Manual de usuario del Appliance de defensa perimetral

Tipo de documento: documento técnico
28/03/2014

Identificador del documento:	
Fecha:	15/05/2014/2014
Actividad:	T1.7
Estado del documento:	
Enlace del documento:	

Abstract:

ecoRaee

Life

UniversidadeVigo

energylab

revertia

Datos de la entrega:

	Nombre	Compañia / Actividad	Fecha	Firma
Autor	Silvia Carrera Álvarez	U. Vigo	15/5/2014	
Verificado por				
Revisado por				
Aprobado por				

Log del documento:

Versión	Fecha	Comentario	Autor

Registro de cambios del documento:

Versión	Item	Motivo del cambio

Índice

1.- Introducción.....5

2.- Reinicio de los servicios configurados.....7

3.- Webmin para gestión web.....8

3.- Filtro de contenidos: Dansguardian.....10

4.- Configuración avanzada de Squid.....13

6.- Configuración avanzada de firewall.....14

6.1.- Firewall transparente con bloqueos específicos.....14
6.1.- Problemática con ips dinámicas de sitios web bloqueados y solución.....19

7.- Procedimiento a seguir en caso de fallo del appliance.....20

Índice de imagenes

Ilustración 1: Esquema de red con appliance....6
Ilustración 2: Login de Webmin....8
Ilustración 3: Pantalla inicial de Webmin....9
Ilustración 4: Bloqueo de Dansguardian....10
Ilustración 5: Opciones de Dansguardian en Webmin....11
Ilustración 6: Cambio del valor del peso....11
Ilustración 7: Estadísticas de Dansguardian....12
Ilustración 8: Opciones de Squid en Webmin....13

1.- Introducción

El objetivo de este documento es la creación de un manual de usuario para la gestión del appliance de seguridad perimetral desarrollado en el Demostrativo III del proyecto Life-ecoRaee.

El sistema desarrollado es capaz de realizar funciones de antivirus, antispam, control de contenidos y firewall.

En la actualidad casi cualquier entidad pública o privada 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 entidad y en el mejor de los casos la contratación incluirá licencia para algún software antivirus para su instalación en los equipos informáticos de la entidad.

Si bien la instalación de antivirus de forma local en cada equipo de la entidad 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€.

Muchas veces este tipo de desembolsos no son asumibles por las entidades, que además no ven la seguridad informática como un riesgo grande para el desarrollo de sus funciones, por norma 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 distintas entidades 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.

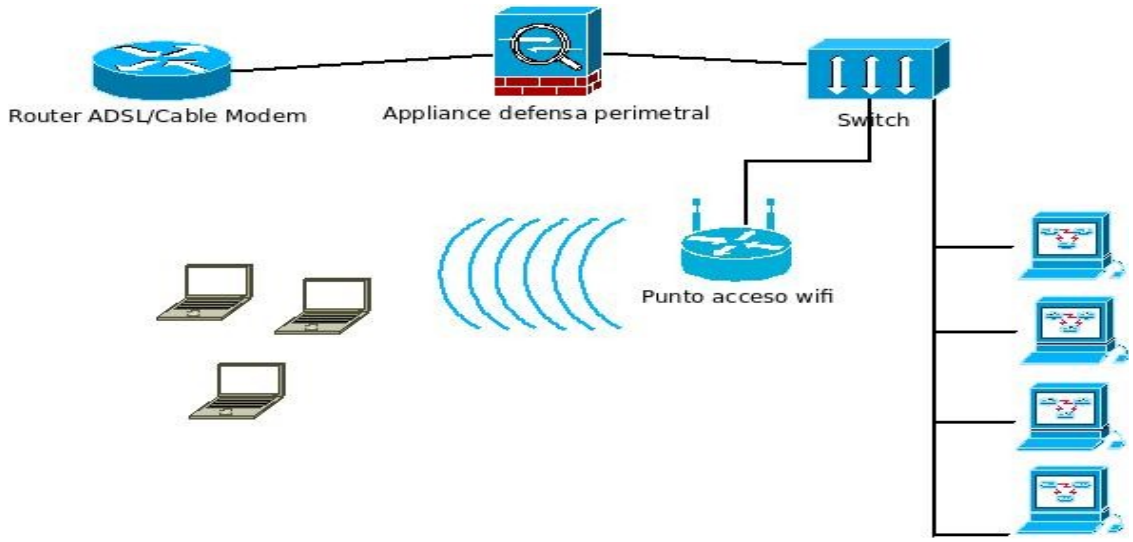


Ilustración 1: Esquema de red con appliance

2.- Reinicio de los servicios configurados

Podemos reiniciarlos todos los servicios del appliance para la aplicación de 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.

3.- Webmin para gestión web

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.

