# TRABAJO FIN DE GRADO

## Implantación de un servidor de red para el acceso compartido a Internet en un entorno mixto de red interna y pública inalámbrica.

Grado de Tecnologías de Telecomunicación

Javier Martín García-Asenjo
Consultor: Antoni Morell Pérez

# 1. INDICE

## 2. Tabla de Ilustraciones.

# 3. Introduccion

## 3.1. Abstract

In this project we face the implementation of a network server for the control and management of a shared Internet access in a mixed environment of internal local network and a public wireless network. The baseline scenario is the public library of my hometown where a few months ago a pilot program for offering free Internet access had to be cancelled due to the misuse of the network resources by malicious users. Other considerations to keep in mind are prioritizing the traffic of the librarians over the rest of the users, and keeping an eye on the legal implications of a service of this kind.

During the development of this TFG, a study of the various legal and technical requirements of an environment of this nature was held. We also investigated the usual configuration in corporate solutions where expensive hardware devices provide the services we were looking to implement.

With both technical and legal requirements defined, our goal was clear-cut, find an alternative solution for a captive portal server:

• Suitable for a no-budget environment.

• Running in efficiently on older, cheaper hardware.

After a research, the chosen option was implemented in a physical environment, and the documentation was drawn up with such a level of detail, that it could allow a user with a little knowledge to run a similar solution.

The solution chosen was ZEROSHELL, a Linux based distribution for network servers that was up and running with just a few tweaks. Our goal was accomplished: a fully functional captive portal providing user authentication in an open Wi-Fi network and other advanced features like Bandwidth control, Transparent Web Proxy with Antivirus and Quality of Service with traffic prioritization.

Although the project focuses on the implementation for a simple location, we conducted the study of a high level approach to a more complex environment. The integration of our captive portal in a scenario with multiple distributed wireless zones connected by a wireless WAN.

Beyond the scope of the Municipal Library which served as a starting point, we hope the installation guide included in this document may be useful for someone searching for a solution in a similar environment, not just a library. It can be a primary school or even a home network.

## 3.2. Presentación

En este proyecto trataremos la implantación de un servidor de red para el control y gestión de un acceso a internet compartido en un entorno mixto de red local privada y red pública inalámbrica.

El escenario de partida será una biblioteca pública de un municipio de 10000 habitantes, si bien la implementación es válida para multitud de escenarios similares como colegios o universidades.

Se realizará un estudio de los diversos requerimientos y condicionantes legales en un entorno de estas características, detallándose la configuración de la solución propuesta con un nivel de detalle que facilite su implantación en otras ubicaciones.

## 3.3. Contexto


La Biblioteca Pública Municipal de Sonseca está ubicada en la Casa de la Cultura, en ella se prestan los servicios típicos de las bibliotecas tradicionales como lectura de prensa y préstamo de libros y materiales audiovisuales. La gestión del préstamo y devolución se realiza a través de la aplicación web "Absysnet" que gestiona el acceso al Catalogo Colectivo de la Red de Bibliotecas de Castilla la Mancha, en el que la biblioteca se integró hace 5 años.

Los accesos a la aplicación de préstamo se realizan desde un PC situado en el mostrador principal de la biblioteca, existiendo además un equipo con acceso abierto a los usuarios. Ambos equipos ejecutan el sistema operativo Windows XP y están conectados por cable Internet a través de una línea ADSL.

En otras dependencias de la Casa de la Cultura se ubican entre otros la agente cultural, la radio municipal cuyos equipos están igualmente conectados a internet por cable a través de la misma línea ADSL.

Para simplificar el esquema de red nos centraremos en la parte de la biblioteca donde encontramos la siguiente infraestructura.

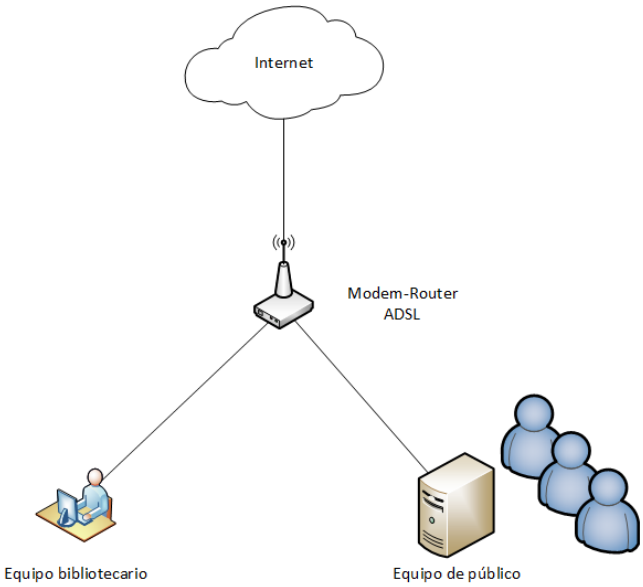



Ilustración 1 Esquema de partida de la red de la biblioteca

De manera experimental se prestó acceso WIFI a Internet usando el router como punto de acceso, pero el servicio se suspendió debido a:

- Ralentización en el acceso a la aplicación web de préstamo.
- Acceso a páginas web de contenido inadecuado por parte de algunos usuarios.

Tampoco se estaban teniendo en cuenta los aspectos legales de la prestación de un servicio público de acceso a Internet.

Si se quiere volver a prestar el acceso servicio WIFI habría que implementar mecanismos para solventar estos problemas a ser posible con un coste cero o mínimo.

La solución pasaría por añadir un equipo intermedio entre los equipos clientes el acceso a internet para poder controlar el uso del ancho de banda disponible y que cumpla con los requisitos necesarios en una instalación de estas características.

## 3.4. Justificación de proyecto.

La elección de un proyecto de estas características tiene como principal motivación la solución de un problema detectado en un entorno que me ha sido cercano en mis largas tardes de estudio en la Biblioteca Municipal.

Durante ese tiempo echaba de menos el disponer una conexión a internet que permitirá completar la información de los módulos de las distintas asignaturas

proporcionaban y acceder al Campus Virtual para realizar consultas a los tutores o exponer en los foros.

Más allá de del ámbito de la Biblioteca Municipal que sirve como punto de partida, espero que la guía de instalación que este documento pretende ser sirva de ayuda a alguien que un momento dado quiera poner en marcha un portal cautivo en algún entorno de acceso a Internet compartido.

Así quizás algún viejo ordenador que esté cogiendo polvo en un trastero prolongara su vida útil como servidor de red y esquivará por unos años el punto limpio de reciclaje.

### 3.5. Objetivos

El objetivo principal además de la solución del problema particular de la Biblioteca es general una documentación que recoja el proceso de instalación de un servidor de red que funcione sobre equipamiento teóricamente obsoleto. Se intentará dar un nivel de detalle suficiente acompañado de capturas de pantalla que permita reproducir y adaptar la configuración en un entorno de características similares.

Asimismo, en la última parte del proyecto se expondrá con un menor nivel de detalle las posibilidades de implantación de la solución en un entorno de múltiples zonas WIFI distribuidas a lo largo de un municipio.

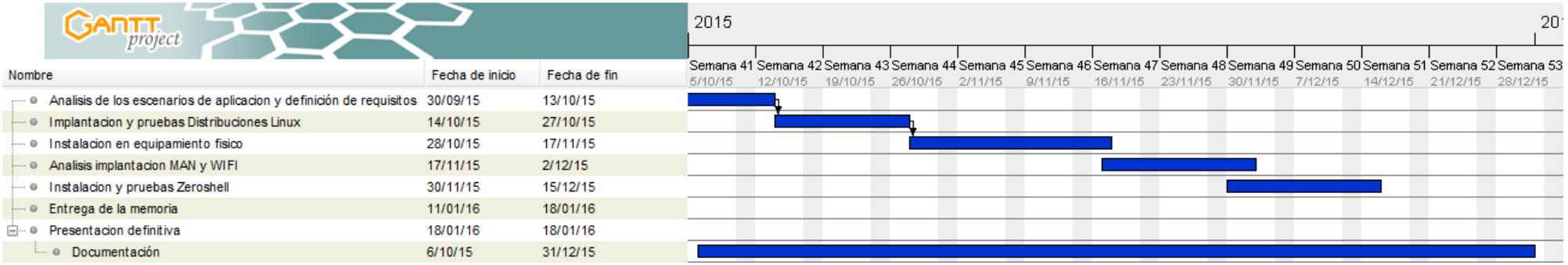
## 4. TAREAS Y PLANIFICACION

Las tareas desarrolladas se reflejan en la estructura del presente documento actual y se corresponden con:

- **Análisis del escenario de aplicación y definición de requisitos:** Se realizará un análisis detallado del escenario de trabajo, detallando los requisitos a cumplir para validar la solución propuesta.
- **Estudio de alternativas.** En base a la información recopilada se realizará un estudio de las alternativas disponible para llevar a cabo la implantación del servidor de red.
- **Diseño de la solución.** En este apartado plasmaremos en un esquema de alto nivel la solución propuesta.
- **Implementación práctica.:** Se implantará la solución propuesta en un equipo físico, detallándose el proceso de configuración de sistema con un nivel de detalle que permita reproducir la solución en un escenario similar.
- **Comprobación de requisitos:** Validación de la solución en base al cumplimiento de los requisitos planteados.

- **Documentación:** En la medida de lo posible la redacción de la memoria se realizará en paralelo al resto de tareas par que la documentación plasme de manera fidedigna las labores realizadas.

En el siguiente diagrama de Gantt se recoge la lista de tareas y sus fechas límite.




| Nombre | Fecha de inicio | Fecha de fin |
|---|---|---|
| Analisis de los escenarios de aplicacion y definición de requisitos | 30/09/15 | 13/10/15 |
| Implantacion y pruebas Distribuciones Linux | 14/10/15 | 27/10/15 |
| Instalacion en equipamiento fisico | 28/10/15 | 17/11/15 |
| Analisis implantacion MAN y WIFI | 17/11/15 | 2/12/15 |
| Instalacion y pruebas Zeroshell | 30/11/15 | 15/12/15 |
| Entrega de la memoria | 11/01/16 | 18/01/16 |
| Presentacion definitiva | 18/01/16 | 18/01/16 |
| Documentación | 6/10/15 | 31/12/15 |

# 5. Desarrollo del proyecto

## 5.1. Requisitos del sistema:

### 5.1.1. Requisitos legales

En función del tipo de servicio de acceso inalámbrico a Internet que se quiera prestar las implicaciones y requisitos legales varían.

En España, la CMT (Comisión del Mercado de las Telecomunicaciones) es el órgano que regula las condiciones legales para instalar redes WIFI municipales, siendo la principal norma regulatoria la **Circular 1/2010, de 15 de junio de 2010, de la Comisión del Mercado de las Telecomunicaciones**, por la que se regulan las condiciones de explotación de redes y la prestación de servicios de comunicaciones electrónicas por la Administraciones Públicas.

En dicha circular se definen tres escenarios de aplicación:

**Autoprestación:**

- Servicio prestado a los trabajadores de la administración que ofrece el servicio.
- Bibliotecas.
- Centros educativos.

**Acceso a Internet limitado (no afecta a la libre competencia):**

- Ancho de banda limitado a 256 kbps.
- Implantación en zonas de uso residencial o mixto.
- Acceso limitado a páginas institucionales.

**Acceso sin restricciones**

En nuestro caso se trataría de un modelo de auto prestación definido en el punto 6 del anexo de la circular antes mencionada

*"No obstante tratarse de prestación a terceros, se considera aplicable el régimen de la auto prestación y, por tanto, se excluye la obligatoriedad de notificación a la Comisión del Mercado de las Telecomunicaciones y de inscripción en el Registro de operadores del servicio general de acceso a Internet en bibliotecas. Y ello habida cuenta de i) la evidente vinculación del servicio de acceso a Internet prestado en las bibliotecas con los fines de promoción de la cultura y el conocimiento que le son propios, teniendo las bibliotecas como obligación legal específica suministrar el*

*servicio de acceso a la información a través de Internet al disponer la Ley 10/2007, de 22 de junio, de la lectura, del libro y de las bibliotecas en el artículo 13, apartado 4 que «4. Se consideran servicios básicos de toda biblioteca pública los siguientes: (...) d) Acceso a la información digital a través de Internet o las redes análogas que se pueden desarrollar, así como la formación para su mejor manejo»; ii) el servicio resulta indispensable para cumplir sus fines y siempre que los usuarios acrediten su vinculación con el servicio mediante algún documento que permita su identificación; iii) la nula incidencia en el mercado que, por ello, tiene el servicio de acceso a Internet prestado desde las bibliotecas."*

Al encuadrase dentro de este tipo de servicio (autoprestación) estaríamos eximidos de la notificación a la CMT e inscripción en el registro de operadores. No obstante, la misma circular define unos principios generales de actuación en el punto 4.4

*Sin perjuicio de lo señalado en los párrafos anteriores, las Administraciones Públicas, en el desarrollo de su actividad como operadores de comunicaciones electrónicas, estarán sujetas al cumplimiento de las mismas obligaciones que los operadores privados de redes y servicios de comunicaciones electrónicas para lo que, deberán garantizar, entre otras, el cumplimiento de sus obligaciones en materia de protección de los datos personales y de la intimidad de las personas, los derechos de los usuarios, la interoperabilidad de los servicios, las obligaciones de calidad de servicio, el secreto de las comunicaciones e interceptación de las comunicaciones electrónicas en los supuestos legales establecidos, así como las de conservación de datos previstas en la Ley 25/2007 de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.*

Esto añadiría entre otras obligaciones la de conservar un registro de las comunicaciones desde nuestra red durante al menos un año según la Ley 25/2007, de 18 de octubre (transposición Directiva 24/2006), de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, esto supone que la Administración a cargo de la red tiene que conservar datos para identificar: origen, destino, fecha, hora y duración, tipo, equipo de comunicación y localización del equipo. Por esta razón es necesario identificar a los usuarios que hacen uso de nuestra red, registrando a los usuarios y almacenando las direcciones IP que utilizan y las direcciones IP a las que se han conectado durante un año.

Ya tenemos por tanto los primeros requisitos:

**Identificación de usuarios:** debemos recabar información de los usuarios que usen el servicio.

Esto se conseguiría mediante la implementación de un *portal cautivo*, un servicio de red que intercepta el tráfico de salida a Internet de los equipos de una red redirigiendo sus peticiones HTTP hacia un formulario donde deben validarse con un usuario y

contraseña para poder seguir navegando. Es en el proceso asignación de usuario/contraseña cuando el usuario se identificarse fehacientemente ante los gestores del servicio (los bibliotecarios) y se le dará de alta en el sistema para poder usar el servicio.

**Registro de conexiones:** hay que implementar algún sistema que mantenga un registro de las conexiones realizadas desde nuestra red y facilite esa información a las autoridades en caso de que exista un requerimiento legal.

### 5.1.2. Requisitos técnicos.

Además de los requisitos legales, nuestro sistema deberá implementar una serie de funcionalidades enfocadas en dos vertientes:

1. Evitar los problemas detectados durante la prestación experimental del servicio (véase punto 4.1):
    a. **Filtrado de contenidos:** Controlar el uso inadecuado de ancho de banda mediante un sistema filtrado.
    b. **Calidad de servicio:** Implementar medidas para poder priorizar el tráfico de los bibliotecarios sobre el de los usuarios.

2. Proveer servicios de red adicionales que faciliten la conexión de los usuarios a la red sin necesitad de unos conocimientos técnicos específicos.
    a. **Servicio DNS:** para la resolución de nombres (función antes realizada por el router)
    **b. Servicio DHCP:** esta función la realizaba igualmente el router y ahora la proporcionara el servidor de red.
    c. **Servidor proxy transparente:** Implementación de un servidor proxy en modo transparente que permita un registro de uso sin que el usuario tenga que modificar la configuración de su equipo.

3. Funcionalidades adicionales opcionales:
    **a. Implementación de antivirus en el servidor proxy:** para evitar la descarga de virus y software malicioso en los equipos que navegan por nuestra red.
    **b. Soporte de múltiples puertas de acceso a internet con tolerancia a fallos y balanceo de carga:** de esta forma podríamos aumentar el ancho de banda de nuestra salida a internet con la contratación de

líneas ADSL adicionales (no existe despliegue de fibra en la localidad).

c. **Soporte de Vlan 802.11q**: para permitir segmentación de tráfico en un mismo interfaz físico de cara a una implementación más compleja de nuestra solución.

