Servidores proxy: montando una pequeña LAN entre máquinas virtuales

Ingeniería de Servidores

Universidad de Granada

Resumen

Los servidores proxy son un mecanismo muy utilizado en el ámbito de la informática. En este texto se explica que es un servidor proxy, las características que posee, así como sus ventajas y desventajas. También explicaremos los distintos tipos de proxy que existen hoy en día y cuáles son los más usados. Finalmente, realizaremos un pequeño experimento montando una pequeña LAN entre máquinas virtuales.

1 Introducción

Hoy en día hablar de un servidor proxy es algo común en el área de informática, pero realmente ¿sabemos lo qué es? Un servidor proxy es un dispositivo que funciona como intermediario entre un servidor web (Internet) y nuestro ordenador (Cliente). [1]

Está basado en el modelo cliente-servidor. El ordenador cliente es quién interactúa directamente con el servidor proxy, en vez de hacerlo con el servidor web. Por lo tanto, el proxy será quien recoja las peticiones lanzadas por el cliente. De todas ellas seleccionará algunas y se pondrá en contacto con el servidor. Obteniendo así las respuestas, que serán mandadas al cliente. De esta forma el cliente no se pone en contacto con el servidor (Figura 1). [2]

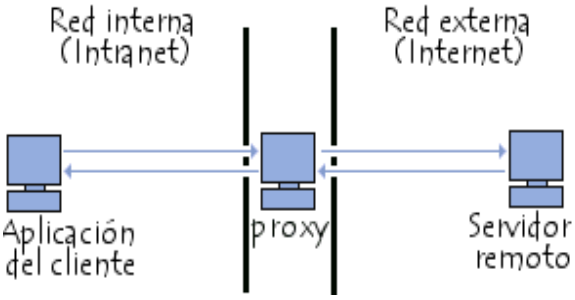

Figura 1: Funcionamiento del Servidor Proxy

Los objetivos principales que presenta son [3]:

- Controlar la navegación de los usuarios.
- Disminuir el tráfico de Internet, evitando el colapso de la red. Esto lo consigue mediante la caché.

***Nota**: se irán explicando estos objetivos en los apartados siguientes.*

Como consecuencia podemos decir que los servidores proxy están muy relacionados con la seguridad en Internet. Gracias a ellos, hemos conseguido mejorarla.

Pongamos un ejemplo para entender mejor lo que acabamos de explicar: Disponemos de una empresa, donde tenemos una red de ordenadores conectados a un servidor proxy. Cuando un trabajador de nuestra empresa se conecte desde cualquier equipo a Internet, lo hará mediante el proxy, que será quién reciba nuestras peticiones. Por consiguiente, en el exterior solo se va a conocer la IP pública del servidor remoto, no la de los ordenadores.

***Nota:** A partir de ahora cuando hablemos de un servidor estaremos haciendo referencia a un servidor remoto.*

2 Características de los Servidores Proxy

Cuando estemos hablando de un servidor proxy, debemos tener en cuenta algunas de sus características [4]:

- Funciona como cortafuegos protegiendo a los ordenadores conectados de los ataques externos, aumentando de esta forma la seguridad.
- Filtra los contenidos.
- Comparte la conexión a la red: un grupo de usuarios conectados a la misma red interna, pueden estar identificados como un solo usuario, es decir, usando la misma IP.
- Almacena los datos en caché.
- Ayuda a mejorar el rendimiento en internet.
- Permite definir los permisos que tienen los usuarios sobre la red interna.

3 Tipos de Servidores Proxy

Existen diversos tipos de servidores proxy:

- Proxy Web.
- Proxy Caché.
- Proxy Transparente.
- Proxy Inverso.
- Proxy NAT o Enmascaramiento.
- Proxy Anónimo.
- Proxy Abierto.

A continuación explicaremos más en detalle cada uno.

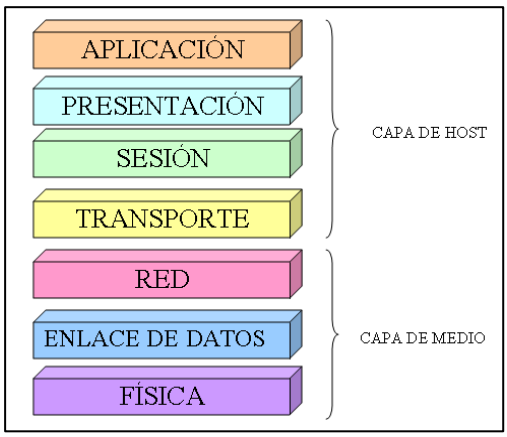

Figura 2: Modelo de Capas OSI

3.1 Proxy Web

[5] Actualmente es el más conocido ya que interviene en la navegación por la web. Se encarga del acceso a la web mediante HTTP y HTTPS, actuando como una aplicación web.

Al ser parecido a una aplicación web, podemos decir que trabaja sobre la capa de aplicación del modelo OSI (Figura 2).

Este proxy se encarga de almacenar el contenido de las páginas web en la caché. Cuando se solicitan, las busca en la caché y comprueba que la versión sea la misma que la que hay en el servidor. Si es la misma, simplemente lo toma de la caché y las envía a nuestro ordenador. En caso contrario, si la versión no coincide con la almacenada, actualiza la caché y carga la nueva página.

En internet, podemos encontrar muchos ejemplos de este tipo de proxy. Por ejemplo, el que podemos encontrar en la referencia [6].

3.2 Proxy Caché

[7] Es muy parecido a Proxy Web. Se diferencia en que, Proxy Caché precarga el contenido de las páginas webs que han sido solicitadas por un usuario, consiguiendo de esta manera disminuir el tiempo de respuesta.

Como ejemplo de Proxy Caché tenemos *Squid* [8].

Más adelante en el *apartado 5*, realizaremos un experimento montando una pequeña LAN de máquinas virtuales, usándolo.

3.3 Proxy Transparente

[9] Este tipo de proxy se encarga de configurar las redes, de manera que el cliente no tiene que configurar los puertos por los que se mandan o reciben las peticiones o respuestas.

