



Naturener, la seguridad en una multinacional de energías renovables

INTRODUCCIÓN

Naturener es una multinacional dedicada a la producción de energías renovables, cuyos orígenes se encuentran en España, donde está ubicada su sede central. Actualmente, la compañía también está implantada en Estados Unidos y Canadá.

La actividad de la empresa se centró inicialmente en la producción de energía hidráulica y posteriormente amplió su negocio introduciéndose en la eólica y la solar fotovoltaica. Además, a lo largo de este año tienen previsto incorporar a su cartera la creación de una planta termosolar (energía solar térmica para borrar).

A mediados de 2006, Naturener puso en marcha un plan de expansión internacional que la llevó a abrir oficina en San Francisco (EE.UU.) y Calgary (Canadá) y a crear un parque de energía eólica en Montana. En la actualidad se está construyendo un segundo en la misma región.

En España la compañía cuenta a día de hoy con (cuatro centrales para borrar) catorce minicentrales hidráulicas y cuatro plantas fotovoltaicas repartidas por distintos puntos de su geografía.

EL DESAFÍO

Naturener cuenta con una plantilla de más de 100 empleados, cuya actividad obliga a una movilidad continua, por ello más del 80% de ellos utiliza ordenador portátil. Durante sus desplazamientos se conectan a los sistemas y aplicaciones de la compañía a través de conexiones inalámbricas, mientras que cuando están en la oficina lo hacen a través de cable o wireless. Según el IT Manager de Naturener, Antonio Martín, *“El gran handicap del departamento de TI de la compañía no reside en el número de usuarios, sino en su movilidad. Tienen que tener garantizada la seguridad de las conexiones allá donde estén. Ese problema es aún mayor en Estados Unidos y Canadá, donde los desplazamientos son mucho más frecuentes”*.

Otro de los factores que contribuyó al cambio fue el desfase horario existente entre la sede central, ubicada en España, y las situadas en Estados Unidos y Canadá. El departamento de TI de la compañía y el Centro de Datos están ubicados en España, por lo que era necesario tener la garantía de que todas las sedes estaban aseguradas y de que las oficinas norteamericanas pudieran trabajar sin que existiera una gran dependencia del departamento de TI.

Partiendo de esa premisa y de que la compañía cuenta con distintas ubicaciones situadas en diferentes puntos geográficos, Naturener necesitaba incrementar su seguridad perimetral y garantizar la seguridad de sus conexiones.

Hasta ese momento, la seguridad de la compañía estaba compuesta por routers y cortafuegos de otro fabricante, una estructura insuficiente desde el punto de vista de la seguridad y cuya administración resultaba excesivamente compleja. Además, sus capacidades de monitorización eran realmente escasas.

LA SOLUCIÓN DE WATCHGUARD

Tras una exploración del mercado, en la que se contemplaron las ofertas de WatchGuard e otros 2 fabricantes de UTM, Naturener se decidió por esta última. El elemento que más valoró la compañía a la hora de realizar la selección fueron las capacidades de monitorización. Así lo destaca Antonio Martín, *“es el gran elemento diferenciador de la oferta de WatchGuard, las capacidades de monitorización y la facilidad de configuración”*.

También contribuyó la especialización de WatchGuard en el negocio de UTM. Para Martín, este factor tiene importantes ventajas tanto desde el punto de vista de I+D, ya que todos sus esfuerzos y recursos se concentran en la misma línea, por lo que se obtienen productos más avanzados, y desde el soporte, puesto que el trato es mucho más claro y directo. *“Frente a otros fabricantes con una oferta más diversificada, WatchGuard ofrece la ventaja de centrar todos sus recursos en una línea de productos. Yo he trabajado con otros fabricantes y por eso*

valoró la alta especialización de WatchGuard”, manifiesta Martín. Por esa razón, otro de los motivos que llevaron a Naturener a elegir la oferta de WatchGuard fue la fiabilidad, junto con la facilidad de administración.

La implantación la realizó ALTAIR Networks, integrador en redes y comunicaciones que actúa como WSP Professional Partner de WatchGuard en España.



