SISTEMA DE PROTECCIÓN PERIMETRAL PARA LA RED DE COMUNICACIONES DEL SISTEMA DE PRODUCCIÓN DE RNE

PLIEGO DE CONDICIONES TÉCNICAS

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

1. Las posibles marcas y modelos citados a lo largo del presente Pliego, lo son a titulo meramente orientativo y al objeto de ilustrar al posible oferente sobre las características operativas y grado de calidad del equipamiento deseado, no presuponiendo en ningún caso preferencia de las marcas citadas sobre otras que pudieran ofrecer el mismo grado de calidad y operatividad solicitado.

2. Los oferentes, en sus propuestas técnicas, incluirán información para la correcta evaluación de las ofertas. Asimismo, deberán aportar relación pormenorizada de la aceptación y cumplimiento, o no, de cada una de las condiciones técnicas de este expediente, especificando en su caso, las diferencias entre lo ofertado y lo solicitado.

3. Todos los materiales ofertados deberán ser nuevos, no-descatalogados y de calidad profesional.

4. Los licitadores incluirán en la oferta técnica las homologaciones, certificados originales de los fabricantes y cualquier documentación que considere necesaria para una correcta evaluación de las ofertas

5. Las características técnicas de los equipos suministrados coincidirán con las aportadas por el fabricante en sus informaciones técnicas y se ajustarán a las exigidas en el presente Pliego de Condiciones. Podrá reclamarse igualmente el cumplimiento de cualquier otra característica técnica que haya sido incluida tanto en la descripción de la composición del suministro ofertado como en la propia oferta.

6. Si las necesidades operativas así lo exigen, la Corporación RTVE se reserva el derecho de efectuar recepciones parciales del lote que no haya sido suministrada en su totalidad. En tal caso, la Corporación RTVE se reserva el derecho de certificar la parte correspondiente, valorándola en función de las prestaciones funcionales obtenidas, con independencia del precio unitario de los equipos suministrados.

7. En el caso que los equipos suministrados no contemplen todas las características ofertadas

aunque sean operativos, o no funcionasen correctamente, el suministro se considerará incorrecto, y no se procederá a certificar hasta que todos los equipos suministrados dispongan de las características ofertadas. La Corporación RTVE se reserva el derecho a utilizar los equipos suministrados si lo creyese oportuno de acuerdo a sus necesidades.

8. El adjudicatario deberá retirar del Centro Receptor de Mercancías de RNE aquellos equipos que no funcionen correctamente, en un plazo de tiempo de 3 días desde la comunicación, de acuerdo al procedimiento que le indique la Dirección de Medios de RNE. Los entregará de nuevo cuando todas las anomalías detectadas hayan sido corregidas, sin que esta consideración, modifique los plazos de entrega establecidos en el lote correspondiente.

9. Las Especificaciones Técnicas y la Composición del suministro a adquirir se describen a continuación:

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.

La tecnología elegida para la securización perimetral es la denominada "Next Generation Firewall (NGFW), que describe dispositivos de seguridad que van más allá de los tradicionales firewalls, añadiendo capacidades de seguridad adicionales como la detección de intrusiones, el control sobre las aplicaciones y datos sobre la red, y la identificación de usuarios, entre otras.

1. SUMINISTRO INSTALACIÓN Y CONFIGURACIÓN DE SISTEMA NGFW (Next Generation Firewall)

1.1. Arquitectura

- El "cortafuegos" de nueva generación propuesto debe contar con funciones de filtrado de estados (stateful firewall), detección y prevención de intrusiones de nueva generación IDS/IPS (NGIPS), Red Virtual Privada VPN, tanto por medio de cliente como site-to-site, control de aplicaciones(AVC) y protección anti-malware integradas, tanto para tráfico encriptado como no encriptado.
    - Los equipos deben tener integradas como mínimo las siguientes funcionalidades:
        - Filtrado de Estados
        - Control de Aplicaciones (Application Control),
        - Prevención de Intrusiones (IPS),
        - Antivirus (AV),
        - Filtrado Web (Web Filtering),
        - Antispam,
        - Entorno de ejecución protegido en la nube (Sandbox Cloud).
        - Protección contra ataques de denegación de servicio (anti-DDoS).
        - Capacidad de despliegue en entornos virtualizados (VMWare, KVM, AWS, Azure e Hiper-V).