Al encargarse de la configuración de red, podemos decir que trabaja sobre la capa de red del modelo OSI (Figura 2).

Es habitual que este tipo de proxy sea usado por empresas proveedoras de acceso a internet.

Existen varios ejemplos, entre ellos *Incloak* [10].

3.4 Proxy Inverso

[11] Se utiliza para proteger al servidor, es decir, el proxy recoge las peticiones, las revisa y si son seguras se las emite al servidor.

No existen en sí ejemplos de este tipo, pero podemos configurar otros servidores proxy para que actúen como uno inverso. Por ejemplo en [12] se muestra como se configuraría Apache.

3.5 Proxy NAT o Enmascaramiento

[13] Para entender que es un Proxy NAT, necesitamos saber lo que es una red NAT.

Definimos una red NAT (*Network Address Translation*) como un traductor de direcciones IP, que enmascara las direcciones privadas en direcciones públicas. Podemos decir que actúa como un intermediario entre el exterior y los equipos conectados a una red interna, permitiendo el acceso a los servicios de la web.

Un Proxy NAT es una herramienta que utiliza una misma IP pública para varios equipos, donde cada uno de ellos tiene una IP privada.

Para entender mejor el funcionamiento vamos a verlo con un pequeño ejemplo: Vamos a suponer que tenemos una empresa con varios trabajadores donde cada uno de ellos dispone de un equipo. Todos los equipos compartirán una misma conexión a Internet, debido a que solo dispondremos de una dirección IP pública. Dentro de nuestra empresa todos los equipos estarán conectados a una red de área local (LAN) y además contaremos con un servidor proxy. Por lo tanto al estar conectados a la red LAN, todos los equipos tendrán asignada una IP privada. Siendo el proxy el encargado de enmascarar cada una de ellas en una sola pública, para así realizar las peticiones y mandar las respuestas a cada uno de ellos.

Al trabajar de esta manera conseguimos:

- Seguridad, ya que desde el exterior no tienen constancia de nuestra IP privada y por tanto podemos evitar ataques externos.
- Facilidad, porque no necesitamos ninguna configuración adicional en los equipos para poder usarlo.

3.6 Proxy Anónimo

[14] Permiten que naveguemos de forma anónima ocultando nuestra IP. Al realizar la conexión simplemente indica que estamos conectados a un proxy.

Normalmente este tipo de proxy se usan en lugares de trabajo y universidades.

La ocultación en un Proxy Anónimo se puede realizar de distintas formas [22]:

1. Proxy simples: Solamente guarda la IP del proxy.
2. Proxy ruidosos: No aporta exactamente la IP del proxy, sino que genera una IP aleatoria.
3. Proxy alta anonimidad: Oculta el hecho de que estamos usando un Proxy.

A modo de ejemplo tenemos Hide-Me [15].

3.7 Proxy Abierto

[16] Se diferencia de los demás, en que este proxy puede aceptar peticiones desde cualquier ordenador, independientemente de que esté conectado a su red.

Por ejemplo, el envío de correo SPAM usa este tipo de proxy.

4 Ventajas y Desventajas de un Servidor Proxy

4.1 Ventajas [17]

Control: Al ser el servidor proxy un intermediario, es quién se encarga de recibir y mandar peticiones, almacenar IP's, gestionar los puertos, etc. Por tanto se libera de ese trabajo a los usuarios y a su vez pierden privilegios y están más controlados.

Velocidad: Cuando varios clientes lanzan simultáneamente peticiones de distinto tipo al servidor, éste puede sufrir lo que conocemos como cuello de botella, es decir, no va a ser

capaz de responderlas todas. Con un servidor proxy se puede solucionar, ya que tiene la capacidad de guardar las respuestas de algunas peticiones (caché) y por tanto será capaz de responder algunas peticiones sin tener que llegar a mandárselas al servidor.

De esta forma podemos decir que con un servidor proxy se disminuye el tiempo de respuesta y por tanto se gana en velocidad.

Filtrado: Un servidor proxy tiene la capacidad de detectar y evitar páginas webs no deseadas o inseguras. Además podemos configurarlo para que no atienda ciertas peticiones tanto por parte del servidor como del cliente.

Modificación: Como hemos dicho antes, un servidor proxy es un intermediario. Si le añadimos ciertos algoritmos podemos permitir que altere la información que pasa por él. Por ejemplo podemos hacer que falsifique cierta información.

Anonimato: El servidor proxy puede decir quién es el usuario que lo está utilizando o no, es decir, que podemos navegar de manera anónima. Por ejemplo, si queremos acceder a Internet lo habitual es que mandemos nuestra IP, dando acceso a nuestra información. Sin embargo, usando un proxy la IP queda oculta.

Ahorro: Normalmente, el usuario es quien dispone de los recursos necesarios para lanzar peticiones. Utilizando proxy se libera de esa carga al usuario, almacenando él los recursos.

4.2 Desventajas [18]

Abuso: El servidor va a responder a todas las peticiones independientemente de su origen. Como esto no lo controla, puede ser que un usuario malintencionado lance una petición para obtener datos y/o servicios de zonas delicadas.

Carga: El servidor atiende a muchos usuarios que lanzan peticiones. Por tanto está estrechamente relacionado con la cantidad de ordenadores que están conectados. En caso de que estén todos a la vez en la red, se puede generar un cuello de botella.

Anonimato: Navegar de manera anónima también es una desventaja, porque en un momento dado quizás necesitemos que nos identifiquen y será muy costoso o no será posible.

Intromisión: Algunos usuarios querrán que el proxy no almacene sus datos en la caché y prefieran realizar una conexión directa con el servidor, sin pasar por el intermediario.

Incoherencia: Al tener una caché se pueden tener almacenados datos ambiguos, es decir, si un usuario lanza una petición, el proxy puede dar una respuesta equivocada por no estar actualizado.

