ALTERNATIVA DE SOFTWARE LIBRE COMO SOLUCIÓN ÚNICA DE LOS SERVICIOS DE GESTIÓN DE RED ENTRE BARCO Y SEDE

Especialidad: Administración de redes y de sistemas operativos

Autor: Alberto Hernández Jiménez
Director: Miguel Martín Mateo
Diciembre de 2016

Este proyecto está bajo una licencia Reconocimiento-CompartirIgual (CC BY-SA 3.0) bajo la misma licencia 3.0 España de Creative Commons. Para ver una copia de esta licencia, puede visitar http://creativecommons.org/licenses/by-sa/3.0/es/

AGRADECIMIENTOS

Deseo expresar mi más sincero agradecimiento a mi amigo y compañero del dpto. TIC de la UTM-CSIC D. Juan Luis Ruiz Valderrama, por su inestimable colaboración en la fase de compresión de las posibilidades del software ZENTYAL y en el desarrollo de la parte de la VPN.

A la toda tripulación del B/O García del Cid, por su trabajo durante la instalación del sistema VSAT.

A mi amigo y compañero del dpto. de Oceanografía Física y Tecnología del ICM-CSIC D. Raúl Bardaji Benach, por su consejos para la redacción de la memoria.

A mi amigo, tutor externo y director de la UTM-CSIC D. Jordi Sorribas Cervantes, por la confianza depositada cada vez que propongo un proyecto.

A mis tutores de la UOC D. Mario Gómez Molina y D. Miguel Martín Mateo, por su ayuda durante este curso.

REFERENCIAS DE SIGLAS Y ABREVIATURAS

UTM:	Unidad de Tecnología Marina
CSIC:	Consejo Superior de Investigaciones Científicas
BAE:	Base Antártica Española
B/O:	Barco Oceanográfico
BIO:	Barco de Investigación Oceanográfica
VSAT:	Terminal de Apertura Muy Pequeñao Very Small Aperture Terminal
LAN:	Red Privada Virtual o Virtual Private Network
DNS:	Sistema de Nombres de Dominio o Domain Name System
DHCP:	Protocolo de Configuración Dinámica de Anfitrión o Dynamic Host Configuration Protocol
FEDER:	Fondos Europeos de Desarrollo Regional
VoIP:	Voz sobre protocolo IP
OPIS:	Organismos Públicos de Investigación
COCSABO:	Comisión de Coordinación y Seguimiento de las Actividades de los Buques Oceanográficos
TIC:	Tecnologías de la Información y de la Comunicación
Cortafuego+UTM:	Cortafuego de Gestión Unificada de Amenazas o Unified Threat Management Firewall
IPS:	Sistema de Prevención de Intrusiones o Intrusion Prevention System
PYMEs:	Pequeñas Y Medianas Empresas
GPL:	Licencia Pública General o General Public License
WAN:	Red de Área Amplia o Wide Area Network
CMIMA:	Centro Mediterráneo de Investigaciones Marinas y Ambientales
ICM:	Instituto de Ciencias del Mar
NMEA:	Asociación Electrónica Marina Nacional o National Marine Electronics Association
ACU:	Unidad de Control de Antena o Anntena Unit Control
BUC:	Supraconvertidor de Bloque o Block Up-Converte
RF:	Radiofrecuencia
LNB:	Bloque de Bajo Ruido o Low Noise Block
ITU:	Unión Internacional de Telecomunicaciones o International Telecommunication Union

INDICE

1. INTRODUCCIÓN **1**

2. ESTUDIO DE VIABILIDAD **2**
2.1. SITUACIÓN ACTUAL 2
2.2. REQUISITOS DEL SISTEMA 5
2.3. ALTERNATIVAS DE SOLUCIÓN 6
2.4. ELECCIÓN DE SOLUCIÓN 9

3. ANÁLISIS DEL SISTEMA **10**
3.1. DEFINICIÓN 10
3.2. REQUERIMIENTOS 14

4. **DISEÑO DEL SISTEMA** **16**
4.1. ARQUITECTURA 16
4.2. IDENTIFICACIÓN DE SUBSISTEMAS 18
4.3. REVISIÓN Y PRUEBAS 19

5. IMPLEMENTACIÓN DEL SISTEMA **21**
5.1. CORTAFUEGOS Y CALIDAD DE SERVICIO 22
5.2. VPN 24
5.3. SERVIDOR DNS 27
5.4. SERVIDOR DHCP 28

6. RESULTADOS **29**

7. CONCLUSIONES **40**

8. REFERENCIAS BIBLIOGRÁFICAS **41**

1. INTRODUCCIÓN

La Unidad de Tecnología Marina que es parte del Consejo Superior de Investigaciones Científicas (UTM-CSIC) tiene como objetivo fundamental proporcionar soporte a la política nacional de I+D+i en ciencia y tecnología marinas y polares. La UTM-CSIC se encarga de la gestión logística y tecnológica de cuatro plataformas de investigación: la Base Antártica Española (BAE) Juan Carlos I y tres Buque Oceanográficos: BIO Hespérides, B/O Sarmiento de Gamboa y B/O García del Cid.

El escenario de partida es que las plataformas tiene conexión de Terminal de Apertura Muy Pequeña (Very Small Aperture Terminal, VSAT) a Internet. Esto conlleva anchos de banda reducido (128-512 kbps) y latencias altas; por esto es necesario gestionar el ancho de banda para asegurar los servicios fundamentales (salida a Internet de servidores o usuarios VIP). Además las plataformas y la sede están interconectadas mediante una Red Privada Virtual (Virtual Private Network, VPN) para la sincronización de datos científicos en tiempo real y la administración remota de los servidores.

Para cubrir estas necesidades se utilizan enrutador CISCO serie 2800, que permiten la gestión del ancho de banda (cortafuegos y calidad de servicio) y crea una VPN entre las plataformas y la sede. Además cada plataformas forma una Red de Área Local (Local Area Network, LAN) por lo que hay que proporcionar servicios de gestión de red como son Servidor del Sistema de Nombres de Dominio (Domain Name System, DNS) y Servidor de Protocolo de Configuración Dinámica de Anfitrión (Dynamic Host Configuration Protocol, DHCP), para cubrir estas necesidades se utilizan servidores GNU/Linux.

El principal problema es la complejidad a la hora de administrar los servicios de red. Los enrutadores CISCO tienen una administración muy complicado (sólo vía comandos) que implica una formación especifica (ningún técnico del dpto. tiene) y no dispone de funcionalidades para filtrar por dirección de Control de Acceso al Medio (Media Access Control, MAC) para evitar la suplantación de IP de los equipos con salida a Internet; y garantizar ancho de banda para usuarios o servicios críticos. Además los servicios de gestión de red están repartidos en varios equipos.

La propuesta es buscar una alternativa de software libre como solución única de los servicios de gestión de red, cuyas características sean equivalentes o superiores a las actuales y con una administración sencilla. Para ello se quiere aprovechar la reciente instalación de sistema VSAT en el B/O García del Cid que era el único barco que carecía de Internet de cobertura global. Se implementará una solución que tendrá las siguientes características:

- Cortafuegos: dar salida a Internet a unos pocos equipos (filtrando por MAC).
- Calidad de Servicio: repartir el ancho de banda por servicios o usuarios.
- VPN: acceder a los equipos del barco y la sede como si fuera la misma red.
- DNS: dar servicio de resolución de nombres de dominio en la red.
- DHCP: dar servicio de configuración automática de parámetros en la red.

2. ESTUDIO DE VIABILIDAD

En el estudio de viabilidad se consideran los aspectos básicos de toda solución informática: el estado actual del sistema y su configuración; qué problemas se deben solucionar y cuáles son los requisitos; y cuáles son las restricciones al sistema. Para todo ello habrá las diferentes alternativas y finalmente elegir la mejor solución.

2.1. SITUACIÓN ACTUAL

La UTM-CSIC por mandato del Ministerio de Economía y Competitividad gestiona cuatro plataformas de investigación: la BAE Juan Carlos I y tres Buque Oceanográficos (BIO Hespérides, B/O Sarmiento de Gamboa y B/O García del Cid). Mediante un proyecto de cofinanciación (ver Figura 1) de Fondos Europeos de Desarrollo Regional (FEDER) se ha conseguido la adquisición de un sistema de comunicaciones VSAT mediante antena de banda Ku en el B/O García del Cid que era la única plataforma que carecía de este tipo de sistema (CSIC13-1E-1560).

Figura 1: Fondos FEDER

En B/O García del Cid (ver Figura 2) se realizaran campañas de investigación con el fin de obtener la máxima información de los ecosistemas marinos. Este buque está equipado con moderna tecnología para poder evaluar de forma precisa y fiable el estado de nuestros mares y sus recursos marinos. El objetivo principal es dotar al buque de comunicaciones de banda ancha necesarias para proporcionar información en tiempo real de las campañas científicas y mejorar todas aquellas actividades para alcanzar los objetivos de los distintos grupos de investigación que hacen uso del buque. Dado que el B/O García del Cid permanece en alta mar periodos de semanas sin entrar en puerto, es necesario dar un servicio de comunicaciones de correo electrónico, telefonía, telemedicina, video conferencia y navegación web; para que la comunidad científica desarrolle sus actividades en las condiciones mas favorables.

Figura 2: B/O García del Cid

De esta adquisición se beneficiarán los grupos de investigación de las Universidades y los Organismos Públicos de Investigación (OPIS), a los que la Comisión de Coordinación y Seguimiento de las Actividades de los Buques Oceanográficos (COCSABO) les concede días de barco ya sea a través del Plan Nacional o de otras iniciativas no financiadas por el Plan Nacional, conformar los grupos de investigación en cuyas campañas se utilizará este sistema.

La COCSABO realiza la planificación conjunta de los buques oceanográficos, en aras de favorecer una visión global y coordinada de la actividad de investigación oceanográfica, en beneficio de nuestra comunidad científica. Permitiendo una planificación coordinada de la actividad de estos buques oceanográficos gestionados por órganos distintos. Los criterios generales que se contemplarán para dar prioridad en la asignación de campañas tendrán en cuenta las obligaciones en el cumplimiento de lo que se establece en la Ley de Pesca y en el Programa Nacional de Datos Básicos que se deben abordar para la Unión Europea, así como el mantenimiento de las series históricas. Igualmente, tendrán en cuenta las prioridades que establezca el Plan Nacional, bien específicamente para unas determinadas campañas, o cuando se indique que los listados de proyectos vienen ya ordenados de acuerdo a su prioridad. Del mismo modo, en los criterios de prioridad se tendrán en cuenta aquellas campañas que sean consideradas como de carácter estratégico por la autoridad competente. Los criterios técnicos considerarán la antigüedad de la convocatoria del proyecto, la estacionalidad que suele afectar a campañas biológicas o ambientales y la economía en los tránsitos entre campañas. También tendrán en cuenta la conveniencia, o no, de que campañas sucesivas empleen el mismo equipamiento e igualmente, procurarán no acumular a un mismo investigador principal campañas sucesivas producidas por retrasos sobrevenidos. El grupo de trabajo, en la memoria que presentará junto con los borradores de los calendarios, deberá justificar a la COCSABO el uso y la forma como ha aplicado los anteriores criterios.

Igualmente, se beneficiarán las líneas de investigación de países extranjeros que por el proyecto EUROFLEETS [1] del cual la UTM-CSIC es miembro. Este proyecto ha permitido una alianza que favorece el desarrollo de proyectos conjuntos compartiendo los recursos de cada centro, tanto en lo referente al uso de barcos oceanográficos como de sus equipamientos científicos asociados

El proyecto EUROFLEETS (ver Figura 3) está subvencionado por la Unión Europea, y ha permitido crear una alianza de 24 centros europeos de investigación marina pertenecientes a 16 Estados Miembros. Esta sinergia permitirá mejorar la calidad de la investigación marina en Europa, conocer mejor los ambientes marinos así como todo el potencial que estos presentan, y dara pie en el futuro al desarrollo de nuevas ideas y proyectos de aplicación específica para cubrir las crecientes demandas de la sociedad.

Figura 3: EUROFLEETS

Las otras plataformas disponen desde hace años de sistema VSAT para conectarse a Internet. Este tipo de sistemas conlleva anchos de banda reducido (128-512 kbps) y latencias altas por lo que es necesario gestionar el ancho de banda para asegurar los servicios fundamentales. Además de las tareas de enrutado y cortafuego es necesario proporcionar otros servicios de red como son el Servidor DNS, el Servidor DHCP, la creación de VPN entre las plataformas y la sede, Servidor NTP, Servicio de NIS, Portal de Intranet, Servicio de Almacenamiento de archivos, etc. Para proporcionar estos servicios conviven soluciones propietarias (enrutador CISCO) y otras de software libre (servidores GNU/Linux para los servicios de DNS y DHCP).

Se utilizan enrutador CISCO serie 2800 para la gestión del ancho de banda (Enrutador, Cortafuegos y Calidad de Servicio) y crea la VPN. Para su configuración se accedía mediante protocolos o aplicaciones TCP/IP desde otra máquina que estuviera conectado en alguna de las redes del enrutador, en concreto utilizando "telnet" ya que esta sería no permitía administración web. Se necesita una formación especifica para trabajar con equipos CISCO, los conocimientos de técnicos del dpto. Tecnologías de la Información y de la Comunicación (TIC) de la UTM-CSIC son muy básicos y se limitan a modificar la configuración proporcionada por la empresa proveedora de los equipos como por ejemplo dar de al nuevos equipos con salida a Internet.

Aprovechando la nueva instalación en el B/O García del Cid se quiere implantar un nuevo sistema de administración de red con un Cortafuego de Gestión Unificada de Amenazas (Unified Threat Management, UTM) basado en software libre. Un Cortafuego+UTM (ver Figura 4) es básicamente un cortafuegos de red que engloban múltiples funcionalidades o servicios en una misma máquina de protección perimetral. Algunas de éstos servicios son:

- Cortafuegos: función de inspección de paquetes.
- VPN: para hacer túneles o redes privadas.
- Antispam: para evitar los correos no deseados o spam.
- Antiphishing y antispyware: evitar el robo de información.
- Filtrado de contenidos: para el bloqueo de sitios no permitidos.
- Antivirus: para evitar ataques con virus.
- Sistema de Prevención de Intrusiones (Intrusion Prevention System, IPS): para la detección y prevención de intrusos.
- Otros: DNS, DHCP, NTP, almacenamiento, etc.

