

Establecimiento de conexiones a la Intranet del Ministerio

La comunicación con la Intranet del Ministerio se realiza mediante el establecimiento de conexiones "https" contra un dispositivo VPNSSL a través de un acceso a Internet. Este dispositivo ofrece una serie de recursos accesibles por los usuarios de la expedición, siempre que se cumplan unos requisitos de seguridad especificados en la plataforma de acceso.

Los recursos accesibles para esta expedición han sido:

1. Correo corporativo: en sus dos modalidades, cliente pesado y webmail.
2. Servidor de ficheros: dos formas de acceder a carpeta del servidor mediante interfaz propietaria, y otro a través del dispositivo Riverbed Steelhead Mobile, que además optimiza el uso del ancho de banda de las comunicaciones.

1. Correo Corporativo

El modo principal de acceso al correo corporativo ha sido a través del cliente pesado. Permite una mayor funcionalidad que el acceso a través del webmail, teniendo como contrapartida una configuración más compleja, y el paso por múltiples dispositivos, lo que implica un mayor número de puntos de fallo.

El principal inconveniente encontrado en el uso del cliente pesado ha sido una falta de disponibilidad de conexión, unas veces debida al escaso ancho de banda de subida en la conexión telefónica, y otras veces debido a problemas de conexión de la plataforma. Otro inconveniente es la configuración del cliente, ya que está personalizada para cada usuario, de manera que si precisan este servicio varios usuarios, hay que crear tantos perfiles como usuarios (ya no son válidos los scripts de configuración) e incluso es aconsejable la configuración de cuentas distintas de acceso al equipo, de tal manera que cada usuario mantenga su configuración.

Por otro lado, el uso del recurso webmail sólo permite el disponer de este recurso a usuarios que se encuentran en determinados servidores, aparte de no permitir el acceso a muchos tipos de aplicaciones desarrolladas bajo Lotus Notes. En determinadas ocasiones, su interfaz gráfica resulta poco funcional, sobre todo a la hora de leer los correos y volver a la bandeja de entrada, ya que vuelve a situarse al principio de la vista.

Esto hace que ambos modos de acceso resulten complementarios, sobre todo en situaciones donde la conectividad y el ancho de banda se encuentran limitados.

2. Servidor de ficheros

La finalidad del uso de este recurso, es la ejecución de operaciones básicas de copia, borrado y modificación de archivos, y creación, borrado y modificación de directorios en una carpeta de un servidor Windows de la Intranet del Ministerio, previa autenticación en el mismo. Estas operaciones nos han permitido, principalmente, el envío de los documentos para la actualización de la página web de la expedición.

Se han habilitado dos formas de acceder a este recurso:

- Carpeta servidor, mediante interfaz propietaria de conexión VPNSSL.
- Cliente pesado, permite acceso a sistema RiverBed en Intranet.

Carpeta Servidor

- Permite acceder a una carpeta de un servidor de ficheros.
- Establecimiento de una conexión contra el dispositivo VPNSSL. Éste va a establecer una nueva conexión contra el servidor de ficheros, utilizando el protocolo CIFS.
- Utilización interfaz propio, con desventaja de tener que adaptarse a él, y con la ventaja de que nos permite distinguir claramente el sistema en el que estamos realizando la operación.
- La negociación hasta que aparece la ventana de autenticación es bastante pesada.
- Una vez iniciada la carga, está condicionada por la velocidad de la línea hasta el dispositivo VPNSSL, ya que la conectividad entre VPNSSL y servidor es bastante rápida.
- Si se opera con más de un archivo, es un poco pesado, ya que hay que seleccionar uno a uno o crear un archivo que contenga todos los archivos. El tiempo desde que realiza la operación hasta que vuelve a aparecer la ventana actualizada es bastante elevado.
- En el caso de caída del sistema o línea de comunicación, existe el inconveniente de tener que volver a reenviar desde el principio el archivo sin poder aprovechar los datos ya enviados previamente.

Sistema Riverbed Steelhead Think fast™

- Permite acceder a un servidor de ficheros.
- Establecimiento de una conexión contra el dispositivo VPNSSL. Éste va a realizar conexiones contra el SMC (SteelHead Mobile Controller) y el SH (SteelHead) de RiverBed ubicados en la red corporativa.
- El cliente instalado en equipo remoto, descargará licencia de los equipos RiverBed y políticas de optimización, a través de la conexión contra el SMC. En función de estas políticas, si procede, enviará tráfico hacia dispositivo SH ubicado en red corporativa, que se encargará de transferir los datos al servidor destino.
- No precisa de interfaz adicional, ya que la conexión que realiza hacia red corporativa a través de dispositivo SH es completamente transparente para el usuario, dando la sensación de estar conectado directamente al servidor de ficheros.
- La negociación para autenticar el usuario en el servidor windows es muy pesada, incluso dando muchas veces error, sin ser posible la validación. A veces fue precisa la reiniciación del equipo cliente para poder validar en servidor destino.
- La transferencia de más de un archivo es muy cómoda, comparando con el método de carpeta en servidor.
- En el caso de caída de sistema o línea, el dispositivo tiene capacidad de saber qué datos ha transferido anteriormente, y evitar su retransmisión, siendo el ahorro en tiempo y datos bastante considerable.
- La mayoría de los datos transferidos fueron fotografías, cuyo formato presenta un índice de compresión elevado, siendo complicado alcanzar una compresión

mayor. Además, hay que tener en cuenta, que al ir todos los datos cifrados, el protocolo de optimización a nivel comunicaciones no mejora mucho.