Irregularidad: Cuando un proxy representa a un grupo de usuarios puede generar conflictos a la hora de activar o desactivar los puertos, es decir, si un usuario de ese grupo quiere habilitar un puerto a la vez que otro usuario lo quiere deshabilitar.

Otras:

- Requiere mantenimiento.
- Todas las comunicaciones externas se hacen a través del proxy por tanto si el servidor cae, no tendremos posibilidad de conectarnos con el exterior.
- Para que las aplicaciones puedan acceder a Internet, debe configurarse el proxy.

5 Configuración de un Servidor Proxy: montando una pequeña LAN de máquinas virtuales

Se puede configurar un proxy para varios SO y máquinas virtuales *VMware*, *VirtualBox*… Nosotros lo vamos a hacer para *VirtualBox* debido a que *VMware* no es gratuita.

Vamos a montar una LAN entre varias máquinas virtuales utilizando un proxy, en concreto, nos crearemos tres máquinas virtuales, dos de ellas actuarán como clientes (ISE1, ISE2) y la restante como servidor proxy (ISE_PROXY). Todas ellas tendrán como sistema operativo Ubuntu 12.04.

***Nota**: No vamos a explicar el proceso de instalación de cada máquina. Damos por hecho que sabemos crearla. Aquí solo nos centraremos en la configuración para crear nuestra LAN.*

Lo primero que haremos será habilitar las redes, para ello nos iremos a “Configuración” y seleccionaremos la pestaña de “Red”. A continuación, explicamos el proceso para cada una de ellas:

1. Configuración de ISE_PROXY: debemos habilitar dos adaptadores de red. El primer adaptador, tendrá una “Red NAT”, con esto conseguimos tener conexión hacia el exterior. Hecho esto, debemos permitir que las otras máquinas puedan acceder a ella. Esto lo conseguimos situándonos en “Avanzadas” y poniendo “Modo promiscuo” como “Permitir todo” (Figura 3). El segundo adaptador, tendrá una red mediante “Adaptador de puente”, que servirá para establecer la conexión con los clientes. Al igual que en el primer adaptador, configuramos el “Modo promiscuo” como “Permitir todo”. (Figura 4)

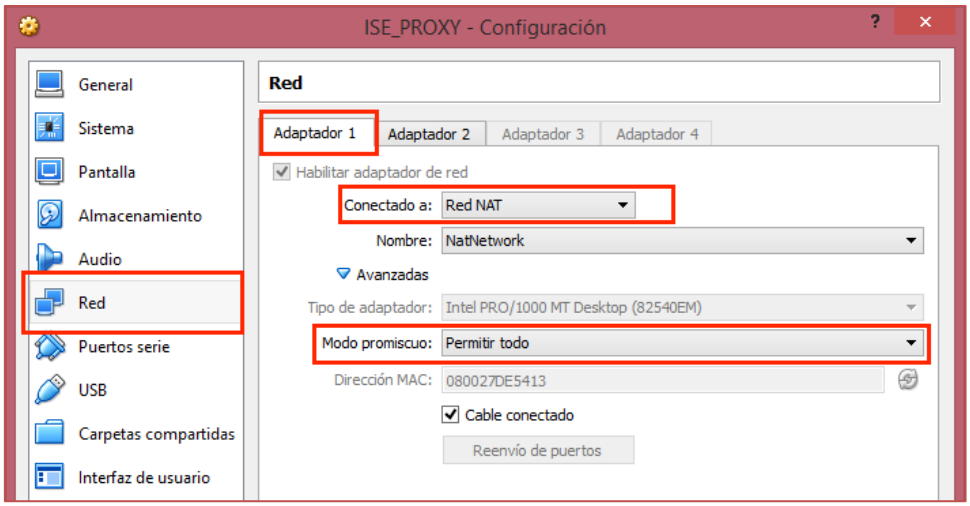

Figura 3: Configuración de “Red NAT” para ISE_PROXY

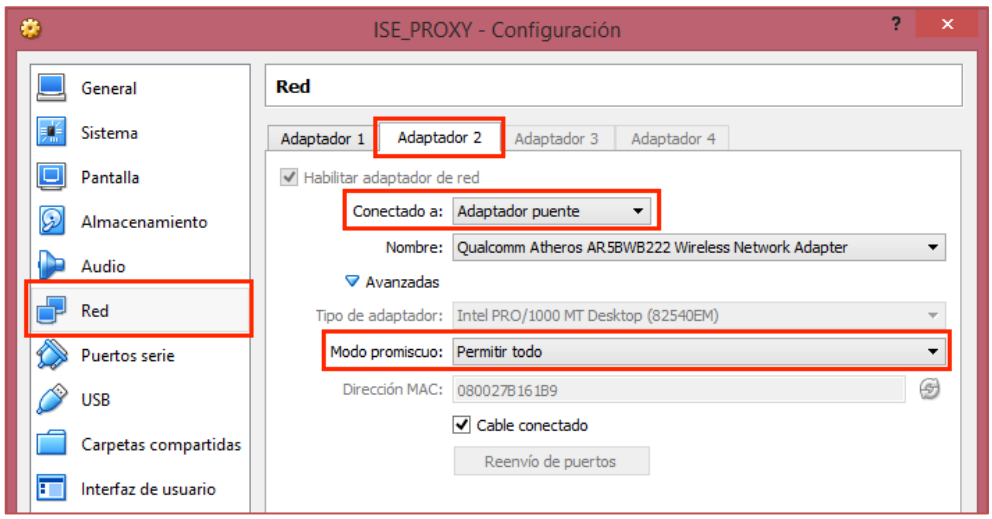

Figura 4: Configuración de “Adaptador puente” para ISE_PROXY

2. Configuración de ISE1 e ISE2: en este caso sólo habilitaremos un adaptador de red que contendrá la misma configuración que el segundo adaptador de ISE_PROXY, porque debemos crear la red interna entre las 3 máquinas (Figura 5).

