

Puesta en marcha de un hotspot inalámbrico mediante la técnica del portal cautivo

por Orlando Alemán Ortiz

Licencia



Esta obra ha sido publicada bajo licencia "Reconocimiento-NoComercial-CompartirIgual 2.5 Spain" de Creative Commons, la cual implica que:

Usted es libre de:

- copiar, distribuir y comunicar públicamente la obra
- hacer obras derivadas

Bajo las condiciones siguientes:



Reconocimiento. Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciador.



No comercial. No puede utilizar esta obra para fines comerciales.



Compartir bajo la misma licencia. Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta.

Y además:

- Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.
- Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor
- Los derechos derivados de usos legítimos u otras limitaciones reconocidas por ley no se ven afectados por lo anterior.

Para ver una copia de esta licencia, visite <http://creativecommons.org/licenses/by-nc-sa/2.5/es/> o envíe una carta a Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

Índice de contenido

Licencia.....	2
Previos.....	4
Introducción.....	4
Implementación.....	4
El software.....	4
Objetivo y material necesario.....	6
Componentes Hardware.....	6
Elementos Software.....	6
Desarrollo.....	7
Configurando el sistema.....	9
Creando un fichero de configuración.....	10
Integrando en Red.....	12
Navegación por Internet.....	13
Adición de usuarios.....	13
Puesta en servicio del Portal cautivo.....	14
Asignación dinámica de direcciones.....	15
Integrando el punto de acceso.....	15

Previos

El presente documento trata sobre la puesta en funcionamiento de un sistema de control de acceso a Internet basado en ZeroShell.

Introducción

En algunas circunstancias los protocolos seguridad usados en las redes inalámbricas, como WPA o WEP, pueden no ser aplicables bien porque no son fáciles de configurar por los usuarios finales, bien porque requieren que los componentes hardware y software implicados los soporten.

Una solución a este problema consiste en pasar el control de acceso de la Capa 2 de TCP/IP a la 3, mediante la técnica de portal cautivo.

Un portal cautivo es un programa o máquina de una red informática que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal. Se instala por tanto en la puerta de enlace de la red, que es el sitio por donde pasa todo el tráfico hacia Internet.

Implementación

Hay varias formas de implementar un portal cautivo:

- Redirección por HTTP : Se intercepta la primera petición HTTP del cliente, y se le envía un datagrama de respuesta que contiene un “HTTP Status Code 302” para redirigir al cliente hacia el portal cautivo.
- Redirección por DNS: Ante una petición DNS de un cliente no autorizado, en lugar de devolver la dirección IP correcta, se retorna la dirección IP del portal cautivo.

El software

ZeroShell es una pequeña distribución de GNU Linux para servidores y dispositivos empotrados, que provee los principales servicios que una red LAN puede necesitar.

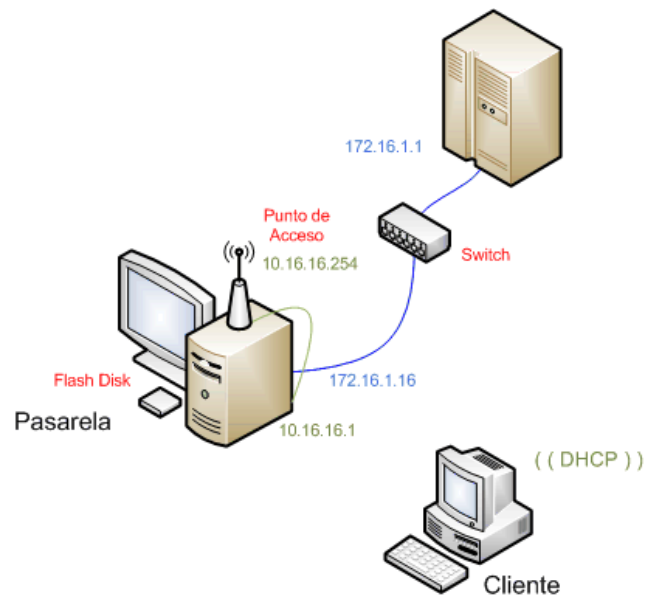
Las características por las que se ha escogido este software y no otro son:

- Implementa Captive Portal para proveer servicios de autenticación web para redes Ethernet e inalámbricas.
- Soporta para NAT
- Incluye servidor de DHCP
- Encapsulado de datagramas Ethernet en túneles SSL/TLS
- Fácil configuración a través de interfaz Web
- Herramientas de diagnóstico
- No requiere instalación en disco duro, ya que se puede correr como *LiveCD* o desde memoria USB
- Es 100% Open Source y funciona prácticamente sobre todo el hardware existente para x86.

