CONSEJO GENERAL DEL PODER JUDICIAL
Centro de Documentación Judicial

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SUMINISTRO DE DOS DISPOSITIVOS FIREWALL, ASÍ COMO DE LOS SERVICIOS DE SOPORTE EXPERTO DE LA PLATAFORMA DE SEGURIDAD PERIMETRAL DEL CENTRO DE DOCUMENTACIÓN JUDICIAL EN SAN SEBASTIÁN.

ÍNDICE:

1.- Antecedentes 2
2.- Objeto del contrato 3
3.- Descripción técnica del servicio a contratar 3
3.1. Características del equipamiento a renovar que sustituirá a los dispositivos ASA (Cisco) 3
3.2. Instalación y migración de los nuevos equipos, y adecuación de la infraestructura existente 6
3.3. Arquitectura física y datos de configuración de la actual plataforma de seguridad perimetral 8
3.4. Soporte experto de la plataforma 9
3.5. Acuerdo de nivel de servicio (SLA) 10

Anexo PPT-I 12

1 – ANTECEDENTES

El Centro de Documentación Judicial (CENDOJ) necesita asegurar la infraestructura tecnológica sobre la que se basan los servicios on-line que ofrece a la carrera judicial y al resto de ciudadanos. La renovación, en algunos casos, y creación de servicios que se ha llevado a cabo a lo largo de los últimos años (correo para jueces, portal web, fondo documental), así como la creciente demanda de estos servicios hace necesario ir adecuando los mecanismos que protegen y al mismo tiempo permiten ofrecer estos servicios de forma segura.

Para ello dispone de una plataforma de seguridad perimetral que consiste básicamente en dispositivos tipo firewall configurada en dos niveles y formada por cuatro equipos: dos para la seguridad más externa de la red (ASA Cisco), y otros dos para la seguridad más interna consistentes en lo que denominan "appliances" (combinación lista para usarse de hardware y software) modelo 4400 de CheckPoint. La duplicidad de los equipos de cada nivel dota a la plataforma de características de alta disponibilidad prácticamente obligatoria para este tipo de instalaciones.

Los equipos actúan como cortafuegos perimetrales encargados de filtrar el tráfico entre el CENDOJ y las redes externas como Internet u otras redes judiciales. El adecuado soporte de los equipos requiere de un conocimiento experto que permita una ágil solución de problemas, la sustitución de piezas y el asesoramiento en actualización de versiones. El soporte de dichos equipos y sus módulos en el caso de los dispositivos Checkpoint finaliza el 31 de diciembre de 2021, pero los equipos ASA de Cisco finalizan su ciclo de vida en agosto de 2022. Esto significa que el fabricante no va a dar soporte sobre este tipo de equipos, situación que obliga a revisar la configuración de la plataforma y actualizarla como mínimo sustituyendo estos equipos por nuevos dispositivos antes de esa fecha.

Con esta licitación se pretende abordar la actualización de la plataforma en 2021, con la sustitución de los actuales equipos ASA CISCO por nuevos dispositivos que además de mantener su función actual permitan mejorar las medidas de seguridad que el conjunto aplica en el acceso a los servicios que se ofrecen desde el CENDOJ. Los nuevos dispositivos de seguridad deberán incluir funcionalidades avanzadas de control por aplicación, DPS/IPS (detección/ prevención de intrusos), antimalware, antispam, filtrado de tráfico web, que se han ido añadiendo a la funcionalidad básica de control del tráfico de red y su aplicación permitirá mejorar la seguridad de acceso a los servicios que se ofrecen. Se tendrá en cuenta la infraestructura tecnológica del CGPJ, con el objetivo de facilitar la gestión tanto técnica como administrativa.

Por todo esto el CENDOJ está interesado en que se promueva el procedimiento de contratación para:

- el suministro, instalación y migración de dos dispositivos tipo NGFW (Next Generation FireWall) en configuración de alta disponibilidad, que sustituirán los actuales dos equipos ASA (Cisco) ya obsoletos. Deberá incluir una garantía del fabricante tanto software como hardware por un periodo de tres años, si bien se valorará la extensión de la misma hasta cinco años.
- un soporte experto del equipamiento que conforma toda la plataforma de seguridad perimetral completa (incluidos los equipos Checkpoint), por un periodo de un año.

