

Sainsel optimiza el tráfico web y securiza su infraestructura con Netasq

Los ingenieros de Sainsel Sistemas Navales trabajaban con un acceso limitado a Internet, que afectaba negativamente a su rendimiento. A este problema se unía la entrada de virus en el parque informático. La implantación de Netasq U120 ha facilitado la discriminación de tráfico entre correo corporativo y navegación web genérica, proporcionando una mayor velocidad de acceso a las aplicaciones y una robusta seguridad perimetral.

Tx: Redacción.

Ft: Netasq.

LA FABRICACIÓN Y EL suministro de sistemas de navegación marítima es la actividad principal de Sainsel Sistemas Navales. Esta empresa española, especializada a su vez en el equipamiento de combate, ha confiado en las soluciones de Netasq, proveedor de seguridad de redes, para solventar sus problemas de seguridad perimetral y mejorar la velocidad de acceso a Internet.

Sainsel dispone de una red local de aproximadamente 65 usuarios, la mayoría ingenieros, involucrados a menudo en trabajos de I+D para organismos oficiales y desarrollo de *hardware* y *software*, tareas que demandan autonomía para poder instalar herramientas y librerías de desarrollo que normalmente descargan de Internet, cuyo acceso se realizaba a través de una única línea con un *firewall* instalado. Esta forma de trabajar, sin embargo, implicaba que al descargar ficheros los usuarios, la línea se ralentizara notablemente. Además, y a pesar de contar con un antivirus, la entrada de *software* malicioso en los PC se producía con regularidad. Ante esta situación, la compañía comprendió que era ineludible la instalación de una solución que resolviese estos y otros problemas de seguridad, además de contratar una segunda línea de acceso a Internet para aliviar la carga.

Concretamente, Sainsel, cuya red consta de dos servidores fundamentales, un controlador de dominio y almacén de ficheros, y otro servidor de bases de datos para sus aplicaciones corporativas, se decantó por el *appliance* Netasq U120 que, entre



José Mateos, director económico y financiero de Sainsel.

otras características, funciona como antivirus perimetral, al tiempo que permite el balanceo de cargas entre las dos líneas de acceso a Internet, desviando el tráfico específico de ciertos sitios de descarga a una línea, y dejando la otra para correo, navegación o accesos remotos.

Seguridad perimetral

Con el apoyo y asesoramiento de Antisa, compañía especializada en soluciones integrales para la creación, adaptación y renovación de estructuras TI, Sainsel se embarcó en un proyecto de actualización de su infraestructura de red y, al mismo tiempo, mejorar de su seguridad perimetral.

A este respecto, y tal y como explica José Mateos, director económico y financiero en Sainsel, "por su infraestructura, Sainsel genera una gran cantidad de tráfico. Tras comprobar que la infraestructura era la correcta y que la lentitud se debía al tráfico generado por los usuarios, se optó

por configurar el equipo U120 de Netasq como balanceador de carga entre dos líneas, optando por priorizar el tráfico necesario en una de ellas (gestionada por Colt) y enviando el tráfico menos importante por la otra (de Telefónica)".

Por otra parte, según Mateos: "Contar con un nuevo elemento anti-virus/*firewall* representa una seguridad adicional en la red. Con dos líneas de acceso a Internet, ahora somos capaces incluso de diferenciar por páginas web o direcciones IP cuál queremos que salga por cada línea". Gracias a la solución de la firma francesa es más sencillo diferenciar entre el tráfico de correo corporativo y la navegación http genérica, -evitando *streaming* o P2P, por ejemplo-, redundando en la optimización de la velocidad de acceso a las aplicaciones y páginas web prioritarias.

La implantación del Netasq U120 se llevó a cabo en dos fases: En la primera se realizó una preconfiguración de la herramienta fuera del entorno de producción, en la cual se configuraron, entre otras, los interfaces del *hardware* para evitar tiempos de caída durante su instalación. Después, se procedió a la instalación física, conexión y finalización de la configuración. Como última medida, se abrieron algunos protocolos para que tanto proveedores como clientes pudiesen obtener acceso desde el exterior en momentos determinados. "Todo este proceso -apunta Mateos-, se realizó en horario de trabajo, con todos los usuarios de la red trabajando normalmente y con apenas unos segundos de interrupción en la conexión a Internet, por lo que la transición fue prácticamente inapreciable para los empleados". ■