Pero además de estas características, ZeroShell implementa muchas características más que hacen de este software una herramienta muy interesante a considerar para nuestras redes locales (DNS, Virtual Servers, etc.).

Objetivo y material necesario

Antes de comenzar la explicación, permítame mostrarle el esquema de red que pretendo montar con el material del que disponemos en el laboratorio.



Componentes Hardware

- 1 x PC con 2 tarjetas de red, grabadora de CDROM y puerto USB, que actuará como pasarela.
- 1 x PC con 1 tarjeta de red, desde donde configuraremos la pasarela y probaremos el resultado de nuestro trabajo.
- 1 x Punto de acceso "D-Link AirPlus Xtreme G DWL-2100AP"
- 1 x Adaptador inalámbrico USB modelo "D-Link AirPlus DWL-120+ Wireless USB"
- 1 x Memoria Flash USB de 512 Mb.
- 1 x cable de red UTP Cat.5 cruzado y con conectores RJ45

Elementos Software

- ZeroShell 1.0.beta4
- En el cliente, Microsoft Windows XP.

Desarrollo

Primeramente nos vamos al sitio web de ZeroShell (<http://www.zeroshell.net>) para descargar la última versión del software, en este caso, en su edición LiveCD. Quemaremos la imagen a un CD-R y arrancaremos la PC pasarela desde el CD recién creado.

Antes de arrancar el PC pasarela nos aseguraremos de tener conectadas correctamente las interfaces de red que van a servir para nuestros propósitos. También conviene tener conectado un dispositivo de almacenamiento, como un disco duro o un pen-drive, al computador para poder guardar nuestras configuraciones.

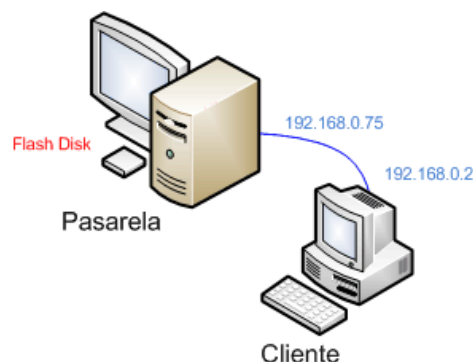
Ahora ya podemos arrancar la máquina. Al final del proceso nos encontraremos con una pantalla similar a la siguiente:

```
ZeroShell - Net Services 1.0.beta4      May 28, 2007 - 12:31
-----
Hostname : zeroshell.example.com
CPU (1)  : AMD Athlon(tm) XP 2400+ 1999MHz
Kernel   : 2.6.19.3
Memory   : 1035828 kB
Uptime   : 0 days, 0:1
Load     : 0.85 0.23 0.08
Database : Temporary EXAMPLE.COM configuration
-----
COMMAND MENU
<A> Activate database           <P> Change admin password
<D> Deactivate database       <T> Show Routing Table
<S> Shell Prompt              <F> Show Firewall Rules
<R> Reboot                    <N> Show Network Interface
<H> Shutdown                 <Z> Fail-Safe Mode
<B> Create a Bridge
-----
Select:
```

Observamos en la parte superior que ahora mismo está funcionando con la configuración inicial por defecto. Los comandos de los que podemos hacer uso en esta consola son bien pocos.

Configurando el sistema

Para configurar ZeroShell debemos acceder desde una segunda máquina utilizando un navegador web. Por defecto, se asigna únicamente dirección IP a la interfaz de red principal, que siempre es ETH0 (con mayúsculas), y que podemos reconocer mediante el comando “Show Network Interface” en la consola que hemos visto antes.



La dirección que por defecto se asigna a ETH0 es 192.168.0.75/24, por lo que nos vemos obligados a improvisar una pequeña red local entre la pasarela y un computador auxiliar, al que asignaremos a

la dirección 192.168.0.2/24.

Una vez montada la red, accedemos a la interfaz web a través de la dirección <https://192.168.0.75>, donde utilizaremos el par usuario y contraseña:

Username: admin
Password: zeroshell

Creando un fichero de configuración

ZeroShell nos da la posibilidad de guardar la configuración en discos y memorias que utilicen como sistema de archivos ext3, reiserfs o fat32, entre otros, sin necesidad de reformatear las particiones.

