Instalación y configuración del appliance

Tipo de documento: entregable
30/06/14

ecoRaee

Life

UniversidadeVigo

energylab

revertia

Tabla de contenidos del proceso demostrativo

Índice de tablas e ilustraciones

1.- Introducción

El objetivo de este demostrativo es la instalación y configuración de una máquina, con hardware basado en el reciclaje de ordenadores usados, que sirva de sistema de defensa perimetral para redes de PYMES y particulares. El uso de herramientas libres y preferentemente gratuitas propiciará una reducción de costes en la solución, frente a otros sistemas comerciales. Se persigue como objetivo esta reducción de costes para favorecer la entrada del producto en PYMES, que normalmente tienden a ser reacias a grandes inversiones tecnológicas, especialmente en el ámbito de la seguridad informática. El sistema será capaz de realizar las funciones de: antivirus, antispam, control de contenidos y firewall.

En la actualidad casi cualquier PYME necesitará para el desempeño de su actividad, sea del sector industrial que sea, tener acceso a una red de datos. Generalmente y a pesar de la popularización y expansión de las redes de datos móviles, la solución adoptada mayoritariamente es la contratación de una linea de datos terrestre. Con este tipo de lineas las operadoras incluyen un router de conexión a la red que hará las funciones de switch (inalámbrico y cableado) dentro de la red local de la empresa y en el mejor de los casos la contratación incluirá licencia para algún software antivirus para su instalación en los equipos informáticos de la empresa.

Si bien la instalación de antivirus de forma local en cada equipo de la empresa debe ser algo que obligatoriamente debemos realizar para intentar garantizar el buen desempeño de las máquinas y la protección de nuestros datos, este tipo de protección de seguridad se antoja insuficiente, teniendo en cuenta la cada vez mayor diversificación de los ataques electrónicos.

Para proteger los equipos de una red de ataques del exterior, sean ataques automatizados en forma de virus o ataques dirigidos, es recomendable el uso de algún tipo de dispositivo de defensa perimetral.

Este tipo de dispositivos se colocan en la entrada/salida de la red y todo el tráfico de la misma se hace pasar por ellos. Así en lugar de tener que proteger del exterior todos y cada una de las máquinas de nuestra organización lo limitamos a un solo punto.

Actualmente, distintas empresas basadas sobre todo en seguridad informática, ofrecen distintas soluciones de defensa perimetral integrando en ella sus herramientas de firewall, antivirus o antispam. Estas soluciones suelen tener un coste relativamente elevado, sobre todo para una PYME, ya que su coste oscila entre los 2.500€ y los 10.000€ de desembolso inicial más el coste de mantenimiento y renovación de licencias anuales, que dependiendo del producto contratado pueden suponer unos costes anuales de entre 1.000€ y 5.000€.

general la mayoría de usuarios no valoran de forma realista el riesgo que puede suponer la perdida de sus datos informáticos o el robo de los mismos, hasta que es demasiado tarde.

La idea es ofrecer a las PYMES un producto de defensa perimetral más asequible que cubra las funciones básicas de protección. Que además el coste anual se base solo en el mantenimiento y actualizaciones, al estar basado en software libre no es necesaria la renovación de costosas licencias. Con todas estás premisas de ofrecer un servicio igual o equivalente pero a un coste mucho menor, es más que probable que muchas empresas estén interesadas en su adquisición.

El desarrollo de este tipo de producto pues, parece más que posible y rentable, aunque parece que de momento no es un mercado que esté siendo explotado por ninguna empresa de forma general. Uno de los motivos sin duda es el hecho de que las empresas que comercializan actualmente este tipo de productos son empresas que se dedican a la seguridad informática pero usando una política de software propietario. Esto hace que sus productos de defensa perimetral, lógicamente, estén basados en sus soluciones, lo que representa un alto coste. Por otro lado no hay actualmente ninguna gran empresa de seguridad detrás de las principales soluciones de seguridad informática basadas en software libre, aunque si podemos encontrar importantes comunidades de desarrollo o funciones como la fundación Apache, que sin duda es una garantía de fiabilidad y confianza en el software.

Además de ser un elemento de seguridad, podemos configurar el appliance para que ejerza como elemento de control de contenidos. Podremos definir que nivel de control queremos que asuma, para así prevenir el uso no autorizado de los equipos de la organización, o para prevenir el tipo de material que se visualiza. Estas opciones son de gran utilidad para su implantación en redes de acceso público o con máquinas accesibles a menores, como pueden ser: escuelas, bibliotecas, puntos de información municipal, …

En general el appliance funciona de forma transparente y debemos conectarlo en la entrada de red entre el router que proporciona conexión y el switch que la distribuye en la red local, tal y como podemos ver en la imagen a continuación.

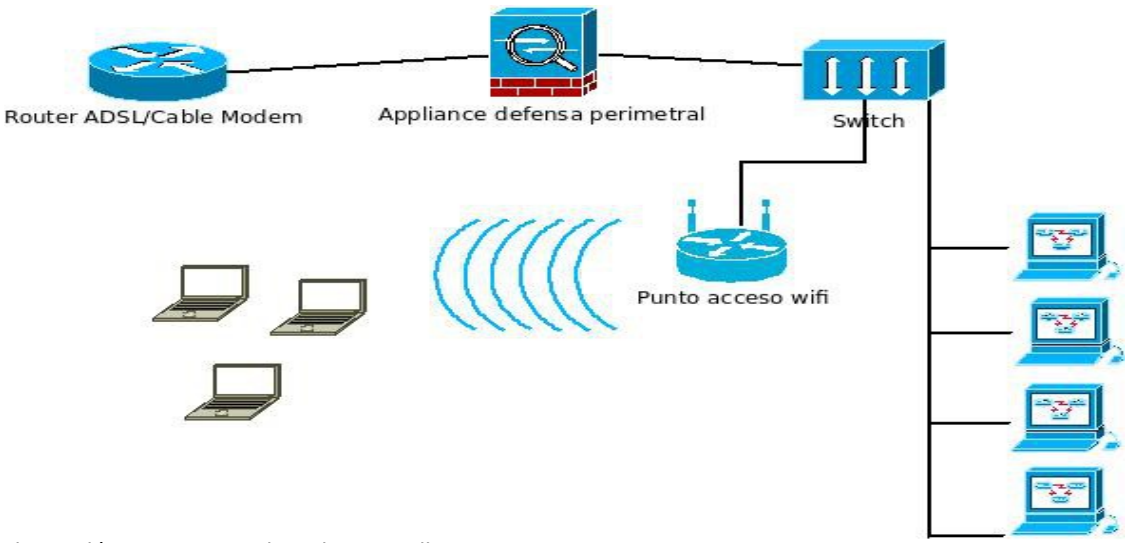

Ilustración 1: Esquema de red con appliance

2.- Configuración del firewall de la máquina

Para configurar el firewall de la máquina, usaremos directamente el sistema de iptables [Ref. 2] presente en los sistemas Linux. A la hora de definir el firewall tenemos que tener en cuenta las tres posibilidades de funcionamiento del appliance que podemos ofrecer:

- Filtrado completamente transparente

Este modo de funcionamiento esta especialmente pensado para centros de trabajo que no requieren un filtrado muy amplio de contenidos y que lo que más preocupa es la seguridad de los mismos. El appliance simplemente analizará ficheros y páginas web en navegación no segura y correo pop o smtp. En caso de detectar algún virus o contenido no deseado, definido en los filtros, será bloqueado.

- Filtrado transparente para navegación web y correo con bloqueos específicos

Este modo de trabajo esta especialmente pensado para centros educativos, en los que las necesidades de filtrado son mayores que en otros lugares. En este caso podremos decidir la política de filtrado que queremos seguir. En una elección típica es habitual filtrar el contenido de navegación segura, ya que este contenido no puede ser analizado por el filtro de contenido. En este caso debemos habilitar en el firewall los rangos de ips que se correspondan con los servicios que el centro quiera permitir. También podemos optar por la opción contraria, permitimos de forma general la navegación segura, pero decidimos que servicios bloqueamos, cerrando todo el tráfico a sus rangos de ips.