## 5.2. Estudio de alternativas

La implementación completa con dispositivos hardware de una solución de acceso Internet compartido como la que estamos intentando modelar se compondría de los siguientes elementos:

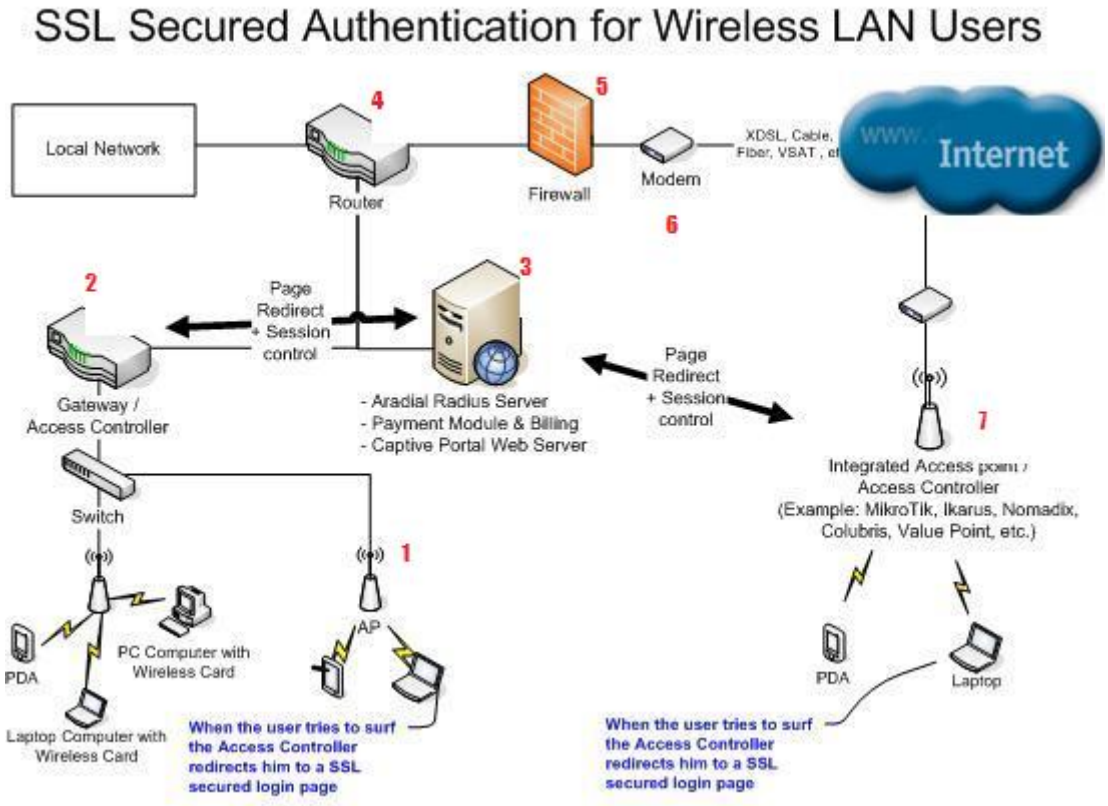



**Ilustración 2 Arquitectura de red completa para entornos corporativos[1].**

1. Los puntos de acceso inalámbrico que sirven de enlace entre la red WIFI y la red cableada.
2. Gateway/controlador de acceso que impide el acceso a la red de usuarios no validados, cuyas peticiones HTTP redirige al portal cautivo.

[1] http://www.wifi-billing.com/images/HotspotNetwork-sm.jpg

3. El portal cautivo que integra el formulario de validación, el módulo de registro de usuarios.
4. El router que separaría la red interna, la red inalámbrica y el acceso a Internet
5. El firewall que protegería nuestra red de los accesos del exterior y limita el tráfico de salida no deseado.
6. El modem/router ADSL.
7. Alternativamente cabe la posibilidad de implementar un punto de acceso que integre el controlador de acceso.

En nuestro caso para simplificar concentraremos en el mismo dispositivo las funciones de

- Gateway
- Portal cautivo
- Router
- Firewall

Nuestro esquema de red por tanto quedará así:

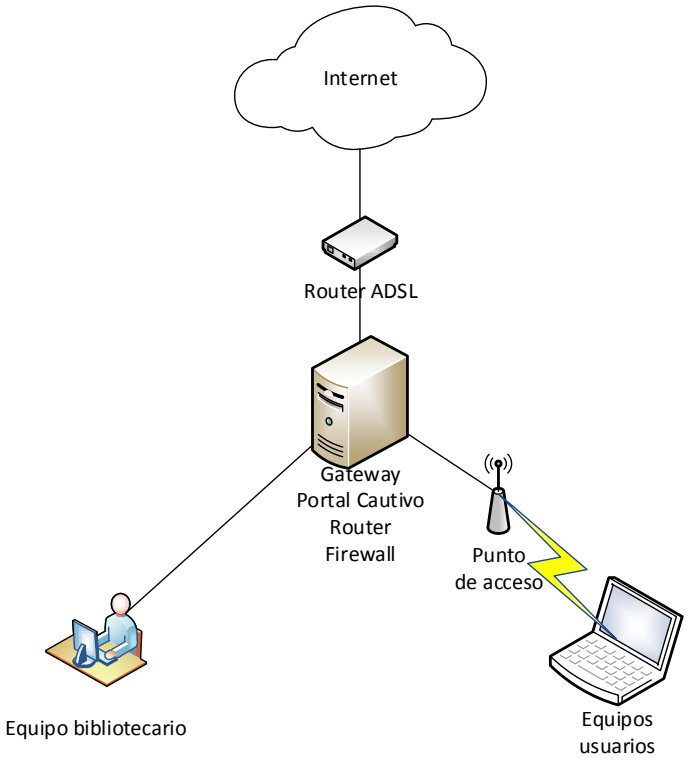



**Ilustración 3: Arquitectura de red propuesta para la biblioteca**

Se trataría por tanto de buscar un sistema capaz aglutinar los elementos de red antes mencionados con un coste mínimo mediante el uso de un software que pudiera correr sobre algún sistema pc antiguo.

Tras realizar un proceso de búsqueda por Internet usando los términos de los servicios que queremos implementar (router, firewall, portal cautivo) encontramos dos posibles candidatos: pfSense y Zeroshell

### 5.2.1. pfSense (www.pfsense.org)

Se trata de un derivado de FreeBSD adaptado para dar servicios de red.

Disponible en versión appliance[2] cuenta también con una versión gratuita (Community Edition) que dispone entre otras de las siguientes funcionalidades[3]:

- Firewall with stateful packet inspection
- NAT (Port Forwards, 1:1 NAT, Outbound NAT, NPt)
- Multi-WAN Support
- Dynamic DNS
- Captive Portal
- DHCP Server and Relay (IPv4 and IPv6)
- Virtual interfaces for VLAN, LAGG/LACP, GIF, GRE, PPPoE/PPTP/L2TP/PPP WANs, QinQ, and Bridges
- Caching DNS Forwarder/Resolver
- Proxy Server (using packages)

### 5.2.2. Zeroshell (www.zeroshell.org)

Se trata de una distribución Linux para servidores y dispositivos integrados destinados a proporcionar los principales servicios de red que una LAN necesita. Está disponible en forma de Live CD o de imagen de Compact Flash. Como su propio nombre indica su administración se realiza desde un interfaz web sin acceder a la línea de comandos.

En la página web del proyecto está disponible la lista de características[4] entre las que destacamos.

---

[2] A **computer appliance** is generally a separate and discrete hardware device with integrated software (firmware), specifically designed to provide a specific computing resource

[3] https://doc.pfsense.org/index.php/Features_List

- **Portal Cautivo** para el inicio de sesión web, en redes cableadas e inalámbricas. Zeroshell actúa como puerta de enlace de las redes en la que el portal cautivo está activo y en la que las direcciones IP (por lo general pertenecientes a las subredes privadas) son asignados dinámicamente por el servidor DHCP. Un cliente que tiene acceso a esta red privada debe autenticarse a través de un navegador web con un usuario y contraseña antes de que el firewall del Zeroshell le permita el acceso a la red.

- **Gestion QoS (Calidad de servicio)** para controlar el tráfico en una red congestionada. Se podrá garantizar el ancho de banda mínimo, limitar el ancho de banda máximo y asignar una prioridad a una clase de tráfico (útil en aplicaciones de red sensibles a la latencia como VoIP). El ajuste anterior se puede aplicar en interfaces Ethernet, redes privadas virtuales, bridges y bondings VPN. Es posible clasificar el tráfico mediante el uso de filtros de nivel 7 que permitan la inspección profunda de paquetes (DPI), que puede ser útil para dar forma a las aplicaciones de VoIP y P2P.

- **Servidor proxy HTTP** que es capaz de bloquear las páginas web que contienen virus. Esta característica se implementa con la solución antivirus ClamAV y el servidor proxy HAVP. El servidor proxy trabaja en modo proxy *transparente* de tal forma que no es necesario configurar los navegadores de los usuarios ya que las peticiones http serán redirigidas automáticamente.

- **LAN virtual 802.1Q** (VLAN etiquetado).
- **Firewall** con Packet Filter y Stateful Packet Inspection (SPI) con filtros aplicables en todo tipo de interfaces, incluyendo VPN y VLAN.

- **NAT** para utilizar la red LAN clase de direcciones privadas ocultas en la WAN con direcciones públicas.

- **Equilibrio de carga y conmutación por error** de varias conexiones a Internet.

[4] http://www.zeroshell.org/

### 5.2.3. Elección de una solución

Las características comunes a ambas soluciones se recogen en la siguiente tabla:

| | Firewall nivel7 | Router | HTTP Proxy con antivirus | Multiple Gateway | Captive Portal | Filtrado de contenidos | Qos | Virtual LAN 802.1Q | Tolerancia a fallos |
|---|---|---|---|---|---|---|---|---|---|
| FPSense | si | si | si | si | si | si | si | si | si |
| Zeroshell | Si | si | si | si | si | si | si | si | si |

A la vista de la comparativa tanto FPSense como Zeroshell parecen soluciones adecuadas para nuestro propositivo, nos decantaremos por esta última por las siguientes razones:

- **Es un derivado Linux:** al contrario que fpSense que deriva de FreeBSD, se trata por tanto de un sistema operativo con el que a priori estaríamos más familiarizados en caso de tener que realizar alguna actuación a bajo nivel (programación de scripts, acceso por línea de comandos)
- **Compatibilidad hardware:** al tratarse de un derivado Linux la compatibilidad hardware estará garantizada
- **Documentación:** amplia documentación en castellano disponible en su página oficial.

## 5.3. Implantación de la solución propuesta.

Para demostrar la funcionalidad de múltiples puertas de enlace (gateways) a la arquitectura de red predefinida le añadimos un segundo router.

En el laboratorio físico usaremos módems-router de los instalados por Movistar, uno de ellos da servicio a través de ADSL y el segundo mediante un enlace 3G. En ambos router se deshabilita el acceso WIFI, que se ofrecerá a través de un punto de acceso configurado de forma trasparente (acceso abierto sin autenticación y sin servicio DHCP)

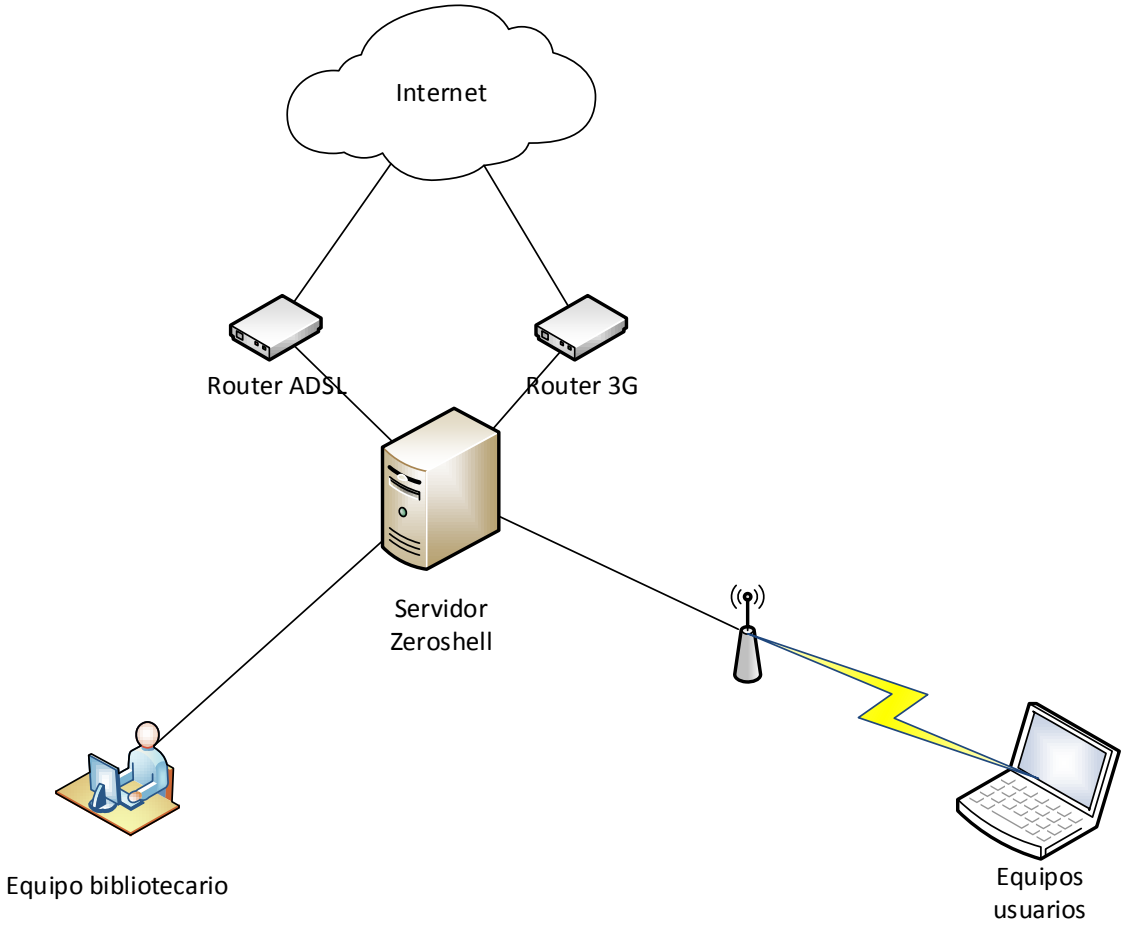



**Ilustración 4: Arquitectura de red con Zeroshell y múltiples gateways.**

Comenzamos a continuación el proceso de instalación sobre el equipo de laboratorio.

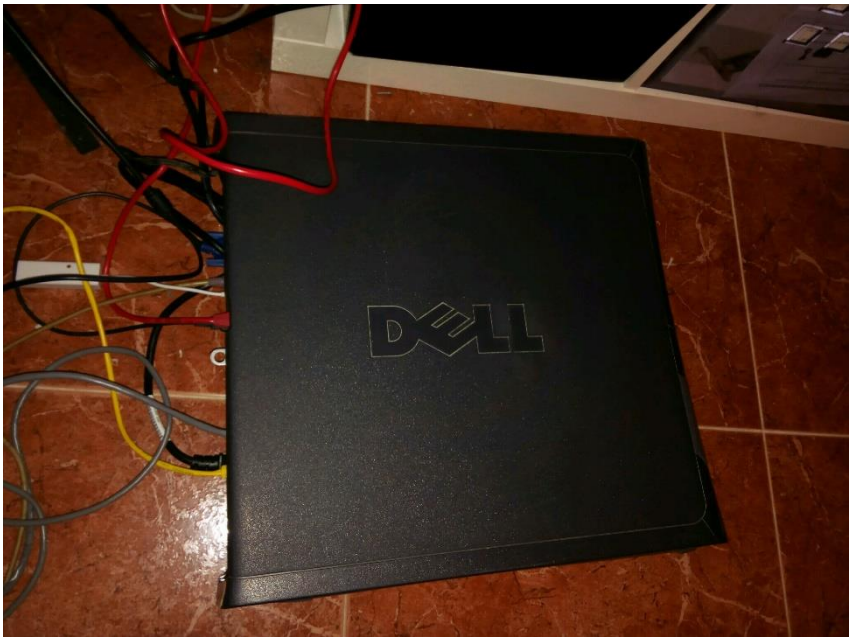
### 5.3.1. Instalación

Para la puesta en marcha de la solución propuesta se ha usado un equipo antiguo que nos permitirá demostrar las posibilidades que equipamiento a priori obsoleto puede ofrecernos. Es evidente que, si conseguimos un funcionamiento adecuado en una plataforma de estas características, el rendimiento en equipos más modernos será mucho más fluido.

