PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA LA CONTRATACIÓN DE UNA SOLUCIÓN CENTRALIZADA DE SEGURIDAD PERIMETRAL PARA LOS ACCESOS A/DESDE INTERNET EN LA ADMINISTRACIÓN DEL PRINCIPADO DE ASTURIAS. Expediente nº 72/2017

Proyecto financiado por la Unión Europea a través del Fondo Europeo de Desarrollo Regional en el marco del Programa Operativo FEDER de Asturias 2014-2020

Unión Europea

Fondo Europeo de Desarrollo Regional

C/ Trece Rosas, 2, 5ª planta, sector derecho, 33005 Oviedo. Tfno: 985 10 59 59. Fax: 985 10 59 45

CONTENIDO

1. INTRODUCCIÓN 3

2. OBJETO DE LA CONTRATACIÓN 4

3. ALCANCE 5

4. DESCRIPCIÓN DEL SUMINISTRO A REALIZAR 5

4.1. Características técnicas 5

4.1.1. Gestión Firewall sobre los accesos a Internet 6

4.1.2. Gestión de VPN 7

4.1.3. Gestión Firewall sobre la publicación de servicios en Internet 7

4.1.4. Manuales de la herramienta 7

4.1.5. Hardware de la solución 8

5. SERVICIOS DE IMPLANTACIÓN 8

6. SERVICIOS DE FORMACIÓN 9

Proyecto financiado por la Unión Europea a través del Fondo Europeo de Desarrollo Regional en el marco del Programa Operativo FEDER de Asturias 2014-2020

Unión Europea

Fondo Europeo de Desarrollo Regional

C/ Trece Rosas, 2, 5ª planta, sector derecho, 33005 Oviedo. Tfno: 985 10 59 59. Fax: 985 10 59 45

1. Introducción

En los últimos años, la Administración del Principado de Asturias ha hecho un importante esfuerzo en el ámbito de las tecnologías de la información, avanzando de forma importante en temas como la administración electrónica, los servicios electrónicos al ciudadano o la interconexión con otras administraciones y redes de terceros. En todo este proceso, la importancia y la criticidad del uso de la red internet ha aumentado decisivamente, hasta convertirse en un servicio crítico para la Administración del Principado de Asturias y que por tanto debe ser objeto de especial salvaguarda, siendo necesario aumentar los controles de seguridad sobre los sistemas informáticos y las redes de la organización que proporcionan dicho servicio.

Es vital que estos sistemas informáticos cumplan con su finalidad en las mejores condiciones técnicas y operativas, sin olvidar la atención prioritaria a la seguridad y a la protección de la información; la actual coyuntura de virulencia de los ataques informáticos obliga a rediseñar los mecanismos de seguridad y a disponer de dispositivos de última generación con el objetivo de garantizar el mayor nivel posible de protección proactiva frente a cualquier ataque malicioso que se ejecute contra las infraestructuras y datos de la organización.

Dentro de la política aplicada en materia de seguridad en la Administración del Principado de Asturias y a la vista de los ataques crecientes y sumamente destructivos que se están dando, se considera necesario ahondar en una seguridad en múltiples niveles sucesivos y coordinados y que potencie la protección de tipo perimetral, entendiendo como tal las defensas sucesivas que se interponen entre nuestros sistemas y el exterior.

Habida cuenta de que nuestros sistemas y redes no son estancos sino que, de una forma u otra, necesitan accesos a sistemas externos, es necesario habilitar unos cauces de comunicación que, inmediatamente, se convierten en potenciales puertos de entrada para amenazas camufladas entre el tráfico aparentemente estándar. En esa línea, un dispositivo siempre presente en los sistemas TIC es el *cortafuegos*, más conocido en el mundo técnico y comercial por su denominación inglesa de *firewall*. Estos elementos, usualmente un hardware dedicado (hardware diseñado para esta tarea específica), realizan funciones de vigilancia en cuanto que posibilitan la comunicación entre sistemas pero estableciendo unos mecanismos de control y bloqueo de aquello que se sospecha o se sabe que es peligroso de acuerdo a una serie de normas que se definen y/o de una inteligencia y aprendizaje acumulado. En esencia permitirán, o bien únicamente un tráfico autorizado explícitamente, o bien todo el tráfico salvo aquel que se haya prohibido explícitamente. Un firewall puede pues alertar, o incluso impedir, que un usuario interno interactúe con un potencial peligro externo, o que desde fuera de la organización se pretendan esquivar accesos controlados para acceder ilegítimamente a

Proyecto financiado por la Unión Europea a través del Fondo Europeo de Desarrollo Regional en el marco del Programa Operativo FEDER de Asturias 2014-2020

Unión Europea

Fondo Europeo de Desarrollo Regional

C/ Trece Rosas, 2, 5ª planta, sector derecho, 33005 Oviedo. Tfno: 985 10 59 59. Fax: 985 10 59 45

nuestros datos o aplicaciones y lo deberá hacer aplicando un adecuado sistema de clasificación y/o filtrado.

