Fraternidad Muprespa: gestión y control del acceso de la red corporativa

Fraternidad Muprespa es una Mutua de Accidentes de Trabajo y Enfermedades Profesionales de la Seguridad Social. Cuenta con más de 100.000 m² en instalaciones sanitarias y administrativas, una red propia con 168 centros asistenciales y oficinas, dos grandes centros hospitalarios en Madrid y dos centros intermutuales. El objetivo de Fraternidad Muprespa es ser la mutua de referencia por la vocación de servicio a los mutualistas y a los trabajadores. Preocupados por la calidad, la eficacia y la eficiencia, Fraternidad Muprespa promueve la austeridad en la gestión, la creatividad y la innovación, máxime si se tiene en cuenta que debe prestar un servicio público. Recientemente la entidad ha acometido un proyecto de gestión y control del acceso de la red corporativa para el que ha contado con la colaboración de Know How Millenium y donde la tecnología CounterACT de ForeScout juega un papel destacado.

Pedro Serrera / Fernando Paniagua

Problemática inicial

En Fraternidad Muprespa necesitábamos una mayor visibilidad y un control en el acceso a nuestra red corporativa de todos los dispositivos IP que se conectan desde cualquier punto (conexión RJ-45, WiFi, VPN), así como saber si cumple las políticas corporativas antes de darle acceso a la red, por varios motivos. El primero era el control básico de qué dispositivos están conectados a la red en cada delegación: desde ordenadores, portátiles, impresoras, tabletas, *smartphones*, máquinas multifunción... y el pasado mes de enero comenzábamos el despliegue de la telefonía IP, y los teléfonos también son máquinas con necesidades de gestión remota.

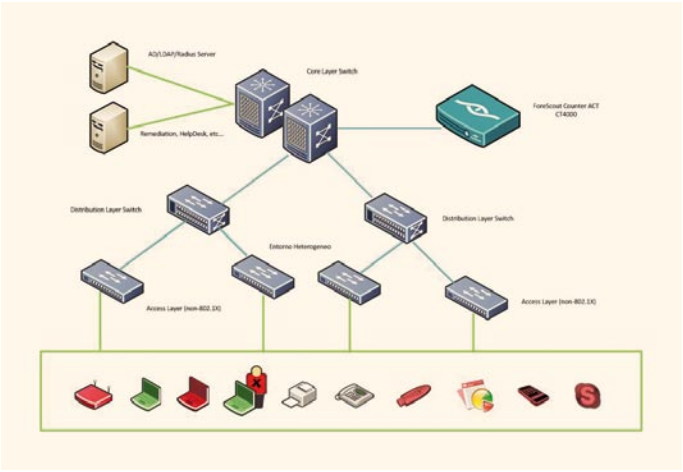
El segundo motivo era la necesidad de aplicación de políticas de seguridad ante situaciones de riesgo; sin entrar en las complejidades de un IPS, existen situaciones básicas como la actualización del antivirus, la instalación del aplicativo corporativo FRAGUA, o la distribución de parches de Windows que nos interesaba controlar y aplicar, en su caso, las medidas correctivas adecuadas.

El tercer motivo viene derivado de la explosión del mundo móvil, y de nuestra intención de abrir nuestra red WiFi a los pacientes que acuden a nuestros centros sanitarios, con las debidas garantías de seguridad y protección. Para ello es clave identificar los equipos, aislarlos en una red diferenciada y gestionarlos adecuadamente.

Lo que buscábamos era un modelo de gestión integral de la red para resolver todas estas necesidades, y otras de naturaleza similar que pudieran plantearse en el futuro. Por lo tanto, la solución pasaba por un dispositivo de la familia NAC (*Network Access Control*).

En la solución NAC no solo se buscaba desplegar una validación 802.1x, sino además un sistema que permitiera en un entorno mixto la flexibilidad de realizar un NAC con o sin 802.1x; y que posteriormente los equipos validados fueran analizados constantemente, para que si en un momento determinado uno de ellos no cumplía con la política de seguridad de la Mutua, se tomaran las acciones correctivas adecuadas.