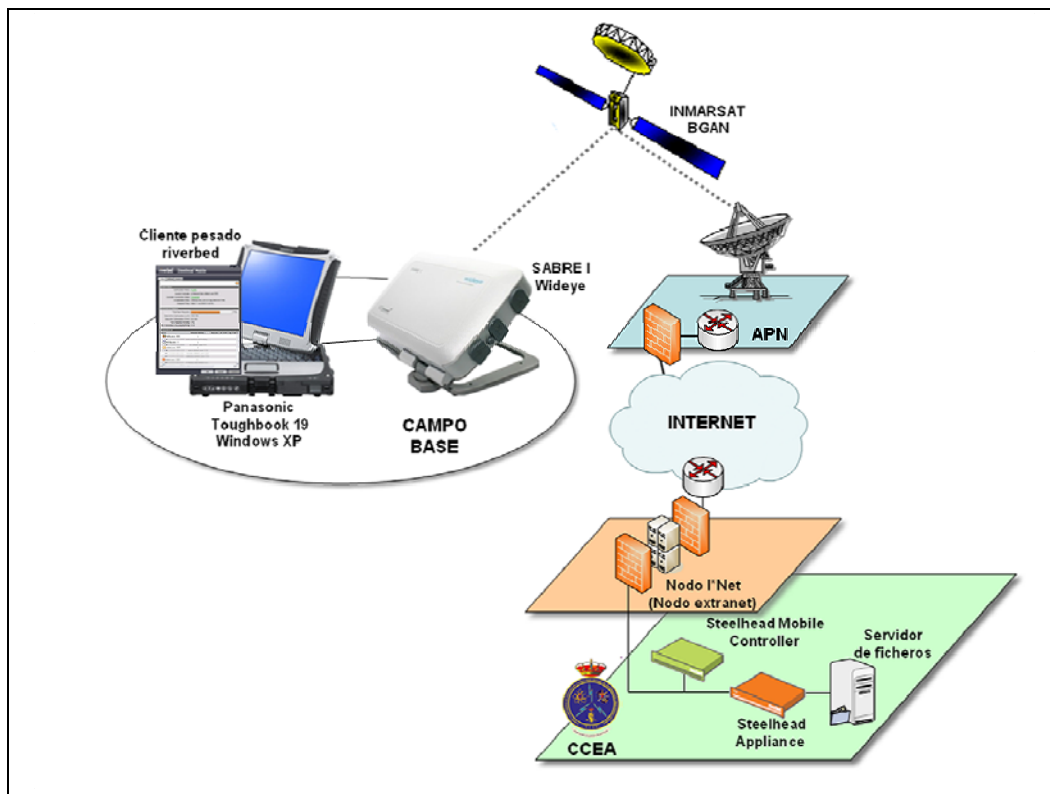


Figura 1. Acceso a la Intranet del MINISDEF

En la siguiente tabla se muestra un ejemplo de tiempos y datos transferidos con ambos sistemas:

Archivo	Tamaño	RiverBed	Carpeta compartida	Observaciones
Imagen01	1335 Kb	36"	1' 09"	
Imagen02	3929 Kb	1' 26"	2' 38"	
Imagen03	3795 Kb	1' 34"	2' 27"	
Imagen04	4080 Kb	1' 41"	2' 36"	
Imagen05	3987 Kb	1' 36"	2' 32"	
Operaciones Intermedias			4' 20"	Operación de seleccionar archivo
Totales	16.7 Mb	6' 59"	15' 42"	
Datos Transmisión Canal Subida		17,66 Mb	17,31 Mb	Registrado en dispositivo transmisión
Datos Transmisión Canal Bajada		389,18Kb	352,65 Kb	Registrado en dispositivo transmisión
Datos capturados interfaz físico		18,29 Mb	17,91 Mb	Realizada con "sniffer"

Según la tabla anterior el dispositivo Riverbed ha precisado de un 56% menos de tiempo para enviar los datos que utilizando el recurso de carpeta compartida. Sin embargo, los datos transferidos ha sido un 2% mayor por Riverbed.

En este ejemplo no hemos tenido en cuenta el tiempo de autenticación, que era superior mediante el acceso por dispositivo Riverbed que accediendo por recurso Carpeta Compartida.

Comparativa y conclusiones

El uso de ambos recursos ha permitido a la expedición la disponibilidad de un servidor dentro de la red corporativa para el envío y recepción de archivos de una forma segura.

El dispositivo RiverBed ofrece funcionalidades adicionales respecto al acceso a través del interfaz propio del dispositivo VPNSSL, entre las que cabe destacar la posibilidad de retransmitir un archivo sin necesidad de enviarlo de nuevo desde el principio, debido a la tecnología de optimización del producto.

Otra funcionalidad de RiverBed, es la de optimización en las distintas capas de comunicación. En este caso, la reducción de datos no ha sido muy alta, debido sobre todo al *encapsulamiento* de los datos necesario para el envío de la información de forma segura.

Continuando con RiverBed, la reducción del tiempo de transmisión ha sido elevada, si bien no se ha observado reducción de datos enviados. La optimización en tiempo ha sido penalizada por el tiempo de validación en el sistema mediante el protocolo CIFS.

Por otro lado, el uso de Carpeta Compartida, tiene la ventaja de no precisar software adicional en el cliente, y una administración menos compleja desde el punto de vista de la gestión de configuración de los sistemas.