta (End-of-Sale) o fin de soporte (End-of-Support). |  |  |  |
| Los dispositivos NGFW deberán contar con soporte activo por parte del fabricante durante un período mínimo de 36 meses (3 años). Este soporte deberá incluir atención a incidentes relacionados con el software o hardware de la plataforma, así como la reposición de partes o el suministro de equipos de reemplazo en caso de fallas de hardware. |  |  |  |
| El oferente debe incluir en su propuesta todas las licencias (suscripción), soporte y mantenimiento necesarios para proveer todas las funcionalidades requeridas. |  |  |  |
| Toda suscripción incluida como parte de la solución deberá tener una vigencia mínima de 36 meses (3 años) a partir de la fecha de inicio del servicio. |  |  |  |

| **ITEM:**  **1.2** | **DENOMINACIÓN DEL EQUIPO:**  **Firewall de Ultima Generación para Perimetro Centro de Datos Alterno** | **ESPECIFICACIONES TÉCNICAS REQUERIDAS** | **ESPECIFICACIONES TECNICAS DEL BIEN OFERTADO** | **MODELO Y/O MARCA** | **PAÍS DE ORIGEN** |
| --- | --- | --- | --- | --- | --- |
| **Lote I: Insfraestructura de Firewall de Ultima Generación (NGFW)**  **Nota: Colocar en el recuadro especificaciones técnicas del bien ofertado, el detalle del requerimiento ofertado junto al número de página dentro de la oferta o manual del fabricando donde se encuentra o especifica dicha información.** | | | | | | |
| **1.2** | **Firewall de Ultima Generación para Perimetro Centro de Datos Alterno** | Se requieren **dos (2) Firewalls de última generación** o NGFW, ambos instalados en el perímetro de la red del Centro de Datos Alternos del Ministerio e instalados bajo el esquema de alta disponibilidad (Modos: activo/activo, activo/pasivo). |  |  |  |
| El NGFW de contar con un motor de ML para prevención de amenazas desconocidas en tiempo real 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. |  |  |  |
| La solución debe permitir la detección de amenazas de día cero complejas a través de una integración con una plataforma Sandboxing. Al mismo tiempo, el dispositivo debe poder acceder y descargar protecciones generadas por el Sandbox contra malware de día 0 en tiempo real. |  |  |  |
| Se debe contar con un módulo de optimización de políticas integrado en el NGFW, que identifica las aplicaciones que han pasado sobre políticas basadas en puertos o de Capa 4, indicando consumo en Bytes, Hits y Fechas de visualización. Con el fin de facilitar la migración de la política de Capa 4 a Capa 7. |  |  |  |
| Incorporar la capacidad de reconocer las aplicaciones que operan en la red, sin importar el puerto utilizado, el protocolo empleado, las técnicas de evasión aplicadas o el tipo de cifrado, ya sea TLS o SSL. |  |  |  |
| Al crear políticas basadas en aplicaciones, si las mismas dependen de otras aplicaciones para su funcionamiento correcto, la interfaz gráfica debe mostrar y permitir agregar las aplicaciones necesarias. |  |  |  |
| Integrar la capacidad de inspeccionar completamente la carga útil de las aplicaciones, incluyendo archivos y patrones de datos, con el objetivo de detectar y bloquear contenido malicioso, así como impedir intentos de exfiltración de datos |  |  |  |
| La solución debe ser capaz de identificar cuando un usuario ingrese credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de phishing. |  |  |  |
| Habilitar la visibilidad de la actividad vinculada a usuarios y grupos específicos, más allá de direcciones IP individuales, permitiendo la aplicación de políticas de seguridad, la generación de informes detallados y la realización de análisis forenses sobre dichas entidades |  |  |  |
| 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 definir multiples grupos de usuarios dinámicos para tomar medidas de seguridad temporales sin esperar a que se aplique ningún cambio a los directorios de usuarios. |  |  |  |
| 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 debe ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el Gartner Magic Quadrant for Network Firewalls en el último informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el The Forrester Wave: Enterprise Firewalls en el último informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el The Forrester Wave: Zero Trust Platform Providers en el último informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el Gartner Magic Quadrant for SD-WAN en el último informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el Gartner Magic Quadrant for Security Service Edge en el último informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el The Forrester Wave: Security Service Edge en el último informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el Gartner Magic Quadrant for Single-Vendor SASE en el último informe publicado. |  |  |  |
| La solución propuesta por el fabricante debe contar con certificación USGv6 para trabajar IPv6 tanto en Firewall como en IPS. |  |  |  |
| Implementar mecanismos de seguridad adaptativos que respondan al comportamiento de los usuarios, permitiendo aplicar restricciones específicas a aquellos identificados como potencialmente sospechosos o maliciosos. |  |  |  |
| Contar con la capacidad de inspeccionar y aplicar políticas de seguridad al tráfico cifrado mediante TLS/SSL, tanto en dirección entrante como saliente, incluyendo comunicaciones que utilicen los protocolos TLS 1.3 y HTTP/2 |  |  |  |
| Ofrecer visibilidad completa del tráfico cifrado mediante el protocolo TLS, permitiendo identificar el volumen de datos cifrados, así como las versiones de TLS/SSL y los conjuntos de cifrado utilizados, sin necesidad de realizar descifrado del contenido. |  |  |  |
