Pliego de Prescripciones Técnicas

Suministro, instalación, mantenimiento y puesta en funcionamiento de un sistema de protección perimetral e interna en la red informática y comunicaciones de la agencia efe.
Nº de Expediente:

ÍNDICE

1.- OBJETO DEL PRESENTE PLIEGO

1.1 DESCRIPCIÓN DEL PROYECTO

El objeto del presente pliego consiste en definir las condiciones técnicas que debe cumplir la oferta presentada por el licitador para el suministro, instalación, mantenimiento, configuración y puesta en funcionamiento de un sistema de seguridad perimetral e interna en la red informática y de comunicaciones de la Agencia EFE, concebido y entendido como un proyecto "llave en mano".

Se definen los requerimientos básicos de los sistemas objeto del proyecto, así como los servicios adicionales en los términos descritos en los siguientes apartados.

El objeto del proyecto consiste en la puesta en funcionamiento de una solución integral, y no el suministro de soluciones independientes que cubran las necesidades planteadas de forma autónoma.

El periodo de garantía, mantenimiento, actualización y soporte será de 48 meses in situ a partir de la fecha de recepción del contrato.

La ejecución de los trabajos necesarios será planificada junto con el personal de la Agencia EFE con el objetivo de ser realizados en el menor tiempo posible, con nulo o mínimo impacto en la normal operativa de la organización.

Con el fin de coordinar adecuadamente estos trabajos a realizar, el integrador nombrará un Jefe de Proyecto, quien actuará como interlocutor principal ante el Responsable del proyecto de la Agencia EFE y supervisará en todo momento la calidad de los mismos.

2.- ESPECIFICACIONES TECNICAS DE LOS EQUIPOS

2.1.- PRESCRIPCIONES TÉCNICAS GENERALES

El equipamiento que se expone a continuación así como los detalles técnicos y funcionales requeridos, definen las características de los sistemas que se instalarán para dar respuesta a las necesidades de la Agencia EFE. En todo caso, el sistema propuesto debe estar formado por una solución integral y unificada, redundante y gestionable.

A continuación se detallan los **requerimientos mínimos de los sistemas** objetos del proyecto. Se valorará positivamente la mejora de los requerimientos mínimos de acuerdo a los criterios de valoración definidos en el presente anexo.

2.1.1.- Suministro de dos equipos para el sistema NGFW (Firewall De Nueva Generación).

2.1.1.1.- Características técnicas.

- 2 equipos físicos para instalación en alta disponibilidad, permitiendo tanto modo activo-activo como activo-pasivo, para lo que se requiere el suministro de dos sistemas con idénticas características técnicas.
- Rendimiento mínimo del servicio Firewall: 72 Gbps (55Gbps 64 byte UDP).
- Rendimiento mínimo de IPS: 11 Gbps.
- Rendimiento mínimo del servicio VPN (IPSec): 48 Gbps.
- Rendimiento mínimo del servicio NGFW (IPS, AppCtrl, WAF): 2.4 Gbps.
- Capacidad mínima de gestión de conexiones: 11.000.000 sesiones concurrentes, permitiendo como mínimo 290.000 sesiones por segundo.
- Los equipos propuestos deberán garantizar los rendimientos mínimos solicitados mediante el uso de procesadores específicos para el tratamiento correcto del tráfico.
- Número mínimo de interfaces:
  - 4 x 10GE SPF/+
  - 16 x GE SFP
  - 18 x GE RJ45
- Número mínimo de dominios virtuales: 10.
- Almacenamiento interno mínimo: 240 GB.
- Tamaño máximo por equipo enracable: 2U.
- Latencia máxima 3 microsegundos.
- Controlador Interno de APs.
- Fuentes de alimentación redundantes.

2.1.1.2.- Características funcionales de los servicios que deberá integrar el sistema requerido.

- Servicio Firewall.
  - Inspección profunda de contenido.