- Capacidad multi-instancia (suministro de capacidad mínima de 3 instancias).

1.2. Conectividad

- Capacidades de Routing estático, policy based routing y routing dinámico.
- Compatibilidad con protocolos de routing RIP, OSPF, BGP, Rip v2 y Multicast, tanto para IPv4 y IPv6 .
- Soporte de las funciones sobre OSPF: IETF Non-Stop Forwarding, OSPF Fast-Hello y BGP Graceful Restart.
- Soporte de IPSEC.
- Múltiples modos de despliegue (modos mirror, transparente y NAT/PAT)
- Gestión de VLAN e integración de 802.1Q.
- 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.
- Balanceo de todo tipo de líneas: Deberá permitir configurar todos sus puertos como líneas WAN y crear múltiples túneles IPSec en cada una.
    - Podrá definir los siguientes tipos de SLA:
        - Best quality. Elige solo el mejor camino posible.
        - Minimum quality. Elige todos los caminos que cumplan con el SLA establecido.

      ó múltiples SLAs definidos para cada política de SDWAN.
    - QoS (Entrada y Salida) y optimización WAN.
    - Deberá poder realizar Traffic shaping, basado en porcentajes, y balanceo de SDWAN, basado en App capa 7 (usando +3000 firmas de App) además de combinarlo con ISDB.
    - Balanceo inteligente por App: Deberá permitir balancear tráfico de Internet, aplicaciones SaaS y aplicaciones corporativas de forma inteligente mediante umbrales de latencia, jitter, ancho de banda disponible... para asegurar que la VoIP o videoconferencia y las aplicaciones críticas siempre vayan por la línea óptima en cada momento.
    - Compatibilidad total con BGP (actualización de rutas, varios caminos usables en BGP, fusión entre ADVPN y SDWAN...).
- Capacidad de red
    - Debe ser capaz de funcionar en modo enrutado y modo transparente.
    - Debe soportar trunking 802.1q y agregación de enlaces (LACP).
    - Debe soportar NAT y PAT (NAT 1:1, NAT n:n, NAT m:n,...)
    - Número mínimo de interfaces:
        - 2 x 10 GE SFP+ / GE SFP Slots.
        - 8 x GE SFP / GE SFP Slots
        - 2 x GE RJ45 Management Ports
        - 1 / 1 x USB Ports (Server/Client)
        - 1 x Console Port

1.3. Funcionalidades

a) Servicio firewall

- Debe ser capaz de reconocer y controlar los accesos basándose en el reconocimiento de aplicaciones y usuarios (mediante la integración con AD de Microsoft y otros servicios de directorio. Utilizará también los servicios de ACS de que dispone RNE).
- Debe ser capaz de analizar tráfico cifrado.
- Debe contar con la capacidad de prevención de amenazas.
- Debe proporcionar protección contra ataques de DoS y DDoS
- Capacidad de control sobre transferencia de archivos y datos.
- Debe tener capacidad de aplicar políticas QoS (marcado y limitación de ancho de banda) por grupos de usuarios, aplicaciones, urls..
- Debe tener capacidad de proporcionar filtrado y categorización URL
- Inspección profunda de contenido.
- Capacidad de securización de VoIP.
- Protección basada en la creación de perfiles aplicables a usuarios individuales y/o grupos.

b) Servicio VPN (Virtual Private Network)

- Protocolos soportados: PPTP, IPSec y SSL.
- Encriptación y autenticación: DES, 3DES y AES. SHA1 y MD5.
- Soporte del protocolo GRE, para el establecimiento y finalización de túneles en el mismo equipo.
- Nat 64 y 46.
- Integración con firma electrónica.
- Modo de funcionamiento cliente/servidor y punto a punto (site-to-site).
- Cliente VPN propietario que asegure la integración completa con los sistemas ofertados, válido para sistemas operativos para PC: Microsoft Windows (7,10), Linux y para móvil: IOS y Android.
- Modo proxy inverso que permita la publicación mediante portal web de aplicaciones tipo WEB, RDP, SSH, Acceso a carpetas y VNC.
- VPN Inteligente: Tendrá que disponer de ADVPN (Auto Discovery VPN) para realizar túneles IPSec automáticos entre sedes. Esto permitirá optimizar las redes SD-WAN, crear caminos de baja latencia y mantener todas las ventajas de una red unificada bajo entorno IPSec centralizado.
- Licencias necesarias para dar soporte VPN a más de 1500 usuarios potenciales y 250 concurrentes como mínimo.

c) Servicio de Filtrado Web.