Se trata de un del Optiplex GX270 con más de 10 años de antigüedad y la siguiente configuración:

- Procesador Pentium IV a 2.8 Ghz
- 1GB de RAM

- 40 GB de disco duro
- 4 interfaces de red: (1 integrado, 2 en tarjetas PCI y uno en adaptador USB-Ethernet)




En primer lugar, conectaremos el interfaz de red integrado en la placa base del PC que será detectado como ETH0 al router ADSL donde también tendremos conectado nuestro PC siguiendo el siguiente esquema.

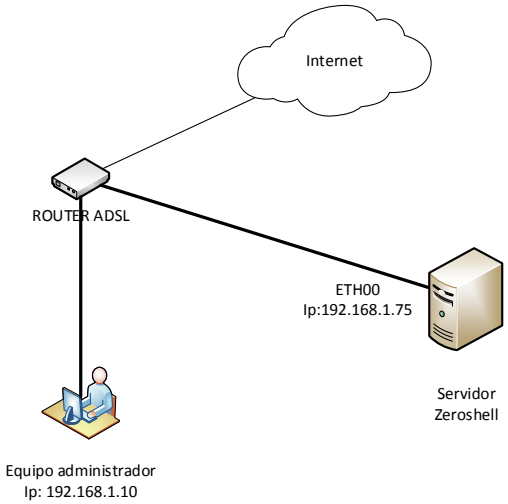
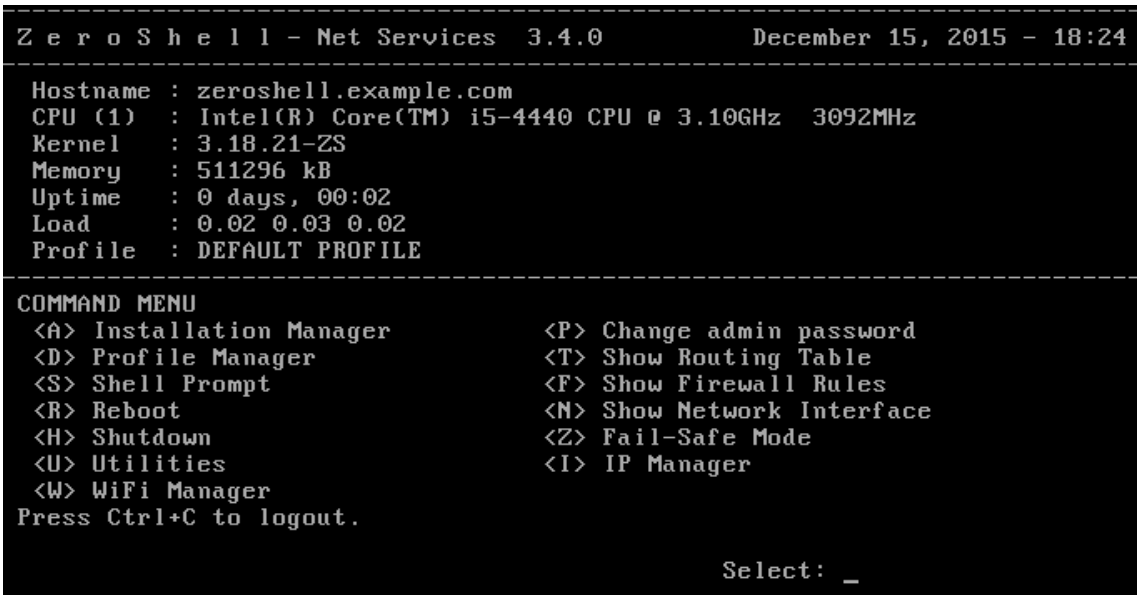



**Ilustración 5 Conexión inicial para la configuración.**

Descargamos la imagen ISO de la versión 3.4.0 "*Install/Live CD*" desde http://www.zeroshell.org/download/, y arrancaremos el equipo desde el CDROM donde previamente habremos grabado la ISO.

Una vez al arranque el equipo tendremos disponible el menú de configuración en modo consola.




Seleccionamos la opción

<I> IP Manager

A continuación, configuramos una dirección IP de nuestra red en la interface ETH0 para así poder acceder al portal web de administración, en nuestro caso la red del router ADSL es una 192.168.1.0/24, configuraremos por tanto el interface con las siguientes opciones:

- IP: 192.168.1.75
- MASCARA DE RED: 255.255.255.0
- GATEWAY DE SALIDA: 192.168.1.1

Volvemos al menú principal y mediante la opción

<A> Installation Manager

Instalamos el sistema en el disco duro y reiniciamos, tras lo cual podremos acceder al interfaz gráfico en la dirección https://192.168.1.75 donde nos logaremos con el usuario/contraseña por defecto *admin/zeroshell*.

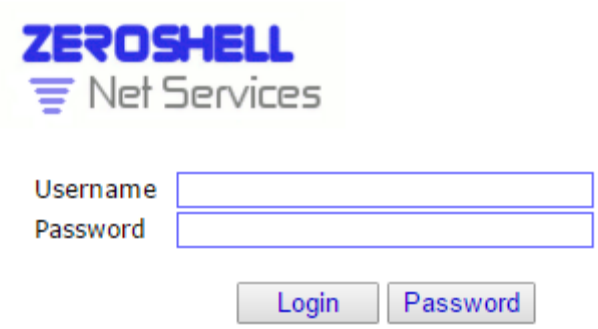



Ilustración 6: Pantalla de login de Zeroshell

### 5.3.2. El interfaz web de Zeroshell


Ilustración 7: El interfaz web de Zeroshll

El interfaz web de administración de zeroshell se divide en 3 partes:

- **Barra de de estado:** Muestra información de estado del sistema como la carga de la cpu, conexiones, uptime, etc. Incluye acceso a los comandos de logout, reinicio del sistema y apagado del servidor.
- **Menú de navegación:** Situado en el lateral izquierdo, permite seleccionar las distintas áreas de configuración del sistema.
- **Menú de configuración:** Acceso al menú especifico de configuración del apartado previamente seleccionado en el menú de navegación.

Durante el resto del documento usaremos la siguiente nomenclatura para señalar la parte del interfaz donde se realiza una configuración concreta.

***Menu>Submenu>pestaña***

Donde **Menu** se refiere a un grupo de opciones del menú de navegación, **Submenu** a una opción dentro de un grupo y **pestaña** a una opción del menú de configuración especifico.

En el caso del acceso a la opción de gestión de perfiles (profiles) ***System>Setup>Profiles***: pulsaríamos en la opción *Setup* del grupo *System*, y a continuación en la pestaña *Profiles* del menú de configuración.

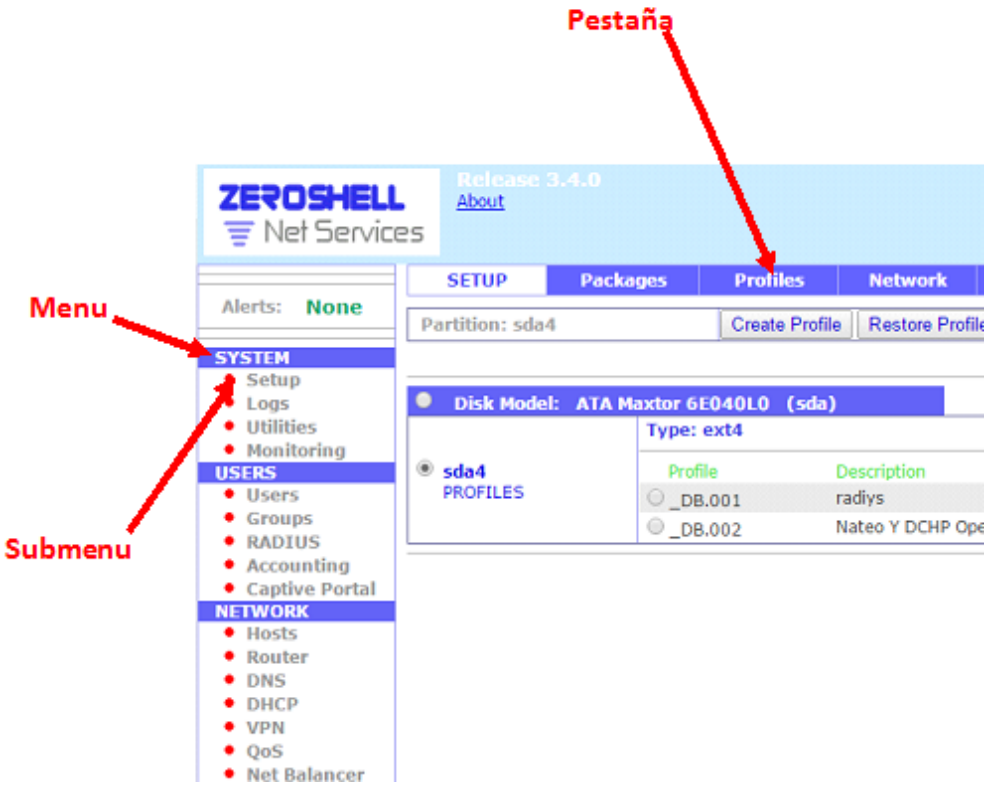
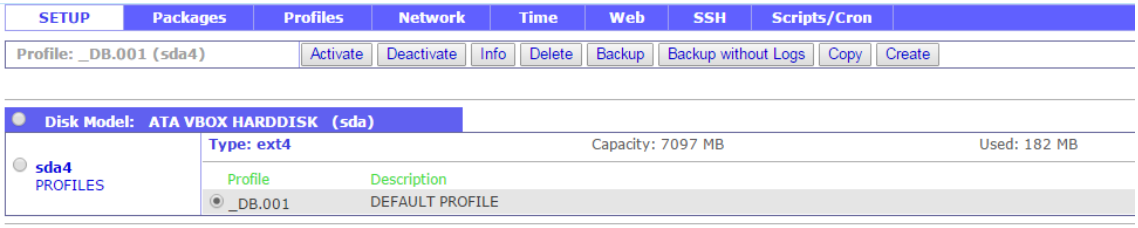



**Ilustración 8: Detalle de la nomenclatura del acceso a menús.**

### 5.3.3. Creación de un perfil

**Zeroshell** permite mantener distintos perfiles (profiles), de tal forma que podemos alternar entre varias configuraciones, o hacer una copia de seguridad las opciones actuales del sistema que nos permita volver atrás en caso de cometer algún error en la personalización de la plataforma.

Lo primero que haremos en nuestro primer acceso será crear un nuevo perfil diferenciado de la inicial (default profile) a través del menú ***System>Setup>Profiles:***




Seleccionamos la partición del disco duro donde queremos guardar la configuración (en caso de que haya varias), seleccionamos crear, y activamos la configuración, tras lo cual se reiniciará el sistema. En este paso es importante tener en cuenta que con cada perfil se guarda la contraseña de administrador que habrá que recordar para evitar perder el acceso a la configuración del sistema.

### 5.3.4. Configuración de los interfaces de red

Desde el menú ***System>Setup>Network*** veremos los 4 interfaces, que configuraremos con su direccionamiento IP correspondiente. Para ello seleccionamos cada interfaz (ETH0X) y pulsamos el botón "Add IP"

La configuración inicial que realizamos será la siguiente:


**Ilustración 9: Configuración inicial de los interfaces de red.**

- ETH00 (cable rojo):
  - Gateway principal
  - Conectada al Router ADSL (IP 192.168.1.1)
  - IP 192.168.1.75/255.255.255.0

- ETH01 (cable azul):
  - Conexión de red Pública.
  - IP 172.16.31.1/255.255.255.0
- ETH02 (cable gris):
  - Conexión de red interna.
  - IP 10.24.7.1/255.255.255.0
  -
- ETH03 (cable amarillo):
  - Gateway secundario
  - Conectada al router 3G (IP 192.168.2.1)
  - IP 192.168.2.75/255.255.255.0

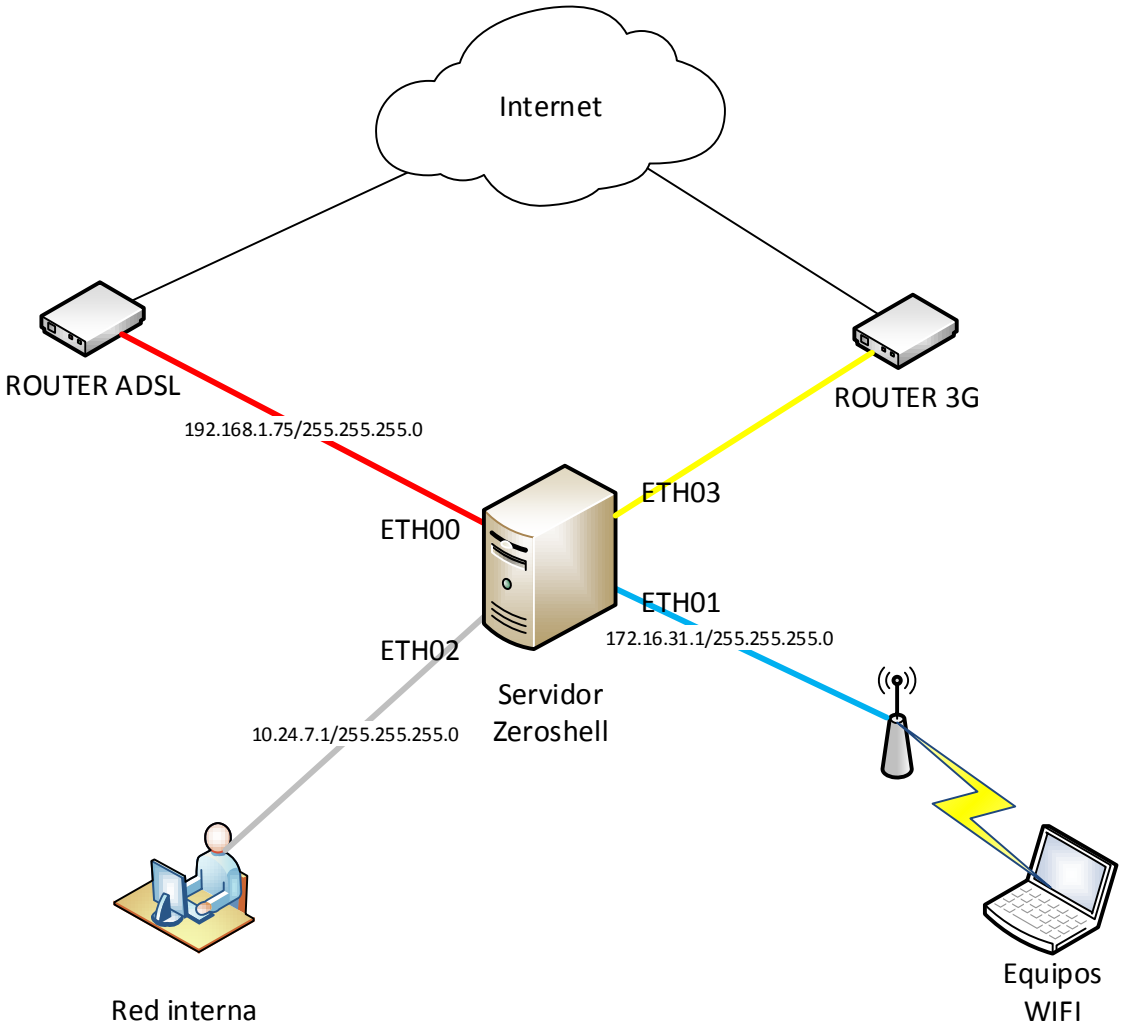



Ilustración 10: Esquema inicial de las conexiones.

Desde el menú ***Setup>Network>Gateway*** comprobamos que la configuración del Gateway de salida corresponde conla IP del router ADSL.

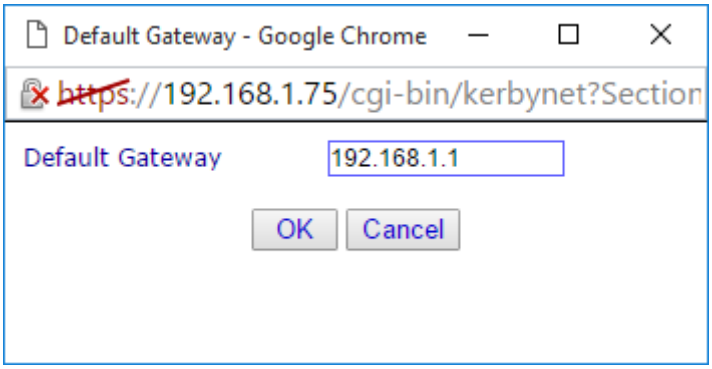



**Ilustración 11: Configuración del Gateway**

### 5.3.5. Configuración DHCP

Una vez tengamos configurados los interfaces de red habremos de ajustar la configuración DHCP[5] , de esta forma los equipos que de la red WIFI recibirán los parámetros de configuración de red de manera automática y podremos llevar un registro la asociación MAC-IP de los equipos que acceden a nuestra red.