Detalles de la solución

A mediados de 2006, Naturener adquirió ocho equipos WatchGuard Firebox® X Core™ 750e UTM. Este dispositivo proporciona una fuerte protección desde el momento en el que se conecta. Potente y fácil de configurar y gestionar, inspecciona el flujo del tráfico de la red en múltiples capas y bloquea de forma proactiva los ataques de Denegación de Servicio (DoS) y de Denegación de Servicio Distribuido (DDoS), así como de virus, spam, gusanos, spyware, troyanos y amenazas ocultas sin confiar en los patrones de firmas para lograr una auténtica protección contra los ataques Día Cero.

Totalmente escalable, este *appliance* permite incrementar el rendimiento, la capacidad y las funciones de seguridad de las comunicaciones que la empresa necesita a medida que crece. Su alta escalabilidad lo convierte en el dispositivo UTM idóneo para medianas empresas que necesitan de una protección extrema y conectividad en remoto, así como una gestión centralizada de la red distribuida.

La implantación se ha realizado en varias fases. En la primera, el proyecto se centró en las oficinas centrales, donde había más urgencia por reforzar la seguridad y mejorar las conexiones. Se instaló una máquina en San Francisco y otra en Calgary. Al estar ubicado el centro de datos en Madrid, en esta oficina se desplegaron dos equipos en Alta Disponibilidad. De esta forma, en esta primera fase, las tres sedes centrales quedaron interconectadas entre sí.

En una segunda fase se instalaron cuatro equipos en las plantas de energía solar fotovoltaica, en las que se desplegaron cuatro cortafuegos. Además, en la oficina central de Madrid la compañía cuenta con IPS y GAV, ya que el Departamento de Informática tiene en proyecto sacar el tráfico de las plantas fotovoltaicas a través de la sede central de Madrid y securizarlo.

Los despliegues se realizaron de forma rápida, ya que los equipos estaban funcionando en un mes.

A lo largo de este año, Naturener abordará una tercera fase del proyecto, que contempla el refuerzo de la seguridad en las plantas hidráulicas y eólicas. La compañía conectará todos los parques a través de VPN, por lo que a finales de 2009 dispondrá de 6 unidades más hasta llegar a un total de 13 equipos.

El objetivo ahora es seguir comunicando sedes. Una vez que estén securizadas las plantas hidráulicas y eólicas, el tráfico pasará a través de la sede central de Madrid. Las oficinas de San Francisco y Canadá seguirán siendo independientes por las necesidades de ancho de banda.

Una vez finalizado el proyecto de conexión de todas las sedes, Naturener ahondará en el área de filtrado de contenidos. Según explica su responsable de TI, *“cuando tenga disponible toda la infraestructura y tenga la capacidad de saber lo que está ocurriendo en la red, profundizaremos en el área de filtrado de contenidos. En estos momentos se está efectuando en la Web y en los servidores ftp, pero en el resto no se realiza de forma exhaustiva”*.

Además, con el incremento de equipos y licencias, pasarán a utilizar WatchGuard® System Manager. *“Ahora mismo la gestión de equipos no está centralizada y creo que según vayamos conectando sedes, será una herramienta muy útil para tener un control sobre todo”*, ha señalado Martín. WatchGuard® System Manager permite gestionar los dispositivos Firebox de forma intuitiva y establecer un control granular sobre los equipos. Además, ayuda a reducir el tiempo de los despliegues, permite conocer en todo momento qué está sucediendo en las redes a través de la monitorización en tiempo real y tomar así medidas preventivas o correctivas. Otra de las ventajas que proporciona es poder actualizar las configuraciones de todas las máquinas de forma centralizada y a través de una sola gestión.