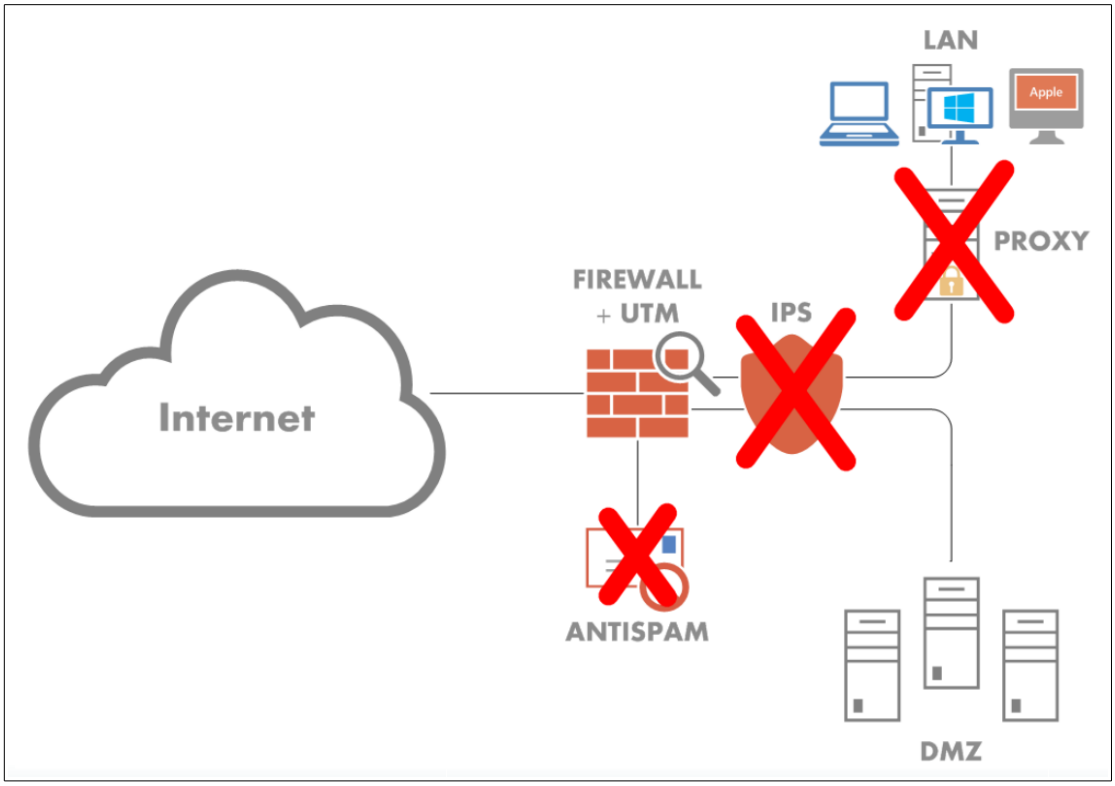

Figura 4: Cortafuegos+UTM

La mayor ventaja de esta solución es la simplicidad, porque funciones que se tenían dispersas en varios sistemas o proveedores ahora se pueden tener todos en una única solución. Permitiendo desempeñar a los técnico del dpto. TIC de la UTM-CISC su labor con mayor autonomía durante las campañas científicas.

2.2. REQUISITOS DEL SISTEMA

El nuevo sistema debe cubrir de manera equivalente o superior las prestaciones del sistema actual. Además se busca una simplificación en la administración por lo que es muy valorado que la herramienta elegida tenga una interfaz de configuración amigable. Además ante los escasos recursos económicos disponibles las solución debe tener el menor coste posible por lo que se buscará una solución software para evitar la compra de hardware.

La alternativa de Cortafuegos+UTM de software libre como solución única de los servicios de gestión de red, debe tener al menos las siguientes características:

- Cortafuegos: control de los equipos con salida a Internet con filtrando por MAC.
- Calidad de Servicio: gestión de servicios o usuarios.
- VPN: acceso a los equipos del barco y la sede como si fuera la misma red.
- DNS: servicio de resolución de nombres de dominio en la red.
- DHCP: servicio de configuración automática de parámetros en la red.

2.3. ALTERNATIVAS DE SOLUCIÓN

Opción 1: ZENTYAL

Es una solución de código abierto GNU/Linux de correo electrónico y groupware, compatible de forma nativa con Microsoft Outlook. Entre las características técnicas (ver Figura 5) [2] incluye gran número de componentes para Infraestructura y Gestión de Red:

- Servidor DNS.
- Servidor DHCP.
- Servidor NTP.
- Autoridad de certificado.
- Servidor y cliente VPN.
- Interfaces estáticos y DHCP.
- Objetos y servicios.
- Filtrado de paquetes.
- Redireccionamiento de puertos.

Figura 5: Características técnicas de ZENTYAL

La distribución de "Zentyal Server" para Pequeñas Y Medianas Empresas (PYMEs) tiene una edición de desarrollo que puede descargarse de forma gratuita licenciado bajo los términos de la Licencia Pública General (General Public License; GPL) de GNU y se ejecuta sobre Ubuntu GNU/Linux. El equipo de desarrollo de ZENTYAL ofrece todas las tecnologías y servicios relacionados con la misma, proporcionando un conjunto completo de implementación, soporte y servicios gestionados por la Red de "Partners Global Zentyal" [3].

Opción 2: ENDIAN

Es una distribución GNU/Linux especializada en cortafuegos, enrutamiento y gestión unificada de amenazas. Originalmente ENDIAN está basado en IPCop. El producto está disponible como

software libre (versión comercial con servicios de apoyo garantizados) o como un dispositivo de hardware (incluyendo servicios de apoyo). Además hay una versión libre "Endian Firewall Comunity" diseñado para su instalación en su propio hardware con licencia GPL GNU y por lo tanto es un software de código abierto que se puede descargar de forma gratuita. Esta versión no incluye soporte ni todas las características de la versión comercial. Entre las características técnicas (ver Figura 6) [4] incluye los siguiente paquetes:

- Cortafuegos bidireccional
- VPN con OpenVPN e IPSec.
- Antivirus, antispam y IPS.
- Multi-Red de Área Amplia (Wide Area Network, WAN).
- Calidad de servicio.
- Monitorización.
- Configuración a través de interfaz Web HTTPS.
- Servidor DHCP.
- Servidor NTP.

endian Products Partners Support Company Community

General	EFW Community	Virtual Appliance	Software Appliance	Hardware Appliance
	endian firewall community			
Network Security	Yes	Yes	Yes	Yes
Application Control	No	Yes	Yes	Yes
Advanced Content Security	No	Yes	Yes	Yes
CYREN URL Filter	No	Yes	Yes	Yes
CYREN Anti-spam	No	Yes	Yes	Yes
Panda Anti-virus	No	Yes	Yes	Yes
Web Security	Yes	Yes	Yes	Yes
URL Filter	1.8 million URLs	150 million URLs	150 million URLs	150 million URLs
Mail Security	Yes	Yes	Yes	Yes
Anti-spam	Single Engine	Dual Engine	Dual Engine	Dual Engine
Quarantine Management	No	Yes	Yes	Yes
Anti-virus	Yes	Yes	Yes	Yes
Anti-virus	Single Engine	Dual Engine	Dual Engine	Dual Engine
Virus disinfection	No	Yes	Yes	Yes
User Authentication	Yes	Yes	Yes	Yes

Figura 6: Comparativa de características técnicas de ENDIAN

Opción 3: OPNSENSE

Es un código abierto basado en FreeBSD para implementar una plataforma cortafuegos y de enrutamiento. Surgió como una bifurcación de pfSense y m0n0wall donde se puso énfasis en la seguridad y la calidad del código. La empresa Deciso ofrece hardware con el software preinstalado y también es posible instalarlo en una máquina propia, el software esta licenciado

bajo cualquiera de las "Open Source Initiative". Entre las características técnicas (ver Figura 7) [5] se incluye:

- Moldeado de trafico.
- Proxy cache transparente con el apoyo de lista negra.
- Portal cautivo.
- VPN con OpenVPN y IPsec.
- IPS.
- Herramienta gráfica de control y monitorización.
- Servidor DNS.
- Servidor DHCP.

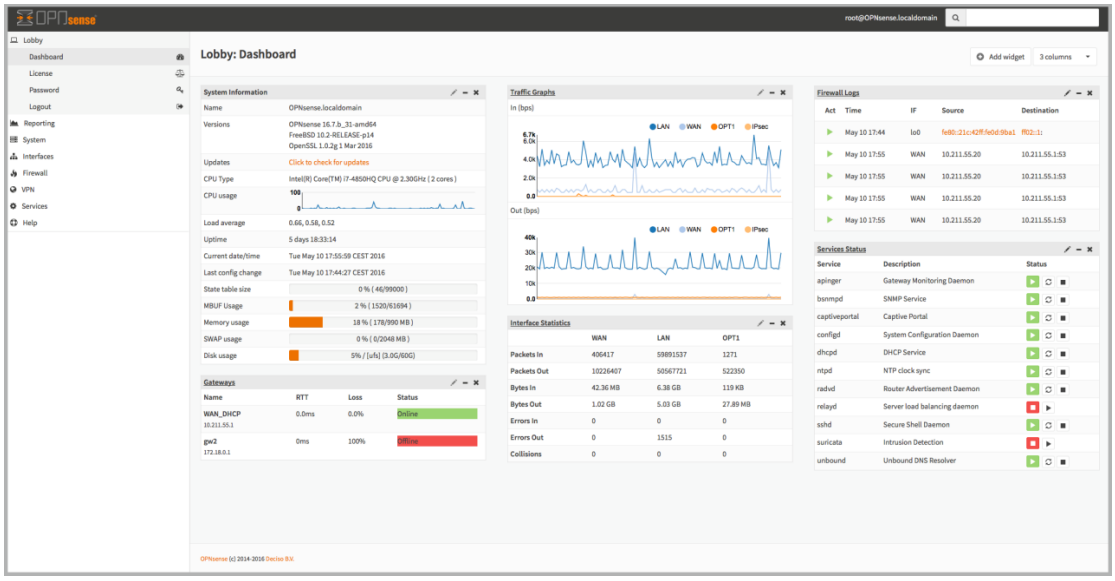

Figura 7: Interfaz gráfica de OPNSENSE

Opción 4: CLEAROS

Es una distribución GNU/Linux basada en CentOS y Red Hat, este sistema operativo implementa un sistema de gestión de red y puerta de enlace. Existen varias versiones del software para hogares, PYMEs y entornos distribuidos; además hay una versión libre "ClearOS Community" para su instalación en su propio hardware con licencia GPL GNU. Entre las características técnicas (ver Figura 8) [6] se incluye:

- Cortafuegos bidireccional.
- VPN con IPSec.
- Antivirus, antispam y IPS.
- Multi-WAN.
- Servidor proxy web.
- Calidad de servicio.
- Monitorización.
- Servidor DHCP.
- Servidor DNS.
- Servidor NTP.

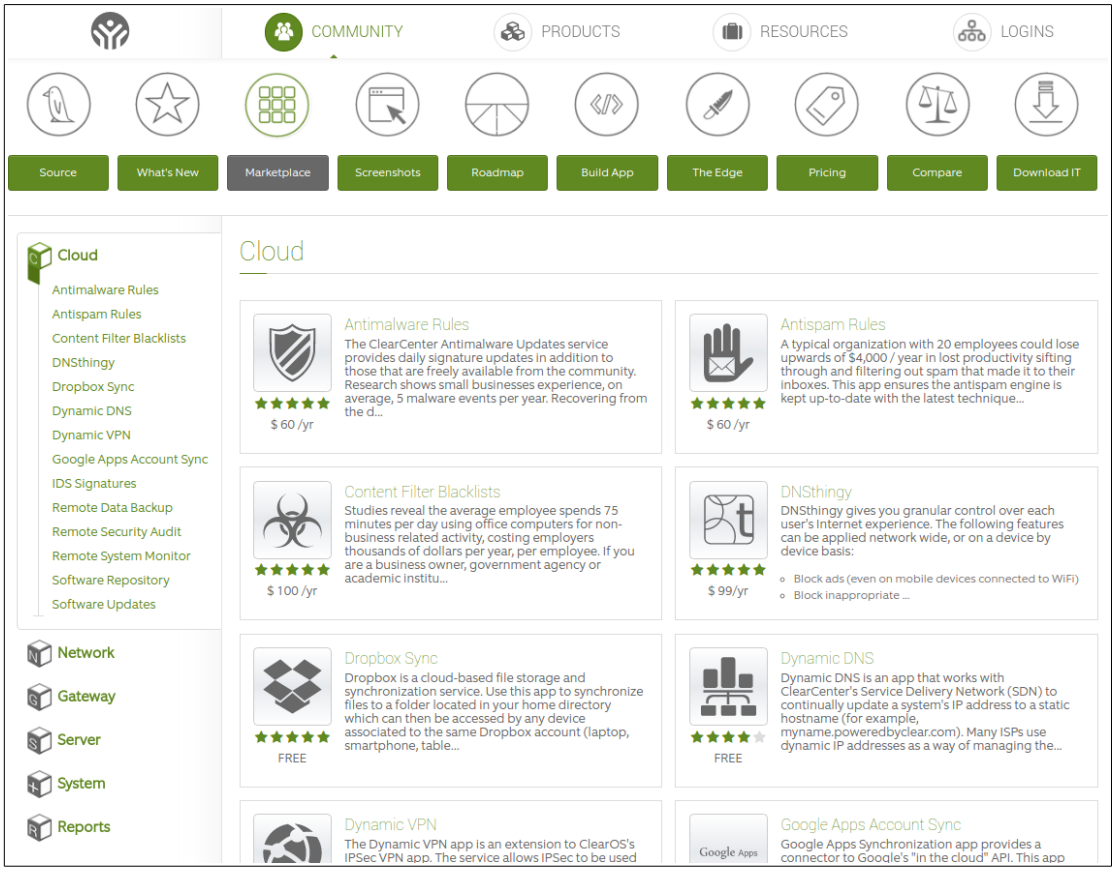

Figura 8: Características técnicas de CLEAROS

2.4. ELECCIÓN DE SOLUCIÓN

Varias de las alternativas encontradas tienen objetivamente las características necesarias para funcionar como solución única de los servicios de gestión de red. Por lo que la elección final se va a basar en criterios más subjetivos.

La UTM-CSIC está adscrita al Centro Mediterráneo de Investigaciones Marinas y Ambientales (CMIMA) del Área de Recursos Naturales de la Agencia Estatal CSIC, al igual que el Instituto de Ciencias del Mar (ICM). En el dpto de Oceanografía Física y Tecnológica del ICM hay un compañero que se ha decidido por ZENTYAL para la gestión de su red. Este compañero me ha proporcionado contactos y documentación de un curso que realizó, esto será de gran utilidad a la hora de llevar a cabo el proyecto. Además en "Zentyal Community" se puede encontrar todo lo referente al proyecto de software libre.

3. ANÁLISIS DEL SISTEMA

En en análisis del sistema es necesario realizar una especificación detallada de la solución con el objetivo de preparar su diseño y su arquitectura. Es muy importante la interacción con los usuarios, en este caso la tripulación, los técnico y los científicos embarcados, para descartar la posibilidad de errores.

3.1. DEFINICIÓN

Se va a describir el sistema VSAT que se adquirió mediante el concurso público del proyecto de cofinanciación FEDER para la adquisición de un sistema de comunicaciones VSAT mediante antena de banda Ku en el B/O García del Cid. Este concurso fue adjudico a la empresa ERZIA que ofertó la el sistema Intellian v80G (ver Figura 9) [7].

Figura 9: Intellian v80G

Este sistema tiene las siguientes características:

- Funcionamiento sin girocompás que permite al sistema adquirir y bloquear a un satélite sin necesidad de una entrada separada del del buque girocompás. Si un dispositivo de partida está disponible, puede ser conectado a través de una interfaz de la Asociación Electrónica Marina Nacional (National Marine Electronics Association, NMEA).
- El diseño simplificado que permite a los usuarios instalar y configurar el sistema sin la necesidad de un ingeniero experto. Del mismo modo, el programa almacenado de la v80G puede actualizarse con una unidad USB externa o por conexión inalámbrica a Internet. La lámpara led dentro de la base del domo proporciona un entorno de mantenimiento más seguro y brillante.
- El nuevo puerto "Intellian LAN" en el Unidad de Control de Antena (Anntena Unit Control, ACU) proporciona una conectividad de red a otros sistemas Intellian que

permitirán la supervisión y el control de todos los dispositivos conectados en la misma red.