Esta configuración se aplicará solo a la red WIFI, puesto que los equipos de la red interna al ser pocos y conocidos dispondrán de IP fija que nos permitirá identificarlos con facilidad.

Usaremos la red de privada[6] de clase B **172.16.31.0/12** que nos permitirá tener un máximo de 253 host con un rango de direcciones (172.16.31.2 - 172.16.31.254) si excluimos la 172.16.31.1 está usada por interfaz ETH01,

Asimismo, en el proceso de concesión de direcciones IP, se configurará el Gateway y servidor DNS por defecto y que será la IP antes mencionada del ETH01 172.16.31.1.

Para llevarlo a cabo accedemos al menú ***Network>DCHP>Manage*** y a través de la opción *New* añadimos un nuevo intervalo DHCP para el interfaz ETH01.

[5] DHCP: En castellano «protocolo de configuración dinámica de host») es un protocolo de red que permite a los clientes de una red IP, obtener los parámetros de configuración automáticamente.
[6] Red privada: Red de computadoras que usa un espacio de direcciones IP solo válido a nivel interno.

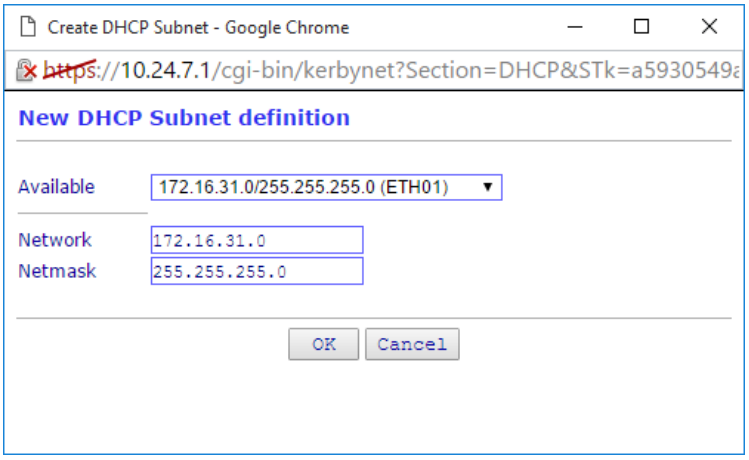



Ilustración 12: Definicion de subred DHCP

Con el rango de direcciones disponibles siguiente:

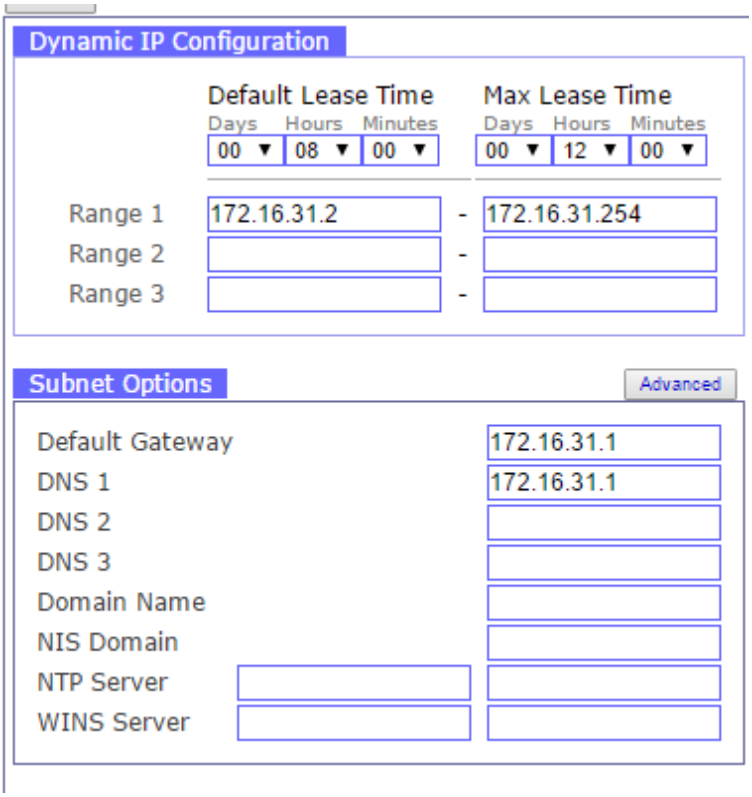



Ilustración 13: Definición del rango de direcciónes.

### 5.3.6. Configuración servidor DNS.

Como hemos mencionado en el punto anterior los clientes recibirán durante el proceso de configuración DHCP, las opciones de servidor DNS que corresponderán con la IP que el propio servidor Zeroshell tiene en la red WIFI (172.16.31.1).

Nuestro servidor DNS llevará a cabo la resolución de las direcciones locales que los clientes soliciten, y reenviara a servidores externos las peticiones de resolución de nombre dominios externos (la gran mayoría) esos servidores externos se denominan forwarders.

Los servidores externos que usaremos serán los del servicio *Family Shield*[7] de OPENDNS (208.67.222.123 y 208.67.220.123), estos servidores realizan un filtrado de la resolución DNS de dominios correspondiente a páginas pornográficas, de contenido sexual, violento así como de los proxys externos que los usuarios pudieran usar para saltarse las restricciones de navegación.

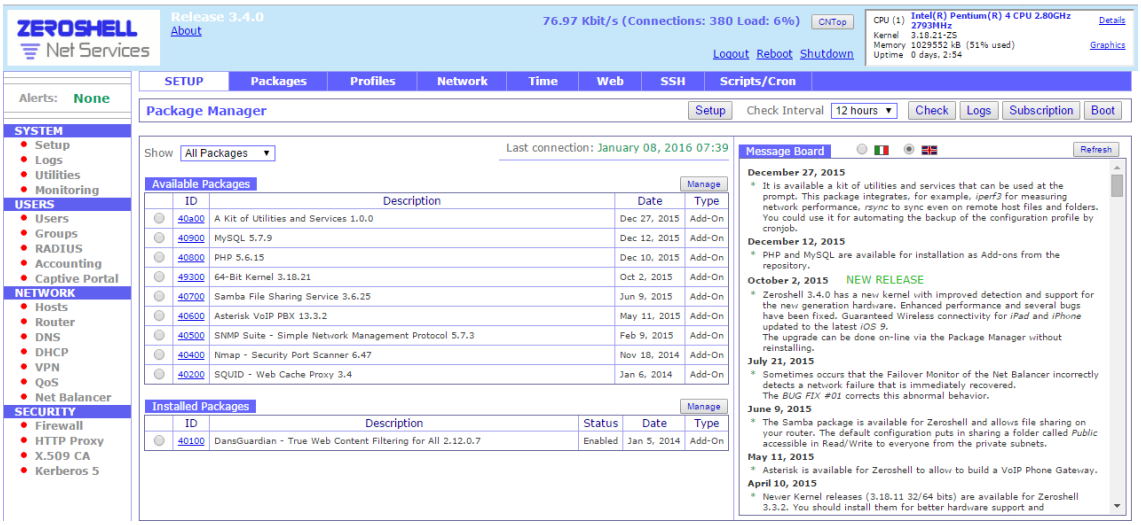
De esta forma conseguimos eliminar de un plumazo gran parte del tráfico inadecuado, cumpliendo con uno de los requisitos propuestos.

Realizamos la configuración mediante la opción del menú ***Network>DNS>Forwarders*** añadiendo en el campo *Domain* "ANY" y en el campo *Server* las direcciones de los dos servidores separados por comas.


**Ilustración 14: Configuración de los DNS forwarders**

[7] https://store.opendns.com/setup/#/familyshield

Si todo ha ido bien podremos comprobar que el servidor accede a Internet desde el menú ***System>setup*** donde veremos como el panel de mensajes (message board) se actualiza con la información del desarrollo de nuevas funcionalidades de Zeroshell.




## 5.3.7. Configuración (NAT)

A continuación, pasaremos a configura la opción de traducción de direcciones de red o NAT (del inglés Network Address Translation), que permitirá que los equipos de nuestra red que tienen direccionamiento del ámbito privado, puedan comunicarse con equipos de Internet con direccionamiento público.

Este tipo de conexiones son posibles gracias a un router (implementado mediante software en este caso) que se encarga de intercambiar paquetes realizando la traducción de direcciones entre dos redes con direccionamiento mutuamente incompatible.

Desde la opción *Network>Router>NAT* seleccionamos los interfaces de red que cuyo tráfico de salida será "traducido", en nuestro caso seleccionamos nuestros gateways de salida "ETH00" y "ETH03" de entre los interfaces disponibles y pulsamos ">>>" para añadirlo a los interfaces NATeados ("NAT Enabled Interfaces") y pulsamos el botón "Save".

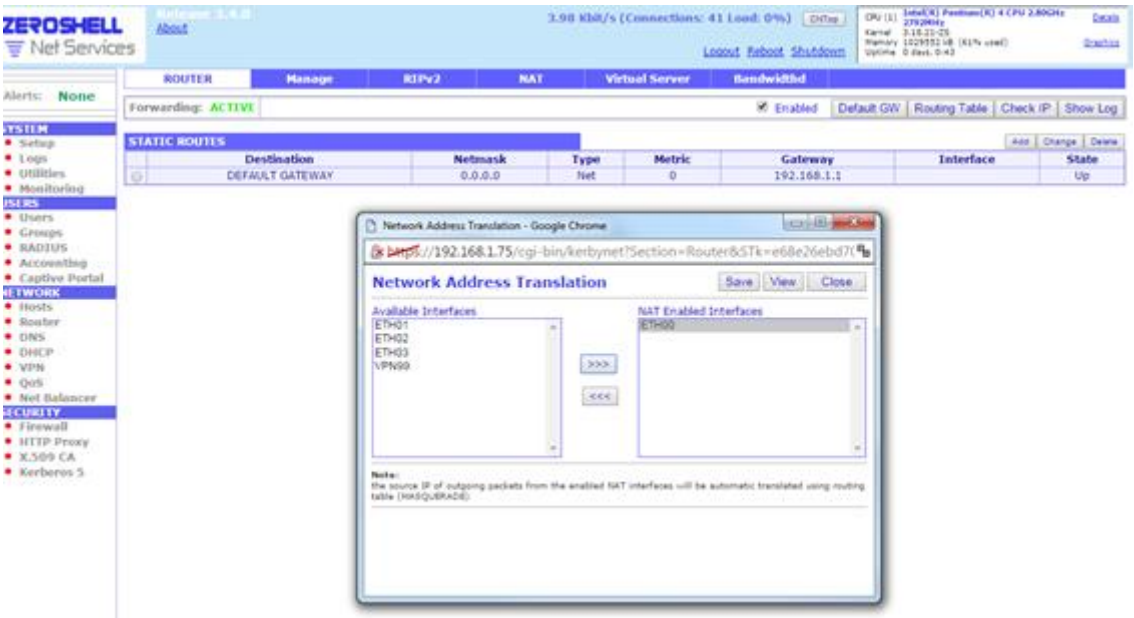



Ilustración 15: Configuración NAT

Si bien, con el solo uso del proxy transparente sería suficiente para que los usuarios pudieran navegar, es necesario activar esta opción para permitir el tráfico HTTPS que de otra forma no funcionarían dado que al no tener la clave privada del servidor Web, no se puede descifrar el contenido y la URL de esta petición que es encapsulada en los túneles de cifrado.

### 5.3.8. Pruebas de la configuración básica de red.

Llegados a este punto, dispondremos de una configuración básica de red que nos permitirá navegar con la limitación del filtrado de nombres DNS.

Realizamos la prueba conectando un equipo con sistema operativo Windows 7 al interfaz ETH01 (red WIFI), cabe señalar queel interfaz de red del equipo cliente tiene seleccionada la configuración automática.

Desde la línea de comandos ejecutando el comando ***ipconfig*** y comprobamos que efectiva el direccionamiento asignado se corresponde con el intervalo DHCP configurado.

```
C:\Users\yomismo>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::282d:693b:b8dd:4840%2
   Dirección IPv4. . . . . . . . . . . . . . : 172.16.31.14
   Máscara de subred . . . . . . . . . . . . : 255.255.0.0
   Puerta de enlace predeterminada . . . . . : 172.16.31.1
```

**Ilustración 16: Configuración IP recibida por nuestro equipo.**

Pasamos a comprobamos la configuración de DNS mediante el comando ***nslookup.***

```
C:\Users\yomismo>nslookup
Servidor predeterminado:  UnKnown
Address:  172.16.31.1
```

**Ilustración 17: Comprobación del servidor DNS asignado.**

La configuración es correcta, y tenemos como servidor DNS principal y único la dirección del interfaz ETH01 del servidor Zeroshell

Lo siguiente que verificamos es la conexión con un host de Internet haciendo un ping a www.as.com y viendo que hay respuesta.

```
C:\Users\yomismo>ping  www.as.com

Haciendo ping a a579.g.akamai.net [185.43.182.58] con 32 bytes de datos:
Respuesta desde 185.43.182.58: bytes=32 tiempo=40ms TTL=59
Respuesta desde 185.43.182.58: bytes=32 tiempo=41ms TTL=59
Respuesta desde 185.43.182.58: bytes=32 tiempo=40ms TTL=59
```

**Ilustración 18: Prueba de conectividad contra un host de Internet.**

Comprobamos la navegación, y el filtrado DNS probando la siguiente url en nuestro navegador www.plaboy.com .

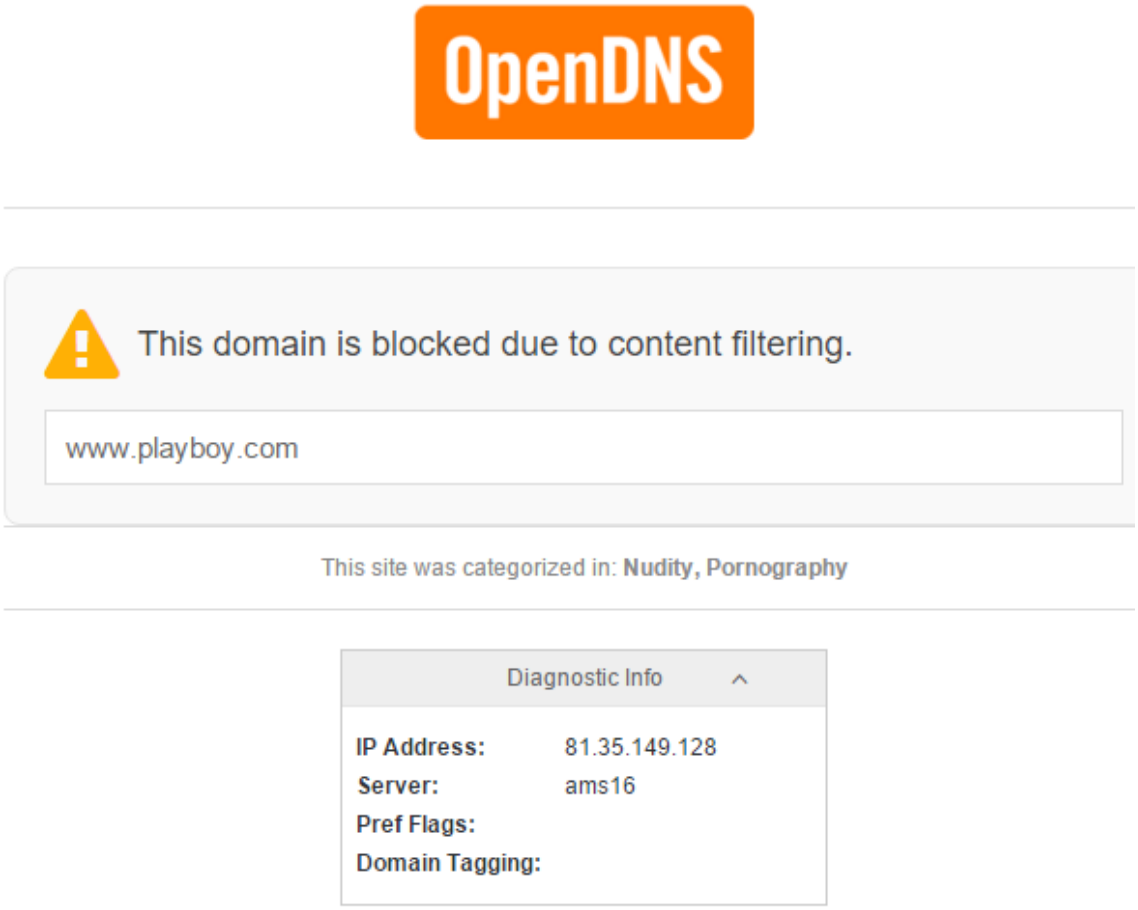



Ilustración 17: Prueba del filtrado de OPENDNS Family Shield

Observamos que la respuesta es la página genérica de bloqueo del DNS de Family Shield por lo tanto la conexión a Internet desde la red pública está funcionado

### 5.3.9. Configuración de la calidad de servicio "Qos"

Una vez comprobado que la conexión a Internet esta funcionado, toca configurar los parámetros de "**Qos" (**calidad de servicio) , que nos permitirá priorizar el tráfico de la red interna sobre el de la red pública WIFI.