Otro de los proyectos que contempla la compañía para este año es pasar los equipos de Canadá y San Francisco a Alta Disponibilidad, para reforzar la seguridad y garantizar la conectividad de ambas sedes

BENEFICIOS

Los principales beneficios destacados por Naturener son la seguridad, la fiabilidad, el rendimiento de los dispositivos y la posibilidad de conectar de forma segura todas sus oficinas, así como que los empleados desplazados se puedan conectar sin problemas a través de VPNs. En ello han jugado un papel fundamental las capacidades de monitorización. Según Martín *“es una gran ventaja el hecho de que una vez que tienes los equipos instalados no tengas que estar controlándolos. Están totalmente desatendidos y es raro que tengas que*

realizar alguna parada, salvo para efectuar actualizaciones. Estos equipos, al estar en la punta de lanza de las comunicaciones, tienen que estar siempre operativos y con los modelos de WatchGuard ese objetivo se consigue”.

Otra de las ventajas apuntadas por la compañía es la sencillez de uso, *“una empresa puede tener un equipo en teoría buenísimo, pero si no tiene la información sobre lo que está ocurriendo en su red resulta muy complejo gestionarla y puede tener agujeros de seguridad que desconoce y estar descubierta. Es fundamental poder detectar de forma sencilla lo que está sucediendo en el sistema y aplicar la seguridad de manera global”*, ha manifestado Antonio Martín. Con los sistemas de WatchGuard, Naturener ha logrado combinar ambas cosas: disponer de una buena tecnología de seguridad y conocer en todo momento qué es lo que está ocurriendo en el sistema y en la red.

La compañía ha destacado el servicio LiveSecurity de WatchGuard, que proporciona soporte técnico con asistencia por parte de los expertos de la compañía en un tiempo de respuesta máximo de cuatro horas; alertas de seguridad sobre las amenazas existentes en la red y asesoramiento sobre cómo solventarlas; recursos de autoayuda y formación on-line a través de vídeos tutoriales, cursos de formación a través de Internet y herramientas específicas para responder a las preguntas de los usuarios. Además, este servicio amplía la garantía de un año del hardware e incluye la sustitución, en caso de fallo, de las máquinas. Para Martín *“este servicio es una baza muy importante porque nos facilita el trabajo. Te envían alertas de seguridad y te da la solución o te indica qué es lo que tienes que actualizar para hacerle frente. Es muy cómodo porque de otra manera tendrías que buscarlo en Internet, con la pérdida de tiempo que ello implica”*. Además, Martín subraya la excelencia del soporte local por parte del partner de WatchGuard, ya que cuando la compañía ha necesitado ayuda o ha requerido documentación técnica, la respuesta ha sido inmediata.

Naturener ha sufrido varios ataques contra sus sistemas. Los más comunes han sido los de Denegación de Servicio, contra los servidores o el correo electrónico. En este caso, el sistema de monitorización de Firebox X Core 750e ayuda a la compañía a detectarlos, neutralizarlos y aplicar las políticas de seguridad correspondientes.

Aunque Naturener no ha realizado un cálculo de costes para determinar el ahorro que supone la utilización de los UTM de WatchGuard, sí identifica importantes beneficios operativos. La restricción de los presupuestos de los departamentos de Informática provoca que los recursos humanos estén muy limitados, por lo que la compañía destaca el hecho de que los despliegues hayan resultado muy sencillos, así como la gestión de los equipos. La monitorización en tiempo real ha jugado una baza muy importante porque permite no tener que dedicar personal especializado para el control de los sistemas. *“Para nosotros es una ventaja que los equipos puedan salir configurados de la sede central y que cualquier persona los pueda implantar directamente en la oficina o parque de destino. Tener control sobre ellos y poder gestionarlos en remoto resulta fundamental para optimizar los recursos de cualquiera de las sedes”*, apunta Martín.

Para más información sobre las soluciones de seguridad de WatchGuard, visítenos en www.watchguard.com/international/es o contacte a su reseller.



ADDRESS:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:

www.watchguard.com

U.S. SALES:

1.800.734.9905

INTERNATIONAL SALES:

+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. Our Firebox X family of unified threat management (UTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. Our newest product line – the WatchGuard SSL – makes secure remote access easy and affordable, regardless of the size of your network. All products are backed by LiveSecurity® Service, a ground-breaking support and maintenance program. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. For more information, please visit www.watchguard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis. ©2009 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, Core, and Firebox are either trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part No. WGCE66640_082809