| Disponer de mecanismos que permitan gestionar el uso de versiones obsoletas del protocolo TLS, algoritmos de cifrado inseguros y certificados mal configurados, con el fin de reforzar la postura de seguridad. |  |  |  |
| Facilitar la activación o desactivación del descifrado de tráfico de forma granular, en función de criterios como la categoría de la URL, el origen y destino, la dirección IP, el usuario, el grupo de usuarios, el tipo de dispositivo y el puerto utilizado. |  |  |  |
| Disponer de mecanismos automáticos de prevención contra malware conocido, desconocido y altamente evasivo, mediante tecnologías avanzadas de detección. |  |  |  |
| Contar con capacidades basadas en inteligencia artificial para la detección de exploits y actividades de comando y control, tanto conocidas como desconocidas. |  |  |  |
| Incluir capacidad de analizar los envíos de nombres de usuario y contraseñas a sitios web por usuarios internos del Ministerio y compararlos con credenciales corporativas válidas. |  |  |  |
| Incluir capacidad de SD-WAN con funcionalidad de cálculo de calidad de la ruta (vibración, pérdida de paquetes y latencia), selección de ruta inicial y cambio dinámico de la ruta |  |  |  |
| Incorporar funcionalidades que permitan la identificación y el control granular de aplicaciones dentro del entorno de red. |  |  |  |
| Para garantizar la seguridad del entorno frente a ataques, el sistema debe integrar un módulo de prevención de intrusiones (IPS), protección antimalware a nivel de red (antivirus) y capacidades antispyware/antibot. |  |  |  |
| Debe permitir capturar el paquete de red (en formato PCAP) asociada a la alerta de seguridad. |  |  |  |
| Debe permitir el bloqueo de virus y software espía en al menos los siguientes protocolos: HTTP, HTTP/2, HTTPS, FTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3, asegurando cobertura tanto para tráfico IPv4 como IPv6 en todos los protocolos mencionados. |  |  |  |
| Implementar mecanismos de protección contra cargas maliciosas ocultas en archivos comunes, como documentos de Microsoft Office y archivos PDF |  |  |  |
| Debe admitir el análisis en entorno controlado de archivos ejecutables (EXE), bibliotecas dinámicas (DLL), archivos ELF (Linux), archivos comprimidos (ZIP, 7ZIP, RAR), documentos de Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos Java (.jar y .class), scripts (.vbs, .ps1, .js), enlaces de correo electrónico, contenido Flash, archivos de MacOSX (mach-o, dmg, pkg) y paquetes APK de Android. |  |  |  |
| Contar con la capacidad de aplicar técnicas de aprendizaje automático (Machine Learning) de forma local en los NGFW, con el fin de identificar proactivamente nuevos sitios de phishing o amenazas de dia ceros para bloquearla en tiempo real (preveniendo el paciente cero) y bloquear su acceso o ejecución en tiempo real. |  |  |  |
| Debe contar con un sistema de categorización de URLs que permita asignar múltiples categorías a un mismo sitio web, facilitando una clasificación más precisa y flexible para la aplicación de políticas de seguridad. |  |  |  |
| Debe incorporar la capacidad de definir políticas basadas en la visibilidad y el control de usuarios y/o grupos de usuarios, mediante la integración con servicios de autenticación como LDAP, Active Directory, Novell eDirectory, Microsoft Exchange y bases de datos locales. |  |  |  |
| La solución debe estar respaldada por un servicio de inteligencia global que permita la detección de decenas de millones de dominios maliciosos mediante análisis en tiempo real, sin depender exclusivamente de firmas estáticas. |  |  |  |
| Debe contar con capacidades para detectar e interrumpir intentos de exfiltración de datos ocultos o tunelizados a través del tráfico DNS. |  |  |  |
| La solución debe ofrecer un rendimiento de firewall de próxima generación (NGFW) igual o superior a 19 Gb/s 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 10 Gb/s 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), Filtro de Archivos, y Logging activo. |  |  |  |
| El equipo debe soportar como mínimo 2,200,000 sesiones simultaneas, medido con paquetes en capa de Aplicación (por ejemplo, HTTP) |  |  |  |
| La plataforma de hardware debe soportar 220,000 sesiones por segundo, medidos con paquetes HTTP de 1 byte |  |  |  |
| Debe ser compatible, como mínimo, con los modos de operación de interfaz L2, L3, TAP y modo transparente (cable virtual) |  |  |  |
| Debe ofrecer soporte, como mínimo, para los siguientes protocolos y funcionalidades de enrutamiento: OSPF v2/v3 con capacidad de reinicio sin interrupciones, BGP con reinicio sin pérdida de estado, RIP, enrutamiento estático, reenvío basado en políticas (PBR) y detección de fallos mediante BFD. |  |  |  |
| Debe ser compatible con el protocolo punto a punto sobre Ethernet (PPPoE), permitiendo su implementación en entornos que requieran autenticación y encapsulamiento de tráfico sobre enlaces Ethernet |  |  |  |
| Debe ofrecer soporte para protocolos de multidifusión, incluyendo PIM-SM, PIM-SSM y las versiones 1, 2 y 3 de IGMP |  |  |  |
| Debe admitir funcionalidades de traducción de direcciones de red (NAT) en modos IPv4, incluyendo NAT con IP estática, IP dinámica, traducción dinámica de IP y puertos (PAT), así como soporte para NAT64 y NPTv6 |  |  |  |
| Plano de Datos y Planos de gestión independientes cada un hardware dedicado para su función |  |  |  |
| Debe ser de 1 RU |  |  |  |
| El equipo debe contar con un mínimo de 12 interfaces Ethernet multigigabit con soporte para velocidades de 1G, 2.5G, 5G y 10G; al menos 10 puertos SFP/SFP+ compatibles con velocidades de 1G y 10G; y 4 puertos SFP28 con capacidad de transmisión de hasta 25G. |  |  |  |