- La antena es compatible con módems de una serie de estándares abiertos que permiten la conectividad de red por satélite.
- Gestión remota mediante el programa APTUS que permite acceder, vigilar y controlar el sistema desde desde cualquier lugar del mundo. Además, las actividades de mantenimiento de rutina pueden ser automatizados como son las actualizaciones del programa almacenado, ajuste de parámetros, el seguimiento y el diagnóstico del sistema, incluyendo la función de historial de registro de eventos.
- Combinación de la potencia del Supraconvertidor de Bloque (Block Up-Converte, BUC) y la señal trasmitida, el sistema ofrece una solución de un solo cable que suministra energía de 48 V DC a través de un cable de Radiofrecuencia (RF) que facilita la instalación.
- La v80G presenta el primer módulo de Bloque de Bajo Ruido (Low Noise Block, LNB) de banda Ku capaz de recibir una gama completa de frecuencias de cualquier satélite VSAT.
- Amplio ángulo de elevación, el pedestal está diseñado para latitudes extremadamente bajas o altas como la península escandinava o las regiones ecuatoriales.

El equipamiento exterior (Antena, BUC y LNB) se ubicó en el mástil donde estaba la antigua antena del FURUNO (ver Figura 10) que fue retirado y dado de baja. Estos equipos vienen integrados dentro del domo que proporciona Intellian.

Figura 10: Instalación de equipamiento exterior

Mientras que el equipamiento interior (ACU, Módem y Cortafuegos+UTM) se instaló en un armario del puente (ver Figura 11) habilitado para tal efecto. Estos equipos se conecta entre ellos siguiendo el esquema de más abajo. El equipamiento exterior e interior se conecta mediante cable RF de categoría LMR400 (ver Figura 12).

Figura 11: Instalación del equipamiento interior

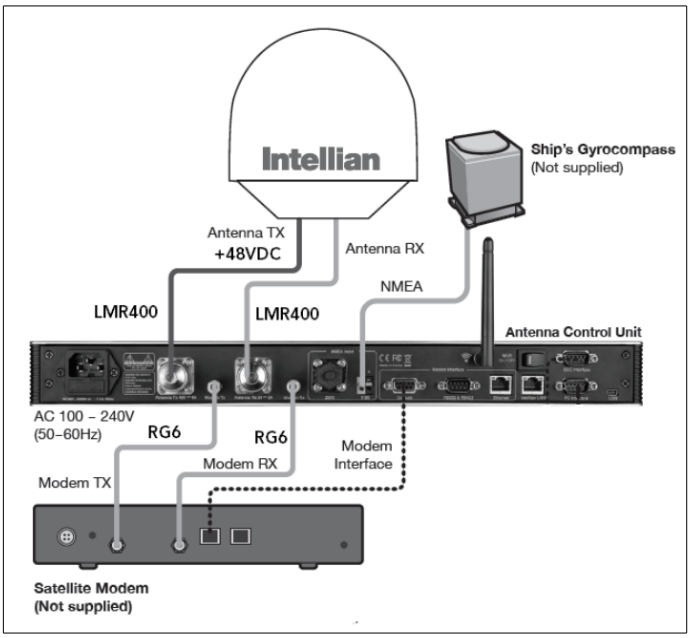

Figura 12: Diagrama básico RF

El cortafuego no aparece en el esquema anterior es conectado mediante un cable Ethernet al módem en el puerto WAN1. Este además se conecta un enrutador 4G en el puerto WAN2 y a un conmutador de la red local del barco en el puerto LAN.

Se ha aprovechado el proyecto para recopilar información de red de todos los equipos que componen la red local del barco como son la MAC, la IP y el sistema operativo. Además como se cambiará todas las IP del actual direccionamiento 193.145.218.0/24 al nuevo direccionamiento 192.168.4.0/24 (ver Tabla 1). Este cambio de direccionamiento va a homogeneizar todas las plataformas que gestiona la UTM-CSIC quedando de la siguiente manera:

- BIO Hespérides: 192.168.1.0
- BAE Juan Carlos I: 192.168.2.0
- B/O Sarmiento de Gamboa: 192.168.3.0
- B/O García del Cid: 192.168.4.0

NOMBRE	MAC	IP VIEJA	IP NUEVA	OS
ZENTYAL	00:1E:68:49:C8:2B	LAN	192.168.4.1	Zentyal
		WAN1-VSAT	216.130.38.113	
		WAN2-Router4G	192.168.40.1	
MODEM-VSAT	--	--	216.130.38.114	iDirect
ROUTER4G-USUARIOS	--	193.145.218..114	192.168.40.2	ZTE
ROUTER4G-INVITADOS	--	193.145.218..113	192.168.4.2	ZTE
METEO/TSS	00:0B:AB:2B:A0:D0	193.145.218.55	192.168.4.21	Windows XP
POSICION	00:0B:AB:2B:B9:A4	193.145.218.54	192.168.4.22	Windows XP
SADO	00:0B:AB:27:97:1C	193.145.218.53	192.168.4.20	CentOS 6.2
PC-LABORATORIO	00:18:FE:68:6C:68	193.145.218.11	192.168.4.30	Windows XP
PC-COMEDOR	00:18:FE:FF:7C:94	193.145.218.10	192.168.4.31	Windows XP
PC-PUENTE	D4:3D:7E:41:B2:69	193.145.218..150	192.168.4.32	Windows 8
PC-MAXSEA	D0:50:99:53:BD:31	193.145.218..100	192.168.4.33	Windows 7
PC-JEFEMAQUINAS	90:FB:A6:00:82:9D	DHCP	192.168.4.34	Windows XP
IMPRESORA-LABORATORIO	00:1C:C4:50:C7:18	194.145.218..103	192.168.4.40	HP
IMPRESORA-PUENTE	--	--	192.168.4.41	HP
AP-COMEDOR	00:1C:10:67:8A:73	193.145.218..121	192.168.4.45	LINKSYS
AP-TRIPULACION	00:1E:E5:F8:9A:4A	193.145.218..122	192.168.4.46	LINKSYS
AP-WHATSAPP	10:FE:ED:F5:03:62	Red Barco	192.168.4.47	TP-LINK
	--	Red WhatsApp	192.168.44.47	
REPETIDOR-WHATSAPP	E8:94:F6:E5:54:F5	Red WhatsApp	192.168.44.48	TP-LINK
CTD1	00:0B:AB:38:D2:C9	DHCP	192.168.4.61	Windows XP
CTD2	00:0B:AB:38:D2:16	DHCP	192.168.4.62	Windows XP
CTD3	00:0B:AB:19:48:63	DHCP	192.168.4.63	Windows XP
EK500	--	Local 193.145.218..99	192.168.4.80	Embeded
		Remota 193.145.218..22	192.168.4.81	
TRACKLINK USBL	00:0B:AB0E:CE:4A	193.145.218..22	192.168.4.81	Windows XP
EA60	--	--	192.168.4.82	--
DOPPLER	4C:72:B9:98:F7:10	DHCP	192.168.4.83	Windows XP
SCANMAR-MARPORT	--	--	192.168.4.84	--
MULTIHAZ	4C:72:B9:98:F8:09	195.0.0.10	192.168.4.85	Windows XP
F180	--	--	192.168.4.86	--
MOXA-GPS	--	--	192.168.4.90	--
DHCP	--	--	192.168.4.100-199	--

Tabla 1: Información de red del B/O García del Cid

3.2. REQUERIMIENTOS

Como se ha comentado en el Estudio de viabilidad la solución de código abierto elegida para implementar un Cortafuegos+UTM es ZENTYAL. Las características que ofrecen los componentes para Infraestructura y Gestión de Red cubren los requerimientos del sistema a implementar: Cortafuegos, Calidad de Servicio, VPN, Servidor DNS y Servidor DHCP.

Cortafuegos

Lo fundamental del cortafuegos es que permita salir a Internet sólo a unas pocas máquinas. Esto hay que hacerlo porque el ancho de banda es tan reducido que si todas tuvieran salida la navegación sería extremadamente lenta e incluso en alguno cosas imposible. La experiencia en otras plataformas hace que para un ancho de banda en 128-256 Kbps que va a tener el B/O García del Cid se limite a 5 máquinas con salida a Internet que serán las siguientes:

- PC-Cientificos: PC de usuario situado en el laboratorio para uso de los científicos embarcados tanto para uso de trabajo como de ocio.
- PC-Puente: situado en el puente de gobierno, lo usarán los oficiales de puente (capitán, primer oficial y segundo oficial) en su actividad de gestión del barco (gestionar el personal, las entradas/salidas a puerto y la logística; para comunicarse con el exterior; para planificar la campaña; etc.)
- PC-Maquinas: situado en el camarote del jefe de máquinas, lo usará el jefe de máquinas en su actividad de gestión de la máquina (mantenimiento de equipos mecánicos, eléctricos e hidráulicos; gestionar la logística; para comunicarse con el exterior; etc.)
- PC-Maxsea: situado en el puente de gobierno, lo usarán de los oficiales de puente (capitán, primer oficial y segundo oficial) exclusivamente para el uso del programa de navegación MAXSEA.
- PC-Tripulacion: PC de usuario situado en la sala de ocio para uso de la tripulación tanto para uso de trabajo como de ocio.

Además de estos PC con salida a Internet, todos los móviles tendrá disponible el uso de la aplicación WhatsApp.

Calidad de Servicios

En la calidad de servicio se quiere garantizar que la navegación de los PC con salida a Internet sea de calidad teniendo en cuenta las limitaciones intrínsecas de sistema VSAT como el reducido ancho de banda y las altas latencias. Para ello hay que garantizar que el servicio de WhatsApp no va a ocupar todo el ancho de banda.

VPN

Establecer una VPN entre el barco y la sede central de la UTM-CSIC ubicada en el CMIMA de Barcelona. Por tanto será necesario implementar con ZENTYAL un Cortafuegos+UTM en cada extremo del túnel. Se establecerá un túnel entre ambos ZENTYAL para que cuando desde el barco (rango 192.168.4.0/24) se quiera acceder al CMIMA (rango 161.111.136.0/22) el ZENTYAL del barco que es la puerta de enlace (192.168.4.1) encamine las peticiones por dicho túnel, y viceversa.

Servidor DNS

El servidor DNS tendrá que resolver los nombre de todos los equipos fijos que están conectados a la red local del barco. Como se ha comentado antes se va aprovechar para cambiar el direccionamiento del actual 193.145.218.0/24 al nuevo 192.168.4.0/24. Además se va a hacer una reorganización poniendo los equipos del mismo ámbito de manera consecutiva y reservando rangos de direcciones IP a otros departamentos, de esta manera en caso de añadir nuevos equipos se podrá mantener el orden.

- Equipos de conexión (cortafuegos y enrutadores 4G): 192.168.4.1-19.
- Servidores: 192.168.4.20-29.
- PC con Internet: 192.168.4.30-39.
- Impresoras: 192.168.4.40-44.
- Equipos de red (conmutadores y puntos de acceso): 192.168.4.45-49.
- Departamento de Electrónica: 192.168.4.60-79.
- Departamento de Acústica: 192.168.4.80-99.
- DHCP: 192.168.4.100-199.
- Reservado: 192.168.4.200-255.

Servidor DHCP

Como se muestra en el apartado anterior el servidor DHCP dará a los equipos configurados con DHCP automático una dirección IP entre 192.168.4.100-199. Para evitar suplantación de direcciones IP de los equipos con salida a Internet dará esas IP filtrando por MAC (ver Tabla 2):

NOMBRE	MAC	IP
PC-LABORATORIO	00:18:FE:68:6C:68	192.168.4.30
PC-COMEDOR	00:18:FE:FF:7C:94	192.168.4.31
PC-PUENTE	D4:3D:7E:41:B2:69	192.168.4.32
PC-MAXSEA	D0:50:99:53:BD:31	192.168.4.33
PC-JEFEMAQUINAS	90:FB:A6:00:82:9D	192.168.4.34

Tabla 2: PC con salida a Internet

4. DISEÑO DEL SISTEMA

En la fase de diseño del sistema consiste en obtener de forma concreta los elementos definidos en la etapa de análisis del sistema. Hay que tener en cuenta que en esta etapa se inicia el proceso de selección de elementos, el desarrollo y la integración; así como definir el entorno de pruebas para comprobar el buen funcionamiento del sistema.

4.1. ARQUITECTURA

La arquitectura del sistema es el primer paso para identificar los elementos de hardware, muchos de ellos se han mencionado en el análisis del sistema pero ahora se procede a listar y describir cada uno de ellos

Antena parabólica: es una antena VSAT de banda Ku que corresponde a la parte del espectro electromagnético entre los 12 a 18 GHz y que está dentro del rango de las microondas. Se usa principalmente en las comunicaciones satelitales, la banda se divide en varios segmentos para dar cobertura a las distintas regiones geográficas de acuerdo a la Unión Internacional de Telecomunicaciones (International Telecommunication Union, ITU). El B/O García del Cid es un barco regional y su zona de actuación es el Mediterráneo, zona ibérica del Atlántico e Islas Canarias, por lo que la es la Región ITU 1. El modelo instalado es la "v80G Intellian" que tiene un diámetro de 80 cm que es un tamaña suficiente para la zona de trabajo y que además se adapta a infraestructuras disponibles en el buque.

Alimentador: es un dispositivo que está conectada a los equipos de transmisión y recepción de RF mediante una guía de ondas y un cable coaxial respectivamente. Típicamente es de baja ganancia como un dipolo de onda-media y está situado en el foco de la parábola. Al estar en el foco durante la trasmisión se emiten las ondas que al rebotar en la antena parabólica se crear un frente de ondas (ver Figura 13) que llega hasta el satélite al que se está apuntando; y durante la recepción el frente de ondas que emite el satélite se concentrar en el alimentador. En el caso de la antena "v80G Intellian" va integrado en el equipamiento exterior.

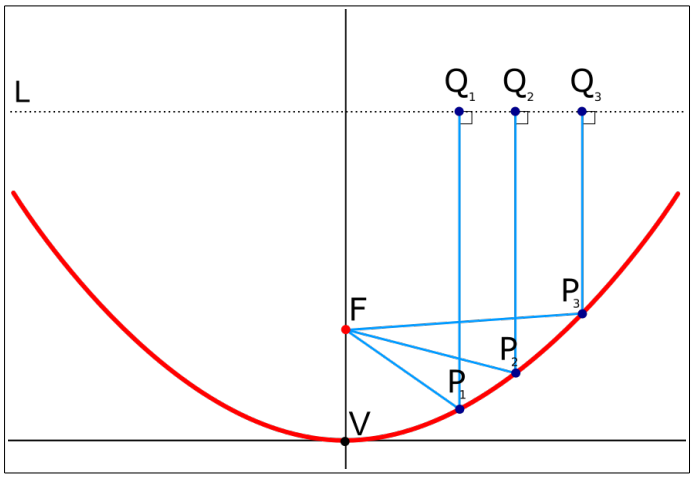

Figura 13: Base geométrica de las antenas parabólicas

BUC: es un dispositivo utilizado en la transmisión de señales de comunicación vía satélite, es decir el enlace ascendente. Convierte la señal de frecuencia intermedia (que entra por un cable coaxial) a frecuencias altas (que sale por una guía de ondas) que el alimentador emite. En el caso de la antena "v80G Intellian" va integrado en el equipamiento exterior.

LNB: es un dispositivo utilizado en la recepción de señales de comunicación vía satélite, es decir el enlace descendente. Convierte la señal de frecuencias altas (que entra por una guía de ondas) a frecuencias intermedias (que sale por un cable coaxial) que el alimentador recibe después de que el frente de ondas que llega desde el satélite rebote en la antena parabólica. En el caso de la antena "v80G Intellian" va integrado.

ACU: es un equipo que controla los motores de la antena para seguir una fuente de señal móvil, el satélite de comunicación. Este equipo es fundamental ya que al tratase de un sistema marino es necesario corregir el movimiento del barco (propulsión, balanceo, cabeceo y guiñada). El modelo instalado es la Intellian ACU que se administra a través de la pantalla, un software especifico (Aptus) o la web de administración.

