Gobierno de Navarra optimiza su servicio de salida a Internet con tecnología de Palo Alto Networks™

ANTECEDENTES

Como institución de carácter ejecutivo en que se organiza el autogobierno de la Comunidad Foral de Navarra, el Gobierno de Navarra es el órgano colegiado que, bajo la dirección de su Presidente, establece la política general y dirige la Administración de la Comunidad Foral de Navarra.

Con clara vocación de ofrecer un mejor servicio a sus ciudadanos, Gobierno de Navarra lleva tiempo centrado en un plan de modernización tecnológica, que incluye, el desarrollo de una Administración Electrónica, y la implantación de mejores soluciones para asegurar tanto la capa de interoperabilidad como la de seguridad y de infraestructuras tecnológicas y de comunicaciones. En este punto, Internet es de vital importancia, ya que a través de la red, el Gobierno presta servicios a los ciudadanos, permite el teletrabajo, y los trabajadores pueden realizar servicios básicos, como correo, navegación web, entre otros. En este sentido, un 20% del tráfico generado proviene de Internet.

OBJETIVO: CREACIÓN DE UNA POLÍTICA DE SEGURIDAD BASADA EN APLICACIÓN

Con más de 30.000 empleados, 12.500 puestos con acceso a Internet, el Gobierno de Navarra dispone de un conjunto de edificios dispersos por todo el territorio unidos entre sí por una red WAN de diversas tecnologías físicas, todas ellas regidas por el protocolo TCP/IP. Asimismo, cuenta con cerca de 100 sedes interconectadas con fibra óptica propia del Gobierno y cerca de 400 sedes remotas conectadas con líneas de menor velocidad.

Partiendo de dicha infraestructura, el Gobierno se enfrentaba a una problemática asociada a su estructura de red: poca efectividad de las soluciones instaladas para resolver problemas como filtrado por aplicaciones o cuellos de botella en su LAN, lo que repercutía en una falta de visibilidad, control y seguridad del tráfico que corría a través de la red. Dicha situación no conseguía solventarse con las soluciones instaladas de otros proveedores: cortafuegos de 1º nivel tipo Proxy de aplicación con bajo rendimiento y seguridad (primer nivel) y otros equipos de defensa perimetral (AV, spam, filtro web básico). De igual manera, el hecho de que, el número de páginas web con malware (troyanos, botnets, etcétera) a las que los usuarios intentan acceder consciente o inconscientemente se incrementase cada día, provocaba innumerables problemas de seguridad. A esto hay que unir una situación de interrupción de servicio severa, que afectó a la Administración seis años atrás.

Ante tales circunstancias, el objetivo del proyecto consistía, entre otras, en implementar un cortafuegos principal que permitiese gestionar la navegación web de los usuarios de un modo eficiente y seguro, detectando diferentes tipos de malware y permitiendo la identificación tanto de tipo de tráfico como de aplicación.

Gobierno de Navarra

ORGANIZACIÓN:
Gobierno de Navarra

SECTOR:
Organismo Gubernamental

PROYECTO:
Sustituir y optimizar la gestión de su perímetro de seguridad en lo que a acceso a datos se refiere.

SOLUCIÓN:
Dos firewall modelo PA-4020 con PANORAMA.

RESULTADOS:

- Menor complejidad en el diseño, menos puntos de fallo.
- Cumplimiento del esquema nacional de seguridad al emplear dos tecnologías diferentes de cortafuegos.
- No es necesario utilizar el cliente Proxy de Microsoft.
- Control granular de las aplicaciones utilizadas por los usuarios.
- Protección frente a una gran variedad de amenazas.
- Filtrado de URLs que permite establecer políticas de control sobre la actividad de navegación.
- Obtención de información en tiempo real sobre las actividades de los usuarios.
- Facilita el descubrimiento de equipos corporativos que generan tráfico malicioso ya que identifica el equipo, usuario y el malware.

paloalto NETWORKS
the network security company™

"Con anterioridad a la instalación de los firewall de nueva generación de Palo Alto Networks, no disponíamos de una visibilidad real de lo que se hacía y se utilizaba en nuestra organización. Ahora, gracias a sus funcionalidades, es posible realizar un control granular de las aplicaciones utilizadas por los usuarios; disponemos de una protección eficaz frente a una gran variedad de amenazas, así como, de información sobre los equipos corporativos que generan tráfico malicioso; y de opciones de filtrado de URLs, lo que permite establecer políticas de control sobre la actividad de navegación".

Eduardo Zariquiegui Aldave
Jefe de la Sección de Infraestructuras Tecnológicas del Gobierno de Navarra

En este sentido, el Gobierno de Navarra, a través de la Dirección General de Gobierno Abierto y Nuevas Tecnologías (DGGANT), optó por la solución de Palo Alto Networks PA-4020 (dos firewall en alta disponibilidad); y no sólo porque Palo Alto Networks ofreciera un producto innovador pero probado, sino también, por su facilidad de uso, potencia, así como, flexibilidad a la hora de poder implementar políticas de seguridad, sin olvidar su capacidad de integración en casi cualquier entorno. Para esta labor, contó con la colaboración de Nextel, partner que asesoró al Gobierno en la compra de la solución.