- Múltiples modos de despliegue (modos mirror, transparente y NAT/PAT).
- Capacidades de routing estático, policy based routing y routing dinámico, soportando BGP, OSPF, Rip v2 y Multicast, tanto para IPv4 y IPv6.
- Gestión de VLAN e integración de 802.1Q.
- Autenticación basada en grupos de usuarios.
- Capacidad de securización de VoIP.
- Protección basada en la creación de perfiles aplicables a usuarios individuales y/o grupos.
- Servicio VPN (Virtual Private Network).
- Protocolos soportados: PPTP, IPSec y SSL.
- Encriptación y autenticación: DES, 3DES y AES. SHA1 y MD5.
- Integración con firma electrónica.
- Modo de funcionamiento cliente/servidor y punto a punto.
- Cliente VPN propietario que asegure la integración con los sistemas ofertados.
- Modo proxy inverso que permita la publicación mediante portal web de aplicaciones tipo WEB, RDP, SSH, Acceso a carpetas y VNC.
- Cliente VPN para sistemas operativos IOS y Android.
- Servicio Antivirus y Antispyware.
- Protocolos que se requieren analizar: HTTP/HTTPS, POP3/POP3S, FTP, SMTP/SMTPS, IMAP/IMAPS, mensajería instantánea.
- Posibilidad de configurar por parte del administrador de la plataforma el funcionamiento en modo proxy (fichero) o en modo stream (flujo).
- Posibilidad de bloqueo de ficheros por tipo y tamaño.
- Posibilidad de gestión de archivos en cuarentena.
- Servicio de actualización de firmas de virus al menos 3 veces al día.
- Servicio IPS (Intrusion Prevention System).
- Análisis de tráfico e inspección IPS basado en los estándares de los diferentes protocolos.
- Debe disponer de más de 8.000 firmas de IPS.
- Deben actualizarse las firmas al menos 2 veces por semana.
- Posibilidad de creación y edición de firmas personalizadas.
- Escaneo de vulnerabilidades programable de servidores basado en las propias firmas de IPS.

- Servicio de Filtrado Web.
  - Protocolos a analizar: HTTP/HTTPS.
  - Categorización de contenidos web con más de 78 categorías con más de 50 millones de páginas categorizadas.
    - Creación de patrones para la definición de listas URL.
    - Bloqueo de contenidos web.
    - Posibilidad de fijación de cuotas de navegación por categoría.
    - Servicio de actualización en tiempo real de categorización de URL.

- Servicio de Control de Aplicaciones.
  - Control de más de 3.000 aplicaciones con independencia de los puertos y protocolo utilizados.
  - Identificación y control de aplicaciones categorizadas por tipo y funcionalidad.
  - Posibilidad de aplicar QoS por aplicación o grupo de aplicaciones, permitiendo tanto limitar el ancho de banda como fijar un ancho de banda garantizado.
  - Posibilidad de solicitar la identificación de nuevas aplicaciones.
  - Disponibilidad de un servicio de actualizaciones de nuevas aplicaciones.

- Servicio de Protección de Fugas de Información (DLP).
  - Soporte de los siguientes protocolos: HTTP/HTTPS, correo y mensajería instantánea.
  - Identificación y control de información corporativa sensible.
  - Análisis de los tipos de ficheros más utilizados (Microsoft Office y pdf).
  - Definición de patrones a nivel binario y de poder calcular el hash de los documentos a proteger para controlar su salida del perímetro.
  - Posibilidad de marcar documentos a proteger mediante una marca de agua identificable para evitar su salida de la organización.

- Servicio Antispam.
  - Protocolos a analizar: SMTP/SMTPS, POP3/POP3S e IMAP/IMAPS.
  - Gestión de listas negras RBL.
  - Posibilidad de bloqueo a nivel de dirección IP.
  - Posibilidad de filtrado por palabras y expresiones.