Aprovechando esta posibilidad, utilizaremos un dispositivo de memoria flash para salvar los cambios. Para ello, accedemos a Setup>Storage y seleccionamos la partición a utilizar.

Model	Capacity
Model: CREATIVE Zen Nano Plus (sda)	Capacity: 475 MB
sda1	Type: vfat Capacity: 474 MB Used: 190 MB 41%

A continuación hacemos clic en CreateDB y rellenamos un sencillo formulario. No debemos preocuparnos de rellenar todos los campos, ya que se pueden cumplimentar posteriormente.

CREATIVE Zen Nano Plus (sda)

New Database on partition sda1

Create Close

Description	<input type="text" value="Prueba"/>
Hostname (FQDN)	<input type="text" value="zeroshell.example.com"/>
Kerberos 5 Realm	<input type="text" value="EXAMPLE.COM"/>
LDAP Base	<input type="text" value="dc=example,dc=com"/>
Admin password	<input type="password" value="•••••"/>
Confirm password	<input type="password" value="•••••"/>
NETWORK CONFIG	
Ethernet Interface	<input type="text" value="ETH00 - Realtek Semiconductor Co., Ltd. RTL-8139/8139C/8139C+ (rev 10)"/>
IP Address / Netmask	<input type="text" value="192.168.0.75"/> / <input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text"/>

Como consecuencia veremos reflejada la nueva base de datos en la lista de particiones disponibles:

Partition: sda1 [Create DB] [Restore DB] [View FS] [Delete] [Format] [RESCAN]

Warning:
This software is NOT guaranteed to be bug free. It is your responsibility to properly test it on scratch disks before to use it on production devices with important data. In any case, the author is not responsible for any data loss or damage caused by this software.

Model: CREATIVE Zen Nano Plus (sda) Capacity: 475 MB

Type: vfat	Capacity: 474 MB	Used: 190 MB	41%
sda1			

Database	Description	Last Activation
<input type="radio"/> _DB.001	Prueba	25 May 2007 18:21

Nótese que podemos tener varios ficheros de configuración distintos, los cuales podremos activar o desactivar desde esta misma página.

Integrando en Red

Una vez creado el fichero de configuración podemos pasar a la configuración de las interfaces de red, en Setup>Network.

Show ALL [GATEWAY] [Make VPN] [Make BRIDGE] [Make BOND] [Make PPPoE] [Refresh]

Interface	Status	MAC
ETH00 Unknown link status Accton Technology Corporation EN-1216 Ethernet Adapter (rev 11)	UP	00C049B36504
10.16.16.1 255.255.255.0	✓	
ETH01 100Mb/s Full Duplex Broadcom Corporation NetXtreme BCM5751 Gigabit Ethernet PCI Express (rev 01)	UP	000E1FDA10DA
172.16.1.16 255.255.255.0	✓	

Habitualmente ETH0 es el adaptador para la red interna y ETH1 para la externa. Usando los botones “Add IP”, “Edit IP” y “Remove IP” podemos asignar las direcciones ip estáticas que queramos a las interfaces de red. En mi caso, he elegido 10.16.16.1/24 para la interfaz interna (ETH0) y 172.16.1.16/24 para la interfaz externa (ETH1).

Al cambiar la dirección de la interfaz ETH0 deberemos conectarnos nuevamente, esta vez a la nueva dirección IP, lo que nos obligará a reconfigurar la interfaz de red del cliente.

Para fijar la puerta de enlace usamos el botón GATEWAY, disponible también en Setup>Network que en nuestro caso es 172.16.1.1.

Navegación por Internet

Para permitir a los clientes internos usar la conexión a Internet activaremos *Network Address Translation* (Router>NAT), de esta forma accederán a Internet a pesar de disponer de una dirección de red privada.

Network Address Translation

Save View Close

Available Interfaces

ETH00

>>>

<<<

NAT Enabled Interfaces

ETH01

Indicaremos la interfaz hacia la cual se traducirán las direcciones, en este caso, ETH1.

A partir de este instante los clientes, que por el momento se reducen a nuestra máquina, dispondrán de acceso a Internet.