| El dispositivo debe disponer de al menos un puerto de gestión fuera de banda con soporte para velocidades 10/100/1000 Mbps, un puerto de consola tipo RJ-45, un puerto USB estándar y un puerto de consola adicional tipo micro-USB. |  |  |  |
| La solución propuesta no debe estar clasificada ni publicada en el sitio web oficial del fabricante como producto en estado de fin de vida (End-of-Life), fin de venta (End-of-Sale) o fin de soporte (End-of-Support). |  |  |  |
| Los dispositivos NGFW deberán contar con soporte activo por parte del fabricante durante un período mínimo de 36 meses (3 años). Este soporte deberá incluir atención a incidentes relacionados con el software o hardware de la plataforma, así como la reposición de partes o el suministro de equipos de reemplazo en caso de fallas de hardware. |  |  |  |
| El oferente debe incluir en su propuesta todas las licencias (suscripción), soporte y mantenimiento necesarios para proveer todas las funcionalidades requeridas. |  |  |  |
| Toda suscripción incluida como parte de la solución deberá tener una vigencia mínima de 36 meses (3 años) a partir de la fecha de inicio del servicio. |  |  |  |

| **ITEM:**  **1.3** | **DENOMINACIÓN DEL EQUIPO:**  **Firewall de Ultima Generación para Oficinas Remotas Tipo A** | **ESPECIFICACIONES TÉCNICAS REQUERIDAS** | **ESPECIFICACIONES TECNICAS DEL BIEN OFERTADO** | **MODELO Y/O MARCA** | **PAÍS DE ORIGEN** |
| --- | --- | --- | --- | --- | --- |
| **Lote I: Infraestructura de Firewall de Ultima Generación (NGFW)**  **Nota: Colocar en el recuadro especificaciones técnicas del bien ofertado, el detalle del requerimiento ofertado junto al número de página dentro de la oferta o manual del fabricando donde se encuentra o especifica dicha información.** | | | | | |
| **1.3** | **Firewall de Ultima Generación para Oficinas Remotas Tipo A** | Se requieren cuatro (4) Firewalls de última generación o NGFW, instalados como NGFW standalone en el perímetro de la red de 4 oficinas remotas del Ministerio. |  |  |  |
| El NGFW de contar con un motor de ML para prevención de amenazas desconocidas en tiempo real 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. |  |  |  |
| La solución debe permitir la detección de amenazas de día cero complejas a través de una integración con una plataforma Sandboxing. Al mismo tiempo, el dispositivo debe poder acceder y descargar protecciones generadas por el Sandbox contra malware de día 0 en tiempo real. |  |  |  |
| Se debe contar con un módulo de optimización de políticas integrado en el NGFW, que identifica las aplicaciones que han pasado sobre políticas basadas en puertos o de Capa 4, indicando consumo en Bytes, Hits y Fechas de visualización. Con el fin de facilitar la migración de la política de Capa 4 a Capa 7. |  |  |  |
| Incorporar la capacidad de reconocer las aplicaciones que operan en la red, sin importar el puerto utilizado, el protocolo empleado, las técnicas de evasión aplicadas o el tipo de cifrado, ya sea TLS o SSL. |  |  |  |
| Al crear políticas basadas en aplicaciones, si las mismas dependen de otras aplicaciones para su funcionamiento correcto, la interfaz gráfica debe mostrar y permitir agregar las aplicaciones necesarias. |  |  |  |
| Integrar la capacidad de inspeccionar completamente la carga útil de las aplicaciones, incluyendo archivos y patrones de datos, con el objetivo de detectar y bloquear contenido malicioso, así como impedir intentos de exfiltración de datos |  |  |  |
| La solución debe ser capaz de identificar cuando un usuario ingrese credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de phishing. |  |  |  |
| Habilitar la visibilidad de la actividad vinculada a usuarios y grupos específicos, más allá de direcciones IP individuales, permitiendo la aplicación de políticas de seguridad, la generación de informes detallados y la realización de análisis forenses sobre dichas entidades |  |  |  |
| 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 definir multiples grupos de usuarios dinámicos para tomar medidas de seguridad temporales sin esperar a que se aplique ningún cambio a los directorios de usuarios. |  |  |  |
| 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 debe ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador. |  |  |  |
| Implementar mecanismos de seguridad adaptativos que respondan al comportamiento de los usuarios, permitiendo aplicar restricciones específicas a aquellos identificados como potencialmente sospechosos o maliciosos. |  |  |  |
| Contar con la capacidad de inspeccionar y aplicar políticas de seguridad al tráfico cifrado mediante TLS/SSL, tanto en dirección entrante como saliente, incluyendo comunicaciones que utilicen los protocolos TLS 1.3 y HTTP/2 |  |  |  |
| Ofrecer visibilidad completa del tráfico cifrado mediante el protocolo TLS, permitiendo identificar el volumen de datos cifrados, así como las versiones de TLS/SSL y los conjuntos de cifrado utilizados, sin necesidad de realizar descifrado del contenido. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el Gartner Magic Quadrant for Network Firewalls en el ultimo informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el The Forrester Wave: Enterprise Firewalls en el último informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el The Forrester Wave: Zero Trust Platform Providers en el último informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el Gartner Magic Quadrant for SD-WAN en el último informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el Gartner Magic Quadrant for Security Service Edge en el último informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el The Forrester Wave: Security Service Edge en el último informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el Gartner Magic Quadrant for Single-Vendor SASE en el último informe publicado. |  |  |  |
