

CASO PRÁCTICO

FABRICANTE DE HARDWARE Y SOFTWARE

Facilidad de gestión y ahorro

El fabricante, que opera en 76 países y cuenta con más de 30.000 empleados, ha desplegado la solución NAC de Cisco basándose en dispositivos NAC. Anteriormente contaba con un número de incidentes de seguridad que rozaba los 4.000 al mes.

La red interna del fabricante de hardware y software interconecta un parque de equipos totalmente heterogéneo, que incluye portátiles, estaciones de trabajo Unix y equipos con una gran variedad de sistemas operativos. La combinación de un amplio grupo de ingenieros con numerosos laboratorios repartidos por el mundo complica especialmente el soporte ya que la utilización de múltiples sistemas operativos hace inviable la construcción de una única imagen para todas las estaciones de trabajo.

Además, el modelo de negocio seguido por este fabricante supone la incorporación y adquisición de otras empresas y esto implica que deben tomarse medidas para evitar los riesgos asociados a conectar nuevas estaciones de trabajo a la red corporativa. La política de reducción de costes hace que se contrate a desarrolladores en remoto y estos muchas veces utilizan sistemas operativos vulnerables y máquinas cuya gestión se complica. Por último, la empresa está especialmente sensibilizada con el cumplimiento de las normativas de seguridad vigentes, como Sarbanes-Oxley.

El número de incidentes de seguridad (definidos como situaciones en las que un ordenador introduce algo no deseado en la red) fluctuaba entre 3.000 y 4.000 al mes. Para el cliente, el objetivo de la introducción de NAC en la red era asegurar la gestión adecuada de los usuarios independientemente del sistema operativo utilizado y definir niveles de acceso a la red de forma que un usuario acceda de forma automática a la sección de la red que le corresponda según su papel en la empresa.

Los tres factores claves que influyeron en la toma de decisión por la propuesta de Cisco fueron la madurez de los dispositivos NAC, su compatibilidad con la arquitectura única de la red del fabricante y la propuesta de evolución futura de la solución que se anticipa a las necesidades específicas de este cliente.

Los dispositivos NAC se despliegan en red con facilidad y pueden detectar, aislar y limpiar dispositivos vulnerables o infectados que tratan de acceder a la red. Estos son los productos NAC con mayor volumen de referencias, ya que Cisco dispone actualmente de más de 1.000 clientes que han instalado dispositivos NAC en sus redes. La solución es aplicable a un rango muy amplio de usuarios: desde 100 a más de 100.000 usuarios repartidos en múltiples ubicaciones de todo el mundo.

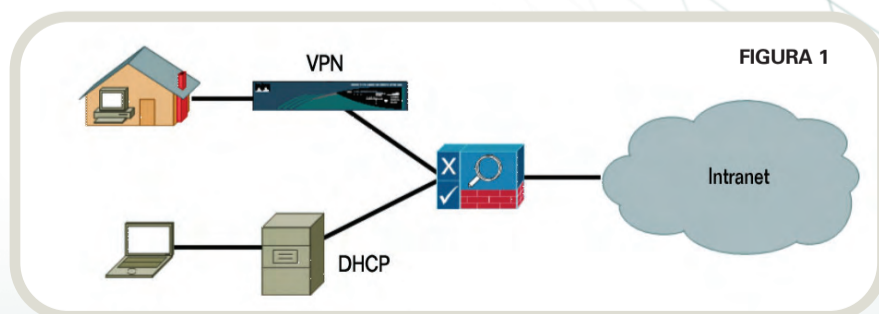
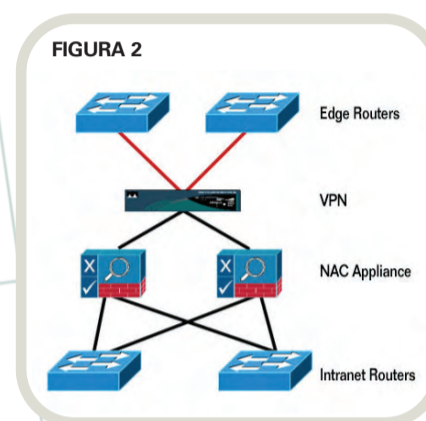


Figura 1. Despliegue típico para usuarios remotos.



La fase inicial del despliegue se dirigió a usuarios remotos que acceden a la red a través de VPNs (ver figura 1). Los usuarios remotos se autentican con el servidor de VPN que pasa las credenciales del usuario al servidor del dispositivo NAC para así proporcionar una solución de firma única. Las credenciales determinan el papel del usuario y en base al papel se comprueba si el dispositivo del usuario cumple con las políticas asociadas a este tipo de acceso. El sistema decide entonces, si se le permite el acceso, o si se le ubica en una red de cuarentena donde podrán realizarse las tareas de remedio necesarias antes repetir el intento de acceso.

El escenario para usuarios remotos hace uso de los dispositivos NAC en su modo de funcionamiento "en línea" en el cual todos los usuarios acceden a la red a través de los dispositivos NAC (ver figura 2).

Posteriormente, se extendió la solución a los usuarios de la red de área local y se aplicó el modo de funcionamiento "fuera de línea". Este tipo de despliegues suponen que los usuarios se comunican a través de los dispositivos NAC en las fases de comprobación de estado y remedio pero se les conmuta al núcleo de la red una vez que se ha comprobado su conformidad con la política de seguridad (ver figura 3).

Los usuarios de la red de área local deben arrancar el navegador para que se comprueben sus credenciales. Si el dispositivo no sigue las políticas corporativas se le ubica en una red virtual o VLAN donde el usuario puede acceder a todas las herramientas de remedio. Por ejemplo, si el dispositivo no dispone de un cortafuegos personal, el sistema le indica como puede instalarlo.

Según la estimación de este fabricante, el rango de costes asociado a cada incidente en la red va de 750 a 1.000 dólares con un número de incidentes mensuales de entre 3.000 y 4.000. Este número de incidentes va a reducirse significativamente una vez se haya completado el despliegue de los dispositivos NAC en verano del 2007 y así se está abordando como reducir el coste potencial de unos 4 millones de dólares al mes con lo que el tiempo de retorno de la inversión va a ser realmente corto. Una vez concluido el despliegue se habrá activado la solución NAC en 300 ubicaciones de 14 países.

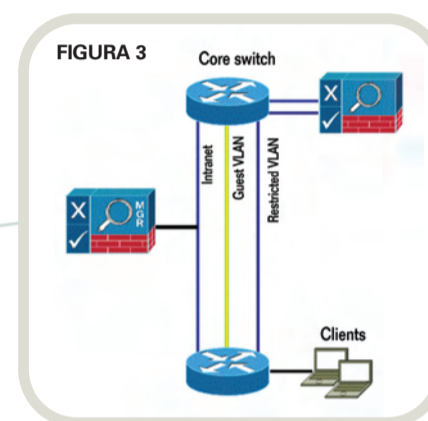


Figura 2. Despliegue "en línea" para usuarios remotos.
Figura 3. Despliegue "fuera de línea" para usuarios de la red de área local.