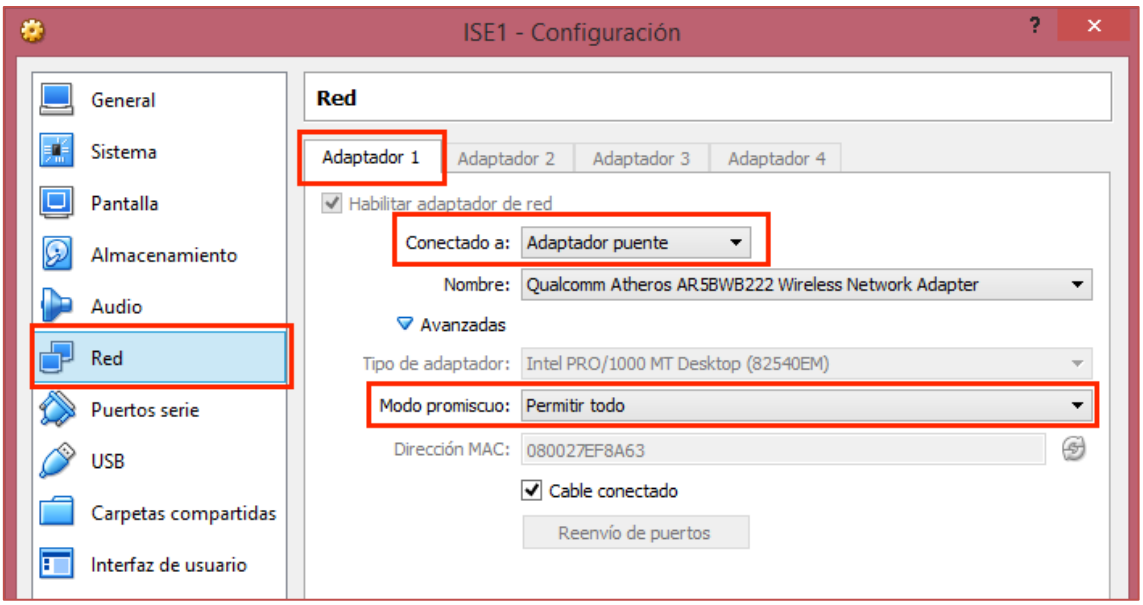

Figura 5: Configuración de "Adaptador puente" para ISE1

Terminado el proceso de habilitar las redes, vamos a configurarlas, iniciándolas. Comenzaremos con ISE_PROXY. Cómo habilitamos anteriormente la "Red NAT" deberíamos tener acceso a Internet y es lo primero que vamos a comprobar (Figura 6).

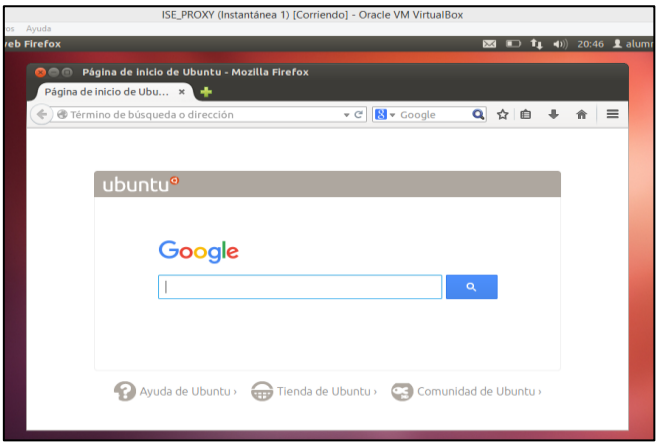

Figura 6: Comprobación de que existe Internet en el proxy

Procedemos a la configuración del adaptador puente. Ejecutaremos el comando *ifconfig* para saber cómo se llama nuestra red. Debido a que lo hemos puesto en el adaptador 2, el nombre que recibe nuestra red en este caso es *eth4* (la segunda que aparece) (Figura 7). Como ya sabemos el nombre de nuestra red, vamos a modificar, en modo administrador (*sudo*), el archivo de configuración de interfaces de red ubicado en *"/etc/network/interfaces*". [19]

Nota: *para mantener el anonimato, ocultamos el "prompt".*

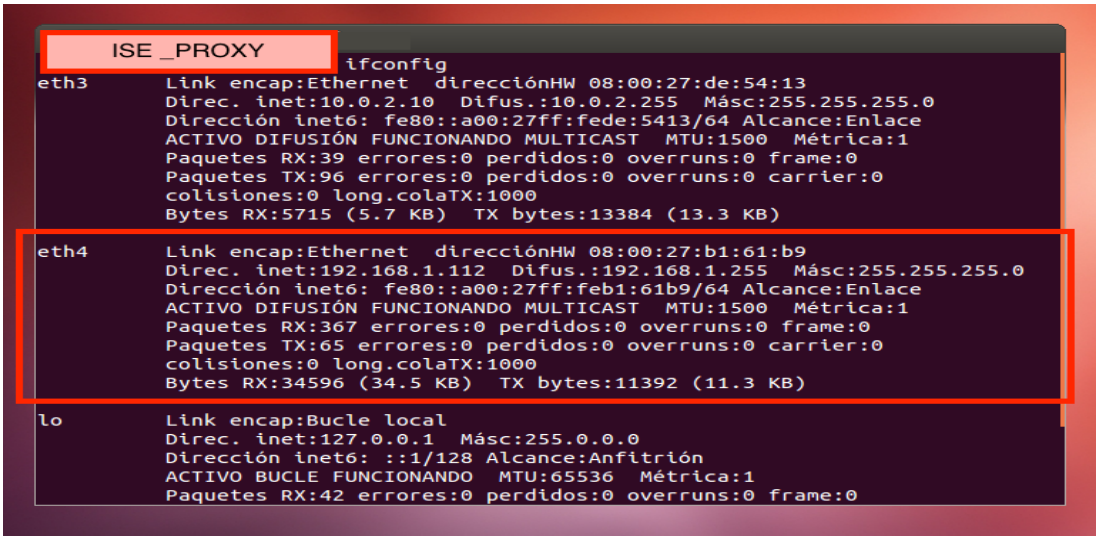

Figura 7: Ejecutando comando ifconfig en ISE_PROXY

Accediendo a él, veremos que contiene algo parecido a la (Figura 8). Lo que hace es asignar una interfaz a la red interna de nuestra máquina. Como a nosotros no nos hace falta, lo que vamos a hacer es eliminarla, así lo que escribamos se verá más claro.

```
auto lo
iface lo inet loopback
```