| La solución propuesta por el fabricante debe contar con certificación USGv6 para trabajar IPv6 tanto en Firewall como en IPS. |  |  |  |
| Disponer de mecanismos que permitan gestionar el uso de versiones obsoletas del protocolo TLS, algoritmos de cifrado inseguros y certificados mal configurados, con el fin de reforzar la postura de seguridad. |  |  |  |
| Facilitar la activación o desactivación del descifrado de tráfico de forma granular, en función de criterios como la categoría de la URL, el origen y destino, la dirección IP, el usuario, el grupo de usuarios, el tipo de dispositivo y el puerto utilizado. |  |  |  |
| Disponer de mecanismos automáticos de prevención contra malware conocido, desconocido y altamente evasivo, mediante tecnologías avanzadas de detección. |  |  |  |
| Contar con capacidades basadas en inteligencia artificial para la detección de exploits y actividades de comando y control, tanto conocidas como desconocidas. |  |  |  |
| Incluir capacidad de analizar los envíos de nombres de usuario y contraseñas a sitios web por usuarios internos del Ministerio y compararlos con credenciales corporativas válidas. |  |  |  |
| Incluir capacidad de SD-WAN con funcionalidad de cálculo de calidad de la ruta (vibración, pérdida de paquetes y latencia), selección de ruta inicial y cambio dinámico de la ruta |  |  |  |
| Incorporar funcionalidades que permitan la identificación y el control granular de aplicaciones dentro del entorno de red. |  |  |  |
| Para garantizar la seguridad del entorno frente a ataques, el sistema debe integrar un módulo de prevención de intrusiones (IPS), protección antimalware a nivel de red (antivirus) y capacidades antispyware/antibot. |  |  |  |
| Debe permitir el bloqueo de virus y software espía en al menos los siguientes protocolos: HTTP, HTTP/2, HTTPS, FTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3, asegurando cobertura tanto para tráfico IPv4 como IPv6 en todos los protocolos mencionados. |  |  |  |
| Implementar mecanismos de protección contra cargas maliciosas ocultas en archivos comunes, como documentos de Microsoft Office y archivos PDF |  |  |  |
| Debe admitir el análisis en entorno controlado de archivos ejecutables (EXE), bibliotecas dinámicas (DLL), archivos ELF (Linux), archivos comprimidos (ZIP, 7ZIP, RAR), documentos de Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos Java (.jar y .class), scripts (.vbs, .ps1, .js), enlaces de correo electrónico, contenido Flash, archivos de MacOSX (mach-o, dmg, pkg) y paquetes APK de Android. |  |  |  |
| Contar con la capacidad de aplicar técnicas de aprendizaje automático (Machine Learning) de forma local en los NGFW, con el fin de identificar proactivamente nuevos sitios de phishing o amenazas de dia ceros para bloquearla en tiempo real (preveniendo el paciente cero) y bloquear su acceso o ejecución en tiempo real. |  |  |  |
| Debe contar con un sistema de categorización de URLs que permita asignar múltiples categorías a un mismo sitio web, facilitando una clasificación más precisa y flexible para la aplicación de políticas de seguridad. |  |  |  |
| Debe incorporar la capacidad de definir políticas basadas en la visibilidad y el control de usuarios y/o grupos de usuarios, mediante la integración con servicios de autenticación como LDAP, Active Directory, Novell eDirectory, Microsoft Exchange y bases de datos locales. |  |  |  |
| La solución debe estar respaldada por un servicio de inteligencia global que permita la detección de decenas de millones de dominios maliciosos mediante análisis en tiempo real, sin depender exclusivamente de firmas estáticas. |  |  |  |
| Debe contar con capacidades para detectar e interrumpir intentos de exfiltración de datos ocultos o tunelizados a través del tráfico DNS. |  |  |  |
| La solución debe ofrecer un rendimiento de firewall de próxima generación (NGFW) igual o superior a 2,6 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. |  |  |  |
| La solución debe ofrecer un rendimiento de Prevención de Amenazas igual o superior a 1,2 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), Filtro de Archivos, y Logging activo. |  |  |  |
| El equipo debe soportar como mínimo 200,000 sesiones simultaneas, medido con paquetes en capa de Aplicación (por ejemplo HTTP) |  |  |  |
| La plataforma de hardware debe soportar 34,000 sesiones por segundo, medidos con paquetes HTTP de 1 byte |  |  |  |
| Debe ser compatible, como mínimo, con los modos de operación de interfaz L2, L3, TAP y modo transparente (cable virtual) |  |  |  |
| Debe ofrecer soporte, como mínimo, para los siguientes protocolos y funcionalidades de enrutamiento: OSPF v2/v3 con capacidad de reinicio sin interrupciones, BGP con reinicio sin pérdida de estado, RIP, enrutamiento estático, reenvío basado en políticas (PBR) y detección de fallos mediante BFD. |  |  |  |
| Debe ser compatible con el protocolo punto a punto sobre Ethernet (PPPoE), permitiendo su implementación en entornos que requieran autenticación y encapsulamiento de tráfico sobre enlaces Ethernet |  |  |  |
| Debe ofrecer soporte para protocolos de multidifusión, incluyendo PIM-SM, PIM-SSM y las versiones 1, 2 y 3 de IGMP |  |  |  |
| Debe admitir funcionalidades de traducción de direcciones de red (NAT) en modos IPv4, incluyendo NAT con IP estática, IP dinámica, traducción dinámica de IP y puertos (PAT), así como soporte para NAT64 y NPTv6 |  |  |  |
| Plano de Datos y Planos de gestión independientes cada un hardware dedicado para su función |  |  |  |
| Incluir al menos 8 interfaces de red de 1Gbps |  |  |  |