- Filtrado en modo gateway

Este modo de trabajo esta pensado para aquellas organizaciones que además del filtrado de contenido y análisis de virus, desean usar el dispositivo como firewall de su intranet. En este caso debemos cambiar no solo la configuración del firewall, sino también la configuración de las interfaces de red. Debemos eliminar el bridge de red creado en la configuración de red inicial y asignar una ip a cada interfaz. Una vez tenemos esto la interfaz que quede como interior a la red local pasará a ser la puerta de enlace de los equipos de la LAN. Este modo de funcionamiento por tanto requiere mayor configuración y adaptación por parte de los usuarios de la red.

2.1.- Creación del firewall inicial

El firewall del sistema lo crearemos añadiendo un fichero con las reglas iptables que deseamos en /etc/iptables.up.rules, usamos este fichero para que luego a la hora de gestionarlo con webmin sea detectado y podamos editarlo desde la interfaz web.

```
# cat /etc/iptables.up.rules
        # Generated by iptables-save v1.4.14 on Fri Mar 28 11:43:46 2014
        *mangle
        :PREROUTING ACCEPT [211923000:155839500823]
        :INPUT ACCEPT [6467442:7265855501]
        :FORWARD ACCEPT [205436007:148574583276]
        :OUTPUT ACCEPT [5455381:7185428958]
        :POSTROUTING ACCEPT [210891388:155760012234]
        COMMIT
        # Completed on Fri Mar 28 11:43:46 2014
        # Generated by iptables-save v1.4.14 on Fri Mar 28 11:43:46 2014
        *nat
        :PREROUTING ACCEPT [505397:47349688]
        :INPUT ACCEPT [43324:2548306]
        :OUTPUT ACCEPT [109664:6667453]
        :POSTROUTING ACCEPT [570983:48948916]
        COMMIT
        # Completed on Fri Mar 28 11:43:46 2014
        # Generated by iptables-save v1.4.14 on Fri Mar 28 11:43:46 2014
        *filter
        :FORWARD ACCEPT [0:0]
        :INPUT ACCEPT [0:0]
        :OUTPUT ACCEPT [0:0]
        :LOGGING - [0:0]
        -A INPUT -i lo -j ACCEPT
        -A INPUT -m state --state RELATED, ESTABLISHED -j ACCEPT
        -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
        -A INPUT -p udp -m udp --dport 22 -j ACCEPT
        -A INPUT -p tcp -m tcp --dport 1:1024 -j DROP
        -A INPUT -p udp -m udp --dport 1:1024 -j DROP
        COMMIT
```

Con esto el sistema acepta conexiones al puerto 22 para el uso de ssh y no hay ningún tipo de interferencia con el tráfico que pasa por el bridge de red. Según vayamos añadiendo servicios al equipo, tendremos que ir añadiendo las reglas correspondientes a este firewall. Hay que tener en cuenta que la forma de actuar tanto del antivirus, como del filtro de contenidos es mediante el uso de proxies [Ref. 3] transparentes que desvien el tráfico para su análisis y posterior decisión de permitir o no el acceso al mismo.

Una vez creado este fichero debemos asegurarnos que se ejecute cada vez que se inicie el sistema de red, para eso creamos un fichero con permisos de ejecución dentro de la configuración inicial de la red, será /etc/network/if-pre-up.d/iptables con el siguiente contenido:

```
#!/bin/bash
/sbin/iptables-restore < /etc/iptables.up.rules
```

3.- Instalación del proxy para el antivirus

Para el análisis de virus usaremos ClamAV [Ref. 4] antivirus el cual no posee por si mismo la opción de proxy anteriormente mencionada, por lo que nos apoyaremos para realizar esta función en el proxy http para análisis de virus Havp [Ref. 5].

Nos bajamos el paquete de los repositorios de Debian sid, ya que en la versión stable que instalamos no se encuentra disponible y lo instalamos con el gestor de paquetes:

```
# wget http://ftp.de.debian.org/debian/pool/main/h/havp/havp_0.92a-2_amd64.deb
# dpkg -i havp_0.92a-2_amd64.deb
```

4.- Instalación del antivirus y antispam

Para instalar el antivirus libre ClamAV usaremos los repositorios del sistema:

```
# apt-get install clamav clamav-freshclam spampd
```

5.- Instalación del proxy de navegación web y el de correo

Para poder realizar el análisis de contenidos web, debemos instalar un servicio de proxy hacia el que el sistema derive toda la navegación, para ser analizada y una vez validada ser redirigida a su destinatario correspondiente, o en caso de ser rechazada enviar el mensaje de bloqueo con la razón del mismo. Usaremos el proxy de contenidos libre Squid 3 [Ref. 6] disponible en los repositorios de Debian para la navegación web y P3SCAN para el correo. Los que instalaremos haciendo:

```
# apt-get install squid3 p3scan
```

6.- Instalación del filtro de contenidos

Para poder realizar el filtrado de contenido web autorizado, debemos instalar un filtro de contenidos que analice el tráfico que pasa por el proxy anteriormente instalado. Para la realización de este appliance seleccionamos Dansguardian [Ref. 7] como filtro de contenidos. Su instalación se realiza desde los repositorios de Debian, usando:

```
# apt-get install dansguardian
```

7.- Configuración integrada de los servicios

Una vez que tenemos instalado, el proxy para analisis de ficheros, el proxy para navegación web, el antivirus y el filtro de contenidos debemos realizar la integración de todos estos servicios entre si para que trabajen juntos y el sistema permita el control y los análisis requeridos de forma lo más transparente posible al usuario.

A continuación se exponen los ajustes de configuración que debemos hacer para tener estos servicios funcionando de manera integrada. Estos ajustes básicamente consisten en fijar los parámetros de conexión e interoperatividad de los mismos.

7.1.- Configuración de Dansguardian

Para el caso de Dansguardian debemos editar el fichero de configuración /etc/dansguardian/dansguardian.conf. Tal y como podemos ver al principio del fichero lo primero que debemos hacer en cuanto empecemos a aplicar nuestra propia configuración es comentar la linea que comienza con UNCONFIGURED para que el servicio sepa que ya no tiene los parámetros por defecto. Además verificamos los valores siguientes:

```
# the port that DansGuardian listens to.
filterport = 8080

# the ip of the proxy (default is the loopback - i.e. this server)
proxyip = 127.0.0.1

# the port DansGuardian connects to proxy on
proxyport = 8090
```

Para redirigir el tráfico web que pase por el bridge de red y sea así analizado por Dansguardian debemos incluir la siguiente regla en el firewall:

```
-A PREROUTING -i br0 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 8080
```

7.2.- Configuración de Squid 3

Para el caso de Squid 3 debemos editar el fichero de configuración /etc/squid3/squid.conf debemos añadir transparent en la siguiente linea:

```
http_port 3128 transparent
```

Para Squid además configuramos el uso de cache para mejorar la velocidad y eficiencia de la navegación web, para ello debemos añadir las siguiente linea al fichero:

```
cache_dir ufs /var/spool/squid3 256 16 256
```

Para redirigir el tráfico web que pase por el bridge de red y sea así analizado por Dansguardian debemos incluir la siguiente regla en el firewall:

```
-A PREROUTING -i br0 -p tcp -m tcp --dport 3128 -j REDIRECT --to-ports 8080
```

7.3.- Configuración de HAVP

Para el caso de HAVP debemos editar el fichero /etc/havp/havp.conf en el que añadiremos las siguientes lineas:

```
PARENTPROXY 127.0.0.1
PARENTPORT 3128
PORT 8090
ENABLECLAMLIB true
CLAMDBDIR /var/lib/clamav
```