Figura 8: Contenido inicial del archivo "interfaces"

Lo que vamos a poner es lo siguiente (Figura 9):

- **"auto eth4":** Se especificará qué interfaz se va a modificar cuando se inicie el sistema.
- **"iface eth4 inet static":** Definiremos el nombre de la interfaz (*eth4*), especificando la configuración IPv4 (*inet*) de manera fija (*static*).
- **"address IP":** Pondremos la IP que le queremos asociar a esta máquina para esta interfaz. En nuestro caso hemos elegido 192.168.0.4
- **"netmask MÁSCARA":** Pondremos la máscara que le queremos asociar a esta máquina para esta interfaz de red. En nuestro caso hemos elegido 255.255.255.0

```
auto eth4
iface eth4 inet static
address 192.168.0.4
netmask 255.255.255.0
```

Figura 9: Contenido final del archivo interfaces en ISE_PROXY

Una vez modificado el archivo lo que haremos será guardarlo y además deberemos reiniciar las redes mediante (*"sudo /etc/init.d/networking restart"*). Si hacemos ifconfig veremos que la IP se ha modificado (Figura 10). En caso de no ser así reiniciaremos la máquina.

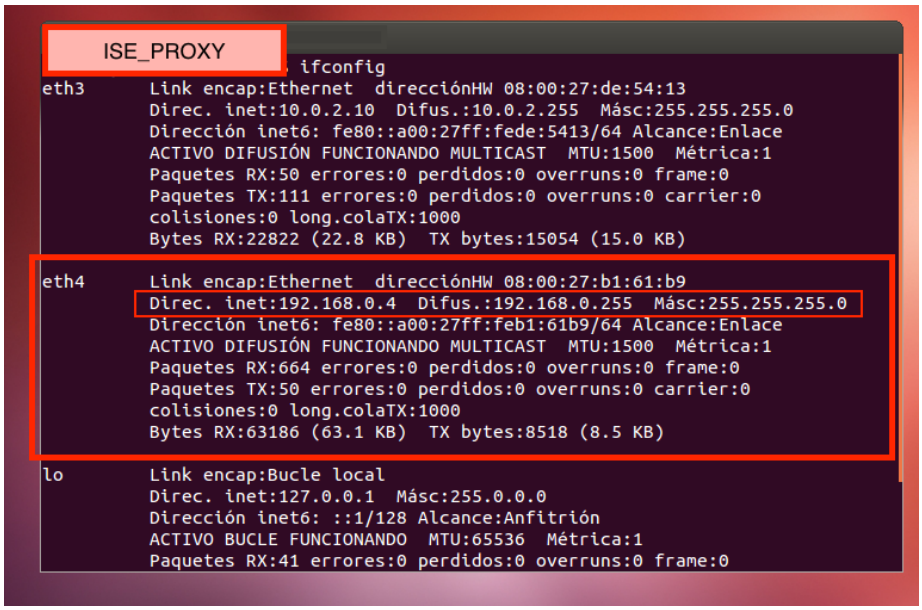

Figura 10: Ejecución de ifconfig, para ver los cambios realizados en nuestra red

Ahora, empezamos con la configuración de red para los clientes, en concreto, para ISE2. Volvemos a ejecutar el comando *ifconfig* (Figura 11), y veremos que esta vez la red a modificar se llama *eth3*. Como hicimos anteriormente accedemos en modo *root* al archivo de configuración de la interfaz de red "*/etc/network/interfaces*".

Incluiremos lo mismo que antes, cambiando *eth4* por *eth3* y la IP por otra (en nuestro caso 192.168.0.5). Además añadiremos una nueva línea: "*gateway IP*" en la que especificaremos la puerta de enlace a otra máquina. En nuestro caso la tenemos que enlazar con ISE_PROXY y por tanto pondremos la IP que le hemos especificado anteriormente (192.168.0.4). Tras hacer estas modificaciones el archivo nos debería quedar como el de la (Figura 12).

```
auto eth3
iface eth3 inet static
address 192.168.0.5
netmask 255.255.255.0
gateway 192.168.0.4
```

Figura 12: Contenido final del archivo interfaces en ISE2

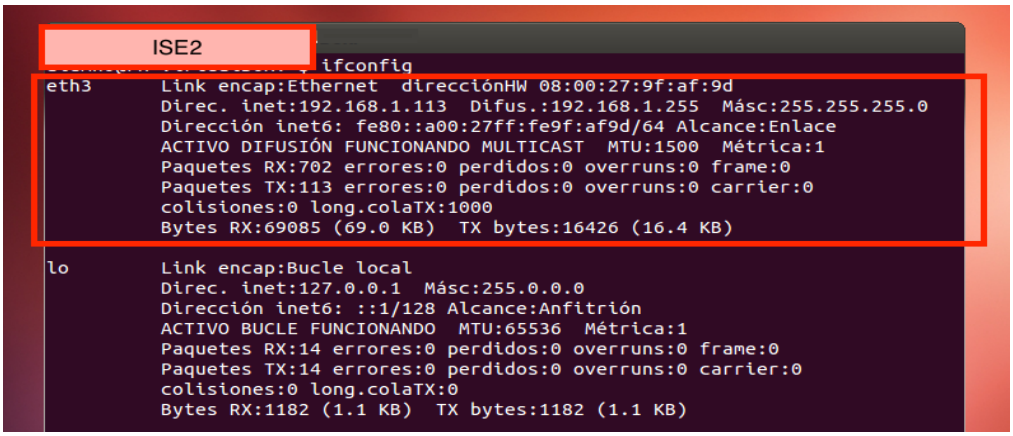

Figura 11: Ejecutando ifconfig, para la máquina ISE2

Al igual que antes reiniciamos las redes y veremos que el cambio se ha producido (Figura 13). Para configurar ISE1, haremos el mismo procedimiento que para ISE2, cambiando la IP a (192.168.0.3) y escogiendo la red adecuada.