- Otras funcionalidades que otorgan valor añadido a la solución requerida.
  - Integración con Active Directory y con RADIUS/802. 1 X, pudiendo aplicar QoS a nivel de usuario o grupo de usuarios.
  - Licencias de usuario ilimitadas.
  - Capacidad de integrar, sin coste adicional, la funcionalidad de controlador de redes Wifi pudiendo aplicar políticas de control de aplicaciones, filtrado de URL, antivirus, IPS y calidad de servicio (QoS) a tráfico Wifi. Dispondrá de la posibilidad de suministro de Access Points adicionales, tanto de interior como de exterior, con varias antenas para la detección de Rogue Access Points. Dispondrá de una herramienta gratuita para planificación de cobertura.
  - Disponibilidad de certificaciones reconocidas en la industria (NSS Labs, ICSA Labs, Common Criteria EAL 4+, VB100).
  - Soporte del protocolo GRE, para el establecimiento y finalización de túneles en el mismo equipo.
  - Balanceo de líneas de acceso a internet con monitorización basado en ip origen o en anchos de banda.
  - Balanceo de carga a granjas de servidores.
  - Funcionamiento en modo proxy explícito.
  - Nat 64 y 46.
  - Control de ancho de banda basado en, IP, usuarios y/o aplicaciones.
  - Capacidad de aplicar perfiles de protección específicos (WAF) para entornos y aplicaciones web.

2.1.2.- Suministro de un equipo para el Sistema de Protección de Amenazas Avanzadas (APTS).

Los cibercriminales actualmente son más sofisticados y cada vez más, sortean las soluciones de antimalware tradicionales y son capaces de insertar en profundidad amenazas persistentes avanzadas en las redes. Estos ataques altamente dirigidos evaden la detección basada en firmas al

enmascarar la naturaleza malintencionada de muchas formas: compresión, cifrado, polimorfismo...

Combatir los ataques actuales requiere un enfoque amplio e integrado con una solución de Sandbox. Por este motivo es requisito que la arquitectura propuesta sea una solución sólida de detección y mitigación proactivas, información sobre las amenazas que requiere acción, y una implementación sencilla e integrada totalmente con la solución de NGFW anteriormente mencionada.

Características técnicas mínimas a cumplir.

- Debe admitir configuraciones vía interfaz web y CLI.
- Permitirá la creación de múltiples cuentas de administrador.
- Podrá realizarse la copia de seguridad y restauración de archivos de configuración.
- Generará un informe semanal para la lista de correo electrónico global y administrador.
- Tendrá actualizaciones automáticas de firmas frecuentes.
- Permitirá la supervisión de estado de VM.
- Soporte de enrutamiento estático.
- Entrada de archivos: Modo sin conexión/analizador de protocolos, carga de archivos a demanda, envío de archivos desde dispositivos integrados.
- API basada en web en la que los usuarios puede cargar muestras para explorar de forma indirecta.
- Opción para crear una red simulada de archivos explorados a los que acceder en un entorno de red cerrado.
- Integración de dispositivos:
  - Entrada de envío de archivos del Firewall, Sistema de Gestión segura de Mails.
  - Alojamiento de bases de datos de actualización.
  - Registro remoto: Servidor de Syslog o similar.
- Instancias de Windows simultáneas.
- Técnicas antievasión: sleep calls, consultas de registro y procesos.
- Detección de devolución de llamadas: visitas a URL malintencionadas, comunicación de C&C de botnet y tráfico de atacantes procedente de malware activado.
- Descarga de paquetes capturados, archivos originales, registros de seguimiento y capturas de pantalla.