| Incluir al menos 1 puerto de gestión fuera de banda 10/100/1000 Mbps, 1 puerto de consola RJ-45, 1 puerto USB y 1 puerto de consola micro-USB. |  |  |  |
| La solución propuesta no debe estar clasificada ni publicada en el sitio web oficial del fabricante como producto en estado de fin de vida (End-of-Life), fin de venta (End-of-Sale) o fin de soporte (End-of-Support). |  |  |  |
| Los dispositivos NGFW deberán contar con soporte activo por parte del fabricante durante un período mínimo de 36 meses (3 años). Este soporte deberá incluir atención a incidentes relacionados con el software o hardware de la plataforma, así como la reposición de partes o el suministro de equipos de reemplazo en caso de fallas de hardware. |  |  |  |
| El oferente debe incluir en su propuesta todas las licencias (suscripción), soporte y mantenimiento necesarios para proveer todas las funcionalidades requeridas. |  |  |  |
| Toda suscripción incluida como parte de la solución deberá tener una vigencia mínima de 36 meses (3 años) a partir de la fecha de inicio del servicio. |  |  |  |

| **ITEM:**  **1.4** | **DENOMINACIÓN DEL EQUIPO:**  **Firewall de Ultima Generación para Oficinas Remotas Tipo B** | **ESPECIFICACIONES TÉCNICAS REQUERIDAS** | **ESPECIFICACIONES TECNICAS DEL BIEN OFERTADO** | **MODELO Y/O MARCA** | **PAÍS DE ORIGEN** |
| --- | --- | --- | --- | --- | --- |
| **Lote I: Infraestructura de Firewall de Ultima Generación (NGFW)**  **Nota: Colocar en el recuadro especificaciones técnicas del bien ofertado, el detalle del requerimiento ofertado junto al número de página dentro de la oferta o manual del fabricando donde se encuentra o especifica dicha información.** | | | | | |
| **1.4** | **Firewall de Ultima Generación para Oficinas Remotas Tipo B** | **Se requieren cuatro (4) Firewalls de última generación o NGFW**, instalados en pares de NGFW en el perímetro de la red de 2 oficinas remotas del Ministerio e instalados bajo el esquema de alta disponibilidad (Modos: activo/activo, activo/pasivo). |  |  |  |
| El NGFW de contar con un motor de ML para prevención de amenazas desconocidas en tiempo real 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. |  |  |  |
| La solución debe permitir la detección de amenazas de día cero complejas a través de una integración con una plataforma Sandboxing. Al mismo tiempo, el dispositivo debe poder acceder y descargar protecciones generadas por el Sandbox contra malware de día 0 en tiempo real. |  |  |  |
| Se debe contar con un módulo de optimización de políticas integrado en el NGFW, que identifica las aplicaciones que han pasado sobre políticas basadas en puertos o de Capa 4, indicando consumo en Bytes, Hits y Fechas de visualización. Con el fin de facilitar la migración de la política de Capa 4 a Capa 7. |  |  |  |
| Incorporar la capacidad de reconocer las aplicaciones que operan en la red, sin importar el puerto utilizado, el protocolo empleado, las técnicas de evasión aplicadas o el tipo de cifrado, ya sea TLS o SSL. |  |  |  |
| Al crear políticas basadas en aplicaciones, si las mismas dependen de otras aplicaciones para su funcionamiento correcto, la interfaz gráfica debe mostrar y permitir agregar las aplicaciones necesarias. |  |  |  |
| Integrar la capacidad de inspeccionar completamente la carga útil de las aplicaciones, incluyendo archivos y patrones de datos, con el objetivo de detectar y bloquear contenido malicioso, así como impedir intentos de exfiltración de datos |  |  |  |
| La solución debe ser capaz de identificar cuando un usuario ingrese credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de phishing. |  |  |  |
| Habilitar la visibilidad de la actividad vinculada a usuarios y grupos específicos, más allá de direcciones IP individuales, permitiendo la aplicación de políticas de seguridad, la generación de informes detallados y la realización de análisis forenses sobre dichas entidades |  |  |  |
| 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 definir multiples grupos de usuarios dinámicos para tomar medidas de seguridad temporales sin esperar a que se aplique ningún cambio a los directorios de usuarios. |  |  |  |
| 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 debe ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador. |  |  |  |
| Implementar mecanismos de seguridad adaptativos que respondan al comportamiento de los usuarios, permitiendo aplicar restricciones específicas a aquellos identificados como potencialmente sospechosos o maliciosos. |  |  |  |
| Contar con la capacidad de inspeccionar y aplicar políticas de seguridad al tráfico cifrado mediante TLS/SSL, tanto en dirección entrante como saliente, incluyendo comunicaciones que utilicen los protocolos TLS 1.3 y HTTP/2 |  |  |  |
| Ofrecer visibilidad completa del tráfico cifrado mediante el protocolo TLS, permitiendo identificar el volumen de datos cifrados, así como las versiones de TLS/SSL y los conjuntos de cifrado utilizados, sin necesidad de realizar descifrado del contenido. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el Gartner Magic Quadrant for Network Firewalls en el ultimo informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el The Forrester Wave: Enterprise Firewalls en el ultimo informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el The Forrester Wave: Zero Trust Platform Providers en el ultimo informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el Gartner Magic Quadrant for SD-WAN en el ultimo informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el Gartner Magic Quadrant for Security Service Edge en el ultimo informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el The Forrester Wave: Security Service Edge en el ultimo informe publicado. |  |  |  |