Módem: es un módem satélite que controla la transmisión y recepción. Desde el dispositivo de envío (cortafuego+UTM o ZENTYAL) recibe un flujo de bits de entrada y lo convierte o modula en ondas y viceversa (demodula las ondas en flujo de bits). Por lo que proporciona dos tipos de conectividad:

- Conectividad de cable coaxial a la antena de satélite.
- Conectividad ethernet al cortafuego+UTM o ZENTYAL.

El modelo instalado es "iDirect Evolution X5" que se administra a través del comando "telnet" o un software especifico (iSite)

Conmutadores: son 2 conmutadores configurables de 8 puertos, uno conecta los equipos del subsistema VSAT y se configuran 2 VLAN; y el otro los del subsistsema LAN sin VLAN. El modelo instalado es el "Ubiquiti TOUCHSwitch TS-8-PRO" que se administrar a través de la web de administración.

PC de administración: es un PC utilizado para acceder al resto de los equipos para administrarlos. En otros barcos ERZIA proporciona un portátil cuyo uso exclusivo es poder conectarse a los otros equipos; en el caso del B/O García del Cid por falta de espacio y presupuesto se aprovechar un PC cuya función principal era otra, el PC-Puente. El modelo instalado es el "Lenovo S500 SFF" con una CPU "Intel i5", 8 GB de RAM y 500 GB de disco duro; y Windows 8 como sistema operativo.

Cortafuegos+UTM o ZENTYAL: es un equipo que proporciona una gestión unificada de amenazas, es decir un cortafuegos de red que engloban múltiples funcionalidades: cortafuegos, calidad de servicio, VPN, servidor DNS y servidor DHCP. El modelo instalado es el mismo qye para el PC de administración. Venía de fabrica con Windows 8 como sistema operativo, pero posteriormente se cambia a "Zentyal Server 4.1" que es la edición de desarrollo con licencia GNU GPL y que está basado en Ubuntu GNU/Linux.

4.2. IDENTIFICACIÓN DE SUBSISTEMAS

Una vez descrito el sistema en el apartado anterior se pueden identificar 2 subsistemas; uno que corresponde a la parte VSAT que conecta con el equipamiento externo y otro que corresponde la parte de la LAN del barco. El único equipo que está en los dos subsistemas es ZENTYAL y que los conecta.

Subsistema VSAT

En el subsistema VSAT (ver Figura 14) que se corresponde a la red de ERZIA, suministrador del servicio de Internet de banda ancha por satélite, con los equipos que permiten conectarse a la red satelital. En este subsistema se configuran 2 VLAN mediante un conmutador configurable: VLAN1 y VLAN302.

La VLAN1 con los equipos que permiten a ERZIA controlar el equipamiento VSAT para proporcionar el servicio de Internet satelital. Esta red tiene el direccionamiento 10.30.1.0/24 y los equipos que la componen tiene las siguientes direcciones IP:

- Módem: 10.30.1.1/24.
- Conmutador: 10.30.1.3/24.
- PC-Puente: 10.30.1.4/24.
- ACU: 10.30.1.20/24.

La VLAN302 con los equipos que hacen de puerta de enlace, el módem al ZENTYAL y este a su vez a resto de los equipos de la LAN del barco. Esta red tiene el direccionamiento 62.81.251.80/30 y los equipos que la componen tiene las siguientes direcciones IP:

- Módem: 62.81.251.81/30.
- ZENTYAL: 62.81.251.82/30.

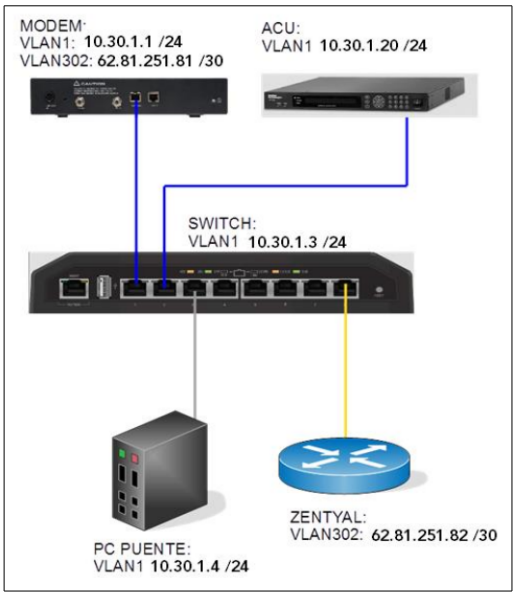

Figura 14: Esquema VSAT

Subsistema LAN

En el subsistema LAN que se corresponde a la red local de barco con los equipos existentes en el barco. Como se ha comentado ZENTYAL está también en este subsistema y hace de puerta de enlace para el resto de los equipos. Este subsistema tiene el direccionamiento 192.168.4.0/24 y los equipos que la componen tiene las siguientes IP (ver Tabla 3):

NOMBRE	IP NUEVA
ZENTYAL	192.168.4.1
ROUTER4G-INVITADOS	192.168.4.2
METEO/TSS	192.168.4.21
POSICION	192.168.4.22
SADO	192.168.4.20
PC-LABORATORIO	192.168.4.30
PC-COMEDOR	192.168.4.31
PC-PUENTE	192.168.4.32
PC-MAXSEA	192.168.4.33
PC-JEFEMAQUINAS	192.168.4.34
IMPRESORA-LABORATORIO	192.168.4.40
IMPRESORA-PUENTE	192.168.4.41
AP-COMEDOR	192.168.4.45
AP-TRIPULACION	192.168.4.46
AP-WHATSAPP	192.168.4.47
CTD1	192.168.4.61
CTD2	192.168.4.62
CTD3	192.168.4.63
EK500-1	192.168.4.80
EK500-2	192.168.4.81
TRACKLINK USBL	192.168.4.81
EA60	192.168.4.82
DOPPLER	192.168.4.83
SCANMAR-MARPORT	192.168.4.84
MULTIHAZ	192.168.4.85
F180	192.168.4.86
MOXA-GPS	192.168.4.90

Tabla 3: Listado equipos LAN

4.3. REVISIÓN Y PRUEBAS

Para comprobar el correcto funcionamiento del sistema se planifican una serie de pruebas. Por un lado las pruebas unitarias que comprobaran el correcto funcionamiento de cada uno de los elementos del sistema por separado y después pruebas globales de cada sistema o subsistema.

Pruebas unitarias

Las pruebas unitarias van a consistir en la revisión del cableado, de las conexiones y el correcto encendido de cada elemento:

- Antena parabólica, alimentador, BUC y LNB: revisar conexión de los cables coaxiales con las ACU, en "Antena TX" y "Antena RX".
- ACU: revisar conexión de los cables coaxiales con la antena ("Antena TX" y "Antena RX"), los cables coaxiales con el módem ("Modem TX" y "Modem RX"), el cable de par trenzado con el girocompás, el cable Ethernet con el Conmutador-VSAT y el cable USB con el PC-Puente. Encender la ACU y comprobar que en la pantalla no se muestran errores.
- Módem: revisar conexión de los cables coaxiales con la ACU ("Modem TX" y "Modem RX") y el cable Ethernet con el Conmutador-VSAT. Encender el módem comprobar que se los led "POWER" y "STATUS" están en verde fijo.
- Conmutadores: para el Conmutador-VSAT revisar conexión de los cables Ethernet con la ACU, el módem, el PC-Puente y el ZENTYAL. Para el Conmutador-LAN revisar conexión del cable Ethernet con el ZENTYAL. En ambos casos encender el conmutador y comprobar que se los led "POE" y "LINK" están en naranja fijo que significan 12 V y 10/100 Mbps respectivamente.
- PC-Puente: revisar conexión del cable Ethernet con el ZENTYAL y el cable USB con la ACU. Encender el PC y comprobar que arranque.
- Cortafuegos+UTM o ZENTYAL: revisar conexión de los cables Ethernet con ambos conmutadores. Encender el PC y comprobar que arranque.

Pruebas global de cada subsistema:

- Subsistema VSAT:
  - Comprobar que desde el PC-Puente se puede acceder a la administración de los equipos del subsistema VSAT: módem, conmutador, ACU y ZENTYAL.
  - Comprobar que desde el ZENTYAL se puede ejecutar el comando "ping", y llega al módem y al DNS de Google (8.8.8.8). También se puede ejecutar el comando "mtr" que es como el comando "traceroute" en tiempo real.
- Subsistema LAN:
  - Comprobar que desde un equipo con salida a Internet (PC-Laboratotio, PC-Comedor, PC-Puente, PC-Maxsea y PC-Jefemaquinas) se puede ejecutar el comando "ping", y llega al ZENTYAL y al DNS de Google (8.8.8.8).
  - Comprobar que un equipo configurado con DHCP automático le asigna una IP entre el rango 192.168.4.100-199
  - Comprobar que desde un equipo sin salida a Internet se puede ejecutar el comando "ping", y llega al ZENTYAL y no al DNS de Google (8.8.8.8).
  - Comprobar que el DNS resuelve bien los nombres, para ello se puede ejecutar el comando "nslookup" con el nombre de una máquina y resuelve la dirección IP.
  - Comprobar que desde un móvil funciona el WhatsApp, pero sólo el texto.
  - Comprobar que desde el ZENTYAL se puede acceder por la VPN a los equipos de la sede en Barcelona. Para ello se pueden ejecutar los comandos "mtr" y "ssh".

5. IMPLEMENTACIÓN DEL SISTEMA

La implementación del Cortafuegos+UTM con el software libre ZENTYAL tendrá que cumplir los requerimientos enunciados en los apartados anteriores que abarcan los siguientes aspectos: Cortafuegos y Calidad de Servicio; VPN; Servidor DNS; y Servidor DHCP.

En la pestaña de "Dashboard" (ver Figura 15) se muestra un resumen del estado del cortafuegos: los servicios arrancados, el tráfico entrante y saliente, el estado de la VPN, las máquinas conectadas, etc.

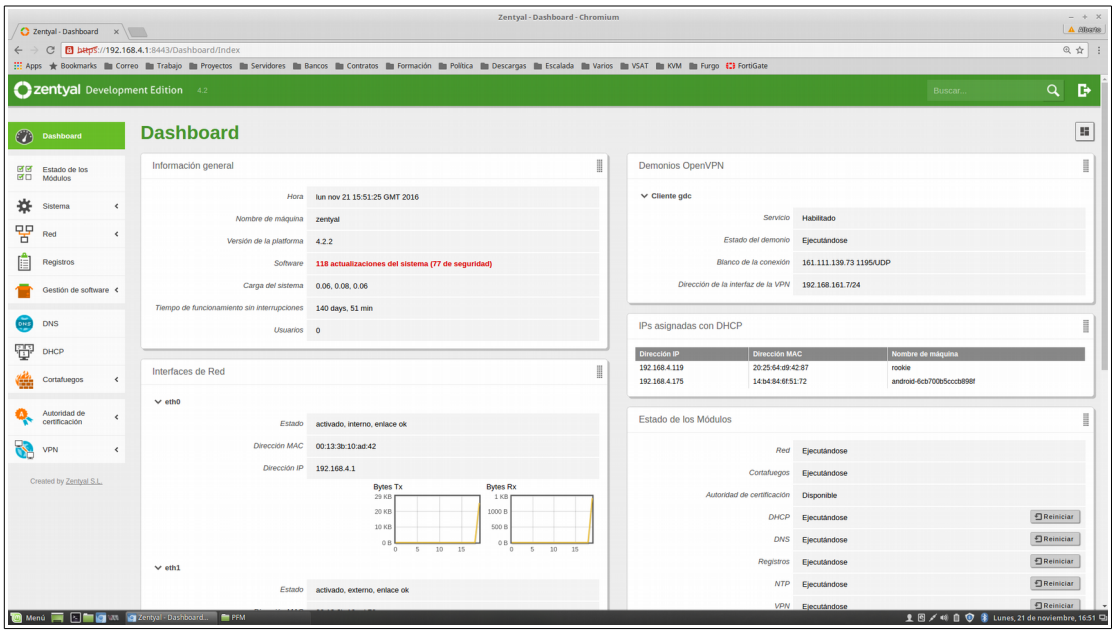

Figura 15: Pestaña "Dashboard" del ZENTYAL

La configuración básica del cortafuegos es donde se configuran las interfaces de red y la puerta de enlace (ver Figura 16). El sistema tiene 3 interfaces de red, una LAN que es la red del barco y 2 WAN hacia el exterior por el Módem-VSAT o el Enrutador-4G:

- eth0 (192.168.4.1/24): está conectada a la LAN del barco y es la puerta de enlace para los equipos que tienen salida a Internet.
- eth1 (62.81.251.82/30): está conectada a la WAN1 que sale por Módem-VSAT que tiene la IP 62.81.251.81/30. Es la conexión a Internet cuando el barco está en alta mar y la comunicación satélite es la única opción.
- eth2 (192.168.40.1/24): está conectada a la WAN2 que sale por Enrutador-4G que tiene la IP 192.168.40.2/24. Es la conexión a Internet cuando el barco está en puerto o cerca de la costa con cobertura de telefonía móvil, de esta manera se consigue un mayor ancho de banda.

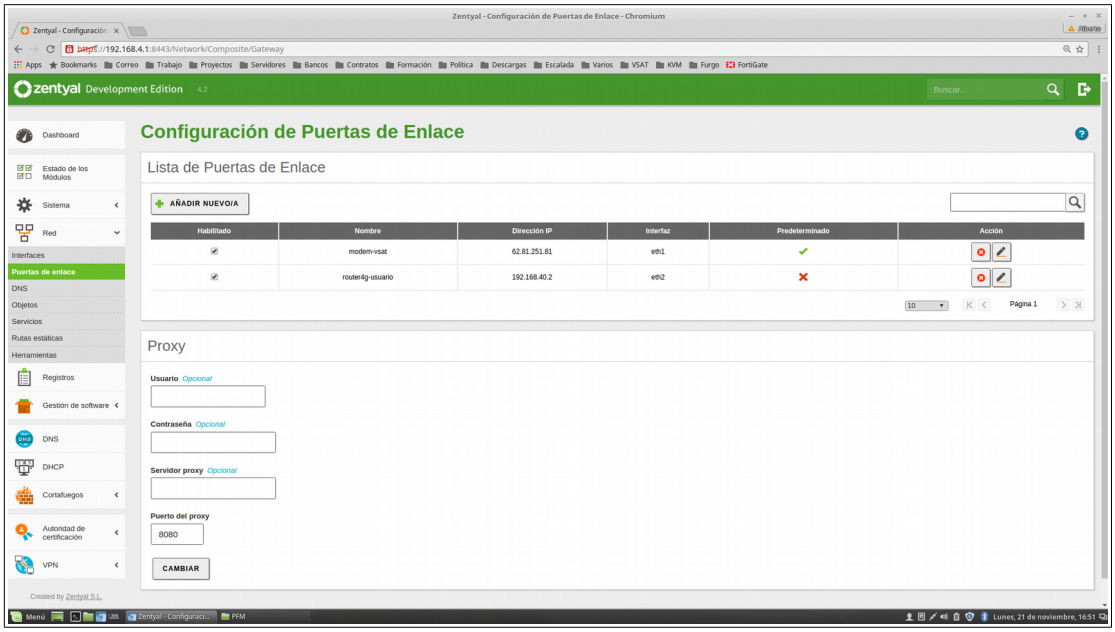

Figura 16: Pestaña "Puerta de enlace" del ZENTYAL

5.1. CORTAFUEGOS Y CALIDAD DE SERVICIO

Como se ha comentado en apartados anteriores lo fundamental es que ZENTYAL permita salir a Internet sólo a unas pocas máquinas. Debido a que el ancho de banda es muy reducido (128-256 Kbps) de esta manera los equipos que tengan salida a Internet (ver Figura 17) podrán navegar con calidad: PC-Cientificos, PC-Puente, PC-Maquinas, PC-Maxsea y PC-Tripulacion.

