La Universidad de Oviedo consolida su estructura de seguridad y mejora el rendimiento de su red con Palo Alto Networks™

ANTECEDENTES

Fundada en 1608 por manda testamentaria del Arzobispo don Fernando de Valdés Salas, la Universidad de Oviedo cuenta actualmente con unos 23.000 alumnos, 2.000 PDI (Personal Docente e Investigador) y 1.000 PAS (Personal de Administración y Servicios) para impartir enseñanzas oficiales de 1º y 2º ciclo, grado, master y Doctorado, así como otros estudios de títulos propios y extensión universitaria.

De igual manera, la Universidad de Oviedo desarrolla una importante actividad investigadora, siendo partícipe de proyectos a nivel regional, nacional e internacional. En este punto, la necesidad de los distintos grupos de investigación que existen en la Universidad de compartir información, investigaciones o cualquier tipo de conocimiento con otros colectivos en el mundo conlleva que el uso de Internet sea imprescindible. Asimismo, la gestión universitaria en cualquiera de sus vertientes también es cada día más dependiente de la integración con servicios de terceros (organismos autonómicos, estatales, etcétera) a lo que hay que sumar la obligatoriedad de la Universidad, como organismo público, de proporcionar a los ciudadanos canales electrónicos seguros para realizar sus trámites.

OBJETIVO: CREACIÓN DE UNA POLÍTICA DE SEGURIDAD BASADA EN APLICACIÓN

Por la gran cantidad de usuarios concurrentes, unas 32.700 conexiones simultáneas de media, la Universidad de Oviedo partía de la siguiente problemática asociada a dicha infraestructura: falta de visibilidad, control y seguridad del tráfico que corría por la misma. Dicha situación, impedía tener una visión específica sobre los contenidos y actividad de los usuarios, debido a la incapacidad de los sistemas implantados en ese momento, dos firewall de otro fabricante, para generar políticas de seguridad basadas en aplicaciones o usuarios.

Ante tales circunstancias, el objetivo del proyecto consistía en crear una política de seguridad basada en aplicación y no en direcciones y puertos, para poder atajar y eliminar la problemática. En este sentido, y después de analizar todas sus necesidades, la Universidad de Oviedo optó por dos firewall modelo PA-5050, y no sólo porque Palo Alto Networks ofreciera un producto capaz de trabajar en la capa 7 sin penalizar el rendimiento del sistema, sino también, por su facilidad de uso, integración con otros sistemas, y flexibilidad a la hora de implementar políticas de seguridad. Para esta labor contó con la colaboración de Acuntia, partner integrador del proyecto.

"El objetivo inicial del proyecto fue la modernización de la seguridad perimetral de la red universitaria, mejorando la capacidad de análisis de tráfico y adecuando el equipamiento al nuevo caudal de conexión hacia RedIRIS-NOVA (red avanzada de investigación de I+D), explica Javier Pérez Arenal, Jefe de Área Técnica de Informática y Comunicaciones de la Universidad de Oviedo. "Asimismo", continúa, "requeríamos de una solución que nos permitiese consolidar muchos de los servicios tanto de 'firewalling' como 'helpers' de la red perimetral en una única máquina, y que, además, asegurase la visibilidad de los equipos en la red. Todo esto lo hemos conseguido gracias a la tecnología de próxima generación de firewall de Palo Alto Networks, ya que la nueva infraestructura nos permite la conexión a 10 Gbps y un mayor control de lo que ocurre entre nuestra red e Internet".

UNIVERSIDAD DE OVIEDO

ORGANIZACIÓN:
Universidad de Oviedo

SECTOR:
Unidad Educativa de Enseñanza Superior

PROYECTO:
Consolidar y optimizar sus sistemas de protección TI, y mejorar la visibilidad, el control y la seguridad del tráfico que corre por su red.

SOLUCIÓN:
Dos firewall modelo PA-5050.