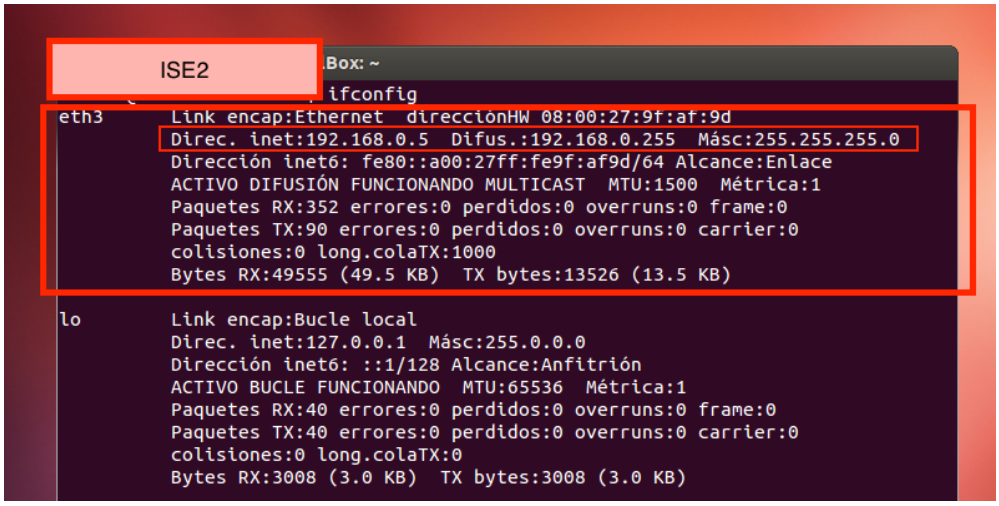

Figura 13: Ejecutando ifconfig, para ver los cambios realizados en nuestra red

Ahora podemos decir que tenemos las tres máquinas configuradas, y por tanto si no tenemos ningún fallo todas las máquinas podrán acceder entre ellas. Esto lo podemos comprobar haciendo *PING* entre las máquinas. Por ejemplo en la Figura 14 vemos que ISE_PROXY tiene conexión con las otras dos máquinas y en Figura 15 que ISE1 tiene acceso a ISE_PROXY.

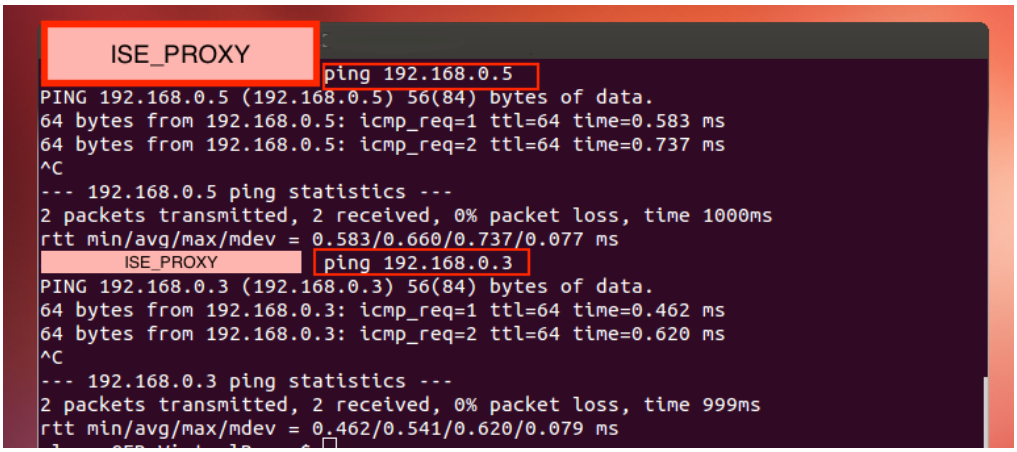

Figura 14: Realizamos PING a las máquinas clientes desde ISE_PROXY

Si no se ha producido ningún fallo hasta el momento, podemos decir que ya tenemos creada la LAN entre las tres máquinas. A continuación, lo que vamos a hacer es configurar ISE_PROXY para que funcione como un proxy, para ello debemos instalar uno. En nuestro caso hemos elegido instalar SQUID3 ya que es uno de los más fiables y más conocidos.

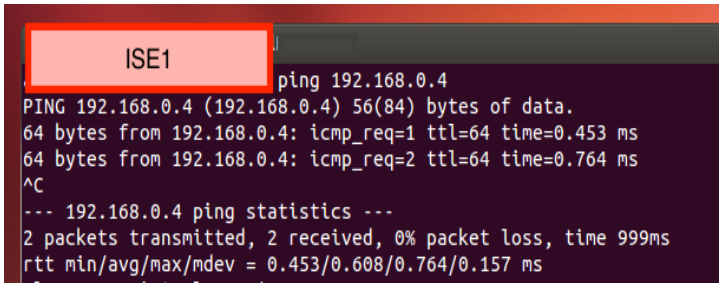

Figura 15: Realizamos PING a ISE_PROXY desde ISE1

Utilizaremos la orden "*sudo apt-get install squid3*" para instalarlo [20]. Cuando finalice, debemos modificar, en modo administrador (*sudo*), el archivo de configuración, ubicado en "*/etc/squid3/squid.conf*", para permitir que las máquinas clientes (ISE1 e ISE2) se puedan conectar a él. Una vez que tengamos el archivo de modificación abierto, deberemos buscar la línea "*#INSERT YOUR OWN RULES HERE*" e introducir a partir de esa línea las reglas que queramos, ya que si lo hacemos antes nos dará problemas. Tenemos que añadir seis cosas muy importantes (Figura 16). Las tres primeras tendrán que ver con la conexión al proxy y las tres segundas estarán relacionadas con los permisos para poder acceder.