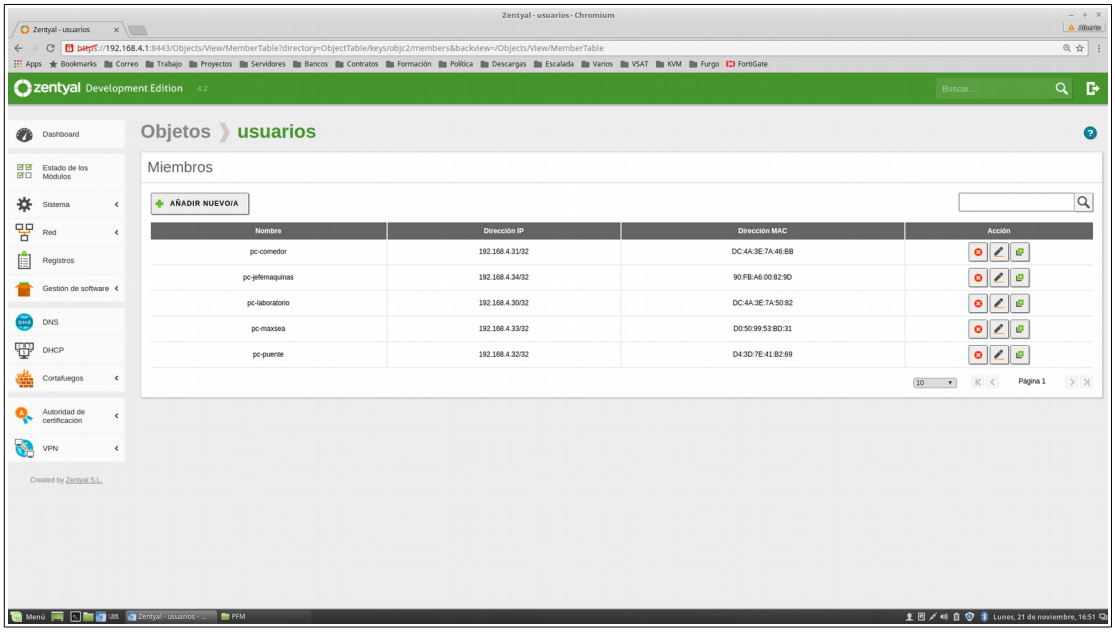

Figura 17: "Objeto" de equipos con Internet o "usuarios"

Además de estos PC con salida a Internet, todos los móviles tendrá disponible el uso de WhatsApp pero limitado a texto para que este servicio no ocupe todo el ancho de banda. Para dar este servicio se configura un punto de acceso "ap-whatsapp" con la IP 192.168.4.47/32 al que se conectarán los móviles. Este punto de acceso tiene el DHCP activado y dará a los móviles direcciones IP en otro rango 192.168.44.0/32 y como puerta de enlace el mismo (192.168.44.47).

Para conseguir que sólo se trasmita los mensajes de texto y no las imágenes ni los vídeos; hay que configurar un servicio donde se habilita sólo el tráfico por el puerto TCP/UDP 5222 que es por el cual la aplicación WhatsApp envío los mensajes de texto (ver Figura 18).

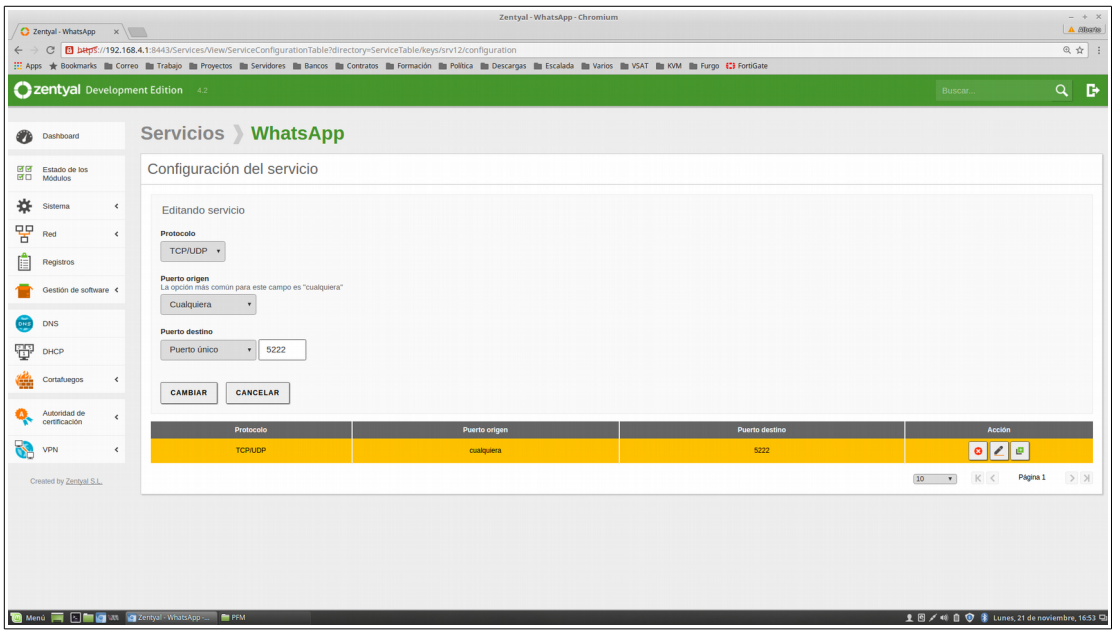

Figura 18: "Servicio" que permite el texto de WhatsApp

Una vez creados los objetos y los servicios se configuran las reglas del cortafuegos (ver Figura 19). Permitiendo todo tipo de tráfico para los "usuarios" y el tráfico del puerto TCP/UDP 5222 (servicio "WhatsApp") al "ap-whatsapp"

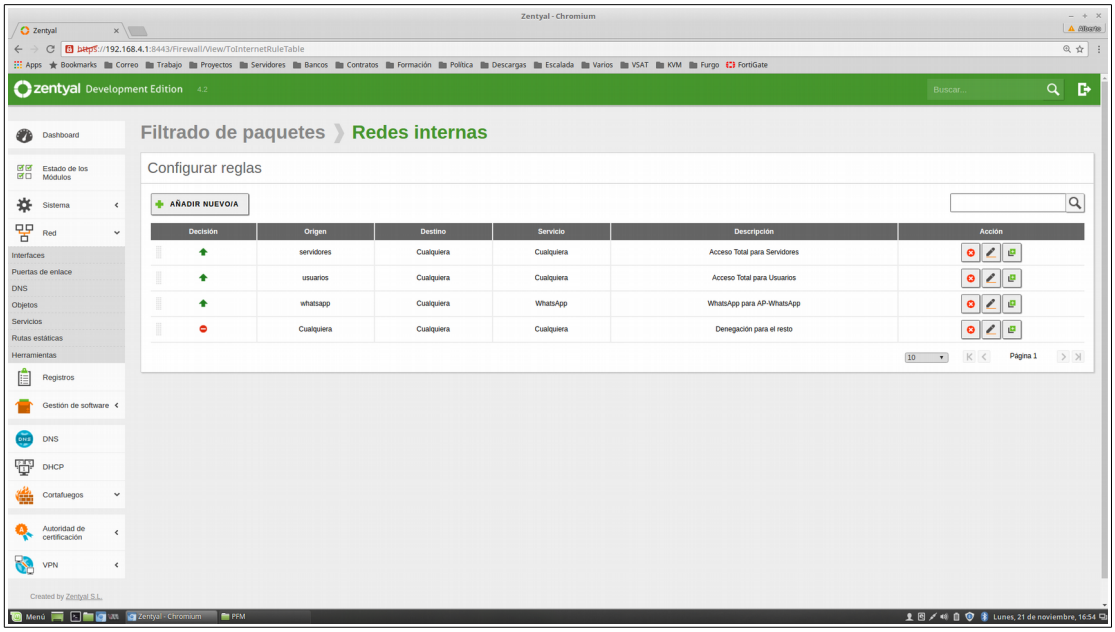

Figura 19: Reglas de la pestaña "Cortafuegos" del ZENTYAL

5.2. VPN

Para establecer una VPN entre el barco y la sede central será necesario tener un ZENTYAL en cada extremo del túnel. La UTM-CSIC gestiona más plataformas aparte del B/O García del Cid por lo que se diseña una estructura en estrella, donde los ZENTYAL de las plataformas se conectan a la sede para crear su túnel. De esta manera cuando desde el barco (rango 192.168.4.0/24) se quiera acceder al de la sede central (rango 161.111.136.0/22) el ZENTYAL del barco que es la puerta de enlace (192.168.4.1) encamine las peticiones por dicho túnel, y viceversa.

El ZENTYAL de la sede se instala en una máquina virtual donde ya hay instalados otras servidores en máquinas virtuales. Para ello se usa el software "Virtual Manager Machine" [8] que es el administrador de máquinas virtuales de RedHat, es un administrador de escritorio licenciado bajo GNU GPL v3+. La máquina física es "Sun Fire X2200 M2" que tiene las siguientes características: 8 CPU, 16 GB de RAM y 2 discos duros de 500 GB. A la máquina de ZENTYAL se le da el nombre de "iris" tiene las siguientes características: 2 CPU, 2 GB de RAM y 8 GB discos duros.

Como se ha mostrado antes en la pestaña de "Dashboard" se muestra un resumen del estado del cortafuegos, en este caso del ZENTYAL de la sede sólo se utiliza para la VPN así que mostrará si está conectado el "garciadelcid" (ver Figura 20).

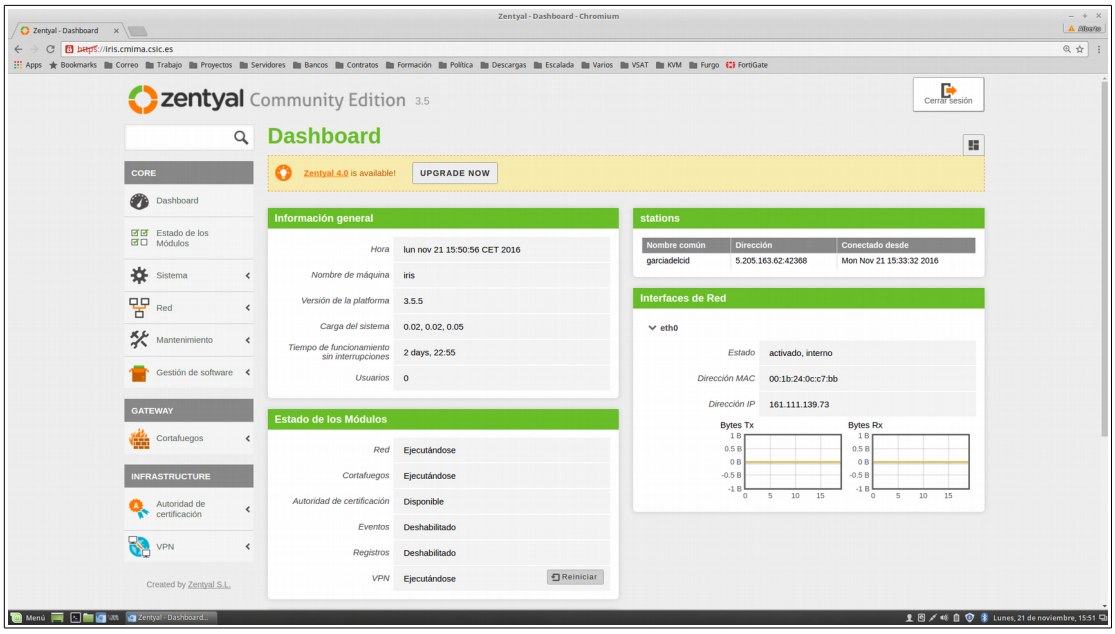

Figura 20: Pestaña "Dashboard" del ZENTYAL de la sede central

Para configurar la VPN hay que habilitar el ZENTYAL como "Autoridad de certificados" y determinar los parámetros en el pestaña "Servidores" del apartado en cuestión (ver Figura 21).

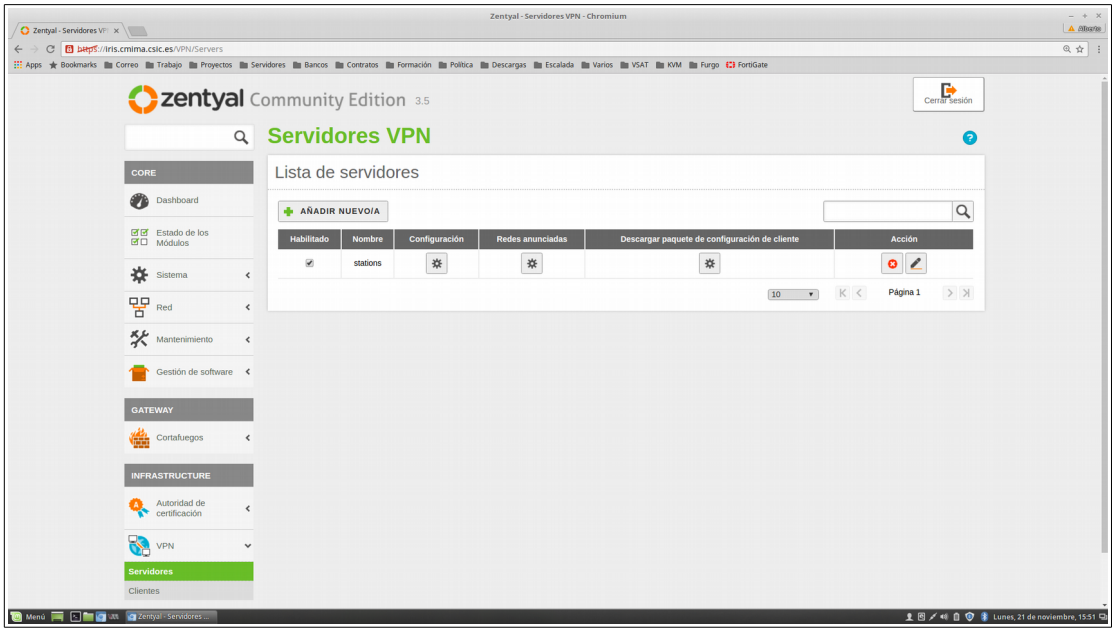

Figura 21: Pestaña "Servidor" de la VPN del ZENTYAL

Los parámetros a determinar están en la sección "Configuración" y "Redes anunciadas" de la pestaña anterior (ver Figuras 22 y 23). En la segunda sección se lista los servidores de la sede central a la que se tendrá acceso desde el barco.