| El fabricante ofrecido debe ser clasificado como lider en el Gartner Magic Quadrant for Single-Vendor SASE en el ultimo informe publicado. |  |  |  |
| Disponer de mecanismos que permitan gestionar el uso de versiones obsoletas del protocolo TLS, algoritmos de cifrado inseguros y certificados mal configurados, con el fin de reforzar la postura de seguridad. |  |  |  |
| Facilitar la activación o desactivación del descifrado de tráfico de forma granular, en función de criterios como la categoría de la URL, el origen y destino, la dirección IP, el usuario, el grupo de usuarios, el tipo de dispositivo y el puerto utilizado. |  |  |  |
| Disponer de mecanismos automáticos de prevención contra malware conocido, desconocido y altamente evasivo, mediante tecnologías avanzadas de detección. |  |  |  |
| Contar con capacidades basadas en inteligencia artificial para la detección de exploits y actividades de comando y control, tanto conocidas como desconocidas. |  |  |  |
| Incluir capacidad de analizar los envíos de nombres de usuario y contraseñas a sitios web por usuarios internos del Ministerio y compararlos con credenciales corporativas válidas. |  |  |  |
| Incluir capacidad de SD-WAN con funcionalidad de cálculo de calidad de la ruta (vibración, pérdida de paquetes y latencia), selección de ruta inicial y cambio dinámico de la ruta |  |  |  |
| Incorporar funcionalidades que permitan la identificación y el control granular de aplicaciones dentro del entorno de red. |  |  |  |
| Para garantizar la seguridad del entorno frente a ataques, el sistema debe integrar un módulo de prevención de intrusiones (IPS), protección antimalware a nivel de red (antivirus) y capacidades antispyware/antibot. |  |  |  |
| Debe permitir el bloqueo de virus y software espía en al menos los siguientes protocolos: HTTP, HTTP/2, HTTPS, FTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3, asegurando cobertura tanto para tráfico IPv4 como IPv6 en todos los protocolos mencionados. |  |  |  |
| Implementar mecanismos de protección contra cargas maliciosas ocultas en archivos comunes, como documentos de Microsoft Office y archivos PDF |  |  |  |
| Debe admitir el análisis en entorno controlado de archivos ejecutables (EXE), bibliotecas dinámicas (DLL), archivos ELF (Linux), archivos comprimidos (ZIP, 7ZIP, RAR), documentos de Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos Java (.jar y .class), scripts (.vbs, .ps1, .js), enlaces de correo electrónico, contenido Flash, archivos de MacOSX (mach-o, dmg, pkg) y paquetes APK de Android. |  |  |  |
| Contar con la capacidad de aplicar técnicas de aprendizaje automático (Machine Learning) de forma local en los NGFW, con el fin de identificar proactivamente nuevos sitios de phishing o amenazas de dia ceros para bloquearla en tiempo real (preveniendo el paciente cero) y bloquear su acceso o ejecución en tiempo real. |  |  |  |
| Debe contar con un sistema de categorización de URLs que permita asignar múltiples categorías a un mismo sitio web, facilitando una clasificación más precisa y flexible para la aplicación de políticas de seguridad. |  |  |  |
| Debe incorporar la capacidad de definir políticas basadas en la visibilidad y el control de usuarios y/o grupos de usuarios, mediante la integración con servicios de autenticación como LDAP, Active Directory, Novell eDirectory, Microsoft Exchange y bases de datos locales. |  |  |  |
| La solución debe estar respaldada por un servicio de inteligencia global que permita la detección de decenas de millones de dominios maliciosos mediante análisis en tiempo real, sin depender exclusivamente de firmas estáticas. |  |  |  |
| Debe contar con capacidades para detectar e interrumpir intentos de exfiltración de datos ocultos o tunelizados a través del tráfico DNS. |  |  |  |
| La solución debe ofrecer un rendimiento de firewall de próxima generación (NGFW) igual o superior a 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), Filtro de Archivos, y Logging activo. |  |  |  |
| El equipo debe soportar como mínimo 945,000 sesiones simultaneas, medido con paquetes en capa de Aplicación (por ejemplo HTTP) |  |  |  |
| La plataforma de hardware debe soportar 100,000 sesiones por segundo, medidos con paquetes HTTP de 1 byte |  |  |  |
| Debe ser compatible, como mínimo, con los modos de operación de interfaz L2, L3, TAP y modo transparente (cable virtual) |  |  |  |
| Debe ofrecer soporte, como mínimo, para los siguientes protocolos y funcionalidades de enrutamiento: OSPF v2/v3 con capacidad de reinicio sin interrupciones, BGP con reinicio sin pérdida de estado, RIP, enrutamiento estático, reenvío basado en políticas (PBR) y detección de fallos mediante BFD. |  |  |  |
| Debe ser compatible con el protocolo punto a punto sobre Ethernet (PPPoE), permitiendo su implementación en entornos que requieran autenticación y encapsulamiento de tráfico sobre enlaces Ethernet |  |  |  |
| Debe ofrecer soporte para protocolos de multidifusión, incluyendo PIM-SM, PIM-SSM y las versiones 1, 2 y 3 de IGMP |  |  |  |
| Debe admitir funcionalidades de traducción de direcciones de red (NAT) en modos IPv4, incluyendo NAT con IP estática, IP dinámica, traducción dinámica de IP y puertos (PAT), así como soporte para NAT64 y NPTv6 |  |  |  |
| Plano de Datos y Planos de gestión independientes cada unos hardware dedicado para su función |  |  |  |
| Incluir al menos 8 interfaces de red de 10/100/1000Mbps, 4 interfaces de red de 1G/2,5G/5G, 6 interfaces de red de 1G SFP y 4 interfaces de red de 1G/10G SFP/SFP+. |  |  |  |
| Incluir al menos 1 puerto de gestión fuera de banda 10/100/1000, 1 puerto de consola RJ-45, 1 puerto USB y 1 puerto de consola micro-USB. |  |  |  |