Lo primero debemos definir una regla que nos permita conectarnos a nuestra propia red. Para ello pondremos "*acl <nombre> src <mi_IP/máscara>*". Por ejemplo como es para acceder desde mi red, yo le he puesto el nombre "*TODOS*" y en mi caso *mi_IP* contendrá "192.168.0.4/255.255.255.0". La segunda y tercera reglas son para permitir la conexión a las máquinas ISE1 e ISE2. Para conseguirlo simplemente pondremos "*acl <nombre_máquina> src <IP_máquina>*". Por ejemplo para ISE1 sería "*acl ISE1 src 192.168.0.3*".

Y por último debemos darle permiso a las máquinas para que puedan acceder. Esto lo conseguiremos escribiendo "*http_access "allow" <nombre_de_acl>*". Por ejemplo si queremos darle permiso a ISE1 debemos escribir "*http_access allow ISE1*".

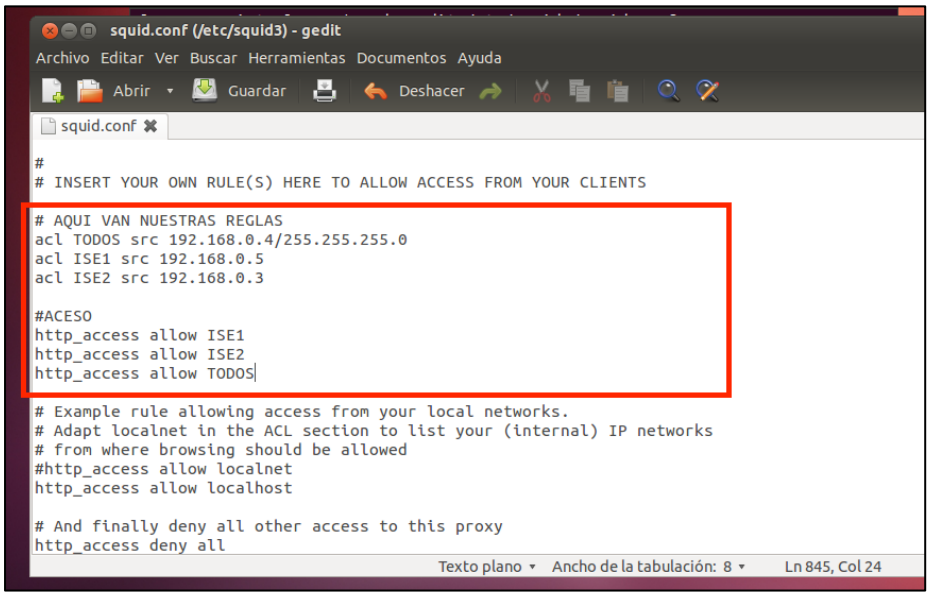

Figura 16: Archivo "/etc/squid3/squid.conf"

Cuando acabemos de modificarlo lo guardaremos y además estableceremos la nueva configuración ejecutando en modo administrador (*sudo*), "*squid3 -k reconfigure*". Es posible que salgan algunos *Warnings* pero no hay nada de lo que preocuparse.

Con esto habremos acabado con ISE_PROXY, ahora tenemos que comprobar que las máquinas clientes, es decir, ISE1 e ISE2 tienen conexión a internet sin problema. Si tratamos de conectarnos con alguna de las dos a internet (por ejemplo ISE1), veremos que no hay

conexión y nos dará un error (Figura 17). [21] Para solucionar esto debemos establecer la conexión al proxy, para ello aprovechando que tenemos interfaz gráfica, nos situaremos en "Sistema" → "Red" → "Proxy de la red" y le daremos a método "manual" donde podremos escribir en "Proxy para HTTP" la IP de nuestro servidor proxy (en nuestro caso debemos escribir "192.168.0.4"). Además deberemos especificar el puerto por el que se va a conectar. Si no lo hemos cambiado, por defecto el puerto que usa SQUID3 es "3128" (Figura 18). Finalmente le daremos a aplicar en todo el sistema y habremos acabado con la configuración. Es posible que nos salga un cartel diciendo que necesitamos permisos especiales y nos pedirá una contraseña. Deberemos introducir la contraseña del administrador.

