



NORBEGA

SEGURIDAD PERIMETRAL Y COMUNICACIONES

PERFIL DEL CLIENTE

Norbega, la planta de Coca Cola en Galdakao (Bizkaia) es una empresa con más de 55 años de vida, líder en el sector de bebidas refrescantes, que fabrica, comercializa y distribuye las bebidas carbonatadas, no carbonatadas, aguas y zumos de las marcas propiedad de The Coca-Cola Company.

Tiene presencia en Bizkaia, Gipuzkoa, Araba, Navarra, La Rioja, Cantabria y Burgos, ofreciendo servicios de preventa, distribución y reposición de sus más de 300 referencias, en diferentes formatos y sabores.

Norbega mantiene un serio compromiso con el medioambiente porque trata de incrementar la sostenibilidad y el ahorro energético de todos sus procesos, utilizando las más avanzadas técnicas para producir anualmente más de 210 millones de litros.



PRINCIPALES FASES DEL PROYECTO:

- *Sustitución del antiguo Firewall.*
- *Reconfiguración de la electrónica de red.*

SITUACIÓN PRESENTADA

Norbega partía de una situación en cuanto a seguridad y comunicaciones que quería mejorar. Por un lado, su firewall no proporcionaba un sistema de gestión unificado de amenazas, a nivel perimetral.

Por el otro, en el área de sistemas y comunicaciones, la empresa contaba con un entorno heterogéneo y multifabricante, con problemas de integración entre los diferentes dispositivos y con necesidades de renovación. Además, se unían dos necesidades más para obtener mayor eficiencia y productividad.

- ▶ Ampliar su infraestructura de red por la construcción de un nuevo Silo automático de palets.
- ▶ Separar los entornos de producción de los servicios corporativos.



SOLUCIÓN

Tras realizar los análisis, estudios y pruebas de concepto pertinentes en función de las necesidades del cliente, Inycom decidió que la solución pasaba por renovar todo el equipamiento de switching en su red LAN homogeneizándolo a HP.

Además, debido a que la nueva red iba a dar soporte a servicios que requerían de un alto grado de disponibilidad, se adoptó una solución de redundancia mediante IRF (Intelligent Resilient Framework) en la electrónica de red y de clusterización de UTM de Cyberoam a nivel de Firewall.

El proyecto ha llevado a cabo en dos fases:

- ▶ Sustitución del antiguo Firewall.
- ▶ Reconfiguración de la electrónica de red.



FASE I: SUSTITUCIÓN DEL ANTIGUO FIREWALL

- ▶ Configuración de alta disponibilidad:
 - A nivel de físico mediante la creación de un clúster con dos equipos UTM s minimizando el tiempo de parada en caso de fallo hardware en alguno de ellos.
 - A nivel de acceso internet mediante la configuración de líneas ADSL redundantes, de manera que ante la caída de una de ellas la conmutación es inmediata.
- ▶ Configuración de VPNs para comunicación con usuarios externos en oficinas remotas tanto a nivel nacional como internacional.
- ▶ Parametrización de seguridad perimetral a nivel de usuario:
 - Configuración de políticas de filtrado Web.
 - Configuración de antivirus perimetral
 - Configuración de filtrado de aplicación (programas que pueden utilizar los usuarios contra internet, como por ejemplo programas de descarga P2P, control de remoto, etc.).

FASE II: RENOVACIÓN/RECONFIGURACIÓN DE LA ELECTRÓNICA DE RED

- ▶ Configuración de pilas IRF para aportar alta disponibilidad y aumento del ancho de banda mediante la agregación de enlaces activo-activo tanto a nivel de servidores como en las conexiones entre switches bien sea por cobre o fibra según proceda.
- ▶ Reconfiguración la red actual de forma que el proceso productivo ha quedado segregado mediante redes virtuales que son propagadas tanto a través del entorno inalámbrico como a través de la red cableada según sea necesario.
- ▶ Securización de la red mediante la creación de listas de acceso (ACLs) pudiendo de esta forma controlar el flujo de tráfico entre equipos de manera que el tráfico es permitido o denegado hacia un destino en función de la red o IP origen.



BENEFICIOS

- ▶ Mayor optimización y conocimiento del uso de internet debido a:
 - Implementación de políticas a nivel de usuario.
 - Reporting resultante de la monitorización que ofrece Cyberoam.
- ▶ Aumento del rendimiento de la red permitiendo incrementar el ancho de banda.
- ▶ Alta disponibilidad permitiendo paradas de partes de la red sin perder el servicio gracias a la redundancia de equipamiento y a la distribución de los enlaces entre los diferentes equipos físicos.
- ▶ Facilidad de gestión:
 - Cada pila IRF queda gestionada bajo una única IP.
 - Todas las amenazas perimetrales quedan gestionadas bajo un único dispositivo.
- ▶ Reducción de costes de explotación de la red debido a la eliminación de complejos protocolos causantes de múltiples problemas.
- ▶ Disminución en la transmisión de tráfico mediante la segmentación de la red.
- ▶ Aumento de seguridad en la red gracias a la creación de listas de acceso aplicadas a las diferentes redes virtuales.

"Inycom fue nuestro socio tecnológico en este proyecto porque supo entender nuestras necesidades y darles respuesta de manera rápida y eficaz"

Javier Fernández.

Director de Sistemas de Información de Norbega