- Protocolos a analizar: HTTP/HTTPS, FTP,SFTP.
- Categorización de contenidos web con posibilidad de más de 78 categorías y más de 50 millones de páginas categorizadas.
- Creación de patrones para la definición de listas URL.
- Bloqueo de contenidos web.

- Posibilidad de fijación de quotas de navegación por categoría.
- Servicio de actualización en tiempo real de categorización de URL.
- Capacidad de aplicar perfiles de protección específicos (WAF) para entornos y aplicaciones web.

d) Servicio de Reconocimiento y 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.
- Capacidad de permitir la parametrización de aplicaciones no reconocidas por el dispositivo.
- Posibilidad de definir la identificación de nuevas aplicaciones personalizadas.
- Disponibilidad de un servicio de actualizaciones de nuevas aplicaciones.

e) Reconocimiento de usuarios

- Integración con Active Directory, Servidor ACS, TACACS+ y RADIUS/802. 1 X, pudiendo aplicar QoS a nivel de usuario o grupo de usuarios.
- Autenticación basada en grupos de usuarios.
- Creación de reglas basadas en identidad.
- Posibilidad de identificación de usuario mediante Terminal Server.
- Soporte de autenticación de portal cautivo mediante protocolos HTTP Basic, NTLM y Kerberos.
- Licencias necesarias para dar soporte a más de 1500 usuarios potenciales y más de 250 concurrentes.

f) Filtrado por reputación

- Deberá poder realizar filtrado reputacional basándose en criterios IP (SPAM, C&C, PHISHING) incluyendo IPs personalizables mediante feeds y/o listas.
- Deberá poder realizar filtrado reputacional basándose en criterios DNS, incluyendo DNS personalizable mediante feeds y/o listas.
- Deberá soportar la funcionalidad de sumideros DNS o “DNS Sinkholes”.

g) Función de IDS/IPS(lntrusion Prevention System) de nueva generación

- El equipo propuesto deberá poder realizar funciones de port-mirroring o puerto espejo en modo IDS.
- El equipo propuesto deberá soportar el despliegue IPS en línea o “in-line”.
- El cortafuegos no debe sufrir perdida de rendimiento entre las opciones de despliegue IDS e IPS.
- 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.

h) Función de protección anti-malware

- Capacidad de filtrado por tipo de archivo.
- Se podrán filtrar archivos mediante criterios de reputación (malware vs clean).
- El cortafuegos contará con la capacidad de descompresión de ficheros, incluyendo ficheros anidados para su análisis y filtrado.
- Detección de malware:
  - Los equipos tendrán la capacidad de enviar ficheros sospechosos a entornos de sandboxing centralizados para análisis de comportamiento y detonación.
  - Soporte de entornos de sandboxing tanto en nube pública como on-premise.

i) 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.

j) Servicio Antispam.

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

k) Gestión centralizada (Single pane of glass):

Gestión de todo el entorno SD-WAN desde un único punto, pudiendo controlar los túneles IPSec, el estado de todas las líneas, amenazas, incidencias de red… ofreciendo una completa visibilidad en tiempo real e informes personalizados desde un único punto central.

- VDOM SD-WAN y Red: Pudiendo gestionar VLANS, Routing Dinámico, Routing Estático, NAT Avanzado, IPSec, QoS, ADVPN, DNS, DHCP y conectividad WiFi.
- Deberá tener la funcionalidad de Auto-fallback, entre líneas SDWAN.
- VDOM Seguridad L7: Permitiendo gestionar IPS, AppCtrl, firewall L4, AV, Sandboxing, Filtrado web, autenticación con AD y Gestión.
- Despliegue HA y zero-touch: La solución deberá ser desplegada en un único equipo, ofreciendo un despliegue zero-touch real.
- Deberá además contar con APIs, con las que es posible la integración con cualquier Orquestador (Nuage, HP, OpenStack…).