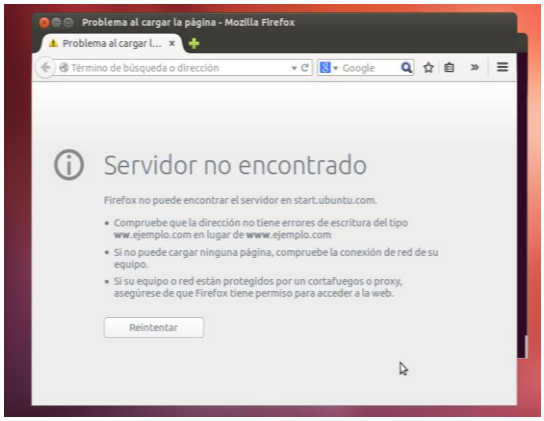

Figura 17: Intento fallido de acceder a Google desde ISE1

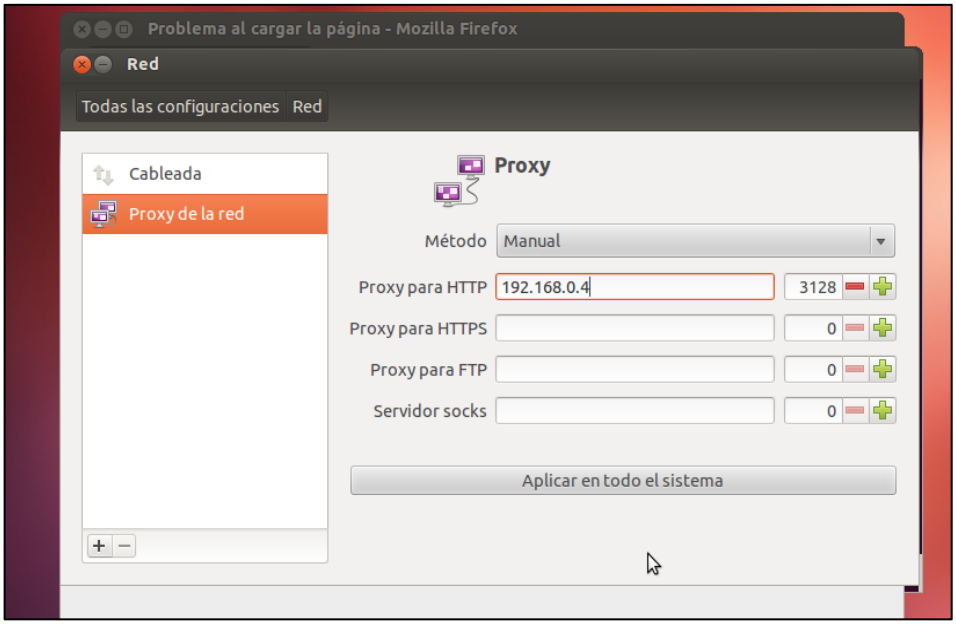

Figura 18: Configuración del proxy para acceder a Internet en ISE1

Si volvemos a intentar conectarnos a internet veremos que en este caso sí podremos hacerlo (Figura 19). Para ISE2 realizaremos exactamente los mismos pasos. Una vez acabado ambas máquina podremos decir que tenemos montada una pequeña LAN con un Proxy.

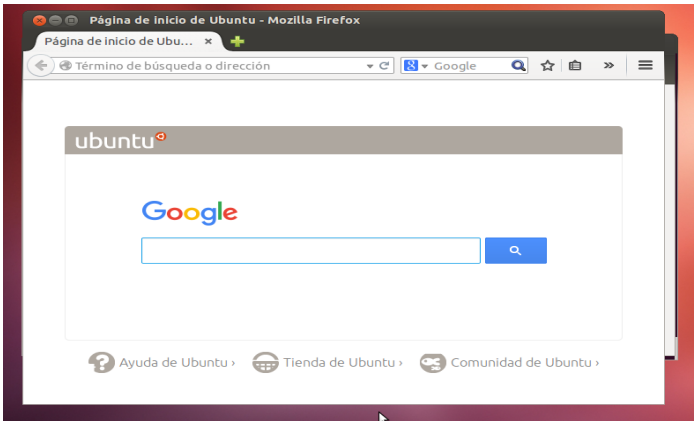

Figura 19: Intento acertado de acceder a Google desde ISE1

6 Conclusiones

El uso de un proxy dependerá de nuestras necesidades. Sería beneficioso si necesitáramos mantener un cierto control, privacidad y seguridad. También su almacenamiento de datos en caché, nos permitirá reducir el ancho de banda. Sin embargo, la caché crece exponencialmente, es decir, cada vez que se actualizan los datos de una página no se borra la versión anterior, simplemente se añade una nueva. Esto a la larga puede suponer un gasto innecesario de memoria.

Debemos tener en cuenta, que configurar un proxy es un proceso sencillo cuando nuestra red de ordenadores es pequeña, sin embargo, si la red es grande, es más costoso configurar el proxy.

7 Bibliografía

[1] Definición de un proxy: http://www.uma.es/servicio-central-de-informatica/info/7888/proxy/

[2] Funcionamiento de un proxy: https://docs.oracle.com/cd/E21692_01/821-1883/aebea/index.html

[3] Objetivos principales: https://technet.microsoft.com/en-us/library/cc939852.aspx

[4] Características de un proxy: http://es.ccm.net/faq/2755-que-es-un-proxy#principio-de-funcionamiento

[5] Definición de Proxy Web: http://www.ipcop.org/2.0.0/es/admin/html/services-webproxy.html

[6] Ejemplo de Proxy Web: https://www.proxysite.com/es/

[7] Definición de Proxy Caché: http://www.um.es/atica/contenidos/proxy/

[8] Ejemplo de Proxy Caché: http://www.squid-cache.org/

[9] Definición de Proxy Transparente: http://www.gfihispana.com/products-and-solutions/network-security-solutions/gfi-webmonitor/specifications/transparent-proxy-mode

[10] Ejemplo de Proxy Transparente: https://incloak.es/proxy-list/

[11] Definición de Proxy Inverso: http://www.ibm.com/support/knowledgecenter/es/SSKTXQ_8.5.0/com.ibm.help.sametime.v85.doc/config/st_adm_port_rvprxy_overview_c.html

[12] Ejemplo de configuración de Apache para que funcione como un Proxy Inverso: https://www.digitalocean.com/community/tutorials/how-to-use-apache-http-server-as-reverse-proxy-using-mod_proxy-extension

[13] Definición y ejemplo de Proxy NAT: http://www.movistar.es/rpmm/estaticos/residencial/fijo/banda-ancha-adsl/manuales/equipamiento-adicional-adsl/guia-instalacion-proxy-nat.pdf

[14] Definición de Proxy Anónimo: http://electronics.howstuffworks.com/how-to-tech/how-to-surf-the-web-anonymously3.htm

[15] Ejemplo de Proxy Anónimo: https://hide.me/en/proxy

[16] Definición de Proxy Abierto: http://www.corpit.ru/mjt/proxycheck.html

[17] Ventajas del Proxy: http://ldc.usb.ve/~daniela/iptables/node15.html

[18] Desventajas del Proxy: http://ldc.usb.ve/~daniela/iptables/node16.html

[19] Configurar el archivo de interfaces de red: http://fpg.66ghz.com/DebianRed/etcnetworkinterfaces.html?i=2

[20] Instalar y configurar Squid: https://www.sospedia.net/tutorial-instalacion-y-configuracion-proxy-squid3/

[21] Configurar Proxy en el cliente: http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m6/proxy_squid.html

[22] Tipos de proxy anónimo: https://seo-en-fiverr.blogspot.com.es/2015/06/niveles-de-anonimato-de-los-proxy.html