Nos interesa particularmente que los equipos que usan los bibliotecarios para realizar conectarse a aplicación web absysnet, dispongan de un ancho de banda mínimo garantizado que impida que el previsible uso exhaustivo de la navegación de los equipos de la red WIFI, ralentice el proceso de préstamo y devolución de materiales.

El ancho de banda de descarga teórico para la línea ADSL de salida será de aprox. 8 Mib/s. Dividiremos esta capacidad entre los distintos interfaces a través de la opción Global Bandwidth del menú ***Network>Qos>Interface manager***, el ancho de banda asignado será el siguiente.

- **Red pública ETH1:**
  - Máximo 6 Mbit/s
  - Garantizado 3 Mbit/s
- **Red interna ETH0**
  - Máximo 8 Mbit/s
  - Garantizado 6 Mbit/s

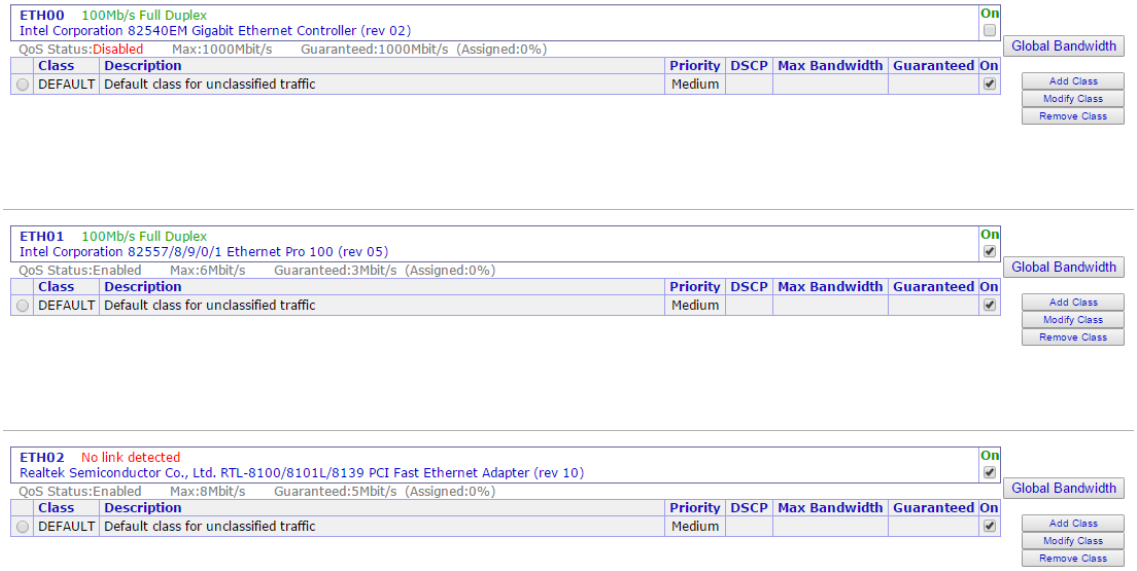



**Ilustración 19: Configuracion del ancho de banda por interfaz.**

Hay que tener en cuenta que el límite de velocidad se refiere a trafico saliente de los interfaces del servidor Zeroshell (la velocidad máxima de descarga que tendrán disponibles los equipos clientes).

Realizamos un test de velocidad antes y después de aplicar los parámetros de calidad de servicio que devuelve unos resultados acordes a lo esperado, descarga de 8374 kbps antes de la aplicación de la calidad de servicio y 5753 kbps después.

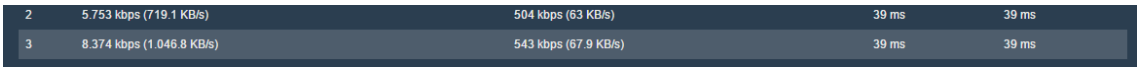



Ilustración 20: Prueba de velocidad con y sin la calidad de servicio activada.

### 5.3.10. Configuración portal cautivo

El uso del portal cautivo cumple con la función de identificación de usuarios que marca la ley en un servicio de estas características. Cualquier sesión de navegación será redirigida hacia el formulario de autenticación hasta que el usuario introduzca sus credenciales.

Para su puesta en marcha accedemos a ***Users>Captive Portal>Gateway*** para a continuación seleccionar el interfaz de red donde queremos que esté activo el portal cautivo, en nuestro caso es el EHT01.

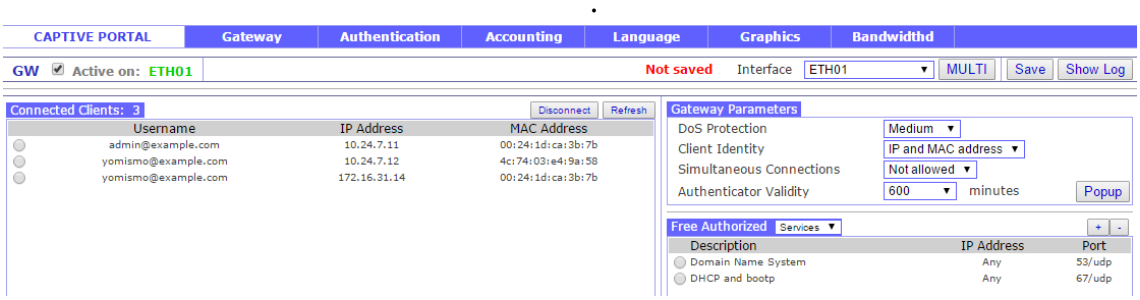



Ilustración 21: Activación del portal cautivo.

Seleccionamos la interfaz ETH01 en el desplegable, activamos el checkbox de la izquierda y damos a *Save*.

La gestión de usuarios se llevará a cabo desde el menú ***Users>Users>*** desde el que podremos realizar funciones básicas como listado de usuarios, añadir usuarios, eliminación, asignación de contraseñas y una hipotética gestión de crédito, que en nuestro caso no es de aplicación al ser un servicio totalmente gratuito.

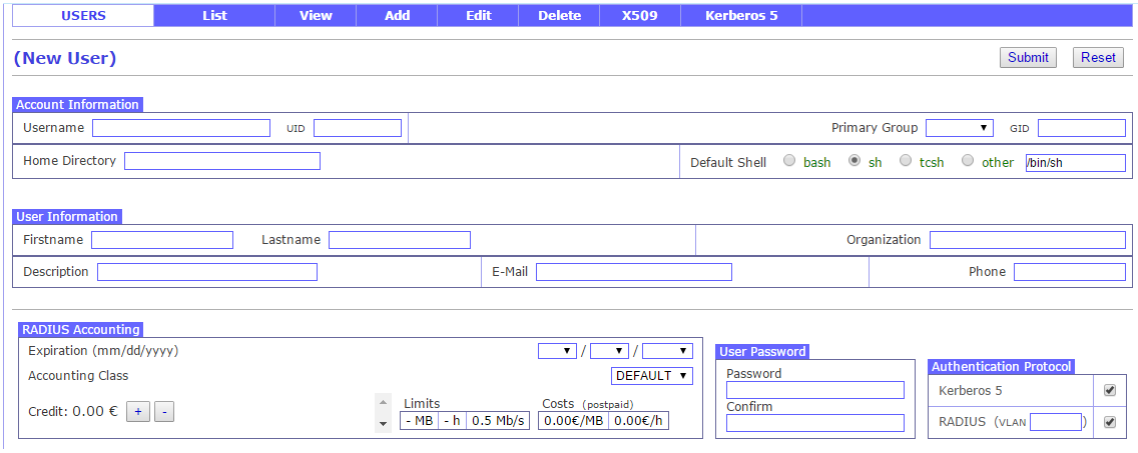



Ilustración 22: Menu de gestión de usuarios

También tenemos la opción de personalización del idioma de las pantalla de login del portal cautivo, accesible en *Users>Captive Portal>Language*

Por defecto tenemos disponibles el idioma ingles y el italiano (idioma nativo del desarrollador).

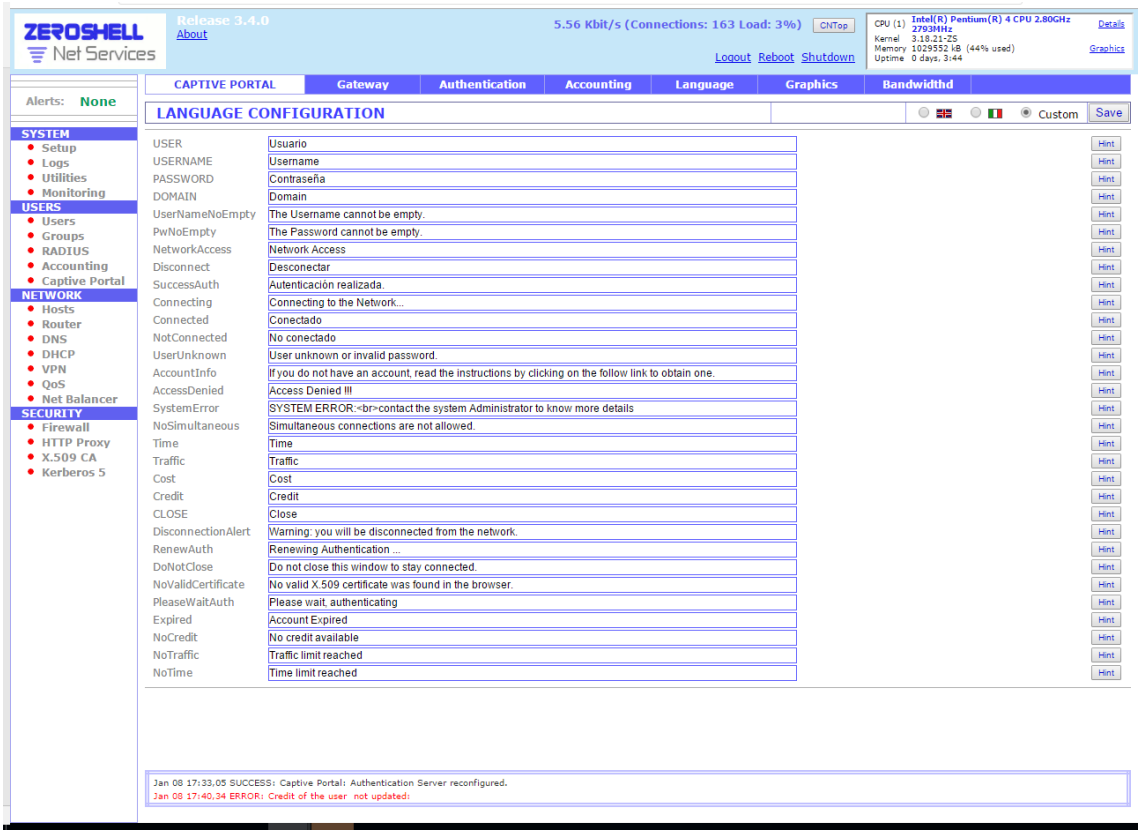



Ilustración 23: Personalización del menú de validación.

### 5.3.11. Configuración del proxy transparente con antivirus.

El uso de un servidor proxy que actué de intermediario entre el cliente y el servidor web permite realizar un registro de la navegación y el filtrado de contenidos inapropiados y de páginas web maliciosas que pudieran introducir virus en nuestros sistemas.

Generalmente su uso implica un cambio en las preferencias de nuestro navegador o del sistema operativo, lo cual puede ser un inconveniente para usuarios con pocos conocimientos, este problema se evita con el uso de un proxy transparente.

Con el uso de un proxy en modo transparente, las peticiones HTTP de los clientes son interceptadas y redirigidas hacia el servidor proxy sin que el usuario tenga que realizar ninguna acción.

En nuestro caso la configuración queda de la siguiente forma dentro de la opción ***Security->HTTP PROXY***.

Añadimos la regla de captura par el tráfico del interfaz ETH01 (la red pública de usuarios.

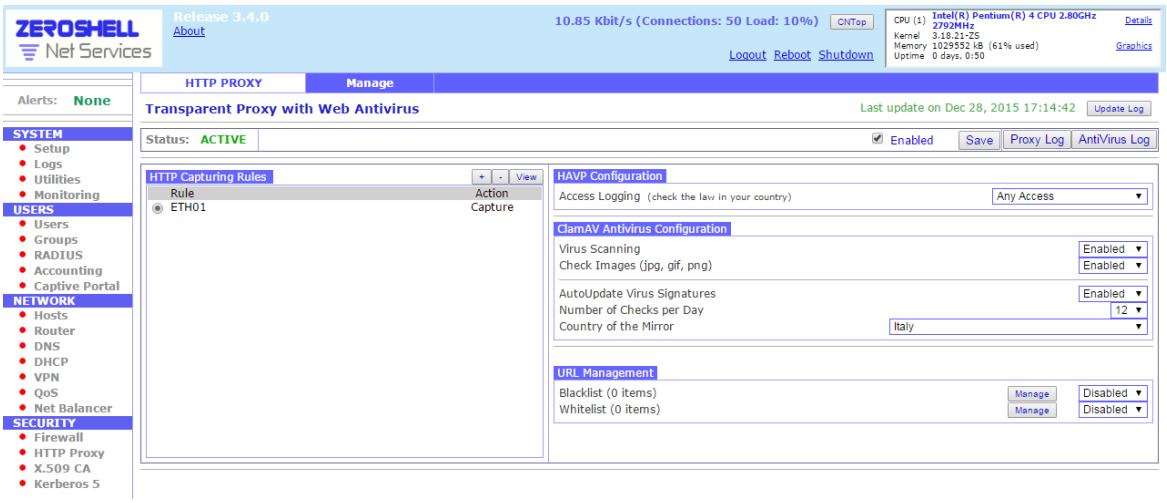



**Ilustración 24: Activación del proxy transparente con antivirus.**

Y realizamos un test del proxy a través de http://www.lagado.com/proxy-test

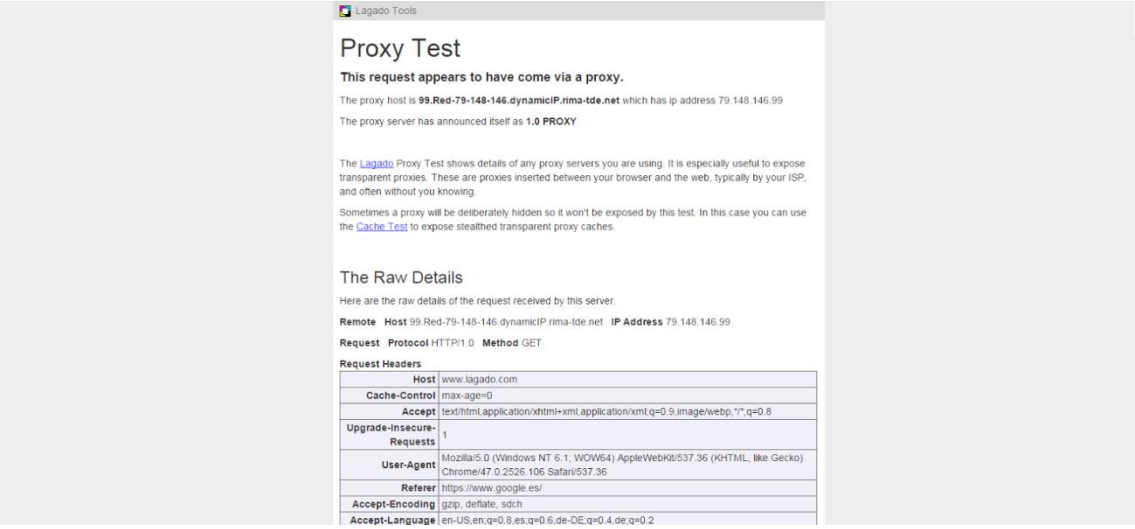



**Ilustración 25: Resultado del Lagado Proxy test**

El test tiene un resultado positivo, estamos navegando a traves de un proxy.