| La solución propuesta no debe estar clasificada ni publicada en el sitio web oficial del fabricante como producto en estado de fin de vida (End-of-Life), fin de venta (End-of-Sale) o fin de soporte (End-of-Support). |  |  |  |
| Los dispositivos NGFW deberán contar con soporte activo por parte del fabricante durante un período mínimo de 36 meses (3 años). Este soporte deberá incluir atención a incidentes relacionados con el software o hardware de la plataforma, así como la reposición de partes o el suministro de equipos de reemplazo en caso de fallas de hardware. |  |  |  |
| El oferente debe incluir en su propuesta todas las licencias (suscripción), soporte y mantenimiento necesarios para proveer todas las funcionalidades requeridas. |  |  |  |
| Toda suscripción incluida como parte de la solución deberá tener una vigencia mínima de 36 meses (3 años) a partir de la fecha de inicio del servicio. |  |  |  |

| **ITEM:**  **1.5** | **DENOMINACIÓN DEL EQUIPO:**  **Plataforma de Gestión Centralizadas de los Firewall de Ultima Generación** | **ESPECIFICACIONES TÉCNICAS REQUERIDAS** | **ESPECIFICACIONES TECNICAS DEL BIEN OFERTADO** | **MODELO Y/O MARCA** | **PAÍS DE ORIGEN** |
| --- | --- | --- | --- | --- | --- |
| **Lote I: Infraestructura de Firewall de Ultima Generación (NGFW)**  **Nota: Colocar en el recuadro especificaciones técnicas del bien ofertado, el detalle del requerimiento ofertado junto al número de página dentro de la oferta o manual del fabricando donde se encuentra o especifica dicha información.** | | | | | | |
| **1.5** | **Plataforma de Gestión Centralizadas de los Firewall de Ultima Generación** | Se requiere una plataforma unificada de gestión y operación, basada en inteligencia artificial, que permita la administración centralizada de toda la infraestructura de firewalls de próxima generación. Esta plataforma debe ofrecer una interfaz de usuario simplificada y centralizada que proporcione visibilidad completa sobre usuarios, ubicaciones remotas, aplicaciones y amenazas, abarcando todos los puntos de aplicación de la seguridad en la red. |  |  |  |
| La plataforma unificada de gestión y operación deberá ser provista como un servicio en la nube (cloud-based), permitiendo la administración centralizada, el monitoreo continuo y la operación eficiente de la infraestructura de Firewalls de Última Generación (NGFW) especificada en la solución |  |  |  |
| La solución debe permitir integraciones nativas con los Firewalls de Última Generación propuestos, asegurando compatibilidad plena para su implementación en el perímetro de red empresarial, el centro de datos y las oficinas remotas. |  |  |  |
| La solución debe incorporar funcionalidades que permitan evaluar la adopción de los distintos servicios de seguridad incluidos en las suscripciones de los Firewalls de Última Generación. Esto incluye la capacidad de consultar qué funciones de seguridad están siendo utilizadas, identificar brechas en la adopción de características disponibles, visualizar tasas de adopción de los servicios contratados, y analizar el grado de alineación de las funcionalidades implementadas con las mejores prácticas, así como detectar oportunidades de mejora para fortalecer la postura general de seguridad. |  |  |  |
| La solución debe ofrecer capacidades para la optimización y depuración de políticas de seguridad, utilizando datos de uso reales y recomendaciones generadas automáticamente, con el fin de mejorar la eficiencia operativa y fortalecer la postura de seguridad. |  |  |  |
| La solución debe incluir funcionalidades de limpieza de configuración, tales como la identificación y eliminación de objetos no referenciados en las políticas de seguridad, así como la depuración de reglas que no presentan tráfico asociado, con el fin de mantener una configuración optimizada y eficiente. |  |  |  |
| La solución debe incorporar funcionalidades de optimización de políticas que permitan identificar reglas excesivamente permisivas y transformarlas en reglas más específicas y restringidas, limitando el acceso únicamente a las aplicaciones que efectivamente están siendo utilizadas por el Ministerio, con el objetivo de reducir la superficie de exposición y mejorar el control de seguridad. |  |  |  |
| La solución debe contar con capacidades de verificación en tiempo real y en línea de la configuración de seguridad, evaluando el cumplimiento de las mejores prácticas establecidas. Estas verificaciones deben asegurar que las reglas de las políticas de seguridad estén alineadas con estándares recomendados, permitiendo ajustes proactivos para mantener una postura de seguridad robusta y actualizada. |  |  |  |
| La solución debe proporcionar visibilidad centralizada del estado de salud y del rendimiento operativo de los Firewalls de Última Generación a través de un panel de control unificado, permitiendo una supervisión continua y eficiente de la infraestructura de seguridad. |  |  |  |
| La solución debe permitir el análisis y monitoreo detallado de la capacidad de recursos de los Firewalls de Última Generación, mediante el seguimiento continuo de métricas de uso específicas según el modelo de dispositivo. Esta funcionalidad debe incluir: |  |  |  |
| Una visión integral del nivel actual de utilización de recursos y de la capacidad disponible hasta el límite máximo. |  |  |  |
| Una visualización tipo mapa de calor que represente gráficamente el uso de métricas por plataforma de hardware en una vista unificada, facilitando el análisis detallado. |  |  |  |
| La capacidad de planificar proactivamente la actualización a modelos de mayor capacidad, en función de las necesidades operativas identificadas. |  |  |  |
