**ANEXO I..- PLIEGO DE ESPECIFICACIONES TÉCNICAS PARA EL SUMINISTRO, INSTALACIÓN Y CONFIGURACIÓN DE DOS FIREWALLS Y LICENCIAS EN MODO HA**

## PRIMERA. PRESCRIPCIONES GENERALES

El presente pliego describe las características técnicas necesarias, según el criterio de la Fundación CENER (en adelante CENER), para el suministro, instalación y configuración de dos Firewalls en modo HA (en adelante, el "**Equipo**") a entregar en el Centro de proceso de datos de CENER sito en Sarriguren (Navarra)**,** Avenida Ciudad de la Innovación nº 7.

Los equipos que a continuación se describen, así como sus características técnicas, tienen el carácter de mínimas aceptables, siendo susceptibles de mejora y ampliación por cada licitador, el cual lo deberá justificar razonadamente a fin de ser tenido en cuenta por la Mesa de Contratación.

## SEGUNDA. DESCRIPCION DEL SUMINISTRO

Las ofertas deberán detallar claramente cada elemento u opción, identificándolos con el fabricante y la referencia de producto o código aplicable. Asimismo, las empresas licitadoras deberán indicar en la documentación de la oferta todas las mejoras y características del producto.

Todo el material deberá ser nuevo, adquirido y registrado a nombre de la Fundación CENER.

La empresa adjudicataria deberá suministrar, instalar y configurar una solución de Firewall en modo HA en formato enracable en bastidores estándar, junto con los elementos adicionales y licencias que sean necesarios para su puesta en funcionamiento.

Para la selección del Equipo seleccionado se tendrán en cuenta los siguientes criterios y sus correspondientes ponderaciones.

### 2.1.- Criterios mínimos:

El Equipo deberá incluir, al menos, las siguientes especificaciones técnicas que son considerados como mínimos indispensables:

#### 2.1.1.- Firewall :

La empresa adjudicataria deberá suministrar dos Firewalls idénticos con las siguientes características mínimas:

- Soporte Equipos en HA, tanto activo/pasivo como activo/activo
- Los equipos deben disponer de hardware independiente de gestión integrado en el equipo, no valdrá usar un plano de gestión que retire CPUs del equipo para este cometido
- Tiene que soportar la inspección de todo el tráfico de la capa 7, lo que permite identificar y clasificar todas las aplicaciones, en todos los puertos y en todo momento
- El equipo debe poder ser completamente gestionado tanto desde entorno Web como desde entorno CLI
- Los equipos deben soportar protocolos de Enrutamiento (routing):
    - Protocolos dinámicos de routing: RIP, OSPF y BGP
    - Soporte de routing para tráfico multicast (PIM Sparse Mode)
    - Soporte de Policy Routing.
- Deben ser capaces de aplicar QoS por aplicación, usuario o URL. Establecimiento de ancho de banda máximo y garantizado. La activación de esta funcionalidad no debe mermar el resto de las capacidades exigidas en la solución, ni en funcionalidad ni en rendimiento.
- Cada equipo al menos debe disponer de los siguientes puertos
    - 8 puertos 10/100/1000
    - Al menos 4 SFP+ 10GB para la unión con la electrónica de red de Cener
    - 1 puerto de gestión fuera de banda 10/100/1000
    - 1 puerto HSCI de 10 Gb de alta disponibilidad
    - 1 puerto de consola RJ-45
- Cada equipo tendrá doble fuente de alimentación
- Requisitos de capacidad y rendimiento:

| REQUERIMIENTO | VALOR MÍNIMO |
|---|---|
| Firewall throughput | 8,9/6,8 Gb/s |
| Threat Prevention throughput con los siguientes servicios activados: App-ID, el sistema de prevención de intrusiones, la protección antivirus y antispyware, WildFire, DNS Security, el bloqueo de archivos y la creación de logs activados | 3,3/3,2 Gb/s |
| IPSEC VPN Throughput | 4,6 Gb/s |
| Capacidad total de sesiones | 945 000 |
| Nuevas sesiones por segundo | 100 000 |

- El fabricante debe tener publicadas las guías de configuración recomendadas del Centro Criptológico de Seguridad, CCN-STIC
- El producto ofertado debe aparecer en el Catálogo de Productos de Seguridad TIC, CPSTIC, recomendados por el Centro Criptológico Nacional.

### 2.1.2.- Licencias /Software

- FW compatible con el sistema operativo PAN-OS

- Al menos las licencias suministradas deben tener la capacidad de:

    - Integración e identificación de usuarios con el Directorio activo.
    - La posibilidad de aplicar políticas de protección ante vulnerabilidades y exploits tanto al tráfico entrante como al saliente.
    - Protección ante ataques de denegación de servicio.
    - Definir políticas de antivirus, que analice descargas de ficheros realizadas en sentido Internet red Interna o viceversa y bloque si su contenido es malicioso.
    - Debe soportar la creación de categorías de URL y la inspección o no del tráfico cifrado SSL en base a dichas categorías. Descifrado de tráfico SSL sobre cualquier puerto.
    - Capaz de detectar el envío de credenciales corporativas, de forma que se pueda advertir, bloquear o permitir dicho envío de credenciales.
    - Servicio de DLP se debe integrar nativamente en el firewall sin necesidad de desplegar ni configurar equipos adicionales
    - Capacidad de detección de malware desconocido en base a tecnología de sandboxing en la nube. El sistema de análisis de amenazas en cloud debe estar ubicado en la Unión Europea, y que pueda acreditar el cumplimiento de las normativas Europeas en materia de protección de datos.
    - Capacidad para detectar y prevenir de manera automática y dinámica las peticiones de DNS maliciosas asociadas con dominios de malware
    - VPNs – site to site ,usuario y móvil (GlobalProtect)

- Todas las licencias software que se suministren deberán ser registradas a nombre de CENER.

### 2.1.3.- Condiciones de suministro:

La Memoria técnica a presentar por el licitador deberá incluir los siguientes extremos:

- **Condiciones de instalación, configuración y puesta en marcha del Equipo:**

    - La empresa adjudicataria entregará los Equipos en el Centro de proceso de datos de CENER sito en Sarriguren (Navarra), realizando previamente una planificación que deberá ser acordada con CENER.
    - El plazo máximo para la entrega de los equipos será inferior a 8 semanas desde la firma del contrato.
    - La Instalación física de los Firewalls la realizara el equipo de sistemas de Cener.
    - Unión de cada Firewall con la electrónica de red de cener, dos conexiones 10Gb por equipo .

- Migración de la política y configuración del equipamiento que va a ser sustituido, incluidos todos los servicios de configuración necesarios para operar en las mismas condiciones actuales (conexiones vpn Sites, reglas, rutas, etc…).
- Revisión y mejoramiento de las reglas actuales.
- Integración con active/directory,y Fortitoken.
- Despliegue de ssl decrypt.

- **Garantía y soporte técnico:**

  - Los componentes hardware y software suministrados deberán contar como mínimo con una garantía y soporte técnico in situ de tres años ofrecido por el fabricante, se deberá indicar el plazo de garantía ofertado.

  - Se garantizará el acceso por parte de CENER al sitio web de soporte de los fabricantes del hardware y del software suministrado.