2 - OBJETO DEL CONTRATO

El objeto del presente expediente es la licitación del suministro de dos dispositivos firewall, así como de los servicios de soporte experto de la plataforma de seguridad perimetral del CENDOJ en su sede de San Sebastián.

En concreto consiste en:

- suministro de dos dispositivos firewall tipo NGFW (Next Generation FireWall) en configuración de alta disponibilidad, que sustituirán a los dos equipos ASA (Cisco) de los que dispone actualmente el CENDOJ, equipos ya obsoletos, incluyendo instalación y migración, así como una garantía del fabricante tanto software como hardware por un periodo tres años, si bien se valorará la extensión de la misma hasta cinco años.
- servicios de soporte experto del equipamiento que conforma toda la plataforma de seguridad perimetral, por un periodo de un año, para la gestión del soporte de primer nivel del fabricante y para la operación de los equipos, tanto los renovados como los existentes.

El adjudicatario desarrollará sus servicios desde sus propias instalaciones, excepto en lo que resulte imprescindible la presencia in-situ en las instalaciones del CENDOJ en San Sebastián para el correcto desarrollo de las tareas que forman parte del servicio.

3 – Descripción técnica del servicio a contratar

3.1 - Características del equipamiento a renovar que sustituirá a los dispositivos ASA (Cisco).

Consiste en el suministro de 2 Firewall de Altas prestaciones (NGFW Next Generation Firewall), que además soporten la característica de IPS. Deberán poder configurarse en alta disponibilidad a nivel físico con un mínimo de cuatro nodos y también deben permitir su particionamiento en firewalls virtuales con

políticas de seguridad independientes. Así mismo, los firewalls virtuales deberán poder comunicarse entre sí mediante enlaces virtuales. También deben incluir un procesador dedicado para las funciones de IPS, inspección SSL y encriptación/desencriptación, y otro exclusivo para tareas relativas a enrutamiento, con el fin de que no se sature la CPU de control en caso de volúmenes de tráfico elevados. Se requiere que los equipos suministrados sean de un sistema del mismo fabricante y como mínimo con las mismas funcionalidades que los equipos existentes, aunque con el dimensionamiento acorde con las nuevas necesidades.

Cada uno de los nodos deberá poder ser accedido de forma independiente y configurado a pesar de no ser el nodo activo. También se requiere que sea posible acceder a ellos de forma directa sin tener que usar terceros elementos para modificar cualquier aspecto de su configuración.

A nivel IP deberán disponer de un mecanismo de MAC virtual que no requiera diferentes direcciones IP en cada uno de los interfaces de servicio para ofrecer la alta disponibilidad, es decir, cada pareja de interfaces (nodo activo/pasivo) dispondrá una sola dirección IP. También debe permitir un modo de funcionamiento de HA (alta disponibilidad) de tipo activo/activo.

Además de los anteriores aspectos también debe soportar las siguientes características:

- Capacidad de SD-WAN
- Proxy Explicito
- IPv6
- Inspección de tráfico fuera de línea (offline Inspection)
- Antivirus
- Antimalware
- Controlador wireless
- Configuración vía API
- Control de aplicaciones
- Control de URLs (Filtrado Web)
- Capacidad de concentrador de VPN IPSec/SSL
- Capacidad Web SSL VPN (sin cliente)
- Soporte para túneles VXLAN nativos

Las características funcionales de la solución ofertada deberán cumplir los siguientes requisitos:

