



PLIEGO DE ESPECIFICACIONES TÉCNICAS PARA LA ADQUISICIÓN DE UNA SOLUCIÓN DE SEGURIDAD INFORMÁTICA PERIMETRAL DE LA UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Introducción

La red de comunicaciones de la UPV, que proporciona servicios a los profesores, investigadores, alumnos y personal de administración de servicios de la universidad, tiene unos elevados requerimientos en términos de seguridad informática. Por ello, y debido al continuo aumento de requerimientos por parte de las aplicaciones y usuarios, de una parte, y de otra la necesaria renovación derivada de la obsolescencia del equipamiento actual, se hace necesaria la adquisición de una nueva solución de seguridad informática perimetral.

Esta solución constará de un **mínimo** de una pareja de equipos que se insertarán en las entradas y salidas de las conexiones a Internet de la UPV y tendrán como función detectar y eliminar las amenazas informáticas que se pudieran producir y, opcionalmente, tomar decisiones en función del tipo de tráfico, reputación del origen o destino del mismo y otros parámetros.

Descripción de la solución

La solución de seguridad informática perimetral debe de cumplir con las siguientes características **mínimas**.

- Alta disponibilidad en modo activo-activo o activo-pasivo
- 2 interfaces 10GbE con transceptor 10GBASE-SR y 6 interfaces 1000BASE-T por equipo.
- Fuente de alimentación redundante en cada uno de los equipos
- Soporte de servicios de reputación basados en firmas
- Soporte de análisis heurístico
- Protección contra ataques DOS y DDOS
- Control de políticas por usuarios
- 5 Gbps de rendimiento de la prevención de amenazas (IPS)
- Soporte de 1.000.000 de sesiones simultáneas
- Soporte de 10.000 reglas diferentes
- Soporte de protocolos IPv4 e IPv6
- Soporte de NAT y NAT64
- Soporte de OSPFv2 y OSPFv3 y Policy-based forwarding
- Soporte de PIM-SM e IGMPv3
- 1000 VLANS 802.1q
- Soporte del estándar 802.3ad (LACP)
- Gestión centralizada de usuarios





**ÀREA DE SISTEMES
D'INFORMACIÓ I COMUNICACIONS**

- Gestión de logs y generación de informes gráficos (con colores)
- Configuración y gestión mediante línea de comandos y APIs

Se valorará de forma adicional estas características

- Calidad y rendimiento del sistema de redundancia y tolerancia a fallos
- Soporte y prestaciones de servicios de reputación de URL
- Soporte y prestaciones de servicios de reputación de antimalware y otras amenazas
- Soporte y prestaciones de servicios de inspección de tráfico cifrado
- Soporte y prestaciones de la respuesta ante nuevas amenazas.
- Capacidades de ampliación de la solución
- Mejoras en el rendimiento y la gestión de la solución
- Conformidad y certificaciones de la solución y específicamente la conformidad con el ENS (Esquema nacional de seguridad)

Garantía y servicio

Todos los equipos aportados en el presente concurso dispondrán de garantía hardware en horario laboral (8x5 NBD) y de versiones de software por una duración mínima de 2 años así como el soporte del fabricante ante problemas de funcionamiento que pudieran surgir. En caso que la oferta incluya servicios de suscripción adicionales, dichos servicios tendrán que tener el mismo nivel de garantía y servicio.

Plazos de instalación

Adjudicado el concurso, el adjudicatario dispondrá de un plazo de 30 días para, conjuntamente con los técnicos de la UPV, realizar un plan de implantación detallado de la solución propuesta. Dicho plan se tendrá que ejecutar necesariamente a lo largo de los siguientes 100 días. Durante este plazo, y de preferencia al iniciarse la instalación se impartirá un curso de formación de al menos 15 horas sobre la gestión y configuración de la solución suministrada.

Cumplimiento de normativa

En cumplimiento con lo dispuesto en el artículo 99.4 de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, y el artículo 18 del Real Decreto 3/2010, de 8 de enero por el que se regula el Esquema Nacional de Seguridad, el licitador incluirá referencia precisa, documentada y acreditativa de que los productos de seguridad, equipos, sistemas, aplicaciones o sus componentes, han sido previamente certificados por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.





UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA

ÀREA DE SISTEMES
D'INFORMACIÓ I COMUNICACIONS

En el caso de que no exista la certificación indicada en el párrafo anterior, o esté en proceso, se incluirá, igualmente, referencia precisa, documentada y acreditativa de que son los más idóneos.

Cuando estos sean empleados para el tratamiento de datos de carácter personal, el licitador incluirá, también, lo establecido en la Disposición adicional única del Real Decreto 1720/2007, de 21 de diciembre.

Valencia, 25 de noviembre de 2015

FDO. Vicente Botti Navarro
Vicerrector de las tecnologías de la información y
de las Comunicaciones

Fdo: Jaime Busquets Mataix
Jefe de Servicio de Sistemas y Redes de
Comunicación
ASIC