El siguiente test será el de sistema antivirus. Conectamos a la página de testeo del antivirus en http://www.eicar.org/85-0-Download.html para comprobar si el filtro antivirus del proxy está funcionando correctamente.

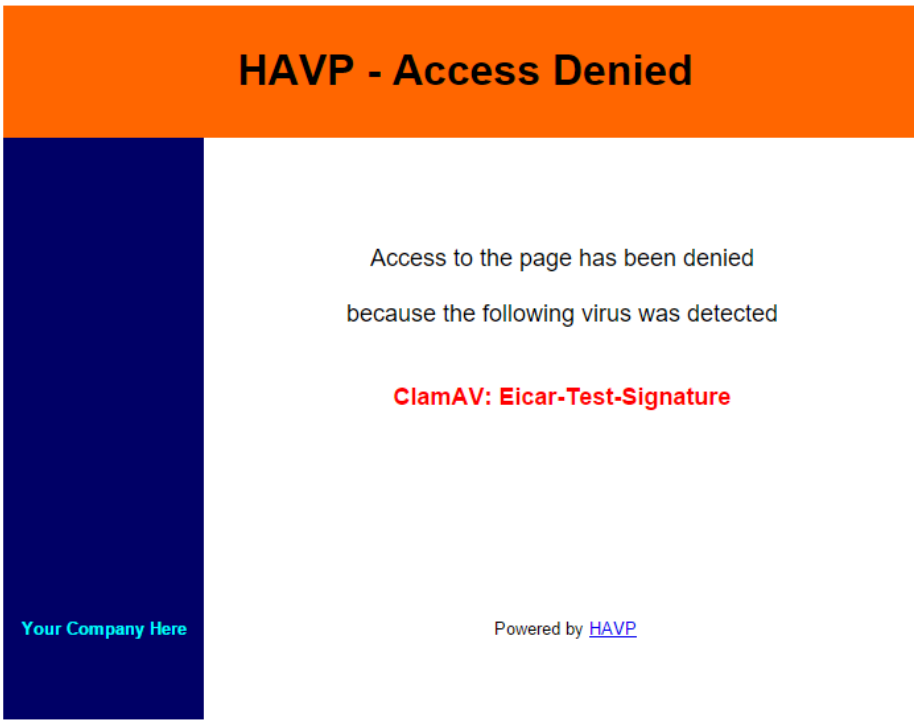



**Ilustración 26: Resultado del test del proxy antivirus.**

### 5.3.12. Pruebas del filtro de contenido web Dansguardian

Como medida adicional de protección frente al uso inadecuado de la red, activamos el filtro web Dansguardian.

Dansguardian es un sistema de filtrado de contenidos web, que al contrario que los sistemas tradicionales no se basa en el uso de blacklist[8] , sino que utiliza otros métodos como:

- Coincidencias de texto en la página web.
- Filtrado de imágenes.
- Cadenas de texto en la url.

Se trata de un sistema altamente flexible, si bien su optimización es algo tediosa al realizarse a través de la edición de fichero de configuración. No obstante la configuración por defecto está enfocada al filtrado de contenidos aptos para una escuela de primaria desearía, y es más que probable que se adapte a nuestro entorno si tener que realizar cambios.

Su instalación se realiza desde ***System>Setup>Packages*** seleccionamos el paquete 40100, pulsamos el botón "Manage" y seleccionamos "install", a continuación, se reiniciará el proxy y el servicio de filtrado ya estará activo.

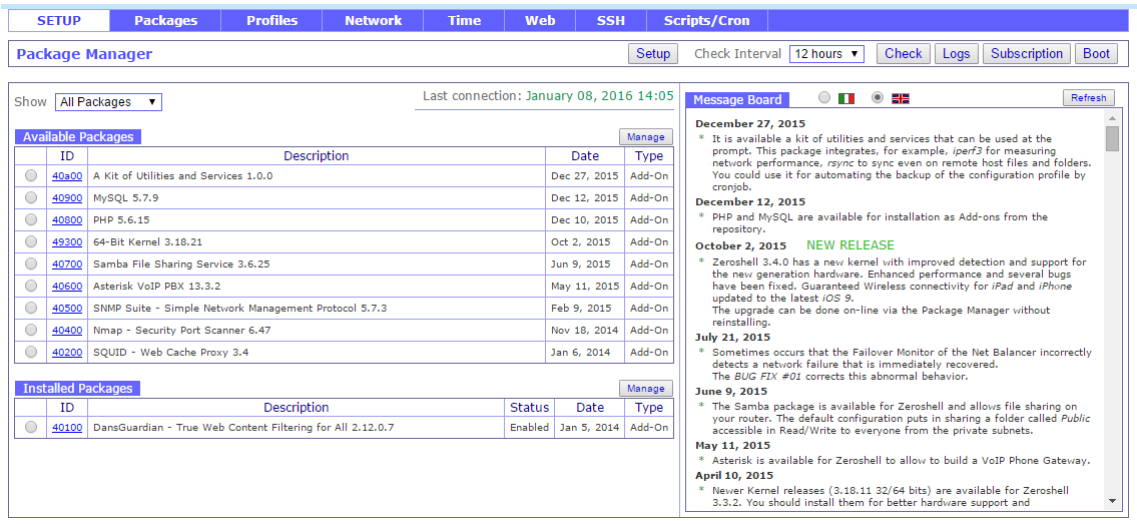



**Ilustración 27: Instalación de paquetes adicionales.**

Lamentablemente durante las pruebas de navegación con el DansGuardian activado se detectaron falsos positivos. En las búsquedas dentro de sitios web como ebay, el uso

[8] **Blacklist** Sistema básico de filtrado de contenidos web, que deniega el acceso a las URLs contenidas en un fichero de texto.

de demasiados filtros cuyos parámetros se pasaban a través de la URL hacia que los resultados de dicha búsqueda fueran bloqueados.


Ilustración 28: Falso positivo de Dansguardian.

Se opta por desactivar el paquete DansGuardian y dar por bueno el filtrado a nivel de DNS.

### 5.3.13. Registro de conexiones (Connection Tracking)

Conservar los datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, en concreto, es obligatorio por ley durante un año.

En concreto la Ley 25/2007, de 18 de octubre (transposición Directiva 24/2006), de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, obliga a que la Administración a cargo de la red tiene que conservar datos para identificar: origen, destino, fecha, hora y duración, tipo, equipo de comunicación y localización del equipo.

Dado que ya tenemos identificados a los usuarios que hacen uso de nuestra red mediante el portal cautivo, nos quedaría registrar las direcciones IP que utilizan y las direcciones IP a las que se han conectan.

Para llevarlo a cabo entramos en ***Security>Firewall>Connection Tracking*** y:

- Activamos el checkbox *Enabled*
- En *events to log* activamos New y Destroy
- Y como filtro de conexión incluimos src=172.16.31.* para registrar las conexiones creadas y destruidas desde la red WIFI.

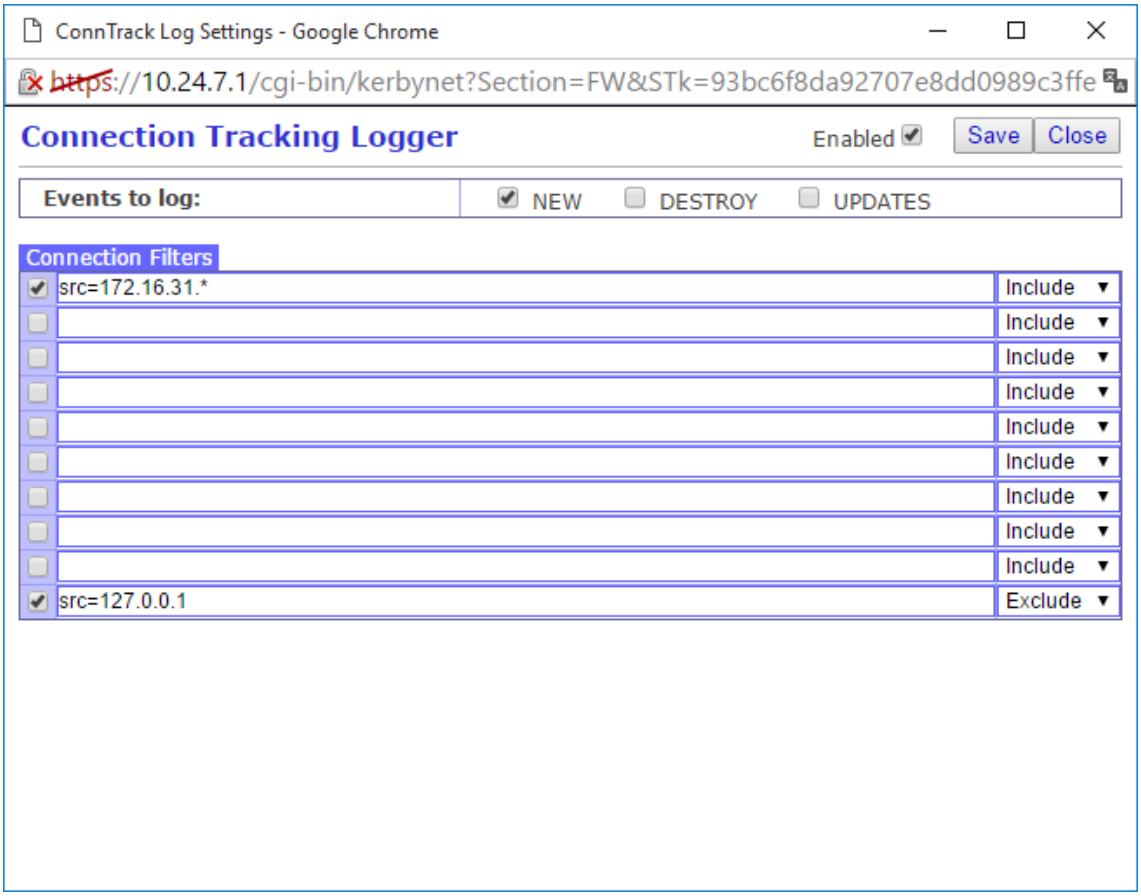



Ilustración 29: Configuración del filtro del registro de conexiones.

### 5.3.14. Securización del interfaz de administración.

Para limitar el acceso al interfaz de administración de Zeroshell a los equipos de nuestra red interna realizaremos las siguientes configuraciones.

Para el interfaz web desde ***System>Setup>Web*** limitaremos las conexiones a la Subred 10.24.7.1/24 y al interfaz ETH02

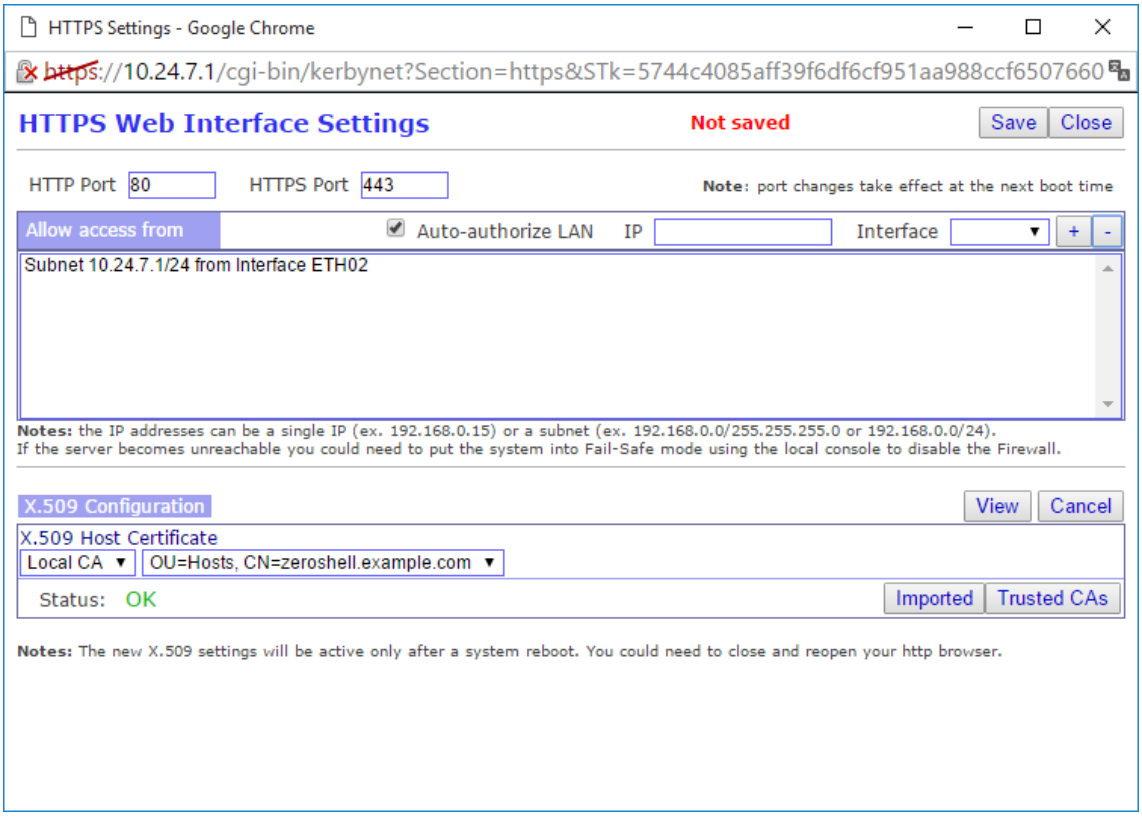



Ilustración 30: Limitación de los accesos al interfaz web.

Análogamente realizamos la misma operación para las conexiones SSH entrando en el menu ***System>Setup>SSH***

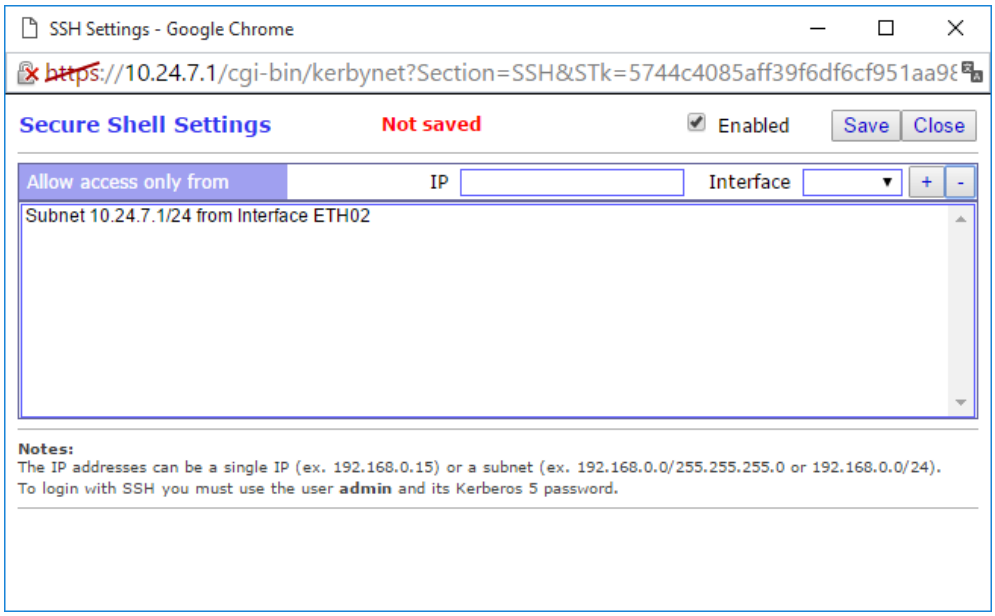



Ilustración 31: Limitación de los accesos SSH al servidor ZeroShell.

### 5.3.15. Balanceo de carga.

La funcionalidad de balanceo de carga de Zeroshell nos permitirá disponer de salidas redundantes a Internet que pueden funcionar en 2 modos:

- **Failover:** El trafico pasa a través de un enlace primario y se conmuta al secundario en caso de fallo.
- **Load balancing and Failover:** El tráfico se distribuye entre los 2 enlaces y en caso se desactiva el enlace con problemas

Este último modo será de gran utilidad en nuestro caso particular puesto que en el municipio las opciones de contratación de banda ancha están limitadas a:

- Acceso ADSL a través de los operadores nacionales con 10 Mbps teóricos de descarga.
- Acceso WIMAX a partir del operador local Wifinity con 12 Mbps teóricos de descarga.