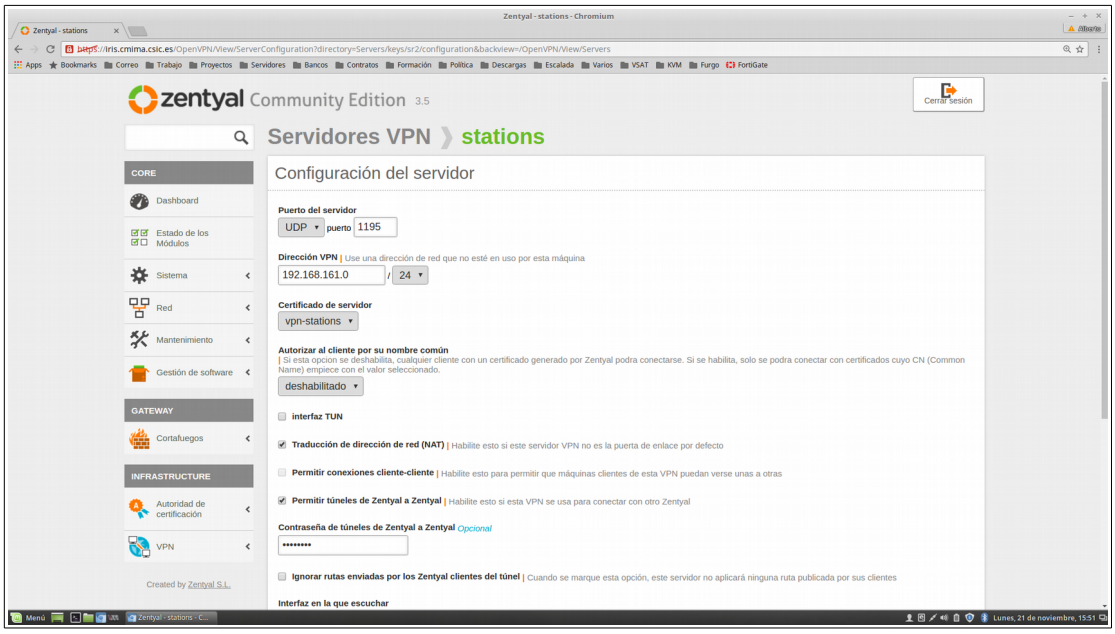

Figura 22: "Configuración" de la VPN del ZENTYAL

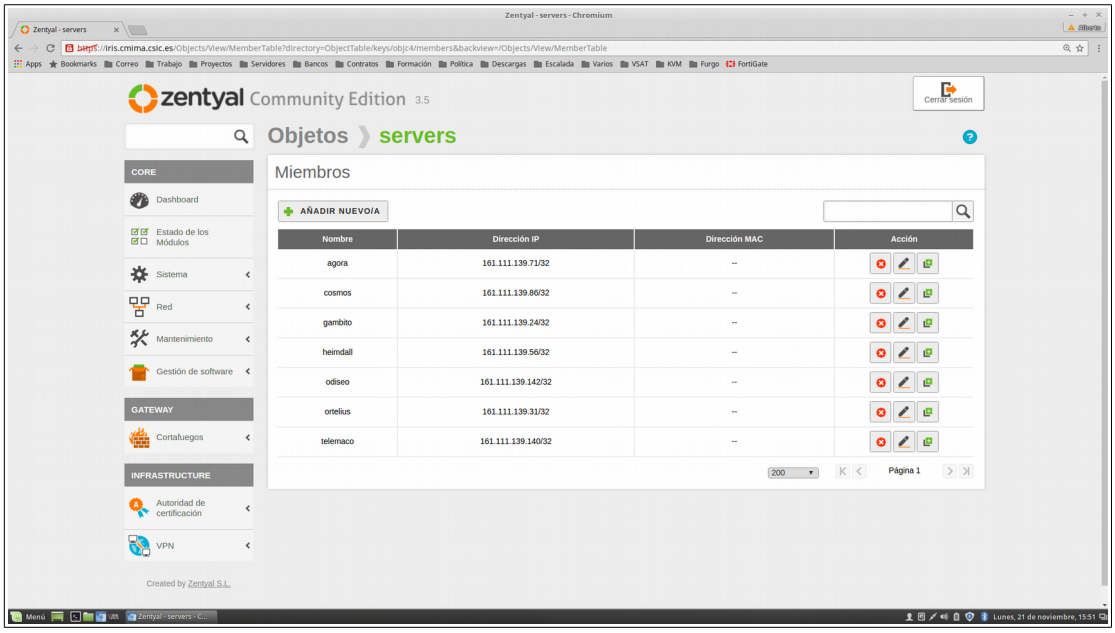

Figura 23: "Objeto" de los servidores que está en "Redes Anunciadas"

5.3. SERVIDOR DNS

El servidor DNS resolverá los nombre de todos los equipos fijos conectados a la LAN del barco. Como se ha comentado antes se ha aprovechado para cambiar el direccionamiento del 193.145.218.0/24 al 192.168.4.0/24. Para ello hay que añadir cada uno de los equipos (nombre y dirección IP) en la pestaña "DNS" (ver Figura 24).

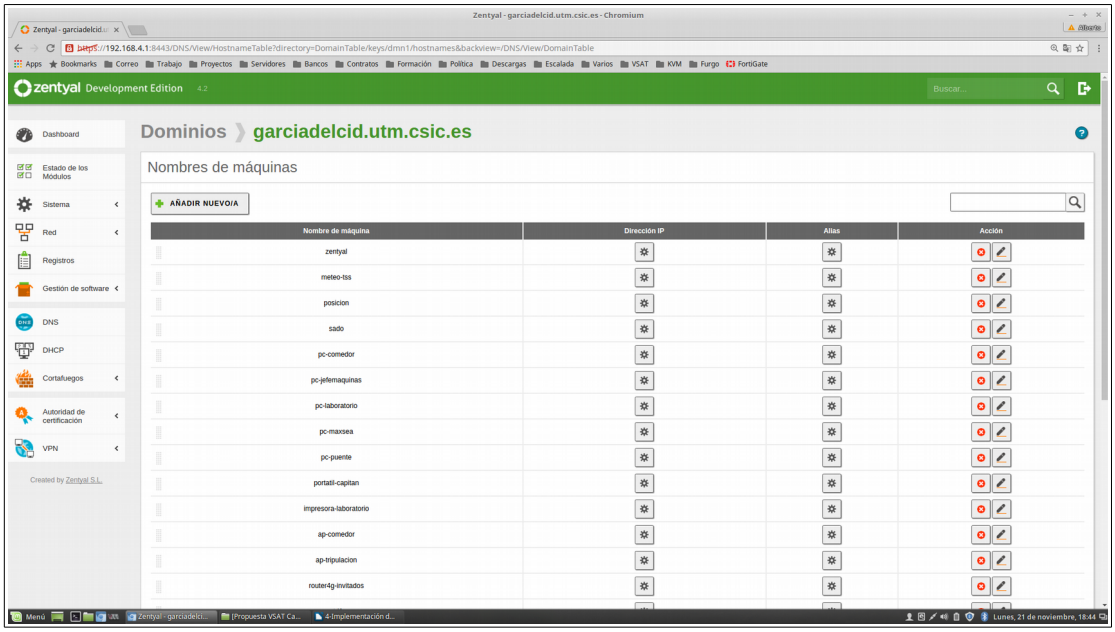

Figura 24: Pestaña "DNS" del ZENTYAL

5.4. SERVIDOR DHCP

El servidor DHCP dará a los equipos configurados con DHCP automático una dirección IP entre la 192.168.4.100 y la 192.168.4.199. Para ello hay que configurar en la pestaña "DHCP" la interfaz eth0 que es la que corresponde a la LAN del barco (ver Figuras 25 y 26).

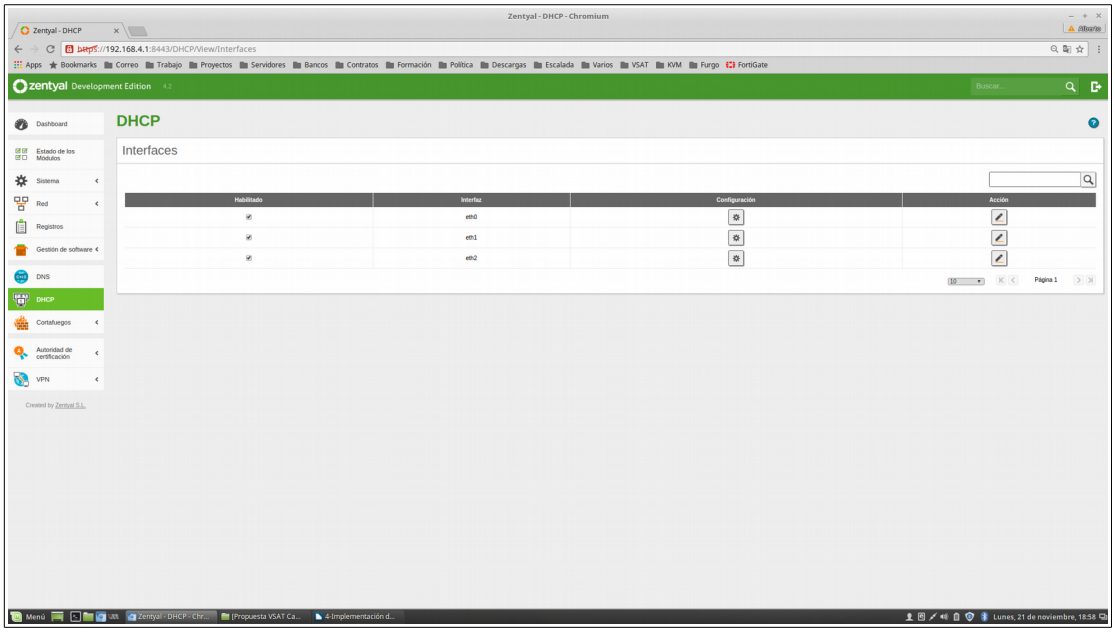

Figura 25: Pestaña "DHCP" del ZENTYAL

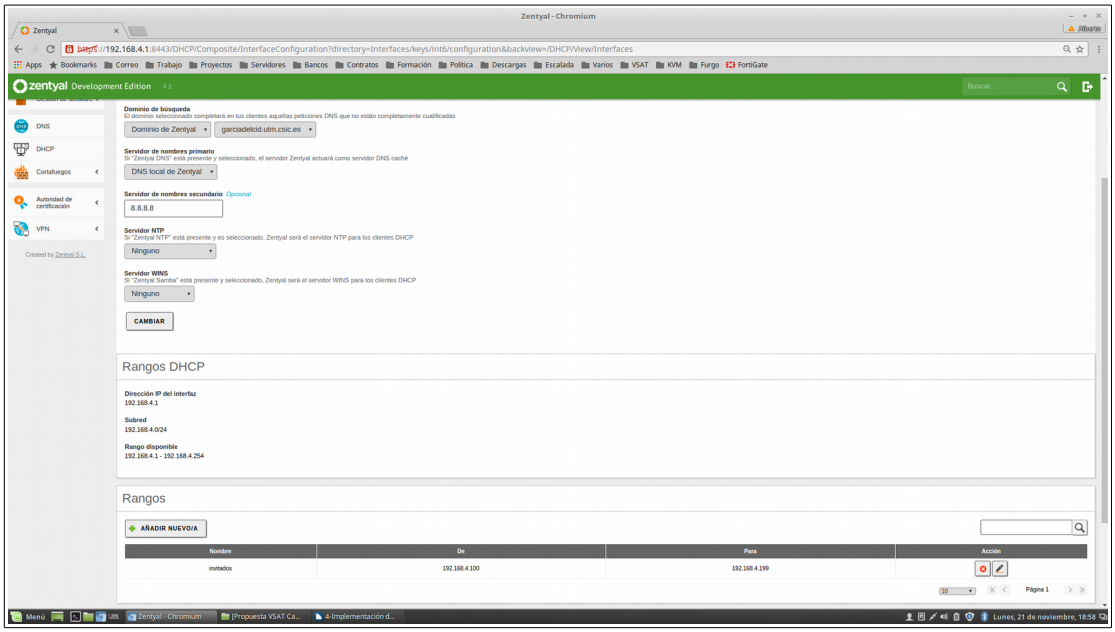

Figura 26: "eth0" de pestaña "DHCP" del ZENTYAL

Además para evitar suplantación de direcciones IP de los equipos que tienen salida a Internet en la pestaña "Objetos" se ha configurado la MAC de equipos con Internet.

6. RESULTADOS

Los resultados de las pruebas unitarias han sido satisfactorios como se puede ver en la imagen todos los equipos están bien conectados y han arrancado correctamente (ver Figura 27), a continuación se describen los resultados por cada equipo:

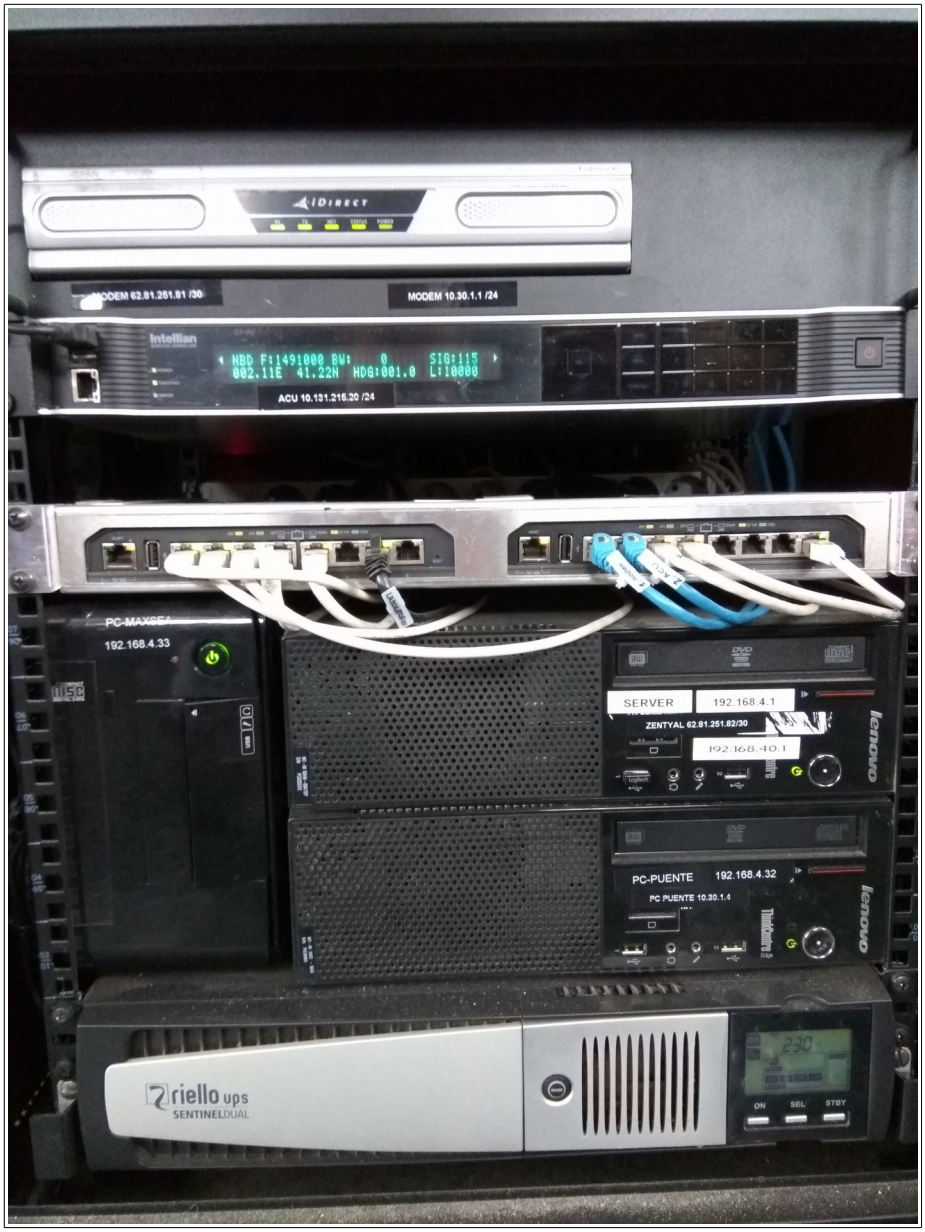

Figura 27: Conexión y encendido de equipos del rack

- Antena parabólica, alimentador, BUC y LNB: la conexión de los cables coaxiales con las ACU, en "Antena TX" y "Antena RX" es correcta.
- ACU: la conexión de los cables coaxiales con la antena ("Antena TX" y "Antena RX"), los cables coaxiales con el módem ("Modem TX" y "Modem RX"), el cable de par trenzado con el girocompás, el cable Ethernet con el Conmutador-VSAT y el cable USB con el PC-Puente es correcta. Al encender la ACU no se muestran errores en la pantalla.