- Permitirá el uso de soluciones de autenticación de doble factor, del mismo fabricante sin suscripción asociada. Estos podrán usados en formato físico y en versión software para Smartphone.

1.4. Rendimiento y capacidad

Las medidas de rendimientos y capacidades que se acrediten para los sistemas ofertados deberán haberse realizado siguiendo los procedimientos recomendados por organismos independientes como NetSecOPEN y utilizando una mezcla de tráfico real como la propuesta por el citado organismo y con una mezcla de tamaños de paquetes tipo IMIX.

- Debe tener un rendimiento del servicio firewall de al menos 35 Gbps en condiciones ideales con paquetes de 1024B y al menos 10 Gbps con tráfico real medido utilizando una mezcla estándard (IMIX, NetSecOPEN).
- Debe tener un rendimiento del servicio NGFW de al menos:
  - 6 Gbps en condiciones ideales con paquetes de 1024B y Control de aplicaciones activado.
  - 5 Gbps en condiciones ideales con paquetes de 1024B con IPS de nueva generación activado.
  - 3 Gbps en condiciones ideales con paquetes de 1024B y con IPS y Control de Aplicaciones activados.
  - 2 Gbps en condiciones ideales con paquetes de 450B y con IPS y Control de Aplicaciones activados.
  - 450Mbps Gbps con tráfico real medido utilizando una mezcla estándard (IMIX, NetSecOPEN), con el 70% de tráfico SSL/TLS, y todas las funcionalidades de Firewall, IPS, Control de Aplicaciones y protección de amenazas activadas.
- Rendimiento mínimo del servicio VPN (IPSec) con las funcionalidades de Firewall, IPS, y control de aplicaciones activadas: 1 Gbps.
- Latencia máxima Firewall (64 byte, UDP) 3.5 µs.
- Capacidad mínima de gestión de conexiones con el control de aplicaciones activado: 1.000.000 sesiones concurrentes, permitiendo como mínimo 15.000 nuevas sesiones por segundo.
- Número mínimo/máximo de Dominios virtuales: 10/250.
- Almacenamiento interno mínimo: 2x 240 GB SSD.
- Tamaño máximo enracable: 2 RU.
- Fuentes de alimentación: Principal y redundante Hot Swappable.

1.5. Análisis y Gestión de amenazas

- Ha de tener capacidad de gestión centralizada del cortafuegos mediante consola de gestión externa que se suministrará con los equipos, en formato de máquina virtual VMware, aunque deberá tener también capacidad de gestión integrada en el propio equipo sin necesidad de software o hardware adicional, en caso de caída o pérdida de conexión a la consola de gestión externa.
- Correlación:
  - El sistema de gestión del cortafuegos deberá permitir la correlación de eventos.
  - Visibilidad de anomalías de tráfico respecto al patrón normal y correlación de las mismas.
  - Capacidad de correlación basada en anomalías del contexto (sistemas operativos, puertos o aplicaciones fuera de los esperados).
  - Capacidad de envío automático de alertas de e-mail basándose en el resultado de la correlación.
  - Basándose en el resultado de la correlación, el sistema deberá contar con la capacidad de ejecutar scripts de forma automática.
- Integraciones
  - Deberá poder integrarse con sistemas SIEM.
  - Compatibilidad con función de cuarentena automática de equipos infectados mediante integración con terceros vía API.
  - Capacidad de integración con herramientas de configuración automática de las políticas de acceso a la infraestructura de red existente en RNE (Cisco ACI).
  - Integración con soluciones anti-malware en PCs.
  - Integración con soluciones anti-malware sobre sistema operativo Android.
- Otros
  - El sistema de gestión permitirá la utilización de Indicadores de Compromiso basados en STIX.
  - El sistema de gestión permitirá la utilización de Indicadores de Compromiso basados en TAXII.
  - Compatibilidad con entornos de gestión multi-tenant.
  - Soporte de RestAPIs.
  - Soporte de MFA para autenticación
  - Soporte de RBAC para permitir administradores diferenciados para cada función del (reglas del FW, reglas del IPS…etc).
  - Se valorará positivamente la capacidad de incorporar reglas IDS Snort, tal y como las publica el organismo CCN-CERT.