La lógica evolución de la realidad tecnológica y funcional, y también de las amenazas cada vez más potentes y masivas, ha llevado a una continua mejora de estos firewalls dotándolos de capacidades específicas de seguridad, de cifrados o de prevención de intrusiones, y llevándolos a un modelo que se ha dado en llamar Firewall de Nueva Generación (NGFW) y que supera a los modelos más básicos y primitivos, que no inútiles, que se limitaban a bloquear puertos, y también a los primeros Firewall UTM que ya incorporaban mejores medidas de protección de perímetros y vigilancia de las navegaciones.

Estos nuevos firewall NGFW no solo deben incluir más "inteligencia" en la detección de lo que no está autorizado, sino más calidad y versatilidad en sus motores de análisis y en sus desempeños, lo que se traducirá en que actúen con celeridad y sin suponer un cuello de botella para el conjunto de transacciones. Su funcionalidad, que evidentemente va más allá de lo que es la mera protección de un puesto individual para atender grandes tráficos que se originan en una red o un centro de proceso de datos, debe dar protección no solo a los entornos "físicos" sino también a los virtuales o a los albergados en nubes. Y sobre todo debe mejorar la potencialidad de los viejos Firewall al securizar las conexiones por VPN (red privada virtual), y gestionar el tráfico en la capa 7 de aplicación en la pila de protocolos de comunicación, controlando de esta forma las peticiones originadas por aplicaciones que se ejecutan en los equipos de los usuarios.

La facilidad para su gestión, para la creación de reglas, para el control efectivo de limitaciones al intento de uso indebido de aplicaciones, son también características que se exigen en estos sistemas cada vez más potentes.

2. Objeto de la contratación

El objeto de esta contratación es el suministro de una solución de seguridad perimetral que incorpore capacidades técnicas y funcionales de seguridad del tipo Firewall de Nueva Generación (NGFW), que se incorporará, sin incompatibilidad alguna, al conjunto de dispositivos de seguridad en uso en los sistemas informáticos de la Administración del Principado de Asturias (en adelante APA), con el fin de disponer de protección Firewall avanzada con posibilidad de realizar trabajo de concentradores de VPN, de securizar la publicación de servicios en internet además del control de navegación de usuarios por internet.

El suministro incluye la implantación de la solución de acuerdo con lo descrito en este pliego.

Proyecto financiado por la Unión Europea a través del Fondo Europeo de Desarrollo Regional en el marco del Programa Operativo FEDER de Asturias 2014-2020

Unión Europea

Fondo Europeo de Desarrollo Regional

C/ Trece Rosas, 2, 5ª planta, sector derecho, 33005 Oviedo. Tfno: 985 10 59 59. Fax: 985 10 59 45

3. Alcance

La solución de seguridad debe asegurar, en un modo de alta disponibilidad con clúster activo-pasivo, un mejor control sobre los accesos, usos y transacciones entre nuestros equipos y redes y el exterior. Esencialmente la contratación de un firewall especializado en este tipo de protección permitirá gestionar todo el acceso de los usuarios a recursos ubicados en internet. Ello debe hacerse partiendo del hecho de que se necesitan sistemas firewall que respondan proactivamente ante los nuevos tipos de ataques y riesgos, en un escenario donde el acceso a internet y la descarga de páginas y materiales desde dicha red se considera un recurso laboral indiscutible. El funcionamiento de los accesos debe acompañarse de cotas de protección adecuadas.

Paralelamente, se pretende que este sistema pueda igualmente ocuparse de la gestión de VPNs para facilitar la conexión de forma segura desde puestos del exterior de la organización a la red interna, garantizando la privacidad, confidencialidad e integridad de la información entre el cliente final y la APA. Estas conexiones deben contar con similares tasas de robustez que lo que serían las comunicaciones internas de la casa, puesto que es un modo de conexión utilizado masivamente por las empresas de soporte en los contratos de mantenimiento que se encargan de muchas de las aplicaciones utilizadas en la Administración y que también es usado por los empleados que, en remoto, deben acceder a puestos y datos internos o incluso para tareas como las de consulta de la intranet cuando no se encuentran en la red interna de la organización. Debe pensarse que es un riesgo a evitar el hecho de depender de equipos para estas tareas que carezcan, por obsolescencia, de los mecanismos de seguridad adecuados.