- Módem: la conexión de los cables coaxiales con la ACU ("Modem TX" y "Modem RX") y el cable Ethernet con el Conmutador-VSAT es correcta. Al encender el módem los led "POWER" y "STATUS" están en verde fijo.
- Conmutadores: para el Conmutador-VSAT la conexión de los cables Ethernet con la ACU, el modem, el PC-Puente y el ZENTYAL es correcta. Para el Conmutador-LAN la conexión del cable Ethernet con el ZENTYAL también es correcta. En ambos casos al encender los conmutadores los led "POE" y "LINK" están en naranja fijo que significan 12 V y 10/100 Mbps respectivamente.
- PC-Puente: la conexión del cable Ethernet con el ZENTYAL y el cable USB con la ACU es correcto. Al encender el PC arranca correctamente.
- Cortafuegos+UTM o ZENTYAL: la conexión de los cables Ethernet con ambos conmutadores es correcta. Al encender el PC arranca correctamente.

Pruebas globales de cada subsistema:

- Subsistema VSAT:
  - Desde el PC-Puente se puede acceder a la administración de los equipos del subsistema VSAT (ver Figuras 28, 29, 30, 31 y 32): módem, conmutador, ACU y ZENTYAL.

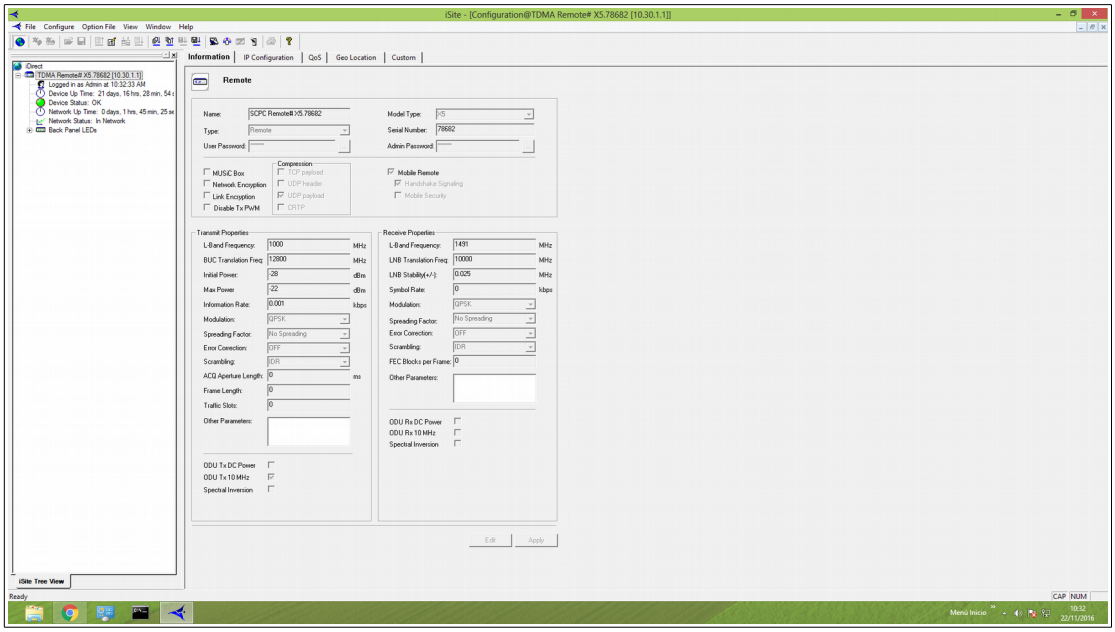

Figura 28: Acceso mediante el programa iSite al módem

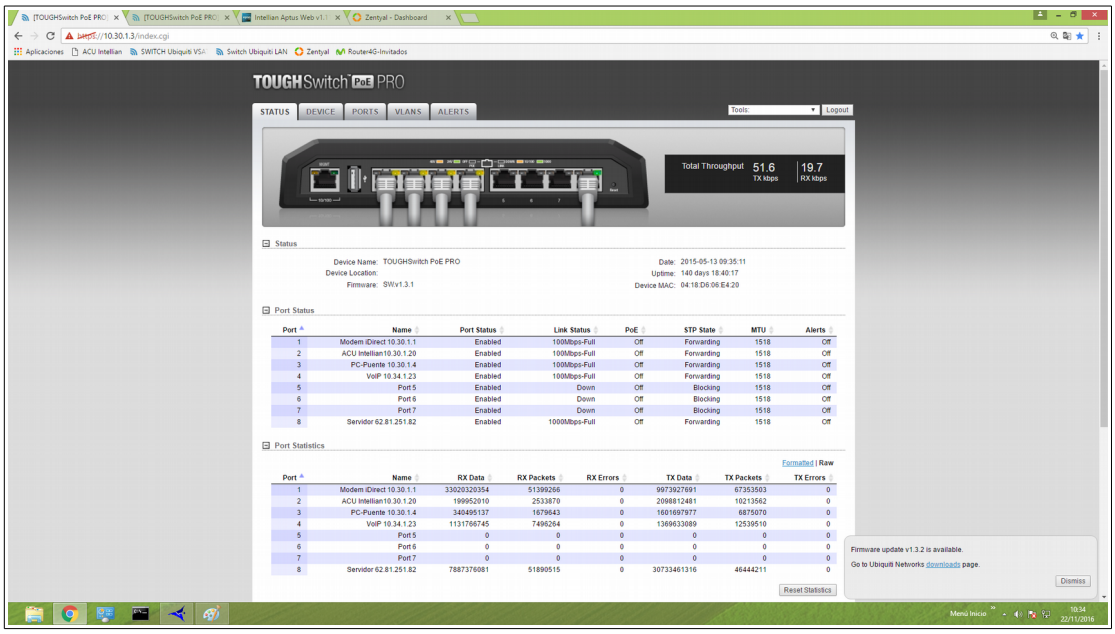

Figura 29: Acceso mediante la web de administración al Conmutador-VSAT

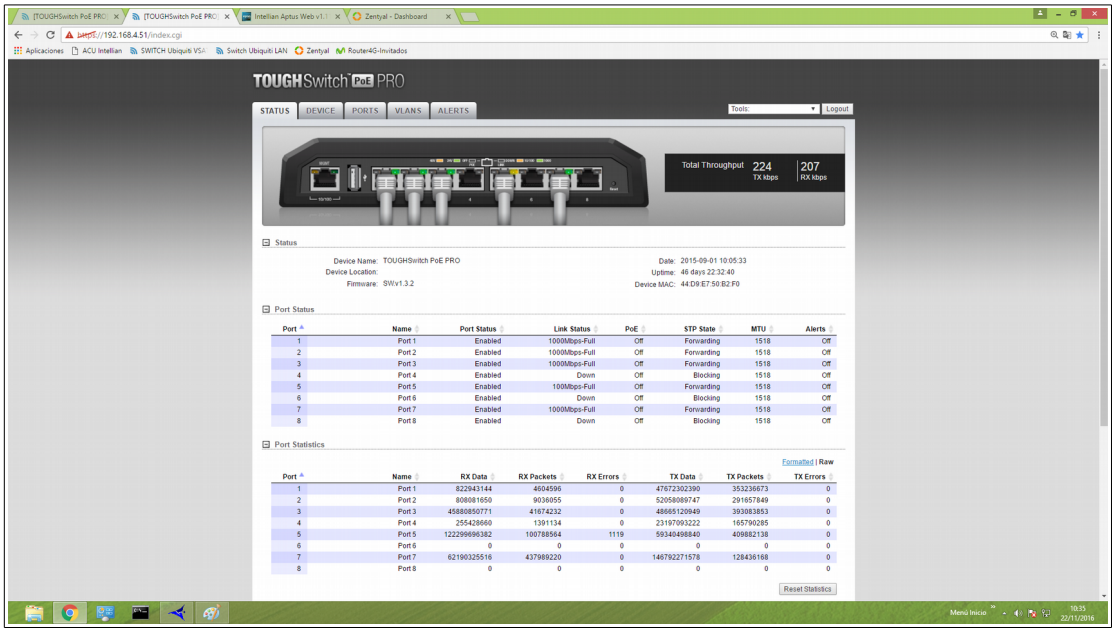

Figura 30: Acceso mediante la web de administración al Conmutador-LAN

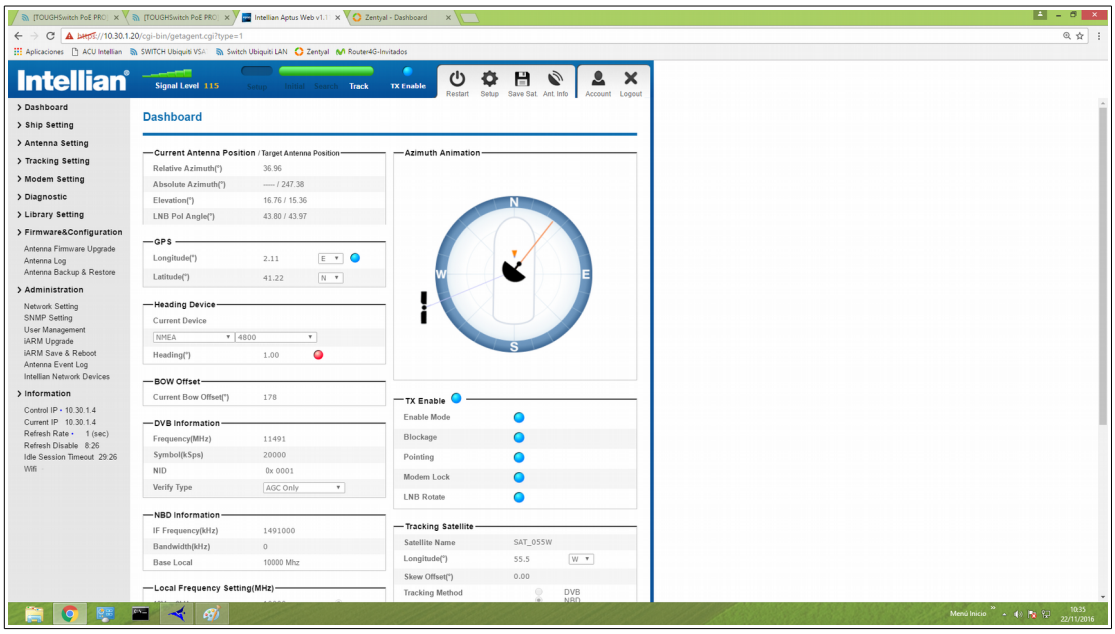

Figura 31: Acceso mediante la web de administración a la ACU

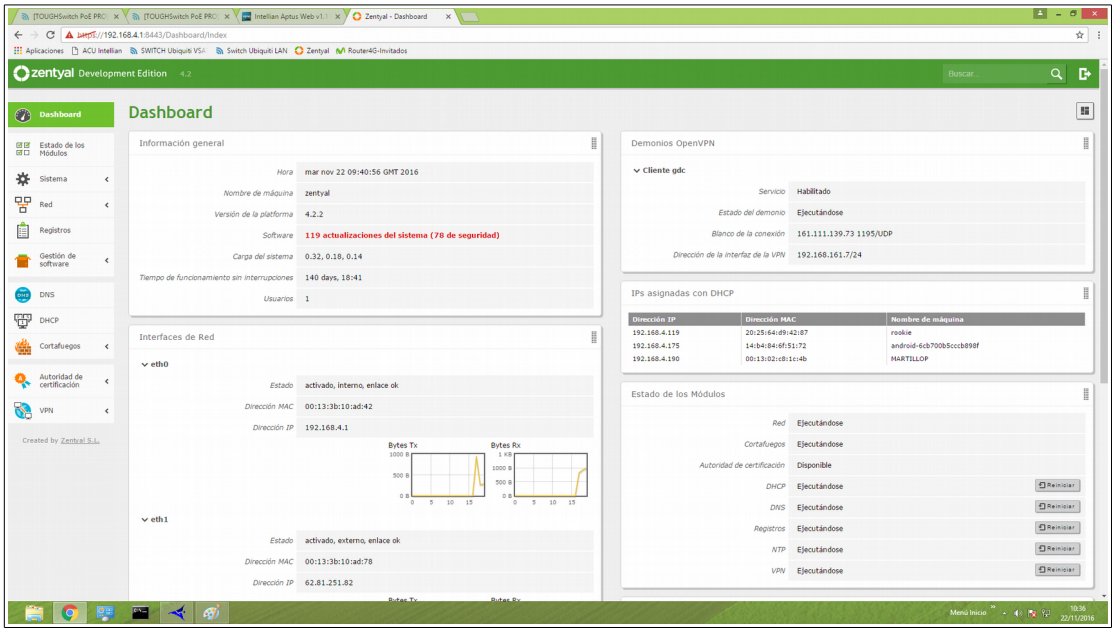

Figura 32: Acceso mediante la web de administración al ZENTYAL

- Desde el ZENTYAL se ejecuta el comando "ping" (ver Tabla 4) y llega al módem y al DNS de Google (8.8.8.8). También ejecuta el comando "mtr" al DNS de Google (8.8.8.8) para ver los saltos (ver Figura 33).

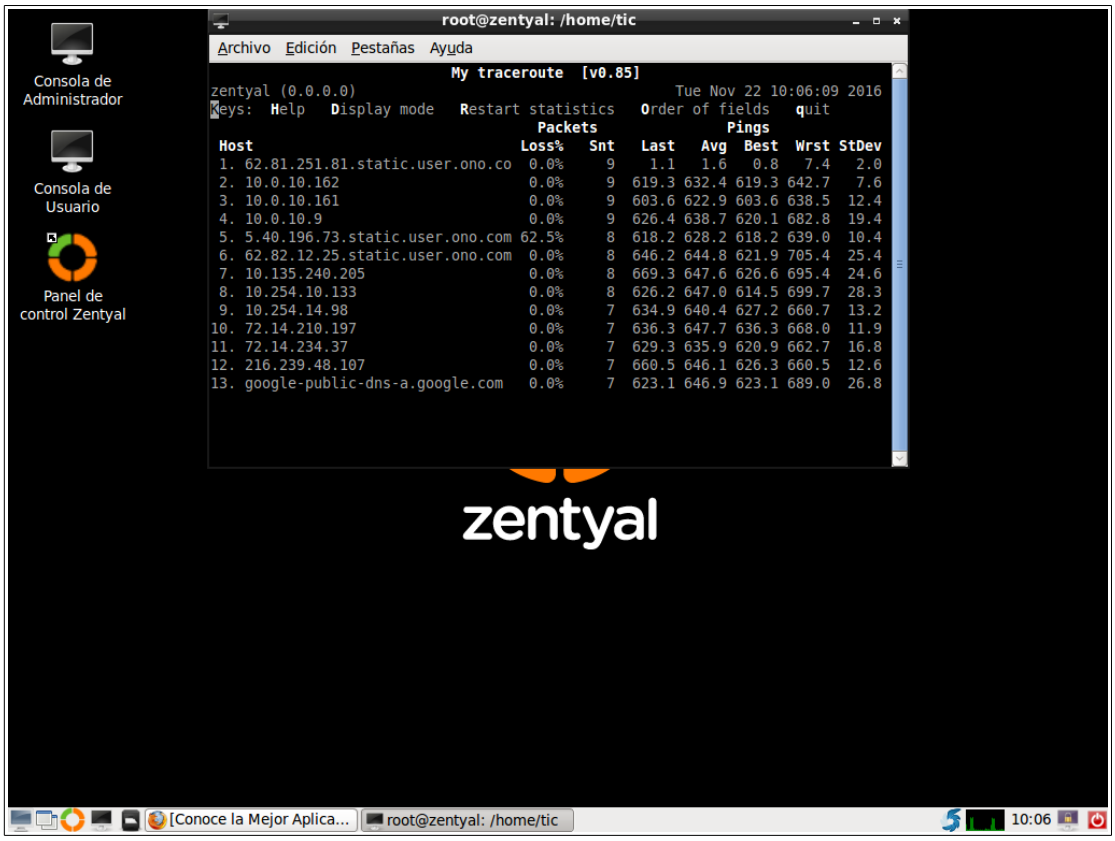

Figura 33: Comando "mtr" del ZENTYAL al 8.8.8.8

```
root@ZENTYAL:/home/tic# ping 62.81.251.81
PING 62.81.251.81 (62.81.251.81) 56(84) bytes of data.
64 bytes from 62.81.251.81: icmp_seq=1 ttl=254 time=1.14 ms
64 bytes from 62.81.251.81: icmp_seq=2 ttl=254 time=0.986 ms
64 bytes from 62.81.251.81: icmp_seq=3 ttl=254 time=0.791 ms
^C
--- 62.81.251.81 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.791/0.927/1.148/0.119 ms
root@ZENTYAL:/home/tic# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=54 time=657 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=54 time=643 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=54 time=747 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2999ms
```

```
rtt min/avg/max/mdev = 643.345/682.927/747.762/46.221 ms
root@ZENTYAL:/home/tic#
```