2. SUMINISTRO DE UNA CONSOLA DE ADMINISTRACIÓN, ANÁLISIS DE RED, GESTIÓN DE AMENAZAS Y GESTIÓN DE INFORMES.

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, en formato de máquina virtual de VMware, para la Administración centralizada de la plataforma, Recogida, Almacenamiento y Análisis del tráfico que atraviesa la red y las vulnerabilidades que existen en la misma, Gestión de Amenazas y Gestión de Informes.
    - Capacidad de recepción de información de más de 1GB/dia y 1TB de almacenamiento.
    - Ratio de Log sostenido (logs/sec): 1.500.
    - Soporte de más de 10.000 Dispositivos/ADOMs/VDOMs.
    - Numero de interfaces soportados (Max/Min): 4/1.
    - Deberá permitir los siguientes hipervisores:
        - VMware ESX/ESXi 6.0/6.5/6.7, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016
    - Licencias de usuario ilimitadas.
- Características funcionales que deberá integrar el sistema.
    - Se requiere la integración total con el sistema NGFW contemplado en el presente pliego de prescripciones técnicas.
    - Administración de todas las funcionalidades de los equipos solicitados en el presente pliego, en particular: Firewall de Nueva Generación (NGFW), IPS de Nueva Generación (NGIPS), Protección contra Amenazas, Protección Avanzada contra Malware.
    - Ha de permitir configurar en una sola política el acceso al Firewall, Control de acceso basado en etiquetas de grupos de seguridad de ISE, en tipos de dispositivos, localización de IP's y contención rápida de amenazas.
    - Ha de permitir la ingestión y correlación de Inteligencia sobre amenazas proveniente de fuentes y plataformas propias, además de poder utilizar fuentes y plataformas de terceros por medio de archivos de intercambio en formato plano o STIX/TAXII.
    - Análisis de tráfico en tiempo real.
    - Gestión continua de los procesos de ataque controlando las fases previas, durante y posteriores a los mismos.

- Correlación de eventos con las vulnerabilidades de red que permitan alertar en caso de ataques con éxito.
- API's abiertas para integración con sistemas SIEM y de Gestión de vulnerabilidades de terceros.
- Indicadores de Compromiso (IOC) basados en STIX 2/TAXII y Open IOC.
- Panel de mando (Dashboard) configurable y personalizable.
- 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, Servidor ACS, TACACS+ y RADIUS/802. 1 X.
- Posibilidad de monitorizar dispositivos SNMP y syslog externos.
- Actualización de Firmas IPS y Amenazas automáticas.

3. 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. Por otro lado, se requiere la perfecta integración con los sistemas disponibles en la red de RNE.
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, así como a mejorar la seguridad 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.

3.1. Servicios adicionales.

- Análisis y Configuración:
  - Análisis. Se requiere la elaboración de un documento de solución que se adapte a las necesidades de RNE.
  - Configuración. Tendrán que contemplarse los servicios profesionales necesarios para la correcta instalación, configuración y adaptación del equipo en la arquitectura de Data-Center existente en RNE.
- Dichas jornadas serán desarrolladas en las instalaciones de RNE y serán consideradas "llave en mano" desarrollados por el integrador.
- El oferente deberá contar como mínimo con 2 ingenieros cualificados y certificados con nivel mínimo NSE-4 y 1 ingeniero NSE-5.

3.2. Formación.

- Deberá incluirse un servicio de formación oficial reglada por el fabricante (NSE-4) durante 5 días en un centro de formación oficial, para al menos 2 personas.

3.3. Soporte

- Mantenimiento de hardware en modo 24x7 con reemplazo "Siguiente Día Laborable". Horario de atención telefónica a incidencias 24x7.
- Mantenimiento de software en modo 24x7. Asistencia web y telefónica personalizada.
- Servicio de actualizaciones de servicios firmware, antivirus, IPS, filtrado web y aplicaciones.
- Soporte a la gestión de cambios sobre configuración de software y plataforma, mediante el posible uso de una bolsa de 16 horas de servicios profesionales, valida por la totalidad del contrato.