- Soporte para tamaños de archivos ilimitados, tamaño de archivo máximo configurable.
- Soporte de tipos de archivos:
  - Archivado .tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj.
  - Archivos ejecutables (por ejemplo, .exe, .dll), PDF, documentos de Windows Office y Javascript.
  - Archivos multimedia: .avi, .mpeg, .mp3, .mp4.
- Detección de amenazas de red en modo de analizador de protocolos: Identificación de actividades de botnet y ataques de red, visitas a URL malintencionadas.
- Opción para enviar archivos sospechosos automáticamente al servicio en la nube para el análisis manual y la creación de firmas.
- Widgets de supervisión en tiempo real (visible por origen y opciones de periodo de tiempo): Estadísticas de resultados de detección, actividades de detección (a lo largo del tiempo), alojamientos dirigidos principales, malware principal, URL de infección principales, dominios de devolución de llamadas principales.
- Visor de eventos de obtención de detalles: Tabla dinámica con contenido de acciones, nombres de malware, clasificación, tipo, origen, destino, tiempo de detección y ruta de descarga.
- Registro: GUI, archivo de registro RAW de descarga.
- Generación de informes para archivos malintencionados: Informes detallados sobre las características y comportamientos de los archivos inspeccionados: modificación de archivos, comportamientos de procesos, comportamientos de registros, comportamientos de redes, instantánea de VM.
- Análisis posterior: Archivos descargables: archivos de muestreo, registros de seguimiento de SandBoxing y captura de PCAP.
- Motor de antivirus en tiempo real basado en CPRL (Compact Pattern Recognition Language).
- Deberá incluir las licencias de Sistemas Operativos necesarias de Windows de 32 y 64 bit así como IE y Office.
- Número mínimo de interfaces 6 GE RJ45.
- Número mínimo de 2 slots de GE SFP.
- Fuentes de alimentación principal y redundante.
- Almacenamiento interno: 4 TB (máx. 8 TB).
- Tecnología de SandBoxing de VM (archivos/hora): 160
- Detección de AV (archivos/hora): 6000
- Número de VM simultáneos: 8
- Tamaño máximo por equipo enracable: 2U.

- Fuentes de alimentación redundantes.

2.1.3.- Suministro de un equipo para un Sistema de Análisis de Red y Gestión de Informes.

Dada la complejidad del proyecto, será necesaria la incorporación de una solución que facilite el análisis centralizado de los posibles incidentes de seguridad, consolidar las funciones de análisis, llevar registro en diario y elaboración de informes en un único sistema. Además, deberá ofrecer funciones de elaboración de informes, minería de datos, análisis forense para la investigación de incidentes, archivado de contenidos, gestión de vulnerabilidades y aislamiento de archivos infectados.

Esta solución será la encargada de la recogida, el análisis y la correlación de datos de seguridad históricos y en tiempo real procedentes de los dispositivos incluidos en el presente pliego. Así pues, deberá ofrecer una representación sencilla y consolidada del estado de seguridad del entorno propuesto, lo que permitirá controlar las amenazas antes de que se abran paso a través del perímetro de seguridad y den lugar a posibles fugas de datos.

Características técnicas.

- Suministro de un sistema de análisis de red y gestión de informes en formato" appliance", equipo físico dedicado.
- Capacidad de recepción de información de más de 250GB/día.
- Ratio de Log sostenido: 3000.
- Soporte de más de 2.000 Dispositivos/ADOMs/VDOMs.
- Almacenamiento en disco duro de más de 8TB de capacidad.
- Numero de interfaces mínimos necesarios: 6x GbE, 2x GbE SFP.
- Deberá permitir la gestión de RAID en almacenamiento (0/1/5/10).
- Deberá disponer de fuente de alimentación principal y redundante conectable en caliente.
- Tamaño máximo por equipo enracable: 2U.
- Fuentes de alimentación redundantes.

Características funcionales que deberá integrar el sistema.

- Se requiere la integración total con el sistema NGFW contemplado en el presente pliego de prescripciones técnicas.
- Análisis de tráfico en tiempo real.

- Creación y gestión de informes predefinidos y personalizables sobre: ataques, virus, eventos, uso de servicios y recursos (correo, web, ancho de banda, entre otros).
- Análisis forense.
- Analizador de red.
- Integración con Active Directory.
- Posibilidad de monitorizar dispositivos SNMP y syslog externos.

2.1.4.- Suministro de un equipo para un Sistema de Gestión de Identidades y Control de Acceso.