- Rendimiento mínimo de Firewall (IPv4/ IPv6 en tamaño de paquetes de 1518 / 512 / 64 byte, UDP): 20 / 18 / 10 Gbps respectivamente.
- Rendimiento mínimo IPS (Optimal Traffic Mix / Enterprise Mix): 2.6 Gbps.
- Rendimiento mínimo del servicio VPN (IPSec): 11.5 Gbps.
- Rendimiento mínimo CAPWAP: 15 Gbps.
- Controlador Interno de APs (Total / Tunnel Mode): 128 / 64.
- Rendimiento mínimo NGFW (Enterprise Mix): 1.6 Gbps.
- Rendimiento mínimo Threat Protection (Enterprise Mix): 1 Gbps.
- Capacidad mínima de gestión de conexiones (TCP): 1.5 Millones concurrentes, permitiendo como mínimo 56.000 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:
    - 12x Puertos Hardware Accelerated GE RJ45.
    - 1x / 2x / 1x Puertos GE RJ45 Management/HA/DMZ.
    - 2x GE RJ45 WAN Ports.
    - 4x GE RJ45 or SFP Shared Ports
    - 4x SFP Slots GE.
    - 2x SFP 10GE
    - 1x USB Ports.
    - 1x Console Port.
- Número mínimo de Dominios Virtuales: 10 los cuales deberán estar incluidos de serie sin necesidad de licenciamiento adicional.
- Almacenamiento interno mínimo: 1x 480 GB SSD.
- Tamaño máximo por equipo enracable: 1 RU
- Latencia máxima Firewall (64 byte, UDP) 4.97 µs.

Los equipos deben tener las funcionalidades integradas de UTP Protection (Application Control, IPS, AMP, Web Filtering and Antispam Service). No se acepta ningún acuerdo OEM con terceros, es decir, todas estas funcionalidades tienen que ser del propio fabricante de seguridad.

El licenciamiento de las funcionalidades ha de basarse por equipo, no por usuario. En concreto las conexiones VPN no deberán estar limitadas en número.

Para asegurar la fiabilidad de los nuevos equipos y una calidad del servicio, el cortafuegos debe tener las certificaciones de ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN, y el fabricante del cortafuegos debe estar clasificado en el cuadrante de Gartner como líder de mercado.

Ninguno de los elementos hardware ofertados podrá encontrarse incluidos en procesos de discontinuidad, descatalogación o fin de vida del fabricante.

Todo el equipamiento suministrado deberá incluir una garantía del fabricante tanto software como hardware, debidamente registrada con el fabricante, por un mínimo de tres años, si bien se valorará la extensión de la misma hasta cinco años.

Esta garantía del fabricante para los nuevos equipos físicos y para el software propuesto para los mismos será en modalidad 24x7xNBD y debe contemplar:

- Reemplazo avanzado de piezas averiadas.
- Acceso al TAC del fabricante para resolución de casos.
- Acceso a las actualizaciones de las versiones de software de los equipos y acceso a parches que resuelvan fallos.
- Acceso a datasheets y especificaciones del fabricante.
- Release Notes.

3.2 - Instalación y migración de los nuevos equipos, y adecuación de la infraestructura existente.

Consiste en la instalación, implantación y migración de la configuración actual de los equipos Cisco a renovar, a los nuevos dispositivos objeto de esta licitación, cuya descripción se detallará en el proyecto de instalación.

Se replicará la configuración actual según las especificaciones del punto 3.3. de este pliego. La solución propuesta por el adjudicatario deberá cubrir la funcionalidad actual también en cuanto a la existencia de redes actuales y grado de conectividad. Se contemplará si es necesario en el proceso de migración la configuración básica de funcionalidad adicionales que los nuevos equipos modernos aporten como novedad a la configuración actual.

El proyecto de instalación, que deberá aportarse como documento, incluirá:

- Informe detallado de las medidas a abordar.
- Plan de migración, con especial hincapié en los cambios que impliquen corte de servicio y duración de estos,

Igualmente deberá entregarse como documentación:

- Medios que la empresa ponga a disposición,

- Cronograma de actuaciones.

El adjudicatario deberá garantizar la total compatibilidad e integración de los componentes que proponga, con los elementos existentes en el Centro de Proceso de Datos (CPD) del CGPJ.

El CENDOJ pondrá a disposición del adjudicatario los recursos de acceso a la infraestructura necesarios para la ejecución del proceso objeto del contrato.

Las versiones de s.o y software que se utilicen serán las más recientes posible, que aseguren la estabilidad y fiabilidad de la plataforma a instalar.

Como parte de la integración con la infraestructura existente, se requiere incluir en el proyecto de instalación la actualización de los equipos Checkpoint a la última versión establece compatible con el modelo concreto de los equipos existentes en el Cendoj (especificaciones detalladas en el punto 3.3) de este pliego.