Por último, y como otra tarea paralela pero igualmente importante a satisfacer, estaría la de securizar el servicio de publicación en internet, que es el que permite el acceso a recursos internos de la organización desde fuera de la red interna; piénsese en el acceso a los portales corporativos o los servicios al ciudadano, de forma pública desde internet. Fortalecer los niveles de protección actuales incorporando sistemas que detecten y/o mitiguen los ataques actuales es otro objetivo de esta contratación.

En cualquier caso el sistema será capaz de centralizar esa seguridad perimetral manteniendo la posibilidad de realizar una gestión individualizada es decir, las "paradas", intencionadas o no, de una de esas tres capas de servicio no deberán afectar a las funciones del resto.

4. Descripción del suministro a realizar

4.1. Características técnicas

Proyecto financiado por la Unión Europea a través del Fondo Europeo de Desarrollo Regional en el marco del Programa Operativo FEDER de Asturias 2014-2020

Unión Europea

Fondo Europeo de Desarrollo Regional

C/ Trece Rosas, 2, 5ª planta, sector derecho, 33005 Oviedo. Tfno: 985 10 59 59. Fax: 985 10 59 45

El objeto del contrato es una solución de seguridad perimetral con capacidades técnicas y funcionales de seguridad del tipo Firewall de Nueva Generación con posibilidad de realizar trabajo de concentradores de VPN, de securizar la publicación de servicios en internet además del control de navegación de usuarios por internet.

La solución ofertada debe constar de los siguientes elementos:

- De un mínimo de dos equipos para garantizar la alta disponibilidad de la solución de seguridad perimetral
- De cualquier software para el mejor uso y gestión del sistema y específicamente de los equipos suministrados
- De cualquier otro software, o incluso hardware, que complemente las funcionalidades básicas del sistema propuesto para el logro total de los requerimientos
- De las licencias necesarias para su funcionamiento, si las precisa
- De los correspondientes periféricos, latiguillos o cualquier otro accesorio necesario para su instalación

Asimismo, la solución debe contemplar:

- Envío de logs para la integración con la plataforma SIEM en uso en la organización
- Soporte para validación de usuarios contra RADIUS, TACACS+ y LDAP (Novell / ActiveDirectory)

Las características técnicas solicitadas en este pliego se dividen en varios grupos, que se detallan a continuación.

4.1.1. Gestión Firewall sobre los accesos a Internet

A continuación se indican las características mínimas que se deben cumplir:

- Throughput Firewall : >= 18 Gbps
- IPSEC Throughput: >= 4 Gbps.
- Threat Protection: >= 7 Gbps.
- Servicio de filtrado WEB (Web filter) basado en categorías
- Servicios UTM: antivirus a nivel de red, IPS y control de aplicaciones para todo el tráfico de navegación gestionado
- Inspección SSL completa para todo el tráfico https
- Personalización de los mensajes de bloqueo por entornos de negocio diferenciados
- Soporte para agregación de puertos mediante LACP

Proyecto financiado por la Unión Europea a través del Fondo Europeo de Desarrollo Regional en el marco del Programa Operativo FEDER de Asturias 2014-2020

Unión Europea

Fondo Europeo de Desarrollo Regional

C/ Trece Rosas, 2, 5ª planta, sector derecho, 33005 Oviedo. Tfno: 985 10 59 59. Fax: 985 10 59 45

- Integración con servicio de RADIUS con el fin de establecer políticas de navegación en base a usuarios o grupos
- Integración con servicio de sandboxing o similar, en local o en la nube, para detección de APT's
- Capacidades de detección de DoS

4.1.2. Gestión de VPN

A continuación se indican las características mínimas de la herramienta relativas a la gestión de VPN's:

- Número de conexiones VPN simultáneas: >= 5000
- Número de conexiones VPN SSL: >= 5000
- Capacidad VPN L2L
- VPN mediante cliente IPSEC compatible con Cisco VPN Client
- Creación de portales SSL para el acceso a servicios WEB y/o RDP sin necesidad de utilizar un cliente VPN
- Cliente VPN con capacidades para detectar conformidad de configuración del cliente final (antivirus, parcheado, entre otros)
- Doble factor de autenticación para el servicio VPN

4.1.3. Gestión firewall sobre la publicación de servicios en internet

A continuación se indican las características mínimas que se solicitan relativas a la publicación de servicios en internet:

- Capacidades de filtrado a nivel de aplicación
- Capacidades para realizar rotura de túnel SSL
- Capacidades de detección DoS

4.1.4. Manuales de la herramienta.

La solución propuesta deberá venir provista con los siguientes manuales en el idioma castellano:

- Manual de instalación
- Manual de configuración
- Manual de uso

Todo ello se realizará atendiendo a los criterios necesarios que puedan ser explicados por el Jefe de Proyecto de la DGTIC y en general siguiendo las metodologías existentes en la Administración del Principado de Asturias.