Será necesario proveer de un sistema de autenticación segura compatibles con todos los dispositivos anteriormente descritos y que permitan la autenticación vía RADIUS o LDAP. Esta solución será de sencillo despliegue protegiendo el acceso a la infraestructura de la red de la Agencia EFE desde el primer momento. Deberá poder ser integrada a la perfección con los servidores LDAP y Active Directory existentes, lo que permitirá implementar una solución de autenticación sólida en el conjunto de la red.

Además el sistema deberá ser capaz de proveer doble factor de autenticación para el acceso seguro a la red, mediante el uso y administración de tokens físicos, virtuales (correo electrónico o SMS) o mobile para iOS y Android.

Características técnicas mínimas a cumplir.

- Deberá proveer autenticación LDAP y RADIUS para SSL VPN.
- Deberá proveer exploración remota SSL VPN con autenticación LDAP.
- Dispondrá de portal social cautivo Wifi (Facebook, Twitter, Google+, LinkedIn, basada en formularios).
- El Sistema dispondrá de funcionalidades para garantizar el acceso mediante doble factor de autenticación físico, virtual o mobile.
- En combinación con el sistema de NGFW solicitado en apartados anteriores, el sistema proveerá de SSO y DC Polling.
- El sistema dispondrá de funcionalidades Single Sign-On.
- Permitirá la posible asignación de usuarios Wifi dinámicamente a VLANs, la autenticación RADIUS y Single Sign-on.
- Número mínimo de interfaces: 4 x 10/100/1000
- Número mínimo de usuarios finales: 2000

- Licencias de usuario ilimitadas.
- Fuentes de alimentación redundantes.

2.2. PRESCRIPCIONES TÉCNICAS ADICIONALES

La naturaleza del proyecto requiere la búsqueda de una solución integral y unificada, que independice las tareas de monitorización con las tareas propias de un sistema de Firewall de nueva generación, sistema anti APTs y autenticación. Para ello se hace necesario el suministro de 3 sistemas independientes y a la vez complementarios entre sí. Por otro lado se requiere la perfecta integración con los sistemas disponibles en la red de la Agencia EFE.

Junto a las prescripciones técnicas y funcionales ya descritas en el apartado anterior, el proyecto deberá contemplar un conjunto de servicios adicionales encaminados a la mejora del rendimiento de la red informática y de comunicaciones de la Agencia EFE, así como a mejorar la seguridad y visibilidad de la información que circula por ella.

A continuación se detallan los requerimientos mínimos que deben cumplir los servicios y características adicionales requeridas. Su mejora será valorada positivamente de acuerdo a los criterios de valoración detallados en el presente anexo.

2.3. SERVICIOS Y CARACTERÍSTICAS ADICIONALES

Servicios adicionales.

- Elaboración de un documento de solución que se adapte a las necesidades de la Agencia EFE.
- Servicio de formación durante al menos dos días en las instalaciones de la Agencia EFE.

Características adicionales.

- Certificaciones emitidas por organismos independientes a favor de los productos ofertados y los servicios que lo integran, teniendo en cuenta el prestigio del organismo certificador, así como los servicios y la fecha de certificación.

3. GARANTÍAS.

Se definen los plazos y detalles de las **garantías mínimas** requeridas al fabricante y licitador.

3.1 GARANTÍA POR PARTE DEL FABRICANTE.

- Duración de la garantía: 4 años.
- Mantenimiento de hardware en modo 24x7 con reemplazo en modalidad de "siguiente día laborable".
- Mantenimiento de software en modo 24x7. Asistencia web y telefónica personalizada.
- Servicio de actualizaciones de servicios firmware, antivirus, IPS, filtrado web y aplicaciones.

3.2 GARANTÍA POR PARTE DEL LICITADOR.

- Mínimo disponer de la certificación Platinum Partnerdel fabricante propuesto.
- Certificado con ISO 9000, 14000, 20000 y 27001.
- Duración de la garantía: 4 años.
- Horario de atención telefónica a incidencias: 24x7.
- Asistencia ONSITE en las dependencias del cliente de un técnico para la reparación y sustitución de hardware deteriorado con la última configuración conocida. Tiempo de respuesta "siguiente día laborable".
- Soporte a la gestión de cambios sobre configuración de software y plataforma.