Pruebas de la nueva arquitectura

Cada uno de los elementos incorporados y/o modificados deberá validar su funcionamiento físico y lógico tanto a nivel individual como desde el punto de vista de la funcionalidad completa que debe proporcionar en un entorno en producción.

Coexistencia de plataformas.

Se requiere la coexistencia de las plataformas, actual y nueva, durante el proceso de migración, que aseguren el servicio y minimicen los cortes. Permitirá la realización de las pruebas de validación de la nueva plataforma y la comparación con la actual, así como la posibilidad de vuelta atrás en caso de problemas hasta la solución de estos y la migración definitiva.

Plazo de instalación y migración.

Se establece un plazo máximo de 3 meses desde la formalización del contrato, para el suministro de dispositivos, instalación y migración. A la finalización de dicho plazo los nuevos dispositivos firewall deberán estar plenamente operativos e integrados en la plataforma de seguridad perimetral del CENDOJ.

Asistencia de integración

El adjudicatario asistirá y se coordinará con los equipos de desarrollo y soporte de las diferentes plataformas de servicios del Cendoj para asegurar la continuidad de los servicios que la plataforma de seguridad web y balanceo ofrece a estas.

Documentación

Finalizados los trabajos se deberá aportar toda aquella documentación del sistema que resulte útil en el soporte posterior del mismo, desde el punto de vista técnico:

- Manuales de explotación, donde se detallen los pasos para manejar cambios simples en los equipos instalados, en base a la arquitectura definida.
- Volcado de las configuraciones de todos los elementos.
- Toda aquella documentación y gráficos detallados que aporten descripción de la arquitectura definitiva.

La documentación generada será propiedad exclusiva del CGPJ.

Formación

El adjudicatario deberá ofrecer al personal del CGPJ unas jornadas de formación con el fin de traspasar el conocimiento básico de la nueva infraestructura.

Dicha formación será al menos de 1 jornada y el lugar de impartición de esta podrá ser en la sede del CENDOJ en San Sebastián.

Certificación de fabricante

El licitador deberá disponer de acuerdos documentados con el fabricante de los productos objeto del servicio, que aseguren su capacidad para la implantación y configuración de estos.

3.3 - Arquitectura física y datos de configuración de la actual plataforma de seguridad perimetral

Por motivos de seguridad la descripción detallada de la arquitectura y configuración de los equipos que forman parte de la infraestructura actualmente instalada se suministrará exclusivamente a petición expresa de las empresas licitadoras que así lo soliciten, de modo que pueden valorar el proceso de migración e implantación requerido.

Las empresas licitadoras interesadas deberán solicitar al correo electrónico *unidad.contratación@cgpj.es* el envío de la documentación anteriormente mencionada. Para ello deberán adjuntar obligatoriamente en el correo de solicitud, el documento "solicitud de documentos y declaración de confidencialidad" que figura como "Anexo PPT-I" en este mismo pliego, que deberá ser cumplimentado, firmado y sellado, siendo requisito previo e indispensable para poder obtener la citada información.

3.4 - Soporte experto de la plataforma.

Consiste en la gestión del soporte del fabricante para los equipos físicos y software que formarán parte de la plataforma de seguridad perimetral de la sede del CENDOJ en San Sebastián, formado por los equipos actuales Checkpoint, y los nuevos equipos a suministrar objeto de este contrato una vez terminada la migración e implantación. El soporte experto incluirá además servicios de service desk integral así como de corrección de problemas y adecuación de las plataformas, cuya descripción se detalla:

- Gestión de una garantía del fabricante según el SLA requerido que incluye:
  - Reemplazo avanzado de piezas averiadas.
  - Acceso al TAC del fabricante para resolución de casos.
  - Acceso a las actualizaciones de las versiones de software de los equipos y acceso a parches que resuelvan fallos.
  - Acceso a datasheets y especificaciones del fabricante.
  - Release Notes.

- Servicios de Service Desk Integral:
  - Service Desk: Como interlocución con el CENDOJ, el adjudicatario deberá contar con un Service Desk (al que se podrá acceder tanto por vía telefónica mediante número gratuito, como web y por correo electrónico) que permita, como mínimo:
    - Gestión y atención de Incidencias
    - Gestión de Reemplazos
      - Gestión de Stock
      - Gestión de la garantía del fabricante.
    - Informe accesible vía web de incidencias.
    - Atención a consultas del servicio.
    - Apertura de casos con el fabricante y gestión de la garantía del fabricante extendida incluida.

