

MAZ obtiene mayor seguridad, visibilidad y control de red con Palo Alto Networks™

ANTECEDENTES

Con más de 80 centros asistenciales y dos hospitales propios, con implantación nacional, MAZ centra su actividad en la gestión de las contingencias de Accidentes de Trabajo y Enfermedades Profesionales, asistencia sanitaria, trámites para prestación económica por incapacidad temporal derivada de la enfermedad común o accidente no laboral, y otros servicios y actividades legalmente atribuidas por el Ministerio de Trabajo. Asimismo, la entidad –séptima mutua en el ranking del sector entra las 20 existentes– presta servicio a más de 88.000 empresas asociadas a nivel nacional, protege a unos 515.000 trabajadores por cuenta ajena, y cuenta con más de 95.000 trabajadores autónomos adheridos protegidos.

Esta filosofía de prestación de servicio a empresas y ciudadanos ha llevado a MAZ a no descuidar facetas tales como la innovación, apostando siempre por el desarrollo de mayores capacidades técnicas y médicas, y por la implantación de las tecnologías más avanzadas. En este punto, MAZ posee dos CPDs ubicados en Zaragoza (primario) y en Barcelona (backup), y dispone, además, de una red WAN que interconecta sus más de 100 centros de trabajo, y de un sistema propio autónomo para la presencia en Internet, al que acceden cerca de 1.300 empleados (1.000 PC y 210 servidores). De igual manera, la entidad dispone de un Área Privada (Extranet) a la que, sin coste alguno, se facilita el acceso a las empresas asociadas de forma personalizada y segura.

MAYOR CONTROL DEL TRÁFICO DE RED

Con un porcentaje de tráfico de Internet de entre 20mb y 30mb, con unas 25.000 sesiones, MAZ partía de la siguiente problemática asociada a su infraestructura de red: imposibilidad de identificar el tipo de aplicaciones no corporativas que atravesaban su red, las aplicaciones se encontraban camufladas dentro del común del tráfico “http”, dentro de túneles cifrados “ssl”, o se hacían indetectables utilizando todo tipo de técnicas evasivas como “port hopping”, etcétera.

Ante tal situación, la empresa decidió acometer un proyecto de modernización de su solución de seguridad perimetral, con el objetivo de obtener un mayor control de las aplicaciones, realizando un examen mucho más exhaustivo del tráfico de red cursado, integrándose con el directorio activo para poder identificar usuarios, y bloqueando, además, todo tipo de malware moderno y APT “Advanced Persistent Threats”.

“Nuestra presencia en Internet es muy alta. MAZ es un sistema autónomo y dispone de un número importante de direcciones IP públicas, por lo que el número de amenazas que recibimos es muy alto”, explica Eduardo Gistau Arbués, Responsable de Telecomunicaciones de MAZ. “El anterior sistema de seguridad perimetral no nos reportaba las respuestas esperadas, y los problemas de gestión eran cada vez más acuciantes. En este punto, nos propusimos migrar a un firewall de nueva generación, en alta disponibilidad, lo suficientemente escalable como para asumir el tráfico que generábamos y lograr un control más personalizado del tráfico de red”.



ORGANIZACIÓN:

Mutua de Accidentes de Trabajo y Enfermedades Profesionales de la Seguridad Social nº 11, MAZ

SECTOR:

Mutua de la Seguridad Social

PROYECTO:

Mejora de su sistema de seguridad perimetral y obtención de un mayor control del tráfico de red.

SOLUCIÓN:

Dos firewall modelo PA-2050 en alta disponibilidad + la plataforma de gestión Panorama.

RESULTADOS:

- Se ha reducido notablemente el tiempo dedicado a gestión y administración.
- Mayor detalle sobre los ataques recibidos y mayor visibilidad del tráfico de la red.
- Gracias al motor WildFire™ de Palo Alto Networks y su servicio de análisis en la nube, es posible luchar de manera efectiva contra “botnets” y malware desconocido “día cero”.
- Se han hecho visibles, de una forma muy sencilla, las aplicaciones que se están utilizando y se han identificado los usuarios que las demandan así como de los riesgos asociados al uso de dichas aplicaciones.
- Gestión integrada con los grupos y usuarios del Directorio Activo, lo que permite construir políticas para grupos específicos de usuarios.
- El diseño se ha simplificado, al no haber requerido elementos extras para proporcionar la totalidad de las funcionalidades requeridas.



the network security company™

“Nuestra presencia en Internet es muy alta. MAZ es un sistema autónomo y dispone de un número importante de direcciones IP públicas, por lo que el número de amenazas que recibimos es muy alto. El anterior sistema de seguridad perimetral no nos reportaba las respuestas esperadas, y los problemas de gestión eran cada vez más acuciantes. En este punto, nos propusimos migrar a un firewall de nueva generación, en alta disponibilidad, lo suficientemente escalable como para asumir el tráfico que generábamos y lograr un control más personalizado del tráfico de red”.