| La solución debe admitir la generación de alertas proactivas que permitan anticipar el consumo de recursos de los Firewalls de Última Generación cuando se aproximen a su capacidad máxima. Estas alertas deberán activarse con al menos tres meses de antelación, con el fin de identificar posibles cuellos de botella de capacidad y permitir una planificación oportuna de acciones correctivas. |  |  |  |
| La solución debe incorporar funcionalidades avanzadas basadas en inteligencia artificial que permitan identificar las causas probables de las alertas generadas y proporcionar recomendaciones específicas para resolver los problemas subyacentes, facilitando una respuesta más rápida y eficaz ante incidentes de seguridad o rendimiento. |  |  |  |
| Incluir funcionalidad de aprendizaje automático que comprenda la implementación y ofrezca alertas e incidentes adicionales adaptados a la tendencias de uso,tales como: |  |  |  |
| - Alertas basadas en pronósticos que permitan a anticipar problemas al proyectar cómo puede cambiar la métrica de un dispositivo y alertarnos de la consecuencia. |  |  |  |
| - Alertas basadas en anomalías que permita establecer un comportamiento de referencia para una métrica del NGFW y le avise cuando esa métrica cruza la configuración de sensibilidad de anomalías que se especifique. |  |  |  |
| La solución debe permitir la aplicación de políticas de seguridad de forma uniforme en toda la infraestructura de Firewalls de Última Generación (NGFW), así como la capacidad de implementar configuraciones tanto de manera global como específica por dispositivo, garantizando una administración flexible y coherente en todos los entornos operativos. |  |  |  |
| La solución debe proporcionar visibilidad integral de extremo a extremo sobre usuarios, dispositivos, aplicaciones y amenazas a lo largo de toda la infraestructura de red, permitiendo un monitoreo completo y contextualizado del entorno de seguridad. |  |  |  |
| La solución debe incorporar paneles de control detallados y capacidades avanzadas de generación de informes, que faciliten la toma de decisiones informadas y respalden la identificación y resolución eficiente de problemas operativos y de seguridad. |  |  |  |
| La solución debe integrar un asistente basado en inteligencia artificial, capaz de identificar vulnerabilidades en la infraestructura, ofrecer recomendaciones detalladas para su remediación y asistir en la ejecución de flujos de trabajo mediante interacción en lenguaje natural, facilitando así una gestión más eficiente y proactiva de la seguridad. |  |  |  |
| El asistente basado en inteligencia artificial debe aprovechar modelos avanzados de IA para potenciar la productividad y optimizar la eficiencia operativa, facilitando tareas complejas mediante automatización inteligente y asistencia contextualizada. |  |  |  |
| La solución debe disponer de un panel de control intuitivo y contextual, que incorpore flujos de trabajo guiados orientados a reducir la complejidad operativa y facilitar la administración eficiente de la infraestructura de seguridad. |  |  |  |
| La solución debe incorporar herramientas centralizadas para la resolución de problemas, que permitan gestionar y atender incidencias de forma eficiente, reduciendo los tiempos de diagnóstico y respuesta operativa. |  |  |  |
| La solución debe cumplir con los principales estándares de la industria en materia de seguridad y cumplimiento, tales como SOC 2 y GDPR, y garantizar una integración fluida con la infraestructura tecnológica existente, así como con sistemas y plataformas de terceros. |  |  |  |
| El oferente debe incluir en su propuesta todas las licencias (suscripción), soporte y mantenimiento necesarios para proveer todas las funcionalidades requeridas. |  |  |  |
| Todas las funcionalidades requeridas por la solución, debe ser entregada en una unica plataforma de manera unificiada, sin la necesidad de añadir componentes adicionales. |  |  |  |
| La solución debe incluir suscripción activa, soporte técnico y servicios de mantenimiento por un período mínimo de 36 meses (3 años), cubriendo tanto actualizaciones de software como atención a incidentes y acceso a nuevas funcionalidades durante la vigencia del contrato. |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ITEM:**  **2.1** | **DENOMINACIÓN DEL EQUIPO:**  **Nodos de Cómputo y Almacenamiento** | **ESPECIFICACIONES TÉCNICAS REQUERIDAS** | **ESPECIFICACIONES TECNICAS DEL BIEN OFERTADO** | **MODELO Y/O MARCA** | **PAÍS DE ORIGEN** |
| **Lote II: Expansión Clúster de Nutanix Base de Datos**  **Nota: Colocar en el recuadro especificaciones técnicas del bien ofertado, el detalle del requerimiento ofertado junto al número de página dentro de la oferta o manual del fabricando donde se encuentra o especifica dicha información.** | | | | | |
| **2.1** | **Nodos de Cómputo y Almacenamiento** | Se requieren un (1) LA NX-3235-G9 2 NODE 2X INTEL SYST XEON-GOLD 5415+ PROC 2.9G 8C 150W, con las siguientes características: - Ocho (8) Memoria RAM de 128GB MEM MOD 4800MHZ DDR5 MEM RDM - Doces (12) Disco Duro SSD de 3.84TB. - Dos (2) Módulos LOM SMC 10GBE 2P WRLS BASE-T AND 2P SFP+ NIC INTEL X710. - Dos (2) SMC 25/10GBE 2PORT NIC INTELCPNT E810 TRANSCEIVER NOT INCL - Dos (2) Power Cord C13/C14 10A 4FT  - Cuatro (4) OPT CBL 3M SFP+ TO SFP+ CM CABL OPT CBL 3M SFP+ TO SFP+ CM - Dos (2) TPM 2.0 MODULE UNPROVISIONEDBOPT |  |  |  |
| Incluir el licenciamiento SW-NCP-PRO-PR, NCP-NCM-PRO-PR y NCP-NCI-ULT-PR para los nodos NX-3235-G9 propuesto por al menos 3 años o 36 meses. |  |  |  |
| Incluir soporte y mantenimiento por parte del fabricante por al menos 3 años o 36 meses. |  |  |  |