3.3 ESPECIFICACIONES DE LAS GARANTÍAS

Servicio de Garantía, Soporte y Mantenimiento.

El periodo de garantía, actualización y soporte será de 48 meses in situ a partir de la fecha de recepción del contrato.

3.3.1 Garantía, soporte y mantenimiento por parte del licitador:

- Duración de la garantía: 4 años (periodo estimado de obsolescencia).
- Horario de atención telefónica a incidencias 24x7.
- Asistencia ONSITE en las dependencias del cliente de técnico para la reparación y sustitución de hardware deteriorado con la última

configuración conocida. Tiempo de respuesta "Siguiente Día Laborable".
- Soporte a la gestión de cambios sobre configuración de software y plataforma.

Dentro del plazo de garantía el adjudicatario estará obligado a realizar gratuitamente, las revisiones preventivas, reparaciones y sustituciones necesarias, incluida la reposición de piezas o la suplencia del equipo averiado mediante otro de reserva, en caso preciso, para un uso continuado de los equipos, sin límite de horas de funcionamiento, así como la inclusión de todos los componentes de cualquier clase. En este sentido, deberán especificarse, pormenorizadamente, los componentes que a juicio del ofertante quedarían excluidos de esta circunstancia.

El soporte técnico para reparación y sustituciones de hardware será in situ.

En el caso de que la avería denunciada afecte al disco duro y su reparación conlleve la pérdida de programas comerciales de una sola carga que residan en el disco duro, el adjudicatario repondrá los programas en el disco reparado.

El adjudicatario se compromete a no dar a la información y datos proporcionados por la Administración, cualquier uso no previsto en el presente Pliego. En particular, no proporcionará sin previa autorización del Organismo, copia de los documentos y/o datos a terceras personas, bajo pena de resolución del contrato con pérdida de la fianza definitiva, todo ello sin perjuicio de la responsabilidad civil o penal que procediere.

El adjudicatario se compromete al cumplimiento estricto de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD) en todos aquellos artículos relacionados con la prestación del servicio informático objeto del Pliego.

En todo caso, el adjudicatario será responsable de los daños y perjuicios que se deriven del incumplimiento de esta obligación.

El adjudicatario se compromete a:

- Suministrar e instalar el material hardware/firmware necesario para mantener actualizados los sistemas.
- Comprobar las versiones del sistema operativo y diagnósticos asociados, manteniendo todos los sistemas al mismo y último nivel.
- Siempre que aparezca en el mercado una nueva versión o release de software se enviará el producto junto a la documentación precisa para su evaluación por la Agencia EFE, quien decidirá su implantación. La empresa adjudicataria, en todo caso, suministrará las copias necesarias para la sustitución de las existentes y sin

que ello suponga coste adicional para la Agencia EFE durante ese período de garantía.

- Se incluirán, para los equipos que dispongan de estos elementos, las suscripciones de firmas y patrones de malware/intrusiones y de filtrado URL, las actualizaciones de software correspondientes.
- La empresa adjudicataria indicará en su oferta el sistema de comunicación a emplear por el usuario, con el fin de minimizar el tiempo de respuesta.
- Dicha solicitud será formulada por el usuario aportando al servicio técnico de garantía los datos que éste estime oportunos, para lo cual la empresa licitadora deberá incluir en la oferta un modelo de petición de asistencia técnica en el que figuren los datos que permitan conocer las características del equipo, su ubicación, el problema existente, la fecha y hora de solicitud de la asistencia, la solución aportada y la fecha y hora en que se produjo ésta.

3.3.2. Garantía por parte del fabricante:

- Duración de la garantía: 4 años.
- Mantenimiento de hardware en modo 24x7 con reemplazo "Siguiente Día Laborable".
- Mantenimiento de software en modo 24x7. Asistencia web y telefónica personalizada.
- Servicio de actualizaciones de servicios firmware, antivirus, IPS, filtrado web y aplicaciones.