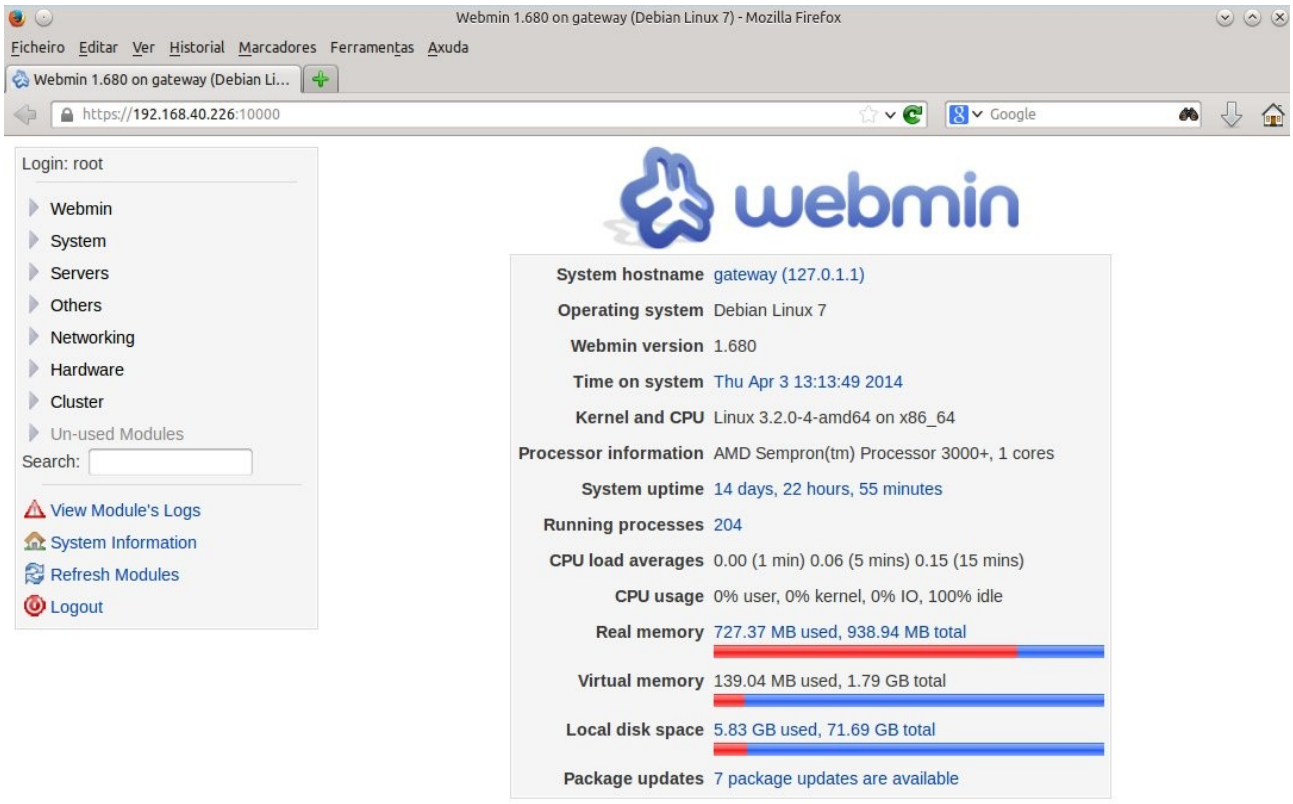


Ilustración 3: Pantalla inicial de Webmin

3.- Filtro de contenidos: Dansguardian.

Una de las principales formas de bloqueo que utiliza Dansguardian 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 estas listas un peso. La suma de estos pesos determina si la página puede ser visitada o no. Cuando una página es bloqueda por Dansguardian, obtenemos el siguiente mensaje en nuestro navegador.