RESULTADOS:

- Creación de una política de seguridad basada en aplicación y no en direcciones y puertos.
- Mejora de la capacidad de análisis de tráfico.
- Consolidación de servicios, tanto perimetrales (firewall) como de usuario (proxy).
- Notable reducción del tiempo dedicado a gestión y administración.
- El control por monitorización de la red, es otro de los aspectos que más se han desarrollado.
- Se han hecho visibles, de una forma muy sencilla las aplicaciones que se están utilizando, junto con la identificación de los usuarios que la demandan así como de los riesgos asociados a dichas aplicaciones.
- Salto cualitativo en el control de los eventos acontecidos en su perímetro de comunicaciones, tanto flujos entrantes como salientes.

paloalto NETWORKS
the network security company™

"El grado de satisfacción con los productos de Palo Alto Networks es muy positivo. Ya en la fase de prospección de soluciones, ésta se reveló como una de las más completas y competitivas de todas las analizadas. El salto cualitativo en el control de los eventos que ocurren en nuestro perímetro de comunicaciones, tanto en flujos entrantes como salientes, ha sido muy importante. Por todo ello, es más que previsible que en futuros procesos de adquisición de hardware, sobre todo en el ámbito relacionado con la seguridad de las comunicaciones, tengamos presentes las soluciones de Palo Alto Networks".

Javier Pérez Arenal
Jefe de Área Técnica de Informática y Comunicaciones de la Universidad de Oviedo

Ya en primera instancia, y tras pocos días con la solución implantada, la Universidad de Oviedo lograba dar un gran salto cualitativo en cuanto a la información recogida. De este modo, ha pasado de contar con cuadros estadísticos de número de bytes –que se reciben en un puerto determinado– a una lista de amenazas, aplicaciones y usos en general de la infraestructura de comunicaciones, lo que les permite definir y aplicar medidas tanto reactivas como proactivas en este campo.

FASES DEL PROYECTO: HACIA UN MAYOR CONTROL DEL TRÁFICO DE RED

Con los objetivos tecnológicos a conseguir definidos, la Universidad de Oviedo inició este proyecto de migración e implantación, para lo que contó con el apoyo y asesoramiento de Acuntia quién, además, promovió la posibilidad de que la Universidad dispusiera de unidades de demostración para realizar una prueba previa a la adquisición de los equipos. Dicha demostración mostraría a la Universidad el nivel de control que podía adquirir con este tipo de equipamientos.

Como punto de partida, se inició la recogida de requerimientos, tanto funcionales como técnicos, revaluando la visión del intercambio de información entre la comunidad universitaria y el resto del mundo. En este estado, era necesaria una visión más específica, más dirigida a contenidos y usos que la que se tenía por entonces, de más bajo nivel.

Establecidos los criterios de partida, se llevó a cabo una prospección de mercado en este ámbito para conocer qué posibilidades había y a qué coste, tanto de inversión como de propiedad, identificando los requerimientos que podían ser cubiertos por las soluciones existentes. Esa información fue evaluada por los gestores correspondientes y se completó la adquisición de la solución propuesta por Palo Alto Networks.

A partir de ese momento, se procedió a la transferencia de las reglas de negocio de nivel 4 de la salvaguarda existente al nuevo equipamiento, y a su puesta en producción en la primera quincena de marzo de 2012. Posteriormente, se redefinieron las reglas y se adecuaron al nuevo entorno de control de aplicaciones, para satisfacer los objetivos de la Universidad.

"Inicialmente, en la fase de transición, se hizo necesario conocer la herramienta que proporciona el fabricante para migrar las reglas de negocio a su plataforma. Posteriormente, el inicio del control de aplicaciones y amenazas ha requerido una adecuación de los criterios establecidos para el intercambio de información entre la Universidad e Internet. Este cambio implica redefinir qué es lo que se quiere gestionar o monitorizar, gracias a la nueva visibilidad que nos proporciona la solución", comenta Javier Pérez. "Podemos considerar que no se ha cerrado el proyecto por parte de la Universidad, dado que la nueva información que aporta la solución hace que la revisión sea continua, entrando en un ciclo PDCA con la realimentación que proporciona el sistema".

MODERNIZACIÓN DE LA SEGURIDAD PERIMETRAL Y MAYOR VISIBILIDAD

Con la instalación de los dos PA-5050, la Universidad de Oviedo ha logrado una mayor visibilidad y control de aplicaciones y usuarios, una mejor prevención de amenazas, y una consolidación de los diferentes servicios, ya sean perimetrales (firewall) o de usuario (Proxy).

"El grado de satisfacción con los productos de Palo Alto Networks es muy positivo. Ya en la fase de prospección de soluciones, ésta se reveló como una de las más completas y competitivas de todas las analizadas", matiza Javier Pérez. "El salto cualitativo en el control de los eventos que ocurren en nuestro perímetro de comunicaciones, tanto en flujos entrantes como salientes, ha sido muy importante. Por todo ello, es más que previsible que en futuros procesos de adquisición de hardware, sobre todo en el ámbito relacionado con la seguridad de las comunicaciones, tengamos presentes las soluciones de Palo Alto Networks".

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com