Eduardo Gistau Arbués
Responsable de
Telecomunicaciones de MAZ

Debido a los altos requerimientos de gestión del grupo, MAZ decidió implantar también el software de gestión Panorama de Palo Alto Networks. En palabras de Eduardo Gistau Arbués: “Panorama es el complemento ideal para los equipos de Palo Alto Networks, puesto que permite consolidar y gestionar los logs de todos los gateway con capacidad casi ilimitada, además, gracias a la consolidación de logs es posible realizar informes unificados de toda la organización. Un gran valor añadido sobre otros fabricantes es que la consola es igual de sencilla de manejar que los propios equipos Palo Alto Networks”.

Tras realizar un análisis de los requisitos y de los productos existentes en el mercado, MAZ optó por la solución de Palo Alto Networks PA-2050, (dos firewall en Alta Disponibilidad) distribuida en España a través de Exclusive Networks Iberia (mayorista que jugó un papel decisivo en la etapa de prescripción y defensa técnica preventiva), y la cual, gracias a sus funcionalidades avanzadas (App-ID™, User-ID™, Content-ID™ y QoS), gestiona flujos de tráfico de hasta 1 Gbps, usando procesadores y memoria dedicados para networking, seguridad, prevención y gestión de amenazas. Independizando, además, el tráfico de gestión del de datos.

UN PROCESO DE IMPLANTACIÓN ESTRUCTURADO EN DIFERENTES FASES

Con los objetivos tecnológicos a conseguir definidos, MAZ inició este proyecto de migración e implantación que, por sus características, tuvo una duración de dos semanas y quedó estructurado en varias fases, puesto que la migración de zonas de seguridad se realizó de una manera escalonada.

En este punto, un equipo de RSC (Redes Sistemas Comunicaciones), integrado por cuatro personas (un responsable comercial y otro técnico, además de dos técnicos) se responsabilizó de la implementación del proyecto, ocupándose de las labores de consultoría, diseño, acción preventiva e implementación del equipamiento de Palo Alto Networks. Gracias a que RSC cuenta con una persona desplazada en las oficinas de MAZ, la entidad podrá asegurar el correcto funcionamiento del día a día.

Como primera medida, y tras llevar a cabo un análisis de los servicios y recursos existentes de MAZ, procedió a ejecutar una fase de planificación, que conllevó, entre otras medidas, el establecimiento de las prioridades de seguridad y de alta disponibilidad de los recursos. Como paso siguiente, y una vez realizada la planificación e instalación de los nuevos equipos e infraestructuras de red, tuvo lugar un proceso migración y de validación desde el sistema anterior a los nuevos Palo Alto Networks (políticas de seguridad a nivel 7), para más tarde proceder a la realización de un test de carga y balanceo. Tras ello, tuvo lugar la puesta en producción, así como, la formación de usuario y administrador sobre la nueva tecnología.

“Entre los recursos del proveedor y los propios de MAZ hemos podido acometer el proyecto en un tiempo record. El firewall PA-2050 es una herramienta muy intuitiva y de sencillo manejo, que nos ha permitido obtener un mayor detalle sobre los ataques que recibimos, y, de esta manera, centrarnos en las amenazas de mayor riesgo. El grado de satisfacción es muy alto, nuestra filosofía en seguridad es estar siempre preparados y en futuros proyectos Palo Alto Networks será una empresa a tener muy en cuenta”.

Eduardo Gistau Arbués
Responsable de
Telecomunicaciones de MAZ

Tras la implementación de los dos equipos PA-2050 con licencias de “Threat Prevention” y “URL filtering”, MAZ ya disfruta de todas sus capacidades: IPS, antivirus, bloqueo de malware moderno, filtrado de URL, e integración con Directorio Activo, entre otras. Asimismo, ha logrado una mayor visibilidad de la red, lo que ha permitido, entre otras, descubrir tráfico que antes sospechaban que existía, pero que eran incapaces de evidenciar. Además, gracias al motor “Wildfire” de Palo Alto Networks y su servicio de análisis en la nube, es posible luchar de manera efectiva contra “botnets” y malware de “día cero”.

“Entre los recursos del proveedor y los propios de MAZ hemos podido acometer el proyecto en un tiempo record. El firewall PA-2050 es una herramienta muy intuitiva y de sencillo manejo, que nos ha permitido obtener un mayor detalle sobre los ataques que recibimos, y, de esta manera, centrarnos en las amenazas de mayor riesgo”, confirma Eduardo Gistau Arbués. “El grado de satisfacción es muy alto, nuestra filosofía en seguridad es estar siempre preparados y en futuros proyectos Palo Alto será una empresa a tener muy en cuenta”.