7.4.- Configuración de P3SCAN

Para configurar P3SCAN debemos editar el fichero /etc/p3scan/p3scan.conf. Debemos configurar el puerto, activar la comprobación de spam y virus y para hacer más fácil la integración con el antivirus usar el mismo usuario que este último. Para realizar estos ajustes cambiamos las siguientes lineas en el fichero de configuración:

```
maxchilds = 10
ip = 0.0.0.0
port = 8110
emailport = 25
user = clamav
notifydir = /var/spool/p3scan/notify
virusdir = /var/spool/p3scan
scannertype = basic
scanner = /usr/bin/clamdscan --no-summary
virusregexp = .*: (.*) FOUND
checkspam
spamcheck = /usr/bin/spamc
```

Para redirigir el tráfico de correo y hacer que pase por el proxy para su análisis debemos añadir al firewall las siguientes reglas:

```
-A PREROUTING -i br0 -p tcp -m tcp --dport 25 -j REDIRECT --to-ports 8110
-A PREROUTING -i br0 -p tcp -m tcp --dport 110 -j REDIRECT --to-ports 8110
-A PREROUTING -i br0 -p tcp -m tcp --dport 143 -j REDIRECT --to-ports 8110
-A PREROUTING -i br0 -p tcp -m tcp --dport 995 -j REDIRECT --to-ports 8110
-A OUTPUT -p tcp -m tcp --dport 25 -m owner --uid-owner 104 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 110 -m owner --uid-owner 104 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 143 -m owner --uid-owner 104 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 995 -m owner --uid-owner 104 -j ACCEPT
```

7.5.- Configuración de antivirus y antispam

Para la configuración del antivirus y antispam debemos revisar tres ficheros. Por un lado el fichero de configuración de ClamAV que está en /etc/clamav/clamd.conf y que inicialmente podemos dejar con la configuración por defecto. Por otro la configuración del módulo para antispam en la que debemos modificar dos ficheros /etc/default/spampd y /etc/default/spamassassin

En /etc/default/spamassassin solo debemos activar el uso de spamd:

```
# Change to one to enable spamd
ENABLED=1
```

En /etc/default/spampd modificamos usuario y grupo:

```
# user ID to run as
USERID=clamav
# group ID to run as
GRPID=clamav
```

7.6.- Arranque de los servicios configurados

Una vez tenemos todos los cambios realizados para la integración de los servicios del appliance podemos reiniciarlos todos para la aplicación de estos cambios y puesta en marcha del sistema. No hay un orden de arranque necesario para el sistema, por lo que no tiene que ser el que vemos a continuación.

```
root@gateway:~# service squid3 restart
[ ok ] Restarting Squid HTTP Proxy 3.x: squid3[....]
Waiting.....................................done.
. ok

root@gateway:~# service havp restart
Stopping havp: havp.
Cleaning up /var/spool/havp... done
Unmounting /var/spool/havp ...done
Mounting /var/lib/havp/havp.loop under /var/spool/havp ...done
Cleaning up /var/spool/havp... done
Starting havp: Starting HAVP Version: 0.92
havp.

root@gateway:~# service p3scan restart
Stopping transparent pop3 virus- and spam-scanner: p3scan.
Starting transparent pop3 virus- and spam-scanner: p3scan.

root@gateway:~# service dansguardian restart
[ ok ] Restarting DansGuardian: dansguardian.

root@gateway:~# service spampd restart
[ ok ing spam checking proxy daemon: spampd .
[....] Starting spam checking proxy daemon: spampd
. ok

root@gateway:~# service clamav-daemon restart
[ ok ] Stopping ClamAV daemon: clamd Waiting . . . . . .
[ ok ] Starting ClamAV daemon: clamd .

root@gateway:~# iptables-restore < /etc/iptables.up.rules
```

Si todos los servicios arrancan correctamente y la aplicación de las reglas de iptables no contiene errores, tendremos el appliance funcionando de forma transparente para los usuarios de la red.

8.- Instalación de Webmin para gestión web

Para facilitar la gestión del appliance a los administradores de red, es recomendable la instalación de alguna herramienta que pueda integrar la configuración del sistema, eligiendo en este caso Webmin [Ref. 8].

Webmin no se encuentra en los repositorios de paquetes de Debian aunque si provee su propio repositorio y paquetes deb. Por tanto para su instalación optaremos por descargar el paquete deb e instalarlo con el gestor de paquetes.

```
# wget http://prdownloads.sourceforge.net/webadmin/webmin_1.680_all.deb
# dpkg -i webmin_1.680_all.deb
```

Usaremos la configuración por defecto de webmin. Puesto que usa para el acceso web el puerto 10000 lo añadimos a la configuración del firewall:

```
-A INPUT -p tcp -m tcp --dport 10000 -j ACCEPT
-A INPUT -p udp -m udp --dport 10000 -j ACCEPT
```

Para acceder a Webmin pondremos en nuestro navegador: https://<ip_del_appliance>:10000 y podremos loguearnos con un usuario válido del sistema.

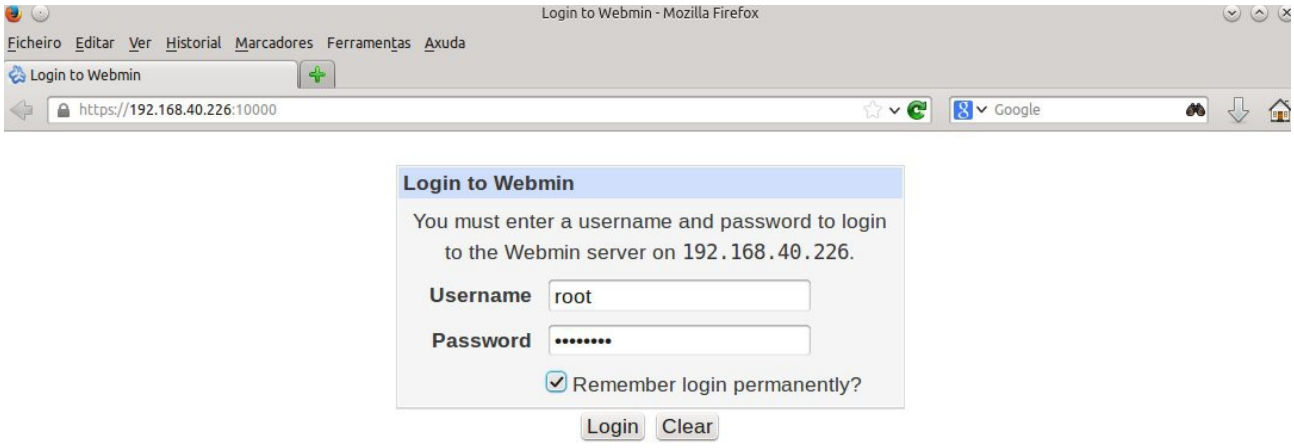

Ilustración 2: Login de Webmin

Una vez dentro del sistema vemos un resumen del estado del appliance y el menú de la izquierda desde el que podremos gestionar los distintos servicios instalados, así como la configuración básica del sistema. Webmin además dispone de un sistema de plugins que nos permite añadir opciones de configuración que nos puedan interesar.