Otro de los objetivos era que el despliegue de la solución NAC no impactara en el funcionamiento diario de Fraternidad Muprespa, que fuera rápido, flexible y que permitiera su integración en un entorno heterogéneo de fabricantes, tanto en el presente como en el futuro.



Solución adoptada

Fraternidad Muprespa, como Mutua de Accidentes de Trabajo y, por tanto, Entidad Colaboradora de la Seguridad Social, está sometida a la Ley de Contratos del Sector Público y, por tanto, era preceptivo licitar la contratación de la solución. Tras una primera fase en la que analizamos el estado del arte de las soluciones NAC debido a su rápida evolución en los últimos años, valoramos varias soluciones. Posteriormente elaboramos un pliego de prescripciones técnicas muy completo. También tomamos la decisión de redirigir nuestro 'Perfil del contratante' a la Plataforma de Contratación del Estado del Ministerio de Hacienda y AAPP, que facilita los trámites de licitaciones públicas, a la vez que otorga máxima publicidad a todos nuestros procedimientos. De hecho, los pliegos están colgados (el número de expediente es el PIC201214307) y se pueden consultar públicamente. Uno de los requisitos que planteábamos en nuestra solución era que no fuera obligatorio realizar un despliegue de protocolos de gestión de red en toda nuestra electrónica, que es muy variada, y nos hubiera supuesto un trabajo de configuración complejo y costoso; es decir, queríamos una solución "no invasiva". Otros requisitos como la gestión a través de SNMP o la integración con nuestro directorio eran obligados y, además, existía la posibilidad de hacer un despliegue con y sin agente.

Aunque, como hemos referido, el pliego está colgado en la Plataforma, y pensamos que es un buen modelo de listado de especificaciones técnicas y funcionales para una solución NAC. Fue una licitación muy concurrida, pues recibimos ofertas de hasta cinco empresas con soluciones todas ellas muy interesantes, tanto en capacidad técnica como en precio. Finalmente se optó por la solución que presentó el integrador *Know How Millenium* del fabricante ForeScout, y concretamente el producto contratado fue *ForeScout CounterACT* para 4000 dispositivos IP en un único dispositivo, es decir, una arquitectura totalmente abierta que puede escalar en función de nuestro crecimiento.

Beneficios conseguidos

Con la solución NAC *ForeScout CounterACT*, el control que consigues sobre tu red es muy superior. La visibilidad es total, y a partir de ahí las políticas que se pueden implementar dependen de tus necesidades. Hemos adoptado la metodología clásica en este tipo de proyectos, en los que existe una primera fase de clasificación de dispositivos y aclaración de las excepciones que realmente nos impresionó, ya que en menos de un día teníamos detectados todos los dispositivos IP en nuestra red y clasificados (tipo de dispositivos, S.O., parches de seguridad, aplicaciones instaladas, etc.); una segunda fase en la que se definen las políticas y se obtienen porcentajes de cumplimiento; y una tercera fase en las que de un modo muy progresivo –y combinando las medidas de concienciación con las de remediación– conseguimos incrementar muy sustancialmente los porcentajes de cumplimiento.

Otros beneficios han repercutido en la mejora del trabajo del Centro de Atención al Usuario, pues conoce de primera mano el origen de los problemas, y puede anticipar la resolución de los mismos de manera preventiva. En cuanto a la seguridad, creemos que hemos mejorado nuestro nivel de seguridad reduciendo el nivel de riesgo. Y en cuanto al *reporting*, la solución proporciona un cuadro de mando que ofrece unos datos agregados de tendencia y cumplimiento muy interesantes.

Un último beneficio es que con esta solución NAC podemos integrar una solución MDM para la nueva tendencia de dispositivos BYOD, no solo de control de acceso, sino también de administración integral. ■

Pedro Serrera Cobos
Subdirector General de Sistemas de Información
FRATERNIDAD MUPRESPA

Fernando Paniagua
Director General
KNOW HOW MILLENIUM
fpaniagua@know-how1.com