Proyecto financiado por la Unión Europea a través del Fondo Europeo de Desarrollo Regional en el marco del Programa Operativo FEDER de Asturias 2014-2020

Unión Europea

Fondo Europeo de Desarrollo Regional

C/ Trece Rosas, 2, 5ª planta, sector derecho, 33005 Oviedo. Tfno: 985 10 59 59. Fax: 985 10 59 45

4.1.5. Hardware de la solución

El hardware proporcionado con la solución debe tener las siguientes características mínimas:

- Interfaces de conexión a 10G y a 1G
- Cada equipo debe disponer de fuentes de alimentación redundante cambiables en caliente sin interrupción del servicio
- Cada equipo debe disponer de soporte para IPv6 con tecnología de doble pila
- Cada equipo de la solución debe contar con certificaciones de bajo consumo, protecciones de seguridad para su manipulación y compatibilidad electrónica

5. Servicios de implantación

El contratista deberá realizar la implantación del equipamiento adquirido, que incluye:

- Consultoría y soporte en remoto y presencial, tanto en las fases iniciales del contrato como a lo largo del proceso de implantación si así es requerido por la Jefatura del Proyecto de la DGTIC

- Diseño de la implantación, realizando un análisis detallado y documentado de la opción más óptima de instalación en la infraestructura tecnológica de la APA, proporcionando los documentos exigidos en las metodologías de la APA (documento de análisis y diseño de la arquitectura) junto con el documento de intervención detallado para la conexión a la red. El diseño de la solución deberá observar todas las normas y recomendaciones que se deriven del cumplimiento efectivo de las indicaciones u obligaciones de organismos como el Centro Criptológico Nacional o de reglamentos como el Esquema Nacional de Seguridad.

- Servicios de instalación, configuración, optimización y puesta en marcha de los equipos, de forma que en función de la infraestructura tecnológica de la organización y de las necesidades para una correcta integración con los sistemas de seguridad ya presentes, se garantice una solución ajustada desde el primer momento. Igualmente la solución pasa por aportar un planteamiento técnicamente razonable para la migración de cualesquier sistema que estuviera en uso y que realizase funcionalidades en la línea de la que se persiguen potenciar con este contrato.

Proyecto financiado por la Unión Europea a través del Fondo Europeo de Desarrollo Regional en el marco del Programa Operativo FEDER de Asturias 2014-2020

Unión Europea

Fondo Europeo de Desarrollo Regional

C/ Trece Rosas, 2, 5ª planta, sector derecho, 33005 Oviedo. Tfno: 985 10 59 59. Fax: 985 10 59 45

- Despliegue operativo de la solución en el Centro de Proceso de Datos (CPD) de la APA.
- Documentación de toda la infraestructura instalada y del proyecto siguiendo las metodologías del Principado de Asturias.

6. Servicios de formación

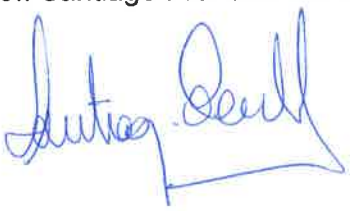
El adjudicatario deberá prestar los servicios de formación o transferencia del conocimiento durante al menos cuatro sesiones (20 horas) sobre la operación y mantenimiento del sistema implantado. El contenido mínimo a impartir será el siguiente:

1. Arquitectura del sistema
2. Instalación del sistema
3. Arranque y parada del servicio
4. Administración del sistema
5. Actualizaciones del sistema
6. Creación de casos de uso, políticas, perfiles
7. Optimización, análisis y resolución de problemas en el sistema
8. Integración con otros sistemas

La formación se realizará en las instalaciones de la Administración del Principado de Asturias.

EL JEFE DE PROYECTOS DE SEGURIDAD,

Fdo.: Santiago Prendes Martínez



Proyecto financiado por la Unión Europea a través del Fondo Europeo de Desarrollo Regional en el marco del Programa Operativo FEDER de Asturias 2014-2020

Unión Europea

Fondo Europeo de Desarrollo Regional

C/ Trece Rosas, 2, 5ª planta, sector derecho, 33005 Oviedo. Tfno: 985 10 59 59. Fax: 985 10 59 45