De esta forma combinando un acceso de cada tipo podríamos tener un ancho de banda de descarga total de 22 Mbps y seguir dando servicio en caso de caída dela conexión de uno de los operadores.

La configuración de estas opciones está accesible en ***Network>Net Balancer***

Seleccionamos el checkbox Status para activar el servicio de balanceo de carga y Add para añadir un segundo Gateway.

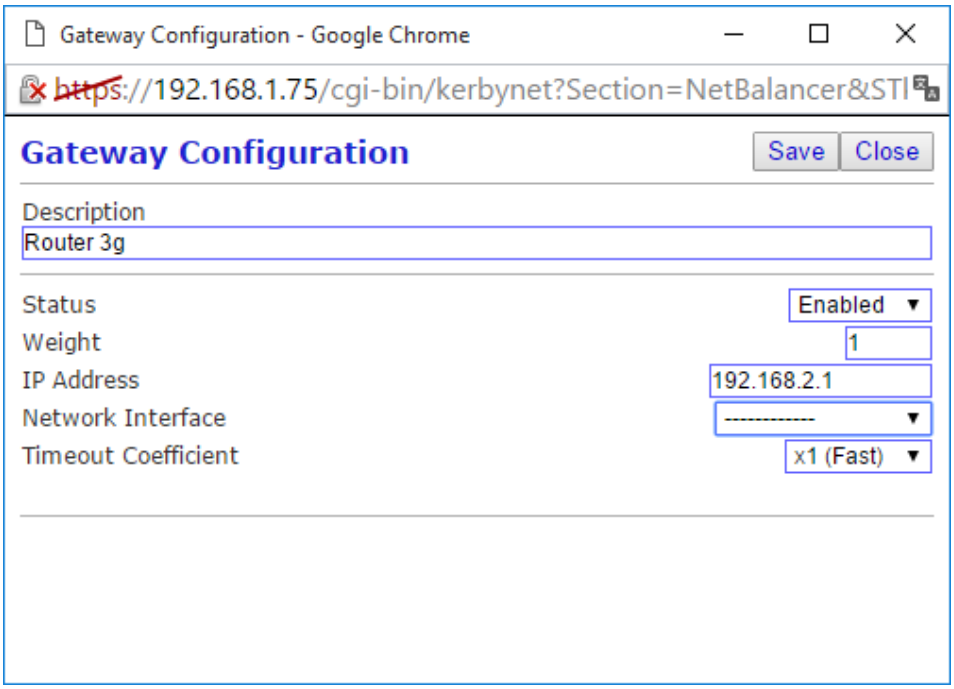



Ilustración 32: Configuración de un segundo Gateway.

La configuración de los Gateway de salida quedará entonces como sigue:

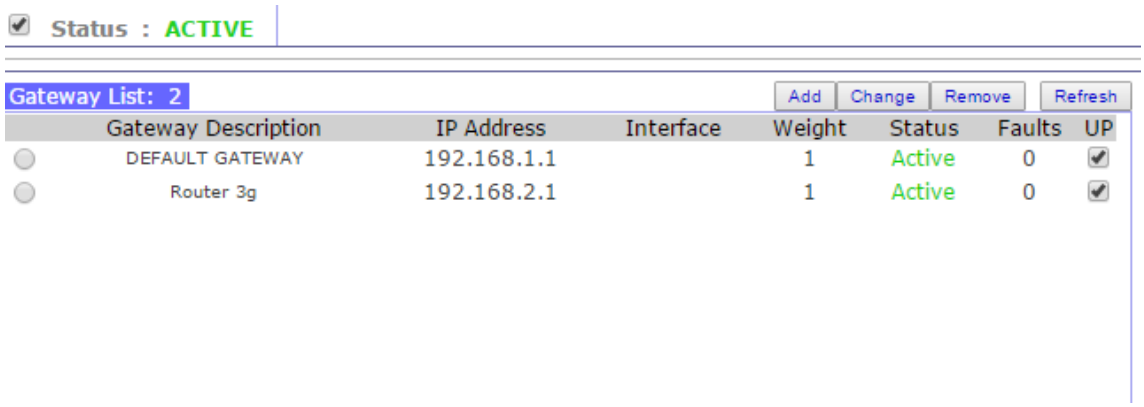



Ilustración 33: Configuración de multiples Gateway.

Adicionalmente para el correcto funcionamiento del balanceo de carga, habrá que activar el "*Failover Monitor"* que se encargará de chequear la conectividad de nuestros Gateway contra unas direcciones Ip de Internet . En nuestro caso configuramos como IPs de test las de los servidores DNS de google, quedando la configuración de esta sección de la siguiente forma.

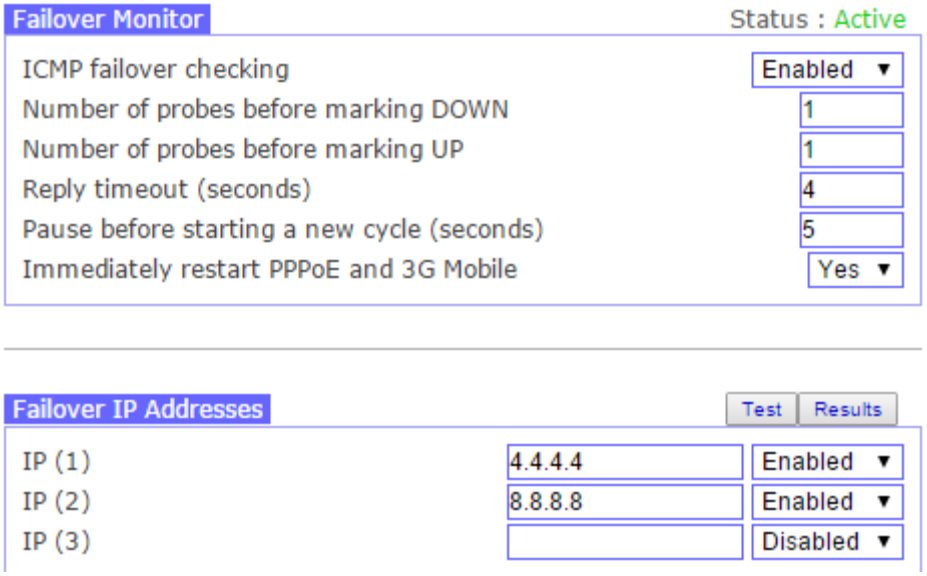
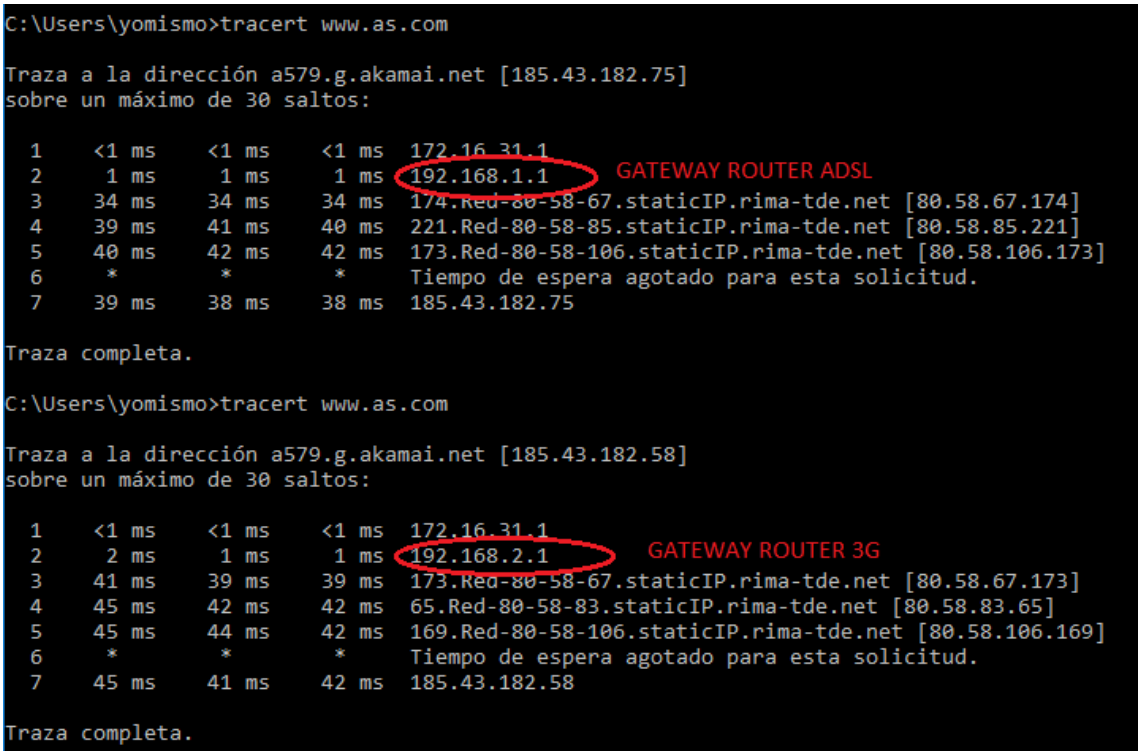



Ilustración 34: Configuración del Failover Monitor.

Comprobamos la configuración realizamos el siguiente proceso:

- Chequeamos nuestra ruta de conexión hasta www.as.com,
- desconectamos el cable de teléfono del router.
- Repetimos el tracert a www.as.com.




Podemos ver en la figura imagen que se ha producido una conmutación en la puerta de salida, y que la segunda conexión se ha realizado a través del router 3G.

### 5.3.16. Comprobación de cumplimiento de los requisitos

Llegados a este punto nos quedaría comprobar que la implementación cumple con los requisitos definidos al principio del comienzo del proyecto:

**Identificación de usuarios:**

Hemos de probar que se identifica identificar a los usuarios que usen el servicio, como hemos señalado con anterioridad la identificación de usuarios se realiza con la validación a través del portal cautivo. Desde la página de configuración del mismo hay una opción para acceder a dichos log.

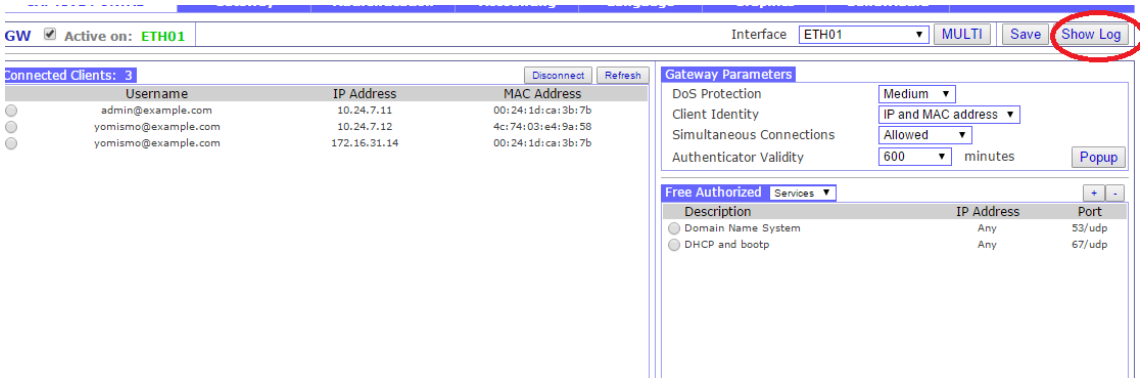



Ilustración 35: Acceso a los logs del portal cautivo.

Comprobamos el registro de nuestra última validación con el usuario "yomismo"

```
17:25:43 AS: Success: user yomismo@example.com (Client: 172.16.31.14) successfully authenticated (Username,Password)
17:25:44 GW: Success: user yomismo@example.com (IP: 172.16.31.14 MAC: 00:24:1d           ) connected
```

Vemos que efectivamente ha quedado registrado:

- Que hemos realizado una validación con éxito.
- La IP que se nos ha asignado.
- Que la MAC registrada coincide con la de nuestra tarjeta de red. (los últimos 6 caracteres están borrados intencionadamente)

Los logs del portal cautivo residen en el fichero */database/LOG/AÑO/Mes/Dia/zeroshell* del disco duro del servidor. Para una gestión correcta de los logs, sería interesante la configuración de algún script para comprimir y copia los logs diariamente a un sistema remoto a un medio de almacenamiento extraíble.

**Registro de conexiones**

El log de conexiones está disponible en ***Security>Firewall>Connection Tracking***

Desde la opcion "*Show Log", y en el fichero* /Database/LOG/2016/Jan/08/zeroshell/ConnTrack del disco duro.

Comprobamos efectivamente el registro de conexiones que contiene los datos de una sesión de navegación desde nuestra IP 172.16.31.14.

```
.14 sport=53 dport=53081
Jan  8 19:17:51 zeroshell ConnTrack:     [NEW] udp      17 30 src=172.16.31.14 dst=172.16.31.1 sport=61170 dport=53 [UNREPLIED] src=172.16.31.1 dst=172.16.31
.14 sport=53 dport=61170
Jan  8 19:17:51 zeroshell ConnTrack:     [NEW] tcp      6 120 SYN_SENT src=172.16.31.14 dst=64.233.167.189 sport=50134 dport=443 [UNREPLIED] src=64.233.167.1
89 dst=192.168.1.75 sport=443 dport=50134
Jan  8 19:17:51 zeroshell ConnTrack:     [NEW] tcp      6 120 SYN_SENT src=172.16.31.14 dst=64.233.167.189 sport=50135 dport=443 [UNREPLIED] src=64.233.167.1
89 dst=192.168.1.75 sport=443 dport=50135
Jan  8 19:17:54 zeroshell ConnTrack:     [NEW] tcp      6 120 SYN_SENT src=172.16.31.14 dst=64.233.167.91 sport=50136 dport=443 [UNREPLIED] src=64.233.167.91
 dst=192.168.1.75 sport=443 dport=50136
^C
root@zeroshell zeroshell>
```

Los requisitos técnicos como filtrado de contenidos y gestión de la calidad del servicio fueron revisados y validados tras la implementación de sus respectivas funcionalidades (puntos 4.4.8 y 4.4.9 respectivamente)

# 6. Implementación de Zeroshell en una red de zonas WIFI municipales.

La solución propuesta cubriría las necesidades de acceso a Internet compartido de un solo edificio, pero con algunos cambios, la solución sería igualmente viable en caso de querer implementar el servicio público de WIFI en otras dependencias municipales, en este punto abordaremos a grandes rasgos una implementación de estas características.

Se tratará un esquema de alto nivel que sin entrar en detalles de implantación recoge los elementos necesarios para la creación de una red de área metropolitana para un ayuntamiento que incluya:

- La integración de las redes locales de varios edificios municipales y su acceso a Internet.
- Un servicio wifi público en dichos edificios.
- Un servicio wifi diferenciado para los trabajadores municipales.
- Acceso a internet controlado desde equipos cableados de libre acceso.
- Configurar un punto único de acceso a Internet para todo el ayuntamiento.

Analizaremos a continuación de manera esquemática una posible configuración de red para la implementación de estos servicios:

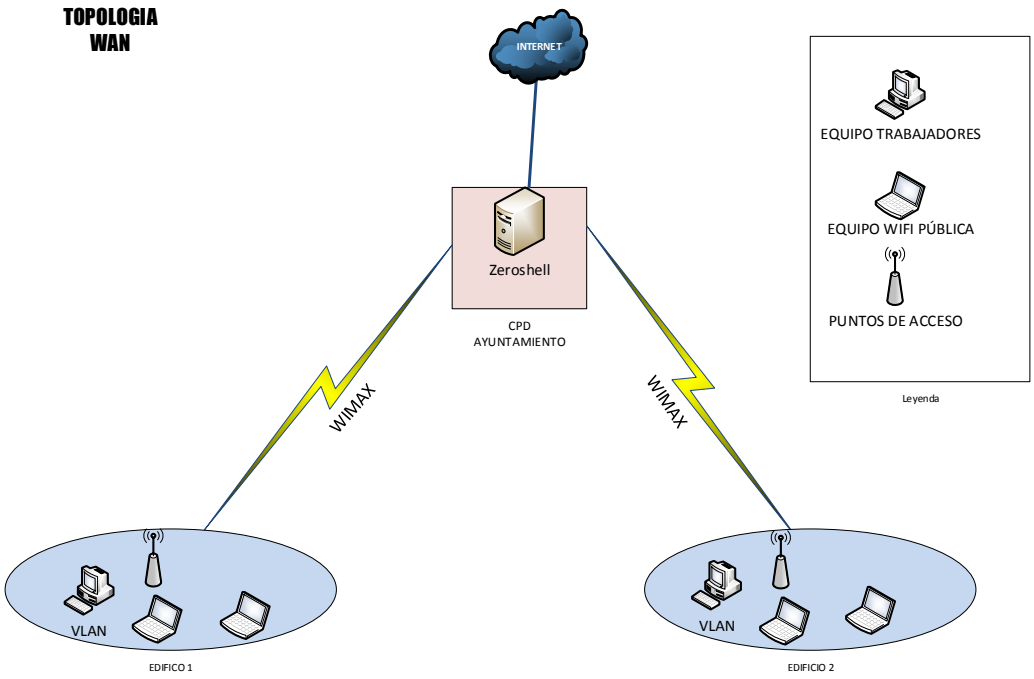



**Ilustración 36: Esquema de la red metropolitana.**

En la figura anterior podemos ver las partes diferenciadas de nuestro proyecto de red que son:

- **La red local de los edifico remotos:** El equipamiento físico de la LAN para interconectar los equipos de los funcionarios y el acceso público inalámbrico en cada uno de los edificios.