Adición de usuarios

Antes de activar el Portal Cautivo, vamos a crear manualmente los usuarios a los que se va a permitir hacer uso del servicio. Esto se consigue yendo a Users>Add y rellenando el formulario correspondiente:

USERS List View Add Edit Delete X509 Kerberos 5

(New User) Submit Reset

Account

Username UID Primary Group GID

Home Directory Default Shell bash sh tcsh other

User Information

Firstname Lastname Organization

Description E-Mail Phone

User Password

Password

Confirm

Enabled Services

Kerberos 5 Authentication

Host-to-Lan VPN (L2TP/IPsec)

802.1X Access (VLAN)

Verificamos la adición de los nuevos usuarios visualizando Users>List:

USERS List View Add Edit Delete X509 Kerberos 5

Entries found: 2 Search Primary Group

	Username	Group	Description	E-mail
<input type="radio"/>	admin	0	System Administrator	
<input type="radio"/>	orlando	nobody	Orlando	?

Puesta en servicio del Portal cautivo

Ya estamos en disposición de activar el portal cautivo, lo cual se consigue en dos pasos:

Paso 1: Ir a Captive Portal > Authentication y activar la casilla STATUS

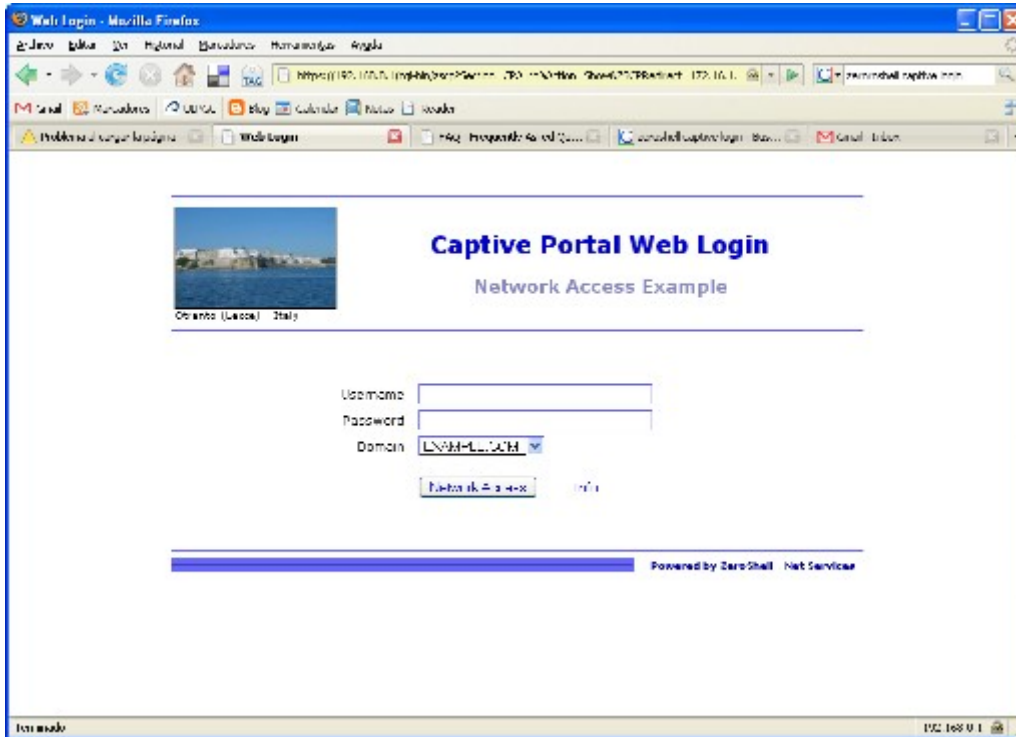
CAPTIVE PORTAL Gateway Authentication Language Accounting

Web Login Authentication Server Status: ACTIVE Save Show Log

Paso 2: Ir a Captive Portal > Gateway, activar la casilla GW, fijar el modo Routed y marcar ETH0 como la interfaz a controlar.

CAPTIVE PORTAL		Gateway	Authentication	Language	Accounting
GW	<input checked="" type="checkbox"/> Active on: NONE	Not saved	Mode: Routed	Interface: ETH0	Save Show Log

Si todo ha ido bien, acto seguido el navegador nos mostrará la página de autenticación obligatoria.



Como resultado de la autenticación, podremos ver la siguiente popup:

Network Access Disconnect

admin@EXAMPLE.COM connected - IP:10.16.16.2

Duration (hh:mm) :	00:00	Refresh
Traffic (MB) :	0.00	
Cost (--):	--.---	

Do not close this window to stay connected.

Asignación dinámica de direcciones

Para terminar de configurar nuestro sistema, pero por ello no menos importante, debemos dar la capacidad al sistema de responder a las peticiones DHCP del punto de acceso.

Elegimos DHCP en el menú lateral izquierdo.