Tabla 4: Comando "ping" del ZENTYAL al modem y al 8.8.8.8

- Subsistema LAN:
  - Desde un equipo con salida a Internet (PC-Laboratotio) se ejecuta el comando "ping" (ver Tabla 5), y llega al ZENTYAL y al DNS de Google (8.8.8.8).

```
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\windows\system32>ipconfig /all

Configuración IP de Windows

   Nombre de host. . . . . : pc-laboratorio
   Sufijo DNS principal  . . . . . :
   Tipo de nodo. . . . . : híbrido
   Enrutamiento IP habilitado. . . : no
   Proxy WINS habilitado . . . . . : no
   Lista de búsqueda de sufijos DNS: garciadelcid.utm.csic.es

Adaptador de Ethernet Conexión de área local:

   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . . : Intel(R) Ethernet Connection (2)
I219-LM
   Dirección física. . . . . . . . . . . . . : DC-4A-3E-7A-50-82
   DHCP habilitado . . . . . . . . . . . . . : no
   Configuración automática habilitada . . . : sí
   Sitio: dirección IPv6 local. . . . : fec0::b45a:7ad:e087:d560%1(Preferido)
   Vínculo: dirección IPv6 local. . . : fe80::b45a:7ad:e087:d560%11(Preferido)
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.4.30(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.4.1
   IAID DHCPv6 . . . . . . . . . . . . . . . : 249317950
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-1F-40-C8-10-DC-4A-3E-
7A-50-82
   Servidores DNS. . . . . . . . . . . . . . : 192.168.4.1
                                               8.8.8.8
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado

Adaptador de túnel isatap.{A59A5159-FA9A-4C85-AB03-316E002CEE2A}:
```

```
   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . . : Adaptador ISATAP de Microsoft
   Dirección física. . . . . . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP habilitado . . . . . . . . . . . . . : no
   Configuración automática habilitada . . . : sí

C:\windows\system32>ping 192.168.4.1

Haciendo ping a 192.168.4.1 con 32 bytes de datos:
Respuesta desde 192.168.4.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.4.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.4.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.4.1: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.4.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\windows\system32>ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=631ms TTL=53
Respuesta desde 8.8.8.8: bytes=32 tiempo=634ms TTL=53
Respuesta desde 8.8.8.8: bytes=32 tiempo=631ms TTL=53
Respuesta desde 8.8.8.8: bytes=32 tiempo=631ms TTL=53

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 631ms, Máximo = 634ms, Media = 631ms

C:\windows\system32>
```

Tabla 5: Comandos "ipconfig" y "ping" del PC-Laboratorio al ZENTYAL y al 8.8.8.8

- Mi portátil que está configurado con DHCP automático le asigna la IP 192.168.4.102 (ver Tabla 6).

```
ahernandez@rookie ~ $ ifconfig
enp4s0    Link encap:Ethernet  direcciónHW 20:25:64:d9:42:87
          Direc. inet:192.168.4.102  Difus.:192.168.4.255  Másc:255.255.255.0
          Dirección inet6: fe80::f92b:32c5:f6d7:3ed4/64 Alcance:Enlace
```

```
      ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
      Paquetes RX:267211 errores:0 perdidos:1 overruns:0 frame:0
      Paquetes TX:167377 errores:0 perdidos:0 overruns:0 carrier:0
      colisiones:0 long.colaTX:1000
      Bytes RX:280696001 (280.6 MB)  TX bytes:15828234 (15.8 MB)

lo     Link encap:Bucle local
      Direc. inet:127.0.0.1  Másc:255.0.0.0
      Dirección inet6: ::1/128 Alcance:Anfitrión
      ACTIVO BUCLE FUNCIONANDO  MTU:65536  Métrica:1
      Paquetes RX:5387 errores:0 perdidos:0 overruns:0 frame:0
      Paquetes TX:5387 errores:0 perdidos:0 overruns:0 carrier:0
      colisiones:0 long.colaTX:1
      Bytes RX:436214 (436.2 KB)  TX bytes:436214 (436.2 KB)
```

Tabla 6: Comando "ifconfig"

- Desde mi portátil que no tiene salida a Internet se ejecuta el comando "ping" (Tabla 7), y llega al ZENTYAL y no al DNS de Google (8.8.8.8).

```
ahernandez@rookie ~ $ ping 192.168.4.1
PING 192.168.4.1 (192.168.4.1) 56(84) bytes of data.
64 bytes from 192.168.4.1: icmp_seq=1 ttl=64 time=0.221 ms
64 bytes from 192.168.4.1: icmp_seq=2 ttl=64 time=0.178 ms
64 bytes from 192.168.4.1: icmp_seq=3 ttl=64 time=0.209 ms
64 bytes from 192.168.4.1: icmp_seq=4 ttl=64 time=0.193 ms
^C
--- 192.168.4.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 0.178/0.200/0.221/0.019 ms
ahernandez@rookie ~ $ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 192.168.4.119 icmp_seq=1 Destination Host Unreachable
From 192.168.4.119 icmp_seq=2 Destination Host Unreachable
From 192.168.4.119 icmp_seq=3 Destination Host Unreachable
From 192.168.4.119 icmp_seq=4 Destination Host Unreachable
^C
--- 8.8.8.8 ping statistics ---
87 packets transmitted, 16 received, +15 errors, 81% packet loss, time 86548ms
rtt min/avg/max/mdev = 48.783/54.149/60.149/3.373 ms, pipe 3
```

Tabla 7: Comando "ping" de mi portátil al ZENTYAL y al 8.8.8.8.

- El DNS resuelve bien los nombres como "sado", "posicion", "PC-Laboratorio", etc. Para ello se ejecuta el comando "nslookup" (ver Tabla 8)

```
ahernandez@rookie ~ $ nslookup zentyal
Server:         127.0.1.1
Address:        127.0.1.1#53

Name: zentyal.garciadelcid.utm.csic.es
Address: 192.168.4.1
Name: zentyal.garciadelcid.utm.csic.es
Address: 216.130.38.114

ahernandez@rookie ~ $ nslookup sado
Server:         127.0.1.1
Address:        127.0.1.1#53

Name: sado.garciadelcid.utm.csic.es
Address: 192.168.4.20

ahernandez@rookie ~ $ nslookup posicion
Server:         127.0.1.1
Address:        127.0.1.1#53

** server can't find posicion: NXDOMAIN

ahernandez@rookie ~ $ nslookup pc-laboratorio
Server:         127.0.1.1
Address:        127.0.1.1#53

** server can't find pc-laboratorio: NXDOMAIN
```

Tabla 8: Comando "nslookup"

- Desde un móvil funciona el WhatsApp, pero sólo el texto (ver Figura 34). Como se pude ver por las horas el mensaje de texto ha sido enviado, pero no la imagen y el mensaje de voz. Además se muestra que al conectar con el "ap-whatsapp" este ha dado a mi móvil la IP 192.168.44.103/32 y como puerta de enlace el mismo (192.168.44.47).

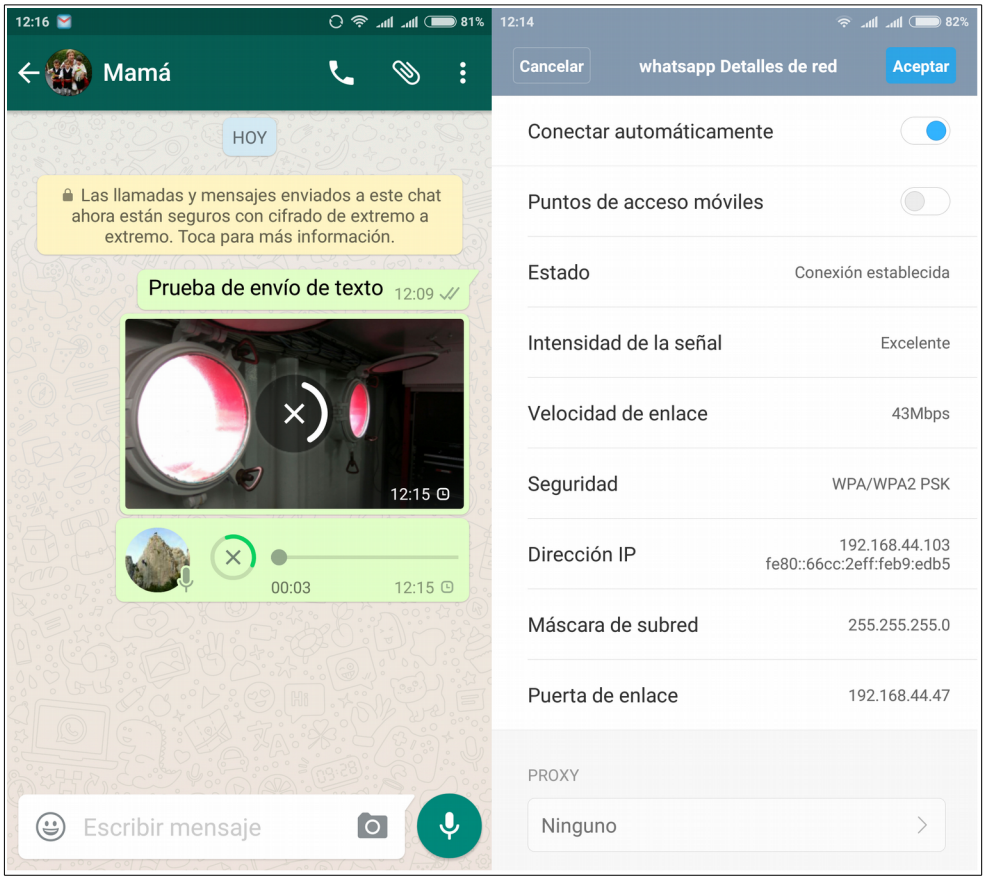

Figura 34: Mi móvil conectado a "ap-whatsapp" envía texto, pero no imágenes y voz.

- Desde el ZENTYAL se puede acceder por la VPN a los equipos de la sede en Barcelona. Para ello se ejecutan los comandos "mtr" (ver Figura 35) y "ssh" a "ortelius" (ver Tabla 9).

Figurav 35: Comando "mtr" de ZENTYAL a "ortelius"

```
tic@ZENTYAL:~$ ssh utmtel@ortelius.cmima.csic.es
utmtel@ortelius.cmima.csic.es's password:
Last login: Tue Nov 22 10:31:40 2016 from 161.111.139.73
[utmtel@ortelius ~]$ ifconfig
eth0      Link encap:Ethernet  HWaddr 98:4B:E1:63:6F:D2
          inet addr:161.111.139.31  Bcast:161.111.139.255  Mask:255.255.252.0
          inet6 addr: fe80::9a4b:e1ff:fe63:6fd2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1400  Metric:1
          RX packets:21537017 errors:62769 dropped:0 overruns:0 frame:62769
          TX packets:4789518 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3478049745 (3.2 GiB)  TX bytes:954994980 (910.7 MiB)
          Memory:feb60000-feb80000

[utmtel@ortelius ~]$
```

Tabla 9: Comando "ssh" de ZENTYAL a "ortelius"

7. CONCLUSIONES

La alternativa de software libre como solución única de los servicios de gestión de red ha tenido resultados muy satisfactorios. Esta solución tiene características equivalentes o superiores a las del sistema antiguo, la administración es sencilla y con un único equipo se cubre todas la necesidades.

- Cortafuegos: dar salida a Internet a unos pocos equipos (filtrando por MAC).
- Calidad de Servicio: repartir el ancho de banda por servicios o usuarios.
- VPN: acceder a los equipos del barco y la sede como si fuera la misma red.
- DNS: dar servicio de resolución de nombres de dominio en la red.
- DHCP: dar servicio de configuración automática de parámetros en la red

Se ha pasado de un escenario con un enrutador en equipo propietario (enrutador CISCO) cuya administración es muy complicado (sólo vía comandos) y no disponía de funcionalidades como filtrar por MAC (para evitar la suplantación de IP de los equipos con salida a Internet) o garantizar ancho de banda (para usuarios o servicios críticos). Y además no cubría todas las necesidades por lo que otros equipos (servidores GNU/Linux) proporcionaban los servicios DNS y DHCP.

La solución elegida ha sido ZENTYAL ya que como otras alternativas encontradas cubría necesarias para funcionar como solución única de los servicios de gestión de red. Pero además se contaba con experiencia, contactos y documentación de un curso que realizó un compañero del centro.

Este proyecto viene impulsado por la necesidad de actualizar los sistemas de comunicaciones del B/O García del Cid, para que la comunidad científica desarrolle sus actividades en las condiciones mas favorables. Incluye la adquisición mediante el concurso público del proyecto de cofinanciación FEDER de un sistema de comunicaciones VSAT mediante antena de banda Ku. Y se aprovecha el proyecto para recopilar información de red de todos los equipos que componen la red local del barco como son la MAC, la IP y el sistema operativo y para actualizar el direccionamiento a 192.168.4.0/24 homogeneizando así todas las plataformas que gestiona la UTM-CSIC.

Para comprobar el correcto funcionamiento del sistema se planifican una serie de pruebas tanto unitarias de cada uno de los elementos del sistema por separado como globales de cada subsistema. Los resultados de las pruebas han sido satisfactorios como se ha mostrado anteriormente.

8. REFERENCIAS BIBLIOGRÁFICAS

[1] Eurofleet 2 (s.f.). Recuperado el 5 de septiembre de 2016, de http://www.eurofleets.eu/

[2] Zentyal Server (s.f.). Recuperado el 6 de octubre de 2016, de http://www.zentyal.com/es/zentyal-server/

[3] Zentyal Wiki 2 (s.f.). Recuperado el 8 de octubre de 2016, de https://wiki.zentyal.org/wiki/Es

[4] Endian (s.f.). Recuperado el 12 de octubre de 2016, de http://www.endian.com/community/features/

[5] OPNsense (s.f.). Recuperado el 12 de octubre de 2016, de https://opnsense.org/about/about-opnsense/

[6] ClearOS 7 Community (s.f.). Recuperado el 12 de octubre de 2016, de https://www.clearos.com/clearfoundation/software/clearos-7-community/marketplace

[7] Intellian v80G Installation and Operation User Guide (s.f.). Recuperado el 24 de octubre de 2016, de http://www.rian-bv.eu/files/1324371474_201100915_v80G.pdf

[8] Manage virtual machines (s.f.). Recuperado el 6 de noviembre de 2016, de https://virt-manager.org/