- **La red troncal:** La espina dorsal de nuestra red, una red de enlaces inalámbricos punto a punto con tecnología WIMAX que conectaría el ayuntamiento con el resto de edificios municipales interconectados

- **El acceso a Internet:** En este caso el acceso se realizaría a través de nuestro servidor Zeroshell, situado en el interior del CPD del ayuntamiento.

Pasamos a analizar con mayor nivel de detalle cada uno de los componentes:

### 6.1.1. La LAN de los edificios remotos

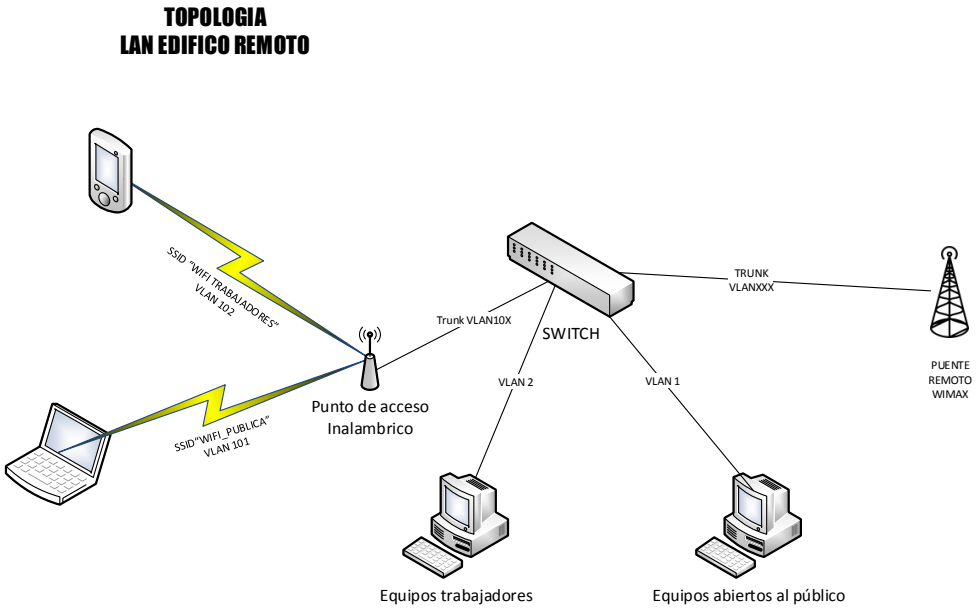



Ilustración 37 Diagrama de red de los edificios remotos.

En los edificios remotos se distinguirán 4 tipos distintos de tráfico separados mediante la implementación de VLANs[9] 802.1Q:

- **VLAN1:** Equipos abiertos al público.
- **VLAN2:** Red interna de los equipos de los funcionarios.
- **VLAN101:** Wifi pública.
- **VLAN102:** Wifi trabajadores.

En el caso de las wifis públicas/trabajadores el servicio se daría a través de puntos de acceso de gama media que permitan la creación de múltiples SSID asignados a VLANs distintas.

Tanto los interfaces Ethernet de los puntos de acceso como el resto de equipos cableados irían conectados a un Conmutador que enviaría el tráfico de todas las VLANS a través de un puerto en modo trunk[10] conectado a la unidad remota WIMAX.

### 6.1.2. La red troncal WAN

Para la interconexión de los edificios municipales se usarán radioenlaces WIMAX[11], una norma de transmisión de datos que utilizando ondas de radio en las frecuencias en torno a los 2,5 GHz, aunque también hay posibilidad de usar la banda de los 5 GHz.

Fue pensada como alternativa de interconexión en áreas donde el entorno o la distancia no es favorable para una red cableada. Este tipo de enlaces soporta distancias de hasta 50 kms., si bien en nuestro caso particular el enlace a mayor distancia será entre el nodo central de nuestra red (el ayuntamiento) y el punto más alejado (la piscina municipal) no sería superior a 1.5 kms.

[9] **VLAN:** acrónimo de *virtual LAN* (**red de área local virtual**), es un método para crear redes lógicas independientes dentro de una misma red física.
[10] **Trunk:** Enlace especial para por el que circula el tráfico de varias VLAN.
[11] https://es.wikipedia.org/wiki/WiMAX


Ilustración 38:Situación geográfica de los edificios municipales

El municipio se encuentra asentado en una planicie sin obstáculos por lo que podríamos suponer a priori que gozaríamos de una línea de visión directa en todos los radioenlaces.

### 6.1.3. El CPD del ayuntamiento.

Una vez modelado la red que permita llevar el tráfico de las distintas sedes hasta el CPD , quedaría adaptar nuestro servidor Zeroshell a la nueva configuración:

En este caso tendríamos un único interfaz físico para conexión a nuestras redes internas, *ETH01* donde llegaría encapsulado todo el tráfico de las distintas VLANs a recogidas en las estaciones base de los radioenlaces punto a punto.

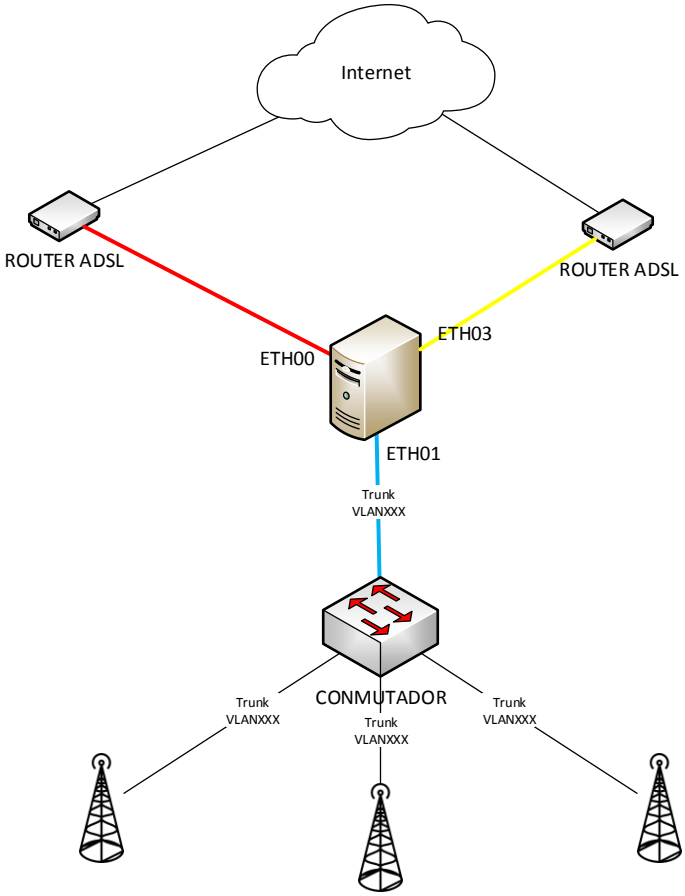



**Ilustración 39 Conexiones físicas del servidor Zeroshell**

Para poder trabajar con las distintas VLANs, tendremos que definirlas dentro del interfaz físico que las contiene.

Para ello entraríamos en el menú *Setup>Network>* y tras seleccionar el interfaz ETH01 pulsamos en "*Create VLAN*"

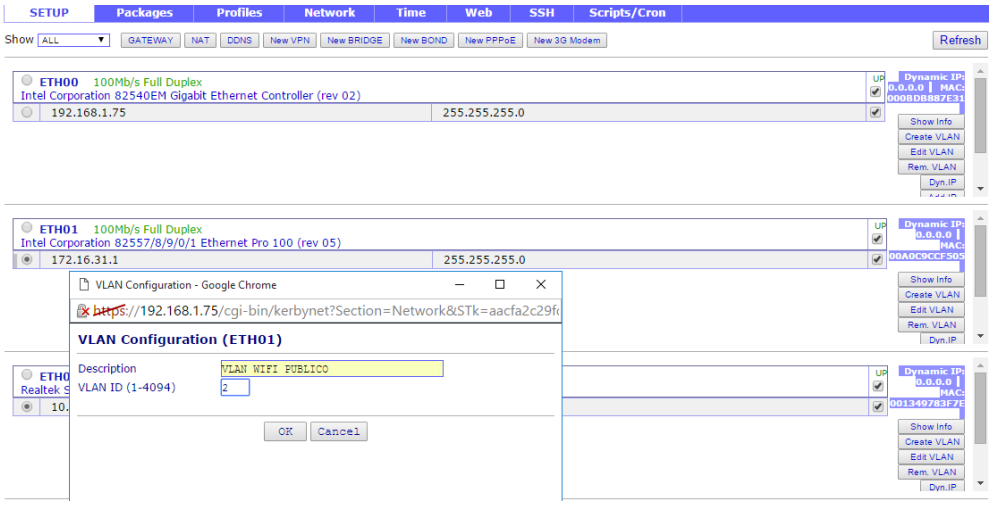



Ilustración 40: Definición de VLANs

Podemos comprobar que una tras salvar los cambios, la VLAN102 , estaría disponible como un interfaz más para realizar las configuraciones necesarias, como p.e. la activación del portal cautivo.

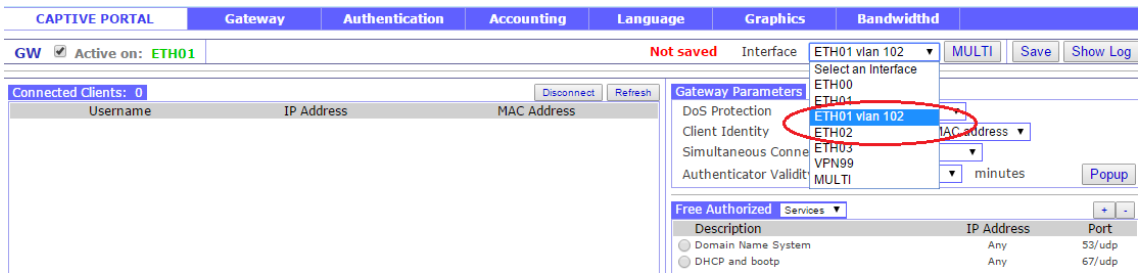



Ilustración 41: Activación del portal cautivo en una VLAN

Llegados a este punto la configuración de "red lógica" que tendríamos seria la siguiente:

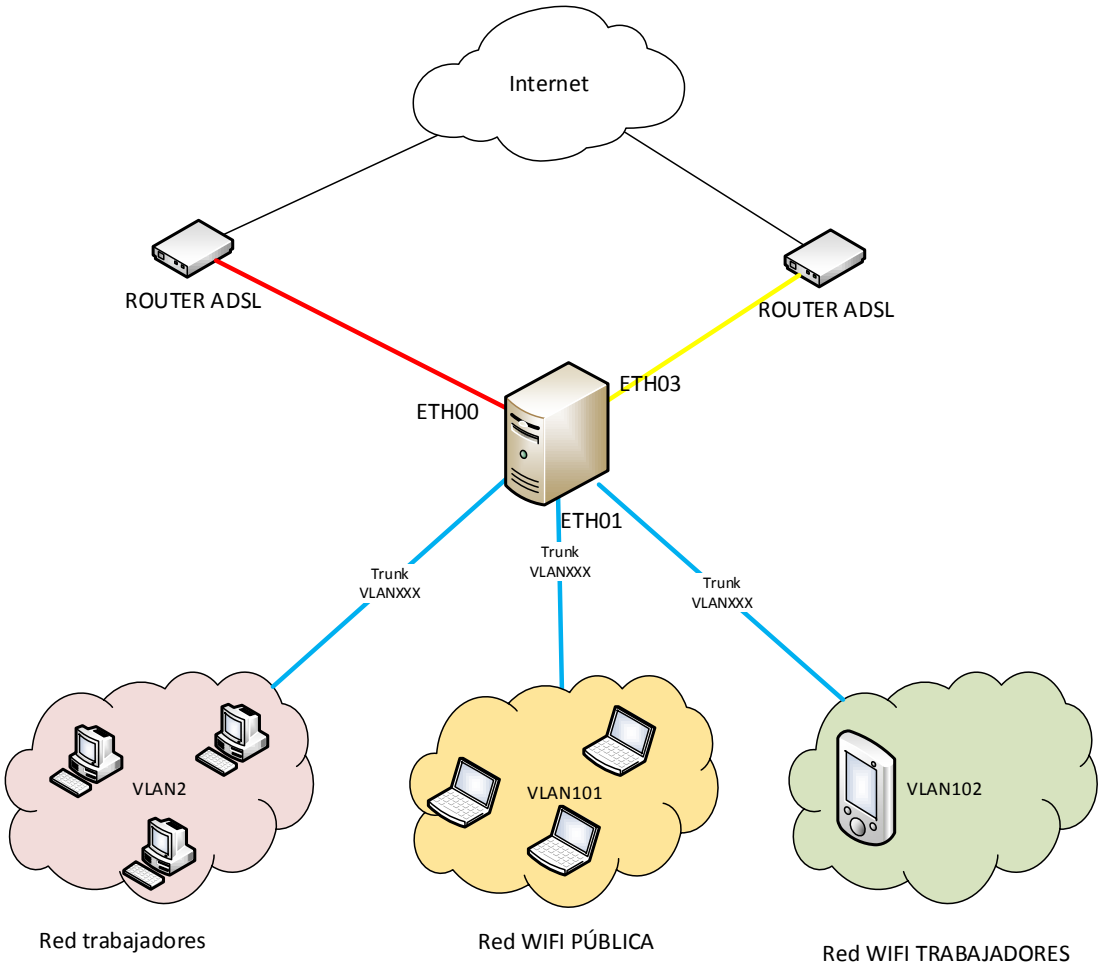



Ilustración 42 Conexiones lógicas de las VLANs al servidor Zeroshell

Llegados a este punto podríamos gestionar las conexiones de los equipos dispersos en cada VLAN como si se tratara de una red física conectada a un interfaz real.

## 7. Temas pendientes y posibles líneas de trabajo adicionales.

Como futuras líneas de trabajo adicionales quedaría pendientes:

- Configuración del firewall para el control de tráfico y aislamiento entre las redes.
- Una configuración más granular de la calidad de servicio a través de una clasificación y filtrado del tráfico mediante filtros que trabajen en el nivel 7 de OSI. P.e. priorización de Voz Ip o filtrado de protocolos P2P, que son complicados de interceptar mediante filtros TCP o UDP.

- Desarrollar con mayor detalle la implantación a nivel municipal, incluyendo puntos de acceso, radioenlaces, etc. incluyendo presupuestos y viabilidad.

# 8. BIBLIOGRAFIA


Junta de Castilla y Leon. *Cómo poner en marcha una red wifi municipal Guía rápida para Ayuntamientos*.

http://wifi.sancotec.com/wp-content/uploads/2014/03/2013-09-manual-jcyl-como-poner-en-marcha-una-wifi-municipal.pdf [Consulta: Noviembre de 2015]

Diputacón de Badajoz. *LAS TECNOLOGÍAS WIFI Y WIMAX*.

http://www.dip-badajoz.es/agenda/tablon/jornadaWIFI/doc/tecnologias_wifi_wmax.pdf [Consulta: Diciembre de 2015]

Pavlina, David. *The Hunt For the Ultimate Free Open Source Firewall Distro*. http://www.mondaiji.com/blog/other/it/10175-the-hunt-for-the-ultimate-free-open-source-firewall-distro [Consulta: Noviembre de 2015]

Martínez Campo, José. *Diseño de una red telemática para proporcionar acceso a Internet* http://openaccess.uoc.edu/webapps/o2/bitstream/10609/23161/7/jmartinezcampoTFC0613memoria.pdf . [Consulta: Octubre de 2015]

OPENDNS. *SET UP FAMILYSHIELD ON YOUR DEVICE*. [Consulta: Diciembre de 2015]