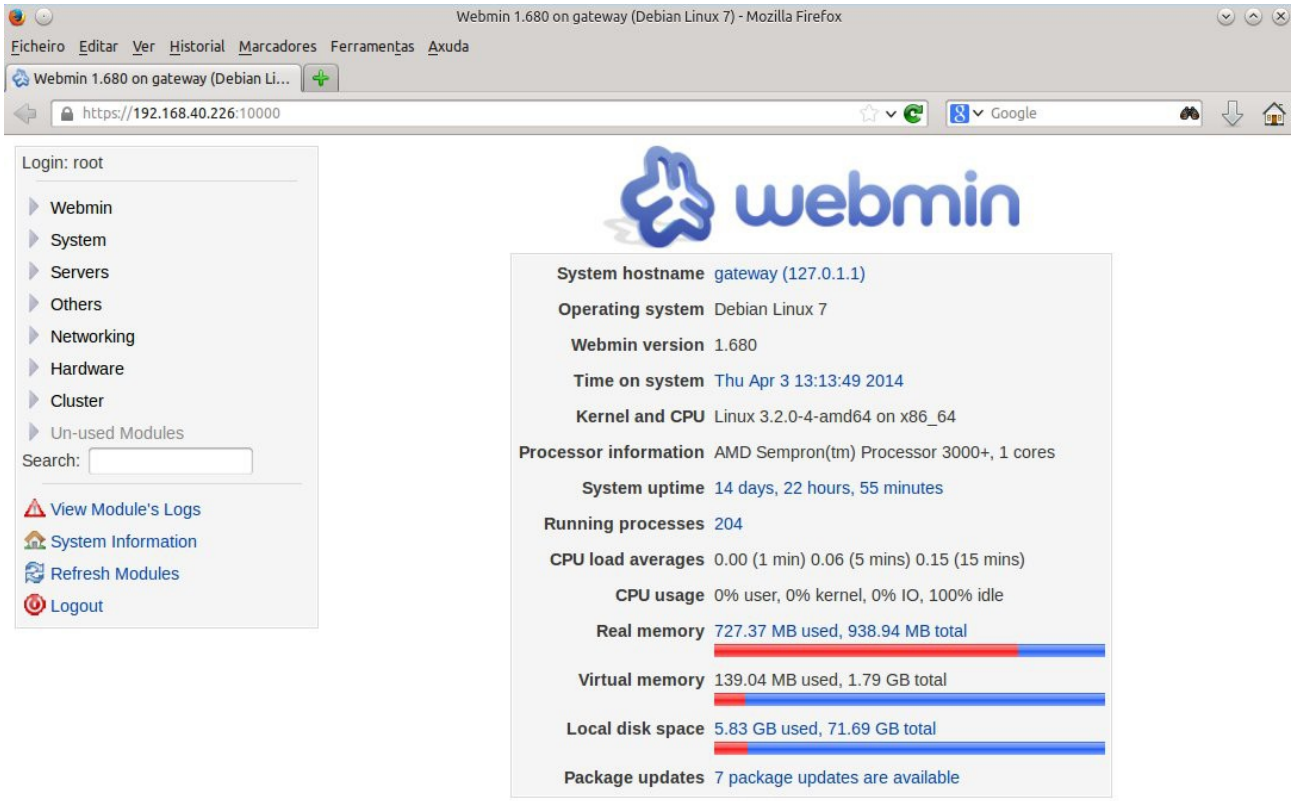

Ilustración 3: Pantalla inicial de Webmin

9.- Personalización de mensajes de error

Podemos personalizar todos los mensajes de error o bloqueo que proporcionan los diferentes servicios instalados en el appliance. Para ello accedemos a las distintas plantillas que proporcionan para incluir los datos de nuestra organización que consideremos importantes.

- Para modificar el error de Dansguadian: /etc/dansguardian/languages/spanish/template.html
- Para modificar el error de HAVP: /etc/havp/templates/es
- Para mofificar el error de Squid: /usr/share/squid/errors/es/

A continuación vemos un ejemplo del mensaje de bloqueo de Dansguardian.

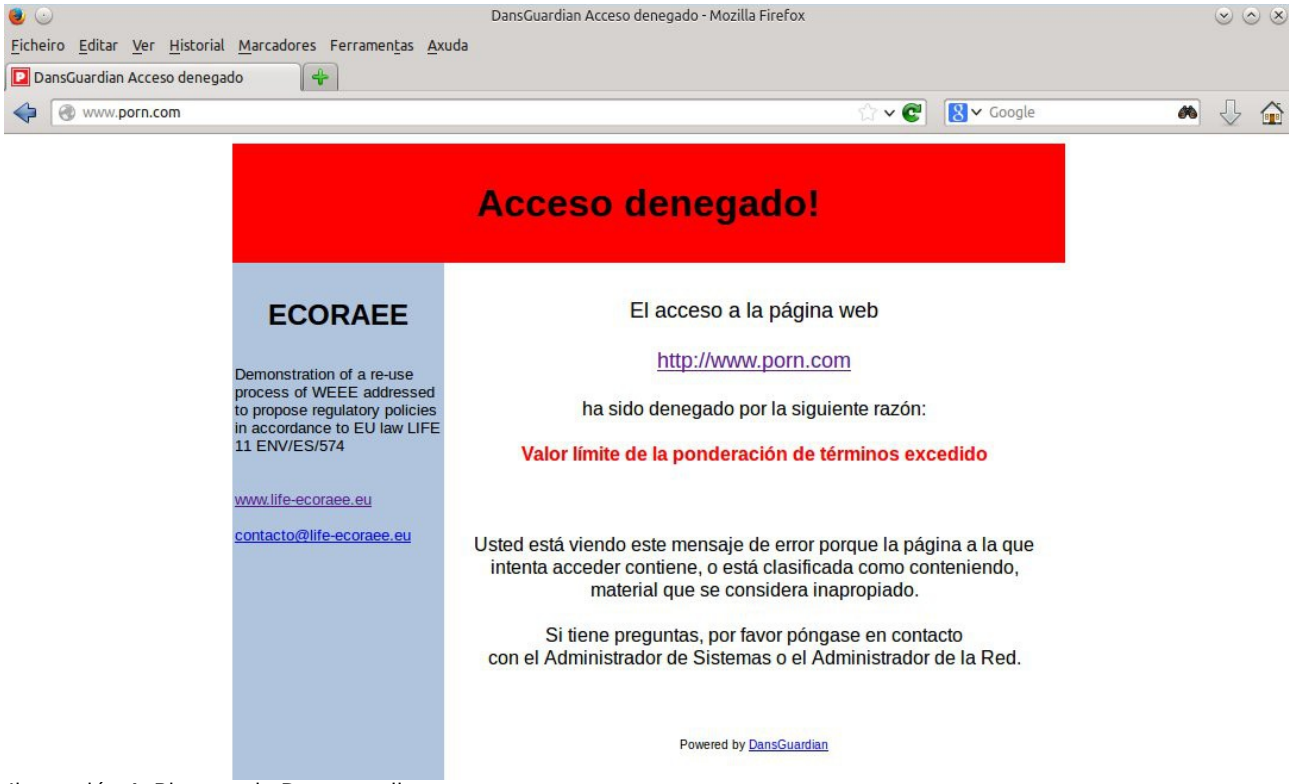

Ilustración 4: Bloqueo de Dansguardian

10.- Configuración avanzada de Squid

A la instalación casi por defecto que tenemos funcionando de Squid vamos añadirle algunas opciones que pueden resultar útiles en la gestión diaria del appliance, así como incluir algunos de parámetros que tratan de optimizar el funcionamiento del servicio.

En algún momento, puede ser necesario o interesante poder forzar a que una página web se recargue en la cache del proxy. Para esto podemos apoyarnos en la herramienta squidclient, que podemos instalar desde los repositorios de Debian:

```
# apt-get install squidclient
```

Una vez instalada debemos configurar Squid para que acepte instrucciones de este cliente que tenemos instalado, para ello añadimos las siguiente lineas al fichero de configuración:

```
acl PURGE method PURGE
http_access allow PURGE localhost
http_access deny PURGE
```

Con esto si queremos eliminar algún elemento de la cache, podemos loguearnos en la máquina y usar el siguiente comando:

```
# squidclient -m PURGE http://www.host.com/
```

Otra opción que es interesante cambiar es el uso de IPv4 e IPv6, por defecto Squid usa primero IPv6 y si obtiene respuesta usa esa dirección en vez de la de IPv4. En las pruebas realizadas encontramos que algunas webs, envían erróneamente la dirección IPv6 haciendo que no se pueda consultar la web, como por ejemplo vemos en la página de Aemet, que en caso de no tener soporte para IPv6 no debería mostrar nada pero muestra :: como vemos:

```
$ host www.aemet.es
www.aemet.es is an alias for B23117.cdn.telefonica.com.
B23117.cdn.telefonica.com is an alias for b23117.1.cdn.telefonica.com.
b23117.1.cdn.telefonica.com has address 81.45.8.13
b23117.1.cdn.telefonica.com has address 81.45.8.14
b23117.1.cdn.telefonica.com has IPv6 address ::
```

Para cambiar esta opción y hacer que Squid compruebe primero la opción de IPv4 debemos activarlo en el fichero de configuración:

```
dns_v4_first on
```

Otra herramienta auxiliar que puede ser muy útil a la hora de analizar y optimizar el tráfico de Squid es Sarg. Con Sarg podremos crear de forma automática una versión html de los logs del servicio, pudiendo concretar por fecha los que nos interesen. Luego estos logs podremos verlos directamente en el propio appliance usando el servidor Apache 2 que se instaló en el mismo como dependencia de otros servicios instalados. Para instalar esta herramienta podemos hacer uso de los repositorios de Debian:

```
# apt-get install sarg
```

Para generar un informe de un día concreto simplemente tendremos que llamar al comando especificando el día que nos interesa, por ejemplo:

```
# sarg-reports manual 19/03/2014
```

Esto creará el informe en la ruta por defecto de la herramienta /var/lib/sarg/, podemos usar el cron del sistema para automatizar este proceso y para ver los informes podemos enlazar esa ubicación con la ubicación por defecto de Apache para acceder a ellos vía web, haciendo:

```
# ln -s /var/lib/sarg/ /var/www/informes_squid/
```

Una vez hayamos hecho este enlace para acceder a los informes podremos hacerlo vía web: http://<ip_appliance>/informes_squid/

Puesto que disponemos de Webmin instalado podemos también modificar desde ahí la mayoría de los parámetros de configuración del servicio, para poder guardar los cambios debemos acceder a webmin como usuario root para que así disponga de los permisos adecuados para volcar los cambios realizados en los ficheros de configuración correspondientes.

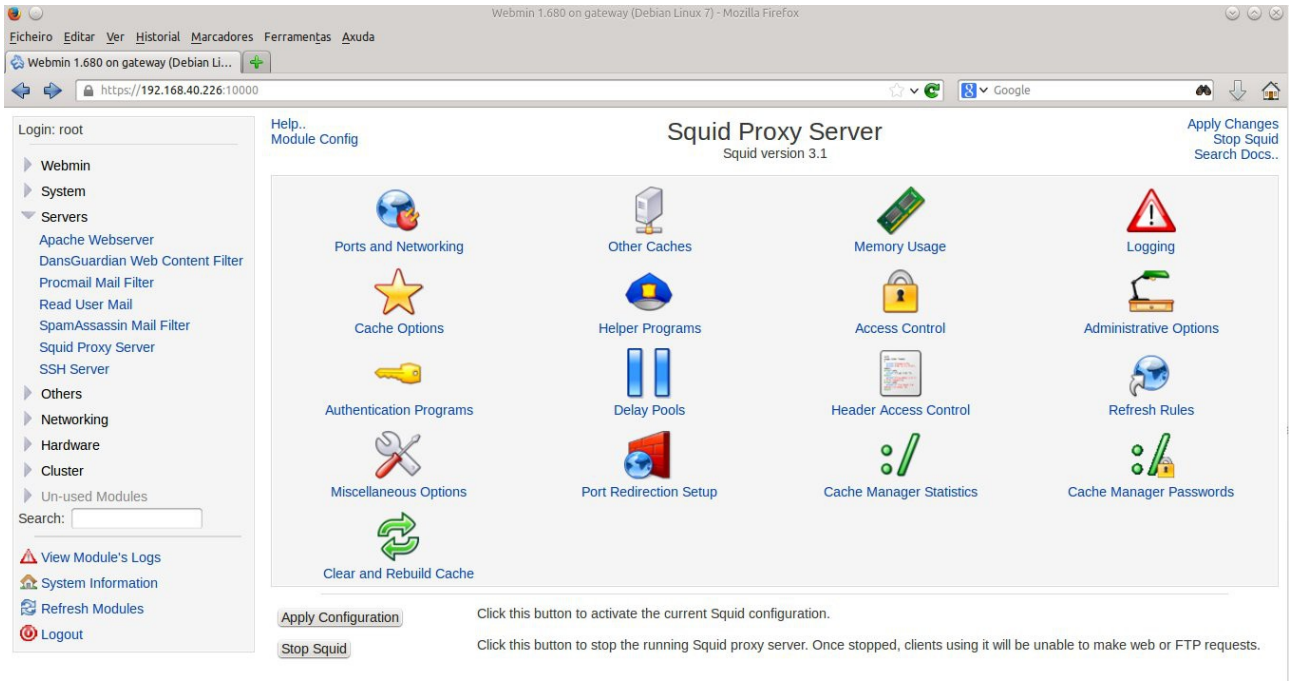

Ilustración 5: Opciones de Squid en Webmin

11.- Configuración avanzada de Dansguadian

La instalación por defecto de Dansguadian trae una configuración por defecto demasiado restrictiva para algunas cosas por ello vamos a ver como parametrizar un poco más la configuración y así adaptarla más a nuestras necesidades añadiendo o quitando restricciones.

Una de las principales formas de bloqueo que usa Dansguadian es basarse en términos que aparecen en la web que estamos visitando, cada término es comparado contra sus listas de términos prohibidos y obteniendo de esas listas un peso. La suma de estos pesos determina si la página puede ser visitada o no. Por defecto la configuración viene con un peso total menor que 50, este nivel de bloqueo se considera adecuado para niños pequeños. Según la ayuda del propio Dansguardian debemos situar este peso en 100 para niños mayores y 160 para adolescentes. De todas formas el valor deberíamos ajustarlo según vayamos viendo en el día a día. En este caso por defecto va fijado en 200 y para cambiarlo solo debemos ir al fichero /etc/dansguardian/dansguardianf1.conf y ajustar el valor:

```
naughtynesslimit = 200
```

Puesto que no queremos restringir el acceso a ningún tipo de archivos debemos dejar en blanco los dos ficheros usados para este tipo de restricción:

```
/etc/dansguardian/lists/bannedextensionlist
/etc/dansguardian/lists/bannedmimetypelist
```

Si queremos que alguna máquina de la red local no tenga el tráfico restringido debemos añadir su dirección ip al fichero /etc/dansguardian/lists/exceptioniplist, podemos incluir también rangos de ips.

Podemos hacer que Dansguardian no analice determinado tipo de fichero según su extensión, en este caso para mejorar el rendimiento no queremos analizar ficheros css ni js. Para hacer esto añadimos las siguientes expresiones regulares en /etc/dansguardian/lists/exceptionurllist:

```
^[^?]*\.css($|\?)
^[^?]*\.js($|\?)
```

Podemos hacer que determinados dominios no sean analizados, es útil para mejorar el rendimiento si añadimos sitios que sean de total confianza. Para ello debemos incluirlos en el fichero /etc/dansguardian/lists/exceptionurllist, en este caso para mejorar la eficiencia se excluyen las llamadas que muchas webs hacen a google-analytics, incluyendo en el fichero:

```
google-analytics.com/
```

Podemos hacer que Dansguardian modifique cabeceras de las webs que visitamos para inducir así comportamientos del navegador. Esto podemos hacerlo añadiéndolas en el fichero /etc/dansguardian/lists/headerregexlist, por ejemplo podemos forzar a que las búsquedas en Youtube siempre sean realizadas con la opción de búsqueda segura activada, para ello debemos añadir las siguientes dos reglas en dicho fichero:

```
"cookie:(.*)PREF=[^&]*?\;"->"Cookie:$1"
"cookie:(.*)$"->"Cookie:$1; PREF=f2=8000000;"
```

Puesto que disponemos de Webmin instalado podemos también modificar desde ahí la mayoría de los parámetros de configuración del servicio, para poder guardar los cambios debemos acceder a webmin como usuario root para que así disponga de los permisos adecuados para volcar los cambios realizados en los ficheros de configuración correspondientes.

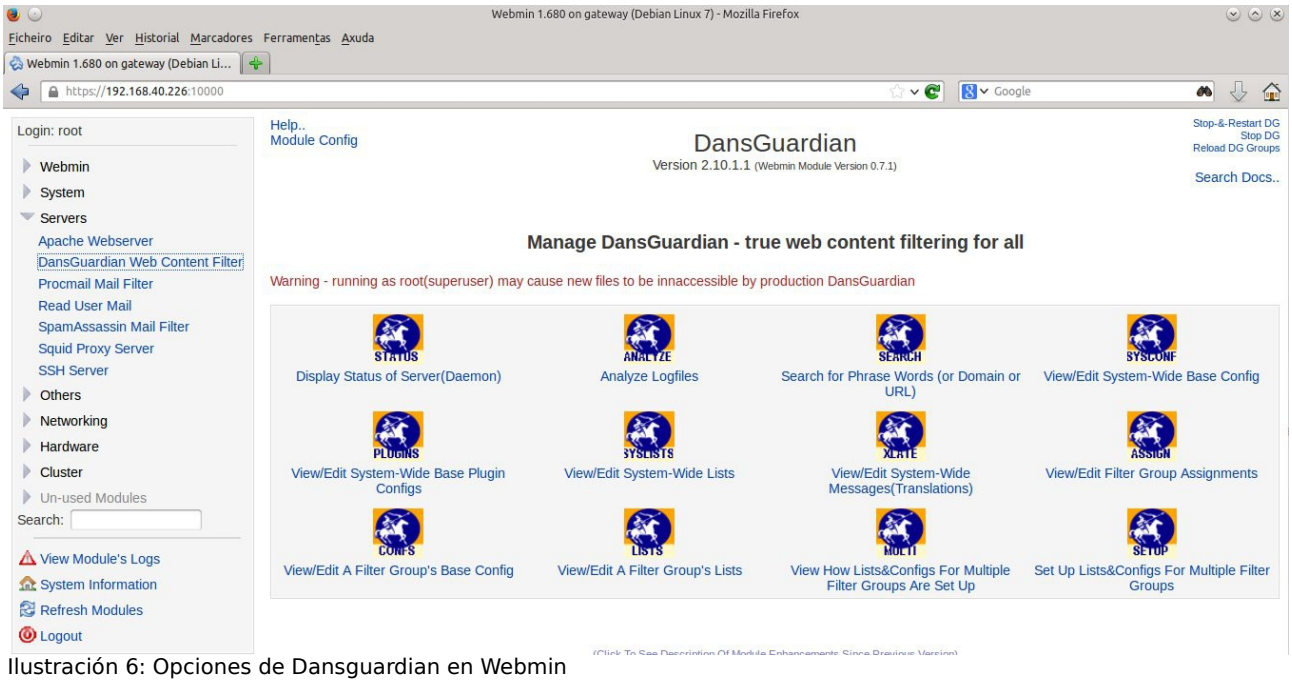

Ilustración 6: Opciones de Dansguardian en Webmin

12.- Configuración avanzada de firewall

Según se menciono anteriormente tenemos tres modos de funcionamiento disponible para el firewall: filtrado transparente, filtrado transparente con bloqueos específicos y modo gateway.

La configuración realizada hasta el momento en el appliance se corresponde con el modo de funcionamiento de filtrado transparente, lo único que se controlan son los virus, el spam y el acceso mediante contenido que podemos regular o incluso desactivar fácilmente. Vemos a continuación los otros dos modos de funcionamiento y que ventajas y problemas aportan a la solución.

12.1.- Firewall transparente con bloqueos específicos

Como comentamos anteriormente este modo está especialmente pensado para centros educativos en los que tenemos unas necesidades de filtrado superiores a otras instalaciones. En este caso puesto que los equipos solo se deben destinar a tareas educativas podemos realizar un filtrado completo del tráfico SSL para evitar así las ventanas de búsqueda y navegación que escapan al filtro de contenidos. Luego debemos eso si ir añadiendo las reglas adecuadas que nos permitan abrir aquellos servicios que haciendo uso de SSL consideremos necesarios para el desempeño del día a día.

Para realizar esto debemos añadir una regla al firewall que bloquee todo el tráfico SSL:

```
-A FORWARD -i br0 -p tcp --dport 443 -j REJECT
```

Si queremos añadir servicios que queramos dejar habilitados debemos antes de esta regla (las reglas iptables se aplican por orden de coincidencia) añadir una regla que acepte la ip o rango que necesite el servicio, por ejemplo para permitir los servicios de Google añadiríamos:

```
-A FORWARD -i br0 -p tcp -d 74.125.0.0/16 -j ACCEPT
-A FORWARD -i br0 -p tcp -d 130.206.0.0/16 -j ACCEPT
-A FORWARD -i br0 -p tcp -d 173.194.0.0/16 -j ACCEPT
```

Cuando queremos habilitar una determinada página web simplemente consultamos su ip con el comando host. Para obtener el rango de ips necesario para un determinado servicio más complejo que usa varias ips podemos usar el siguiente comando:

```
$ whois `host -t a https://messenger.yahoo.com/web |awk 'END{print $4}'`| grep -E
"CIDR|inetnum" | awk "{print $2 $3 $4}"
```

Con este comando podemos obtener dos tipos de resultados, bien obtenemos el CDIR directamente u obtenemos un rango de ips en el campo inetnum del DNS.
En el caso del CDIR el valor ya nos sirve para añadir al firewall, en el segundo podemos usar la herramienta ipcalc para obtener el CDIR a partir del valor de inetnum, por ejemplo:

```
$ whois `host -t a www.nimbuzz.com |awk 'END{print $4}'`| grep -E "CIDR|inetnum"
| awk "{print $2 $3 $4}"
inetnum:        195.211.48.0 - 195.211.51.255

$ ipcalc 195.211.48.0 - 195.211.51.255
deaggregate 195.211.48.0 - 195.211.51.255
195.211.48.0/22
```

Una variación de este modo de funcionamiento es el uso de la política inversa a esta explicada, es decir en lugar de prohibir todo el tráfico SSL, dejarlo habilitado e ir deshabilitando los servicios más usados que nos interese filtrar. Por ejemplo si queremos filtrar el uso de redes sociales, podemos denegar el tráfico de sus rangos de ips:

```
# google services
-A FORWARD -i br0 -p tcp -d 64.18.0.0/20 -j REJECT
-A FORWARD -i br0 -p tcp -d 64.233.160.0/19 -j REJECT
-A FORWARD -i br0 -p tcp -d 66.102.0.0/20  -j REJECT
-A FORWARD -i br0 -p tcp -d 66.249.80.0/20 -j REJECT
-A FORWARD -i br0 -p tcp -d 72.14.192.0/18 -j REJECT
-A FORWARD -i br0 -p tcp -d 74.125.0.0/16 -j REJECT
-A FORWARD -i br0 -p tcp -d 130.206.0.0/16 -j REJECT
-A FORWARD -i br0 -p tcp -d 173.194.0.0/16 -j REJECT
-A FORWARD -i br0 -p tcp -d 207.126.144.0/20 -j REJECT
-A FORWARD -i br0 -p tcp -d 209.85.128.0/17 -j REJECT
-A FORWARD -i br0 -p tcp -d 216.239.32.0/19 -j REJECT
#facebook
-A FORWARD -i br0 -p tcp -d 31.13.64.0/18 -j REJECT
-A FORWARD -i br0 -p tcp -d 173.252.64.0/18 -j REJECT
# twitter
-A FORWARD -i br0 -p tcp -d 199.16.156.0/22 -j REJECT
-A FORWARD -i br0 -p tcp -d 199.96.56.0/21 -j REJECT
# tuenti
-A FORWARD -i br0 -p tcp -d 93.131.160.0/20 -j REJECT
#whatsapp
-A FORWARD -i br0 -p tcp -d  50.22.0.0/15 -j REJECT
```

```
-A FORWARD -i br0 -p tcp -d  173.192.0.0/15 -j REJECT
-A FORWARD -i br0 -p tcp -d  184.172.0.0/15 -j REJECT
#telegram
-A FORWARD -i br0 -p tcp -d  31.210.232.0/21 -j REJECT
#4sq
-A FORWARD -i br0 -p tcp -d  185.31.16.0/16 -j REJECT
-A FORWARD -i br0 -p tcp -d  185.31.17.0/16 -j REJECT
-A FORWARD -i br0 -p tcp -d  185.31.18.0/16 -j REJECT
```

Podemos filtrar el uso de sistemas de mensajería instantánea vía web, para ello debemos buscar las ips de los servicios que queramos bloquear y añadirlas al firewall. Por ejemplo:

```
#IM web services
 #aim.com
 -A FORWARD -i br0 -p tcp -d 64.12.0.0/16 -j REJECT
 #icq.com
 -A FORWARD -i br0 -p tcp -d 178.237.16.0/21 -j REJECT
 #iloveim.com
 -A FORWARD -i br0 -p tcp -d 74.63.192.0/18 -j REJECT
 #imo.im
 -A FORWARD -i br0 -p tcp -d 64.13.128.0/18 -j REJECT
 #iwantim.com
 -A FORWARD -i br0 -p tcp -d 209.239.112.0/20 -j REJECT
 #ebuddy
 -A FORWARD -i br0 -p tcp -d 193.238.160.0/22 -j REJECT
 #koolim.com
 -A FORWARD -i br0 -p tcp -d 74.208.0.0/16 -j REJECT
 #nimbuzz.com
 -A FORWARD -i br0 -p tcp -d 195.211.48.0/22 -j REJECT
 #plus.im
 -A FORWARD -i br0 -p tcp -d 46.4.72.96/27 -j REJECT
 #yahoo.es
 -A FORWARD -i br0 -p tcp -d 46.4.72.96/27 -j REJECT
```

Si seguimos esta filosofía de filtrado no debemos añadir al firewall la regla vista anteriormente que bloquea todo el tráfico SSL por el puerto 443.

Estas reglas, tal y como vimos en el apartado de configuración básica del firewall, podemos introducirlas manualmente en el fichero /etc/iptables.up.rules o a través de Webmin. Vemos a continuación un ejemplo de los pasos a seguir para bloquear por ejemplo el acceso a tuenti.es desde la red local introduciendo la regla correspondiente en Webmin

Vamos a la sección de Linux Firewall en Webmin y buscamos la sección de Forward dentro de las reglas iptables, para añadir ahí una regla que rechace todo intento de acceso a tuenti.es que pase por la interfaz br0, sería el equivalente a añadir al fichero:

```
-A FORWARD -i br0 -p tcp -d 95.131.168.0/21 -j REJECT
```

El rango de ips para bloquear al servicio lo calculamos usando los comandos vistos anteriormente.

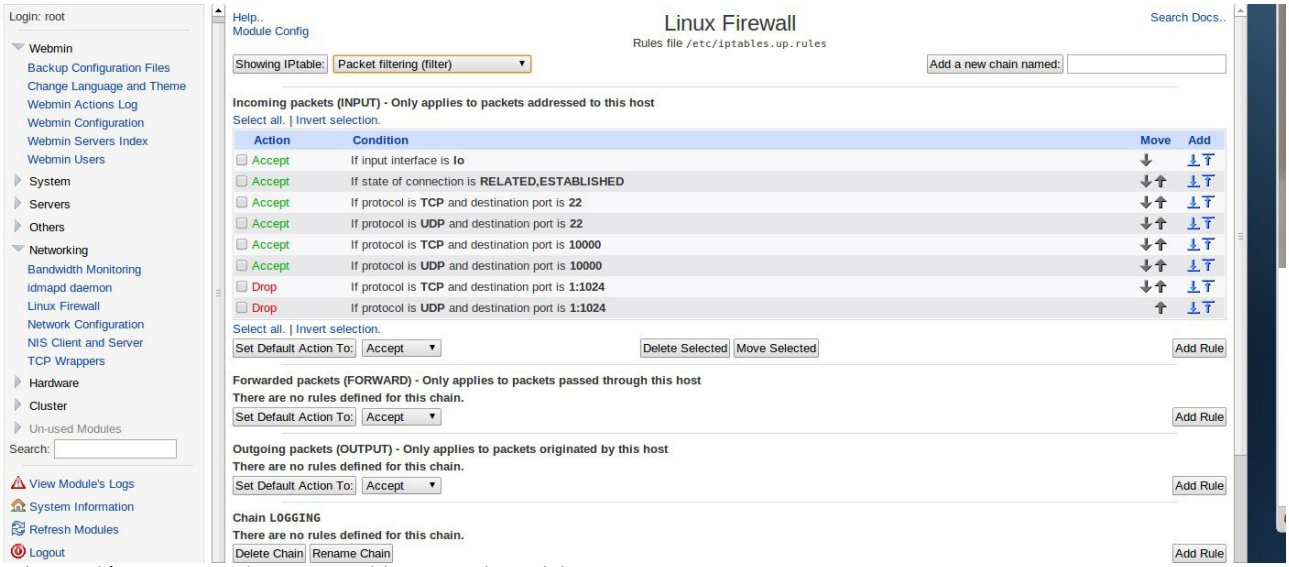

Ilustración 7: Rango de IP's para bloquear el servicio.

Una vez tenemos localizada la sección le damos al botón Add Rule

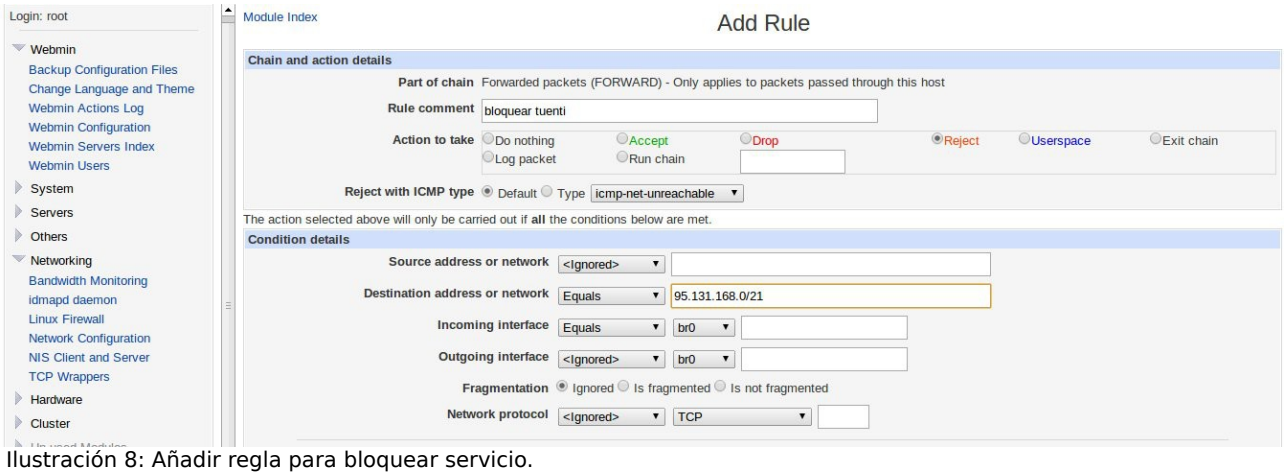

Ilustración 8: Añadir regla para bloquear servicio.