  - Corrección de problemas.
    - Nivel 1: Presencia in situ para reemplazo de piezas si así se solicita.
    - Nivel 2: Diagnóstico y resolución de incidencias complejas.
    - Nivel 3: Apertura y seguimiento de casos específicos con fabricantes.

  - Adecuación de las plataformas.
    - Suministro de información de nuevas actualizaciones.
    - Instalación de nuevas versiones correctivas y/o actualizaciones correctivas que resuelvan un fallo, con presencia in situ en caso de que así se solicita.

Para la estimación de los recursos del servicio, se ha de contemplar con carácter orientativo que el número de incidencias de consultas serán de una consulta al mes. También se tendrá en cuenta en la estimación, la cadencia de publicación de las versiones de los productos que forman parte de la plataforma y que obliguen a una actualización. Así mismo se prevé que la renovación de dos dispositivos de los que forman parte de la plataforma podrá requerir una asistencia puntual extraordinaria posterior a la migración. Esta circunstancia también deberá ser tenida en cuenta.

En todo caso, la actualización de los dispositivos Checkpoint a una versión moderna y estable forma parte del proyecto de instalación referido en el apartado 3.2.

3.5 - Acuerdos de Nivel de Servicio (SLA).

Los Acuerdos de Nivel de Servicio que se establecen para incidencias críticas será de 24x7 (horario de atención de 24 horas durante los 7 días de la semana) con un tiempo de respuesta de 4h desde la apertura de la incidencia. Se consideran incidencias críticas aquellas que provocan corte de servicio.

Para el resto de las incidencias serán:

- Régimen de Prestación: 5x8 (horario de atención de 8 horas durante los 5 días laborables de la semana)
- Tiempo de Respuesta: ≤ Next Bussiness Day (al día siguiente laborable)
- Tiempo de Presencia in situ: ≤ Next Bussiness Day
- Tiempo de Reemplazo: ≤ Next Bussiness Day
- Tiempo de Resolución: ≤ Next Bussiness Day
- El Next Bussines Day tiene las siguientes características:
- Horario de recepción de incidencias: Horario laboral (de lunes a viernes durante la franja laboral diaria de 8 horas, 8:00 – 18:00).
- Reparación o sustitución de material afectado como máximo al siguiente día laborable
- Desplazamiento de un técnico a las instalaciones del CGPJ en los casos en que el soporte remoto no pueda diagnosticar y/o solventar la incidencia en los tiempos establecidos para la prioridad asignada.
- Deberá contemplar una vez al año la actualización del software (firmware) de todos los equipos soportados en este contrato. Igualmente, si el fabricante recomendara una actualización

adicional en casos de grave vulnerabilidad de los equipos, también se incluiría dicha actualización o parcheo.
En cualquier caso, estas actuaciones deberán acordase y ser validadas por el CENDOJ.

ANEXO PPT-I

SOLICITUD DE DOCUMENTACIÓN Y DECLARACIÓN DE CONFIDENCIALIDAD

¡¡ AVISO: este documento deberá ser firmado digitalmente!!

D./Dª , titular del DNI , en representación de la empresa , solicita, a los exclusivos efectos de poder evaluar su participación en el procedimiento de licitación objeto de los pliegos de los que este documento forma parte, la descripción de la arquitectura y configuración de los equipos que integran la infraestructura instalada actualmente.

A tal fin, en la representación que ostenta,

SE COMPROMETE:

A respetar el carácter confidencial de la información que reciba y a mantener absoluta reserva sobre la misma, que no podrá copiar o utilizar con ningún otro fin, ni tampoco ceder a otros ni siquiera a efectos de documentación.

Asimismo en el caso de no resultar adjudicatario, se compromete a destruir la totalidad de la información que reciba y de cuantas copias hubiera realizado, siendo la fecha límite de destrucción la de adjudicación del procedimiento de licitación, o bien con carácter previo si decidiera no participar o desistir de esta licitación.

Y para que conste la conformidad y adecuada comprensión de las obligaciones asumidas, firma el presente documento,

En , a de de 2021

Fdo. D./Dª: