PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE SUMINISTRO Y MANTENIMIENTO DE CORTAFUEGOS DE NUEVA GENERACIÓN PARA ANIMSA (Exp.445)

El objeto de este Pliego es el establecimiento de las especificaciones técnicas con arreglo a las cuales ha de llevarse a cabo la contratación del suministro y mantenimiento de cortafuegos de nueva generación (NGFW) para ANIMSA.

1) DESCRIPCIÓN GENERAL DEL ALCANCE Y OBJETO DEL CONTRATO

El objeto del presente contrato es el suministro y mantenimiento de NGFW para ANIMSA. El alcance incluye suministro, instalación y configuración inicial, y mantenimiento durante 3 años de hardware, software, licencias y suscripciones. Este cortafuegos sustituirá al actualmente en funcionamiento en la infraestructura de ANIMSA como segunda barrera de protección ante ataques informáticos.

2) SITUACIÓN DE PARTIDA, ALCANCE Y CARACTERÍSTICAS DEL CORTAFUEGOS A ADQUIRIRSE

El cortafuegos a sustituir como parte del alcance de este contrato tiene la función de segunda barrera de protección para las conexiones de la red corporativa de ANIMSA con internet. El cortafuegos propuesto deberá realizar la misma tarea, con funcionalidades de NGFW añadidas para mayor protección ante las amenazas existentes en la actualidad y en los próximos años. Específicamente, deberá gestionar los accesos desde la red corporativa hacia internet, establecimiento de VPNs entre la red corporativa de ANIMSA y otras redes, y segunda barrera de acceso entre zonas DMZ y red corporativa.

ANIMSA dispone de dos cortafuegos SSG-550M en alta disponibilidad, con conexión tanto a internet como a una segunda pareja de cortafuegos Checkpoint, también en alta disponibilidad. Las conexiones están redundadas geográficamente entre dos CPDs, en los que se encuentran ambas parejas de cortafuegos. La red corporativa está extendida entre ambos, tanto a través de fibra oscura, como a través de switches Aruba con capacidad de routing. Los cortafuegos están configurados en alta disponibilidad maestro-esclavo activo-pasivo, de forma que ante una caída del máster activo, el esclavo asume el direccionamiento y las funciones del máster, de forma automática y transparente para los usuarios.

El cortafuegos propuesto deberá cumplir con las mismas características de alta disponibilidad, es decir, se suministrarán dos appliances físicos, y se instalarán uno en cada CPD. Se deberán configurar de forma que ante la caída de uno de los dos, el otro asuma sus funciones de forma transparente para el usuario final y con el menor tiempo de caída posible. Se podrán utilizar para ello, igual que en la actualidad, las VLANs y direccionamiento extendidos para que ambos equipos puedan presentar el mismo direccionamiento de forma transparente al usuario, y puedan intercambiar entre sí la información sobre estado, funciones, sesiones, etc.

El cortafuegos objeto de este pliego sustituirá al Juniper SSG-550M, pero el cortafuegos perimetral principal seguirá en uso, por lo que de acuerdo al ENS, la propuesta **no podrá estar basada en tecnología del fabricante Checkpoint**.

Como criterio objetivo para valorar la capacidad del fabricante de la solución para garantizar las funcionalidades deseadas, se valorará su presencia en el sector de líderes en el Gartner Magic Quadrant durante los últimos 3 años (2018 a 2020, ambos inclusive).

Las características mínimas y valorables de hardware y funcionalidades que deberá incluir la solución propuesta, así como los servicios de configuración, puesta en marcha y mantenimiento, se detallan en posteriores epígrafes.

C.I.F.:A31152150 - Inscrita en el Registro Mercantil de Navarra: Hoja NA12872, Tomo 542, Folio 72

3) CARACTERÍSTICAS Y ALCANCE DETALLADOS DEL CORTAFUEGOS Y PUESTA EN MARCHA DEL MISMO

Se presentan en este epígrafe las características solicitadas a la solución y el alcance detallado de los servicios de puesta en marcha de la misma.

3.1) Topología de la solución propuesta

La oferta presentada deberá proponer una topología con dos cortafuegos gemelos, configurados en alta disponibilidad (que puede ser activo-pasivo) y ubicados cada uno en uno de los dos CPDs antes mencionados. Para las conexiones tanto de los cortafuegos entre ellos como hacia internet y hacia la LAN, se podrán utilizar tanto las VLANs extendidas entre ambos CPDs a través de los switches ARUBA como la fibra oscura existente. El adjudicatario deberá, dentro del plan de migración, realizar las instalaciones y configuraciones oportunas en la solución suministrada para establecer esta nueva topología, así como coordinar con el personal administrador de la red de ANIMSA, los cambios necesarios en red y cortafuegos perimetral existente.

3.2) Características de la solución a nivel de red

Las siguientes son características de obligado cumplimiento para la solución:

- 2 interfaces a 10Gbps para producción en cada equipo cortafuegos, con sus correspondientes SFPs. Deberá haber adicionalmente al menos un interfaz de gestión separado (no necesariamente de 10Gbps) en cada equipo cortafuegos, también preparado para conectarse, con conector RJ45 o dotado de SFP según proceda. Los interfaces dedicados (si existen) para intercambio de información entre ambos cortafuegos físicos para alta disponibilidad, deberán ser bien con conector RJ45, bien dotados ya de SFP, según proceda. ANIMSA proveerá los puertos en su red para establecer todas estas conexiones físicas, configurando además las VLANs correspondientes para el correcto funcionamiento de los cortafuegos.
- 802.1Q, DHCP server y relay, NAT, PAT.
- Enrutamiento estático, y protocolos dinámicos de enrutamiento, específicamente OSPF.
- Policy-based routing.
- Soporte de IPv6, incluyendo como mínimo encaminamiento y tratamiento de tráfico IPv6, NAT64 y dual-stack.
- Establecimiento de VPN SSL site-to-site. Establecimiento de VPN SSL client-to-site mediante cliente externo, que deberá estar disponible al menos para sistemas operativos Windows e iOS. La identificación de usuarios para VPN client-to-site deberá poder realizarse bien mediante credenciales locales, bien a través de integración con directorio activo.
- Throughput mínimo total (entrante y saliente) de 800Mbps, medido en condiciones de laboratorio y con aplicación de todas las políticas de seguridad propuestas. Si se da la circunstancia, este throughput total puede darse enteramente a través de VPN-SSL site-to-site.
- Gestión de al menos hasta 1000 políticas, hasta 1 millón de sesiones concurrentes, hasta 200 VPN SSL site-to-site y hasta 300 VPN SSL client-to-site simultáneas.
- Se valorará la posibilidad de creación de diferentes contextos virtuales o cortafuegos virtuales en cada máquina física suministrada, con funcionamiento independiente y tráfico estanco entre ellos, y siempre configuradas en alta disponibilidad entre ambas máquinas físicas (activo/pasivo o activo/activo).

3.3) Funcionalidades de la solución propuesta

Se presentan en este epígrafe las funcionalidades de seguridad que debe incluir la solución propuesta.

3.3.1) Gestión y autenticación de usuarios

La solución deberá poder integrarse con el Directorio Activo corporativo de ANIMSA, a fin de poder aplicar permisos, reglas y políticas concretas a usuarios bien individualmente, bien según pertenencia a grupos del Directorio Activo. Se valorará el que se pueda integrar con más de un Directorio Activo a la vez, para poder utilizar también usuarios o grupos de Directorios Activos de Entidades Locales clientes de ANIMSA.

La solución deberá también disponer de una base de datos local y mecanismos para la autenticación de los mismos, para la gestión y aplicación de políticas y permisos para usuarios que no sean del dominio activo.

3.3.2) Zonas

La solución deberá permitir crear zonas de diferentes niveles de seguridad para simplificar el diseño y aplicación de políticas y la agrupación de dispositivos/usuarios a proteger.

3.3.3) Inspección y aplicación de políticas

La inspección de tráfico y la aplicación de políticas deberá hacerse pudiendo aplicarse las reglas de inspección y las políticas a direcciones IP, o a usuarios o grupos de usuarios, según convenga en cada caso. Como resultado de aplicar la política, se podrá denegar o permitir el tráfico, aplicando además cuando proceda acciones específicas de limitación de caudal en el tráfico permitido, o de aviso a administradores cuando se produzcan ciertos tipos de tráfico.

La solución deberá incluir protección básica contra ataques estándar de denegación de servicio, tales como SYN Flood, ICMP Flood, pudiendo establecerse umbrales para cada tipo de ataque.

3.3.4) Control de aplicaciones

La solución propuesta deberá identificar al menos 3000 aplicaciones a nivel 7, independientemente de qué puertos usen estas aplicaciones. Se actualizarán de forma transparente las aplicaciones identificadas. La solución deberá poder denegar o permitir aplicando criterios de ancho de banda a las diferentes aplicaciones, aplicándose las políticas correspondientes de forma global, por IP o por usuario o grupo de usuarios. Se valorará el que la solución permita agrupar las aplicaciones, de forma que las políticas se apliquen por grupos de aplicación.

3.3.5) Categorización y filtrado de URLs

La solución deberá permitir la posibilidad de filtrar la navegación hacia URLs basándose bien en categorías definidas por el fabricante, bien en listas de URLs específicas. Las categorías deberán ser actualizadas automáticamente por el fabricante de forma periódica o ante nuevos riesgos conocidos, existiendo al menos una categoría de URLs maliciosas o de riesgo para sitios conocidos como potenciales atacantes.

3.3.6) IPS

La solución deberá contar con un Sistema de Protección ante Intrusiones (IPS) integrado en el propio cortafuegos, basado al menos en los siguientes mecanismos de detección: firmas de exploits, anomalías de protocolos y detección basada en conducta. Las firmas deben ser actualizadas de forma automática para reflejar los nuevos exploits detectados. La detección basada en conducta debe cubrir como mínimo ante ataques de fuerza bruta o de escaneo de IPs o puertos.

3.3.7) Monitorización, gestión, logs e informes

La solución deberá contar con una consola de gestión centralizada desde la que se podrán configurar todas sus funcionalidades, así como monitorizar el estado de funcionamiento. Adicionalmente, la solución deberá poder gestionarse por medios habituales (CLI, SNMP,...). La solución deberá asimismo almacenar logs de tráfico, incluyendo las aplicaciones de todas las reglas para todo el tráfico entrante y saliente, así como las actuaciones de todos los mecanismos de protección. Deberá incluir un motor de búsquedas que permita filtrar estos logs en base a los siguientes parámetros:

- Hits en reglas o políticas concretas
- Tráfico desde o hacia IPs específicas, o solicitadas por un usuario o grupo de usuarios concretos
- Tráfico de aplicaciones o grupos de aplicaciones específicas
- Combinación de todos los anteriores

Estos logs podrán además ser exportados a un servidor externo de procesado de logs, o a un SIEM para su correlación con otros eventos.

Se valorará la ergonomía en el acceso al estado de funcionamiento de la solución, la gestión de la misma, el acceso a logs.

3.4) Puesta en marcha y migración

El alcance del contrato incluye la instalación, configuración y puesta en marcha de todos los componentes que integran la solución. Esta puesta en marcha y migración de los servicios se realizará en dos fases:

1) una primera fase que durará no más de 2 meses desde el inicio del contrato, y que incluirá suministro del equipamiento, instalación física, configuración en la nueva topología propuesta, puesta en marcha de los servicios y migración de los mismos desde el cortafuegos actualmente en uso hasta la nueva solución, con al menos las mismas funcionalidades y protecciones que existen en la actualidad salvo las VPNs actualmente existentes, y
2) una segunda fase, que terminará no más de 4 meses tras el inicio del contrato, tras la que deberá quedar la solución funcionando plenamente con todas las funcionalidades y protecciones ofertadas activas, incluyendo todas las VPNs actualmente configuradas. En ese momento a más tardar deberán quedar configuradas todas las licencias, actualizaciones automáticas y suscripciones para todas las funcionalidades del sistema, debiendo el adjudicatario mantenerlas activas hasta el final del periodo de duración del contrato.

Durante la primera fase deberán quedar configurados los accesos remotos actualmente existentes. Para ello, el adjudicatario deberá realizar la integración con directorio activo y crear al menos cuatro perfiles de acceso remoto, dos para usuarios autenticados a través de directorio activo, y otros dos para usuarios con autenticación local, asistiendo a los técnicos de ANIMSA en la configuración de los demás.

Durante la segunda fase deberán quedar configuradas todas las VPNs actualmente existentes. Para ello, el adjudicatario deberá configurar al menos 2 VPNs para cada marca y modelo distintos de cortafuegos remotos actualmente en servicio, asistiendo a los técnicos de ANIMSA en la creación del resto de VPNs. A día de hoy hay activas VPNs con cortafuegos de modelos Netscreen 5GT, Juniper SSG5, Juniper SRX100, Juniper SRX300, además de no más de 6 VPNs con otros modelos, por lo que el número de VPNs que deberán ser configuradas por el adjudicatario no será superior a 16, realizando los técnicos de ANIMSA las demás, tomando como modelo las configuradas por el adjudicatario, y con soporte del mismo.

El licitador deberá presentar en su oferta un Plan de Migración que describirá los procedimientos y mecanismos para ejecutar las dos fases de11l proyecto, así como tareas, dependencias, riesgos, medios materiales y humanos adscritos al cumplimiento del contrato, que permitan garantizar la buena marcha del mismo y la consecución de los plazos

previstos. Se deberá prestar en la oferta especial atención al procedimiento propuesto para minimizar el tiempo de caída de servicio para VPNs. Este procedimiento ofertado puede requerir de cambios temporales en el cortafuegos existentes y en el que es objeto de este contrato, durante el tiempo de migración de las VPNs, así como en la red corporativa de ANIMSA. Una vez consensuado con el adjudicatario el plan de migración, los técnicos de ANIMSA realizarán los cambios oportunos en red corporativa y cortafuegos existentes.

3.5) Documentación y formación

Como parte de la puesta en marcha, se entregará documentación completa de la solución, incluyendo hardware, software, licencias y suscripciones instaladas y activadas. Se incluirá además formación y documentación específica de la configuración y parametrización realizada. El licitador deberá además proponer la formación que se impartirá a los técnicos que ANIMSA designe para la gestión diaria de la solución, en número de 3 personas. Esta formación podrá ser "on the job", realizándose de forma teórico-práctica durante la puesta en marcha y migración.

El objetivo de la documentación entregada y formación impartida es que los técnicos de ANIMSA puedan realizar la gestión rutinaria de la solución, incluyendo pequeños cambios y modificaciones en la topología por introducción de nuevos elementos o servicios, modificación de políticas de seguridad, troubleshooting, generación, comprensión y análisis de logs, toma de decisiones ante alertas o infomes de amenaza, etc.

4) SERVICIO DE MANTENIMIENTO DURANTE EL PERIODO DE VIGENCIA DEL CONTRATO

Tal y como se detalla en el apartado anterior, el adjudicatario deberá mantener activas todas las licencias y suscripciones necesarias para el funcionamiento integral de la solución con las funcionalidades solicitadas. Adicionalmente, el adjudicatario deberá realizar las tareas de mantenimiento correctivo y preventivo necesarias para que la solución presente el funcionamiento óptimo en todo momento. Se distinguen actuaciones correctivas para la resolución de incidencias y mantenimiento preventivo. El licitador deberá proponer en su oferta los procedimientos, mecanismos y medios materiales y humanos utilizados para la prestación del servicio, así como la documentación a presentarse, que deberá presentar en forma de un Plan de Actuación a ejecutarse caso de ser adjudicatario, y deberá tratar como mínimo los aspectos que se detallan a continuación.

ANIMSA accederá a los servicios de asistencia técnica y soporte a través de un punto único de contacto, pudiendo utilizarse para ello un mínimo de dos canales, siendo uno de ellos un número de teléfono, y al menos uno electrónico (correo electrónico o formulario web). A través de este punto único de contacto, se encaminarán todas las peticiones de mantenimiento y soporte experto contempladas en el contrato. Si es posible, se resolverán a través de este punto único de contacto aquellas solicitudes o incidencias de escasa complejidad, si bien se aceptarán y valorarán otras opciones o variantes que permitan un tratamiento más ágil, competente y eficiente de las incidencias y peticiones comunicadas.

El licitador deberá detallar en su Procedimiento de Actuación cuál será el tratamiento que seguirá cada incidencia o solicitud comunicada, detallando los medios que se involucrarán, y los tiempos a los que se comprometa para su resolución o respuesta.

4.1) Clasificación de incidencias y plazos de respuesta y resolución

Se define como incidencia todo funcionamiento anómalo o inadecuado de la solución, o cualquiera de sus funcionalidades. Las incidencias se pueden clasificar respecto a su criticidad:

- Incidencias de criticidad máxima: Aquellas que afectan a la conexión a internet en su totalidad, o a ambos dispositivos físicos.
- Incidencias de criticidad alta: Aquellas que afecten a servicios esenciales para la seguridad en el servicio de conexión a internet, o que supongan una parada total de uno de los dos dispositivos.

- Incidencias de criticidad media: Aquellas que afecten a usuarios o grupos de usuarios concretos, o a funcionalidades de gestión, pero no de conexión a internet o de su securización a nivel global.

Se establecen los siguientes plazos máximos de respuesta y de resolución:

Criticidad	Plazo de respuesta	Plazo de resolución
Máxima	1 hora	24 horas
Alta	2 horas	48 horas
Media	4 horas	3 días laborales

En el supuesto de que la resolución de una incidencia, a pesar de dedicar el adjudicatario todos los esfuerzos y medios posibles, no sea viable en los plazos establecidos, se acordará entre adjudicatario y ANIMSA un plan de mínimos para resolver parcialmente y aminorar el efecto de la misma, hasta su resolución, quedando constancia por escrito de dicho plan. La inviabilidad nunca podrá referirse a sustitución de material averiado, que siempre deberá realizarse dentro de los plazos establecidos.

El incumplimiento por parte del adjudicatario de los plazos de resolución contratados, salvo cuando causas fehacientes y ajenas al control del adjudicatario lo hagan materialmente imposible, constituye una infracción, cuya severidad depende tanto del tipo de actuación, de la criticidad caso de tratarse de una incidencia, y del tiempo transcurrido desde el plazo máximo de respuesta o de resolución, hasta que la respuesta o la resolución se produce. Se tipifican las siguientes infracciones en forma de retrasos en plazo de resolución para diferentes severidades de infracción (expresados en porcentaje del correspondiente plazo máximo de resolución contratado):

Criticidad	Leve	Grave	Muy grave
Máxima	<100%	>100% <200%	>200%
Alta	<100%	>100% <300%	>300%
Media	<100%	>100% <300%	>300%

Las anteriores infracciones suponen los plazos máximos para la prestación de los servicios contratados, y tienen el carácter de acuerdo de nivel de servicio.

4.2) Mantenimiento correctivo

El mantenimiento correctivo incluirá toda actuación necesaria para garantizar el adecuado comportamiento de la solución, incluso reposición de cualquier elemento averiado que forme parte de la solución, así como resolución de bugs de software o firmware necesario para su correcto funcionamiento, o incidencias relacionadas con el funcionamiento de software, licencias o suscripciones, aplicándose para ello los criterios y plazos recogidos en el apartado anterior.

4.3) Mantenimiento preventivo

El licitador deberá incluir en su Procedimiento de Actuación actuaciones de mantenimiento preventivo. Estas podrán incluir monitorización y toma remota de datos, visitas presenciales, análisis de logs, etc., de cara tanto a adelantarse a posibles problemas e incidencias, como a optimizar el funcionamiento de la solución. Se valorarán las acciones propuestas en la medida en que garanticen el cumplimiento de estos objetivos, especialmente si incluyen una interacción periódica entre técnicos del adjudicatario y de ANIMSA donde los primeros informen de los resultados de monitorización y revisiones periódicas, y propongan las actuaciones preventivas o de mejora oportunas.

4.4) Soporte experto

El adjudicatario deberá realizar tareas de soporte experto ante incidencias complejas, o ante inclusión o variación de los servicios y funcionalidades actuales, debiendo estar incluidas en la oferta todas aquellas actuaciones que no impliquen la adquisición de nuevas licencias o suscripción a nuevos servicios. Si es necesario, el adjudicatario deberá poder acceder a los servicios de soporte del fabricante, punto que deberá justificarse mediante compromiso del fabricante de mantener y dar soporte a la tecnología componente de la solución durante los 3 años de vigencia del contrato.

Durante la ejecución del contrato, se prevén los siguientes posibles cambios en los que el adjudicatario deberá prestar este soporte:

- Posible cambio de prestador del servicio de conexión a internet.
- Posible cambio en direccionamiento IP público.

4.5) Seguimiento del contrato

Con periodicidad al menos semestral, tendrá lugar una reunión de seguimiento del contrato, en la que se tratarán las actuaciones relevantes que hayan sucedido en el periodo que concluye. Se consensuarán si proceden las actuaciones a realizarse en periodos sucesivos.