"Hasta ahora disponíamos de sistemas de seguridad basados en puertos y protocolos, con la suposición de que sólo la navegación utiliza los puertos 80 http y 443 http seguro. Sin embargo, las nuevas aplicaciones Web 2.0 son capaces de realizar muchas acciones por estos puertos, a lo que se suma una mayor demanda por parte de los usuarios del uso de este tipo de aplicaciones", explica Eduardo Zariquiegui Aldave, Jefe de la Sección de Infraestructuras Tecnológicas del Gobierno de Navarra. "Con anterioridad a la instalación de los firewall de nueva generación de Palo Alto Networks, no disponíamos de una visibilidad real de lo que se hacía y se utilizaba en nuestra organización. Ahora, gracias a sus funcionalidades, es posible realizar un control granular de las aplicaciones utilizadas por los usuarios; disponemos de una protección eficaz frente a una gran variedad de amenazas, así como, de información sobre los equipos corporativos que generan tráfico malicioso; y de opciones de filtrado de URLs, lo que permite establecer políticas de control sobre la actividad de navegación".

PROCESO DE IMPLANTACIÓN: UN ANTES Y UN DESPUÉS

Con el claro objetivo de consolidar su estructura de seguridad perimetral, Gobierno de Navarra inició este proyecto de implantación que, por sus características, tuvo una duración de siete meses, y se estructuró en dos fases, comenzando la primera de ellas en octubre de 2010.

Como principales medidas, durante el último trimestre del año, el equipo encargado de realizar la implantación del proyecto se centró en la realización de labores de análisis y diseño, de adecuación de la infraestructura de comunicaciones, y de la instalación y configuración de los dispositivos hardware de Palo Alto Networks en alta disponibilidad. Tras ello, se procedió a definir e implantar las políticas de control de filtrado Web para los entornos de Bibliotecas, Agencia Navarra de Emergencias y Servicio Navarro de Empleo; se llevó a cabo una prueba piloto en los sistemas; y se definió y planificó la migración en el resto de entornos.

Posteriormente, y a lo largo del primer cuatrimestre del 2011, se abordó la migración de todos los usuarios de Gobierno de Navarra –aproximadamente 15.000 cuentas de usuarios (Terminal y No Terminal), con unas políticas específicas de navegación–, y se procedió a realizar la formación sobre los nuevos firewall de nueva generación, así como, su difusión.

Por otro lado, y para cubrir las necesidades de navegación con o sin filtros de contenidos y para realizar una optima gestión de usuarios, se crearon también una serie de grupos específicos en el Directorio Activo.

"Referente al proyecto de implantación, no hubo complicaciones importantes, aunque sí se produjeron algunos inconvenientes relacionados con la gestión e integración de los sistemas SIEM, aspectos que se han solucionado con la versión 4 del producto y con la instalación de la consola de gestión centralizada Panorama en enero de 2012", matiza Eduardo Zariquiegui Aldave.

"Tras la instalación y configuración de la consola de gestión centralizada Panorama, prevemos incrementar estos beneficios con la implantación de funcionalidades adicionales, como Reporting y generación de informes, que nos permitirá definir cómo explotar la información sobre el servicio en general y sobre las actividades de los usuarios en particular."

Eduardo Zariquiegui Aldave
Jefe de la Sección de Infraestructuras Tecnológicas del Gobierno de Navarra

CONTROL SOBRE LA NAVEGACIÓN Y MAYOR VISIBILIDAD DE LA RED

Con los dispositivos de Palo Alto Networks funcionando en alta disponibilidad como cortafuegos principal para la navegación web, Gobierno de Navarra ha logrado, entre otras ventajas, una mayor visibilidad y control de aplicaciones y usuarios, una mejor prevención de amenazas, y una optimización de costes, ya que los equipos PA-4020 permiten gestionar la navegación web de los usuarios de un modo más eficiente y seguro, priorizando el ancho de banda.

"El concepto de gestión de aplicaciones por usuario que ofrece Palo Alto Networks, no es una gestión de puertos, protocolos o tráficos sino una gestión que combina la seguridad y el rendimiento con las necesidades del usuario", señala Eduardo Zariquiegui Aldave. "Tras la instalación y configuración de la consola de gestión centralizada Panorama, prevemos incrementar estos beneficios con la implantación de funcionalidades adicionales, como Reporting y generación de informes, que nos permitirá definir cómo explotar la información sobre el servicio en general y sobre las actividades de los usuarios en particular; y la integración con SIEM, de cara a una óptima gestión de logs e integración con Bitácora. La idea es acometer una mejora continúa de los procedimientos", concluye.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com