DISEÑO E IMPLEMENTACIÓN DE REDES DE ACCESO SEGURAS

Autor: Carlos Valderrábano Tornel
Director/es: Carlos Zamorano Pinal

I. INTRODUCCIÓN Y CONTEXTO

Este trabajo desarrolla el diseño e implementación de un proyecto para la asistencia al personal de las Fuerzas Armadas y las escuelas militares. Ante la demanda de un sector de Fuerzas Armadas, que reside dentro de las bases o acuartelamientos, de tener un acceso a internet fiable y seguro, se desarrolla un proyecto para cubrir esta necesidad. Por otro lado, con la entrada del espacio universitario en las escuelas militares, se ha visto necesario que dichos lugares tuviesen acceso a la red Iris de universidades como cualquier otro centro universitario.

Se pretende establecer un acceso a las dos redes, RAP e Iris, en cada localización con la misma infraestructura, pudiendo ampliarse en futuros desarrollos. También se plantea dar de baja, alta o ampliar los accesos según necesidad, de forma sencilla y ágil.

II. DESARROLLO Y RESULTADOS

La solución adoptada ha sido un despliegue distribuido, conectado a través de internet y red Iris, pero controlado de forma centralizada.

Para el proyecto se define un esquema en el que existen unos puntos de acceso (PA) a los que se conectan los usuarios con sus propios dispositivos. El tráfico de estos usuarios, al conectarse a la red, será capturado por un portal cautivo, donde se autenticarán o darán de alta para acceder a Internet o red Iris, de acuerdo con sus necesidades. Todos estos PA estarán conectados a un nodo central localizado en CESTIC, el cual gestionará los accesos, monitorizará y controlará los mismos, sirviendo de concentrador de servicios. Una vez autorizada la navegación, la infraestructura enrutará el tráfico hacia la conexión de internet, pero registrando toda la actividad y enviando los log al repositorio central en el servidor del nodo central en CESTIC.

El despliegue para realizar este proceso en cada nodo, sería una serie de PA conectados a unos switches de acceso, que se conectarían a un switch de agregación. Conectada al switch de agregación estará una controladora wifi, encargada de gestionar todos los puntos de acceso, sus potencias de emisión, canales, usuarios conectados, etc. Los PA

establecerán un túnel VPN con la controladora para cada red, encapsulando el tráfico de forma cifrada y separada de trafico de otras redes.

La salida del sistema ocurrirá mediante un router de la ISP y a través de un firewall NGF de capa 7, que protegerá la red de posibles amenazas y establecerá un túnel VPN con el firewall NGF del nodo central.

El nodo central será el encargado de recibir y enviar el tráfico de soporte y operaciones (tráfico de gestión) de los nodos. En el nodo central estarán alojados los servidores de autenticación, monitorización de la red, configuración de equipos y almacenamiento de log de forma centralizada.

Para ello, tendrá dos accesos a internet con ISP distintas. Cada conexión estará securizada por un firewall y otro de respaldo, de diferente marca que los integrados en los otros dispositivos. En el nodo central estarán también instaladas dos controladoras (principal y de respaldo) para recibir el tráfico de gestión de los diferentes nodos y controlar los equipos de todo el despliegue.

Todo este proyecto se desarrollará con equipos de Aruba, que tiene tanto el hardware como el software descrito con un precio asequible. Esta decisión de utilizar todo de una sola empresa agilizará y facilitará el despliegue de equipos, así como su gestión y control diario. También se ha tenido en cuenta el mantenimiento tanto del hardware como del software, que una empresa como Aruba podría proporcionar y mantener en el tiempo.

III. CONCLUSIONES

El sistema es altamente flexible al haberse estructurado en módulos (nodo central y nodos de despliegue), con equipos comerciales de Aruba. La idea de despliegue sería que, con un pequeño rack, en un acuartelamiento con acceso a internet con FTTH, se podría conectar con el nodo central en muy poco tiempo. Posteriormente se podría dar servicio a las zonas que se quisiese de forma rápida, con un despliegue de cable, switches y puntos de acceso que serían configurados desde nodo central rápidamente. En caso de cerrar un despliegue, el nodo central solo tendría que cortar la conectividad y el personal de la base o acuartelamiento recoger el nodo, los switches y AP.

Como se ha visto en el trabajo el coste del despliegue de un nodo sería de unos 10.000 euros más el cableado, switches y puntos de acceso. Esto quiere decir que la infraestructura tendría un coste asumible. También hay que tener en cuenta que aquellos nodos que se cerrasen podrían ser reutilizados sin ningún problema.

El sistema es altamente escalable ya que si en una base o acuartelamiento se quiere dotar de conectividad a una zona nueva solo se tendría que desplegar puntos de acceso en esa zona y configurarlos desde el nodo central. Por ello, se podría desplegar y recibir servicio desde el momento inicial en algunas zonas e ir ampliando sin que el resto del despliegue se resintiese.

Por último, dentro de la seguridad que se puede obtener de cualquier sistema conectado a internet, hay que decir que la centralización de la monitorización, el software de monitorización utilizado con configuraciones centrales y el hardware de última generación con una defensa en capas con dos firewalls de distinta marca y capacidad, dan una defensa en profundidad aceptable. Esto crea un binomio de seguridad-eficacia adecuado al servicio que se da.

Este trabajo se ha centrado en el despliegue de nodos en territorio nacional, con una gran similitud de accesos e infraestructuras. El futuro del sistema será la ampliación del mismo para dar servicio primero a zonas en el extranjero y zona de operaciones para posteriormente poder continuar con plataformas móviles como embarcaciones o puestos de mando móviles.

La principal diferencia que se puede ver entre estos nuevos despliegues y los presentados son los accesos a internet. Los accesos desde países extranjeros pasan a no ser controlados por la legislación española y no tendría las mismas características de protección.

Los que se desplegasen en zona de operaciones tendrían que acceder a internet a través de grandes terminales satélite que disminuyen el ancho de banda por lo que esto afectaría a las políticas de navegación y servicio, instaladas y controladas por el nodo central.

Por último, en el caso de embarcaciones donde el acceso a internet suele ser recibido por terminales satélite con un ancho de banda reducido, se tendrían mayores restricciones de navegación y servicios, teniendo que almacenar en local todos los productos posibles, quizás a través de una DMZ, que descargase ciertos contenidos en horarios de baja tasa de uso para luego dar servicio en local. Aquí entraría también un problema de licencias de contenidos que tendría que solucionarse.