Esto nos abre el formulario para cubrir la regla, que podemos hacer como vemos en la imagen anterior. Es recomendable cubrir la sección 'Rule comment' para en el futuro saber porqué está añadida dicha regla. Además debemos cubrir las ips que bloqueamos, en que interfaz de red (br0) y marcar la opción 'Reject' como acción a tomar en caso de detectar paquetes que cumplan esas características.

Una vez añadida debemos darle a la opción Apply Configuration, para que los cambios añadidos en el firewall surtan efecto, en caso contrario aunque veamos la regla escrita en el conjunto de reglas del firewall, esta no será aplicada.

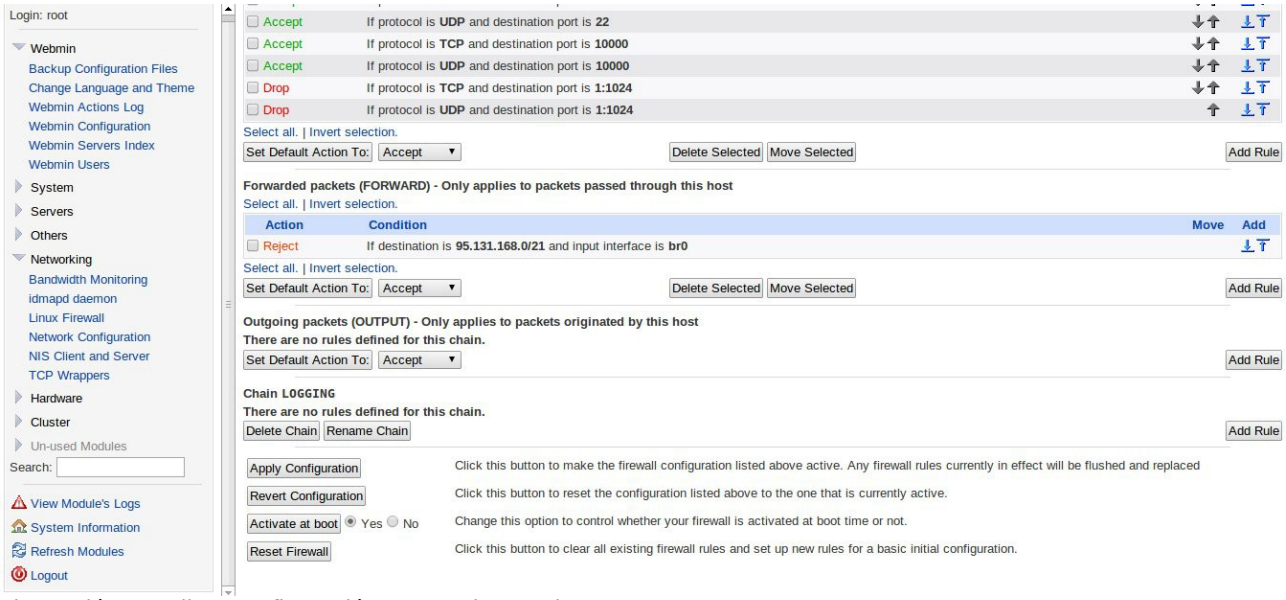

Ilustración 9: Aplicar configuración para activar regla.

Una vez hecho esto si no hay ningún error la regla estará funcionando para nuestro appliance.

12.2.- Firewall en modo gateway

En el modo gateway se varía el modo de funcionamiento del appliance, el cual, pierde su modalidad de transparente. Al trabajar en modo gateway el appliance pasa a ser la puerta de enlace de los equipos que se encuentran colocado detrás de él. Esto implicará la creación de una nueva subred y con ello la re-configuración de los equipos. Para facilitar esta tarea se instalará en el appliance un servidor dhcp que asignará ips en el rango de la nueva subred a las máquinas que así lo soliciten, siendo la configuración dinámica de ip el método de configuración de red más usado en redes pequeñas, se facilitará la re-configuración de los equipos que simplemente tendrán que reiniciar sus servicios de red para tener conexión a través del appliance.

La ventaja de usar el appliance en modo gateway es que nos permitirá un control total del acceso a red a través del mismo, pudiendo utilizar su firewall para securizar completamente los equipos que se encuentran en la subred creada a tal efecto.

Los cambios de configuración, que veremos a continuación, para obtener el modo gateway de funcionamiento son tres: adaptar la configuración de red, instalar y configurar el servidor dhcp y configurar el firewall.

12.2.1.- Configuración de las interfaces de red

El primer paso es la configuración de las interfaces de red, para lo que debemos hacer lo siguiente:

- Editar el fichero /ect/network/interfaces

root@gateway:~# vim /etc/network/interfaces

- Añadir la siguiente configuración al fichero:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
# The loopback network interface
auto lo
iface lo inet loopback

pre-up iptables-restore < /etc/iptables.up.rules
pre-up echo 1 > /proc/sys/net/ipv4/ip_forward
# The external WAN interface (eth0)
auto eth0
iface eth0 inet dhcp

 # The internal LAN interface (eth1)
auto eth1
#iface eth1 inet dhcp
iface eth1 inet static
        address 10.70.70.1
        netmask 255.255.255.0

auto eth0:0
iface eth0:0 inet static
        address 192.168.235.1
        netmask 255.255.255.0
```

12.2.2.-Instalación y configuración del servidor dhcp:

Los pasos a seguir para instalar el servidor dhpc son:

- Instalación del servidor dhcp:

root@gateway:~# apt-get install isc-dhcp-server

- Para configurar el servidor dchp editamos el fichero /etc/dhcp/dhcpd.conf

root@gateway:~# vim /etc/dhcp/dhcpd.conf

- Añadimos a dicho fichero la siguiente configuración:

```
ddns-update-style none;


default-lease-time 600;
max-lease-time 7200;
authoritative;
INTERFACES="eth1";
subnet 10.70.70.0 netmask 255.255.255.0 {
        range 10.70.70.100 10.70.70.200;
        option domain-name-servers 8.8.8.8;
        option routers 10.70.70.1;
}


log-facility local7;
```

12.2.3.- Configuración del firewall:

- Añadimos al fichero /etc/iptables.up.rules las siguientes reglas:

```
*mangle
:PREROUTING ACCEPT [21:4473]
:INPUT ACCEPT [8:1690]
:FORWARD ACCEPT [13:2783]
:OUTPUT ACCEPT [4:556]
:POSTROUTING ACCEPT [17:3339]
COMMIT


*filter
:INPUT ACCEPT [2:612]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [1:76]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i eth1 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 10000 -j REJECT --reject-with icmp-port-unreachable
-A INPUT -i eth0 -p udp -m udp --dport 10000 -j REJECT --reject-with icmp-port-unreachable
-A INPUT -p tcp -m tcp --dport 1:1024 -j DROP
-A INPUT -p udp -m udp --dport 1:1024 -j DROP
-A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i eth1 -o eth0 -j ACCEPT
COMMIT


*filter
:INPUT ACCEPT [2:612]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [1:76]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i eth1 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 10000 -j REJECT --reject-with icmp-port-unreachable
-A INPUT -i eth0 -p udp -m udp --dport 10000 -j REJECT --reject-with icmp-port-unreachable
-A INPUT -p tcp -m tcp --dport 1:1024 -j DROP
-A INPUT -p udp -m udp --dport 1:1024 -j DROP
-A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i eth1 -o eth0 -j ACCEPT
COMMIT
```

13.- Referencias

1 http://www.debian.org/distrib/netinst#smallcd
2 https://wiki.debian.org/es/iptables
3 http://es.wikipedia.org/wiki/Proxy
4 http://www.clamav.net/lang/en/
5 http://www.server-side.de/features.htm
6 http://www.squid-cache.org/
7 http://dansguardian.org/
8 http://www.webmin.com/