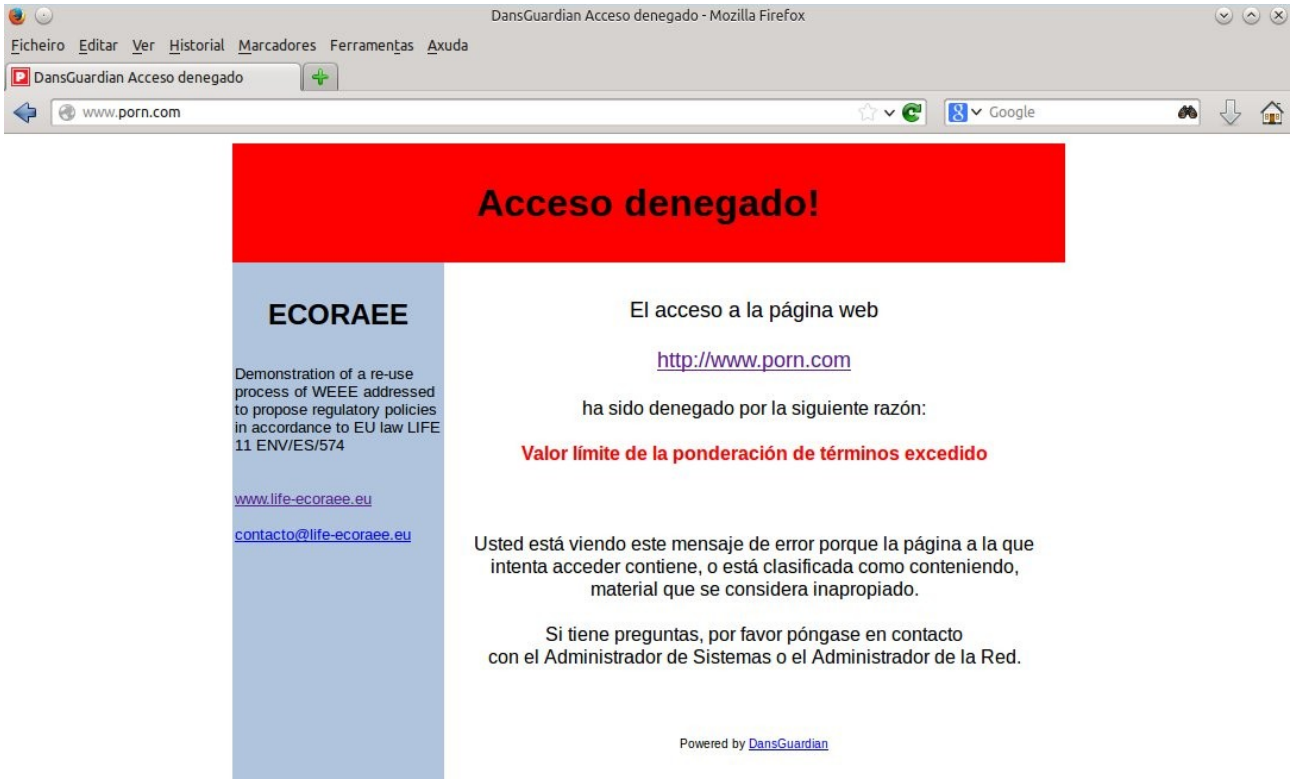


Ilustración 4: Bloqueo de Dansguardian

Por defecto, la configuración de Dansguardian viene con un peso total menor que 50, este nivel de bloqueo se considera apto 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 irlo ajustando según vayamos viendo en el día a día.

Por defecto, se ha fijado este valor en 200 y para cambiarlo debemos realizar los siguientes pasos a través del Webadmin.

Entramos en Servers y seleccionamos Dansguardian web content filter.

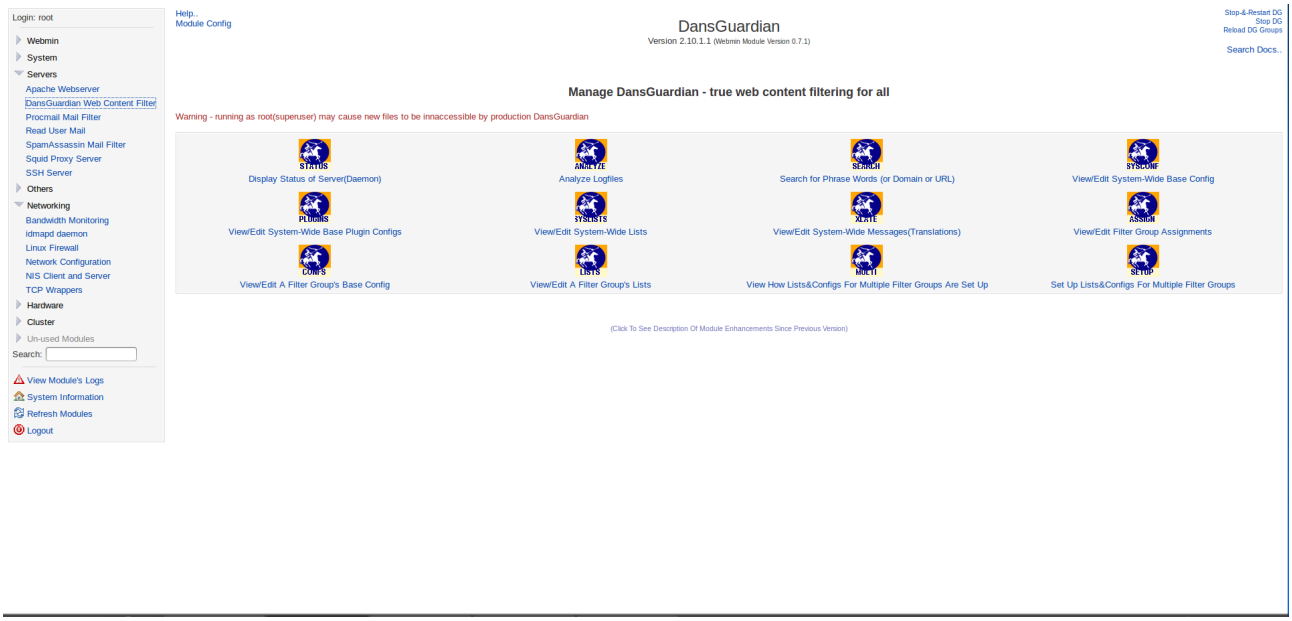


Ilustración 5: Opciones de Dansguardian en Webmin

Seleccionamos Confs y ajustamos el valor en la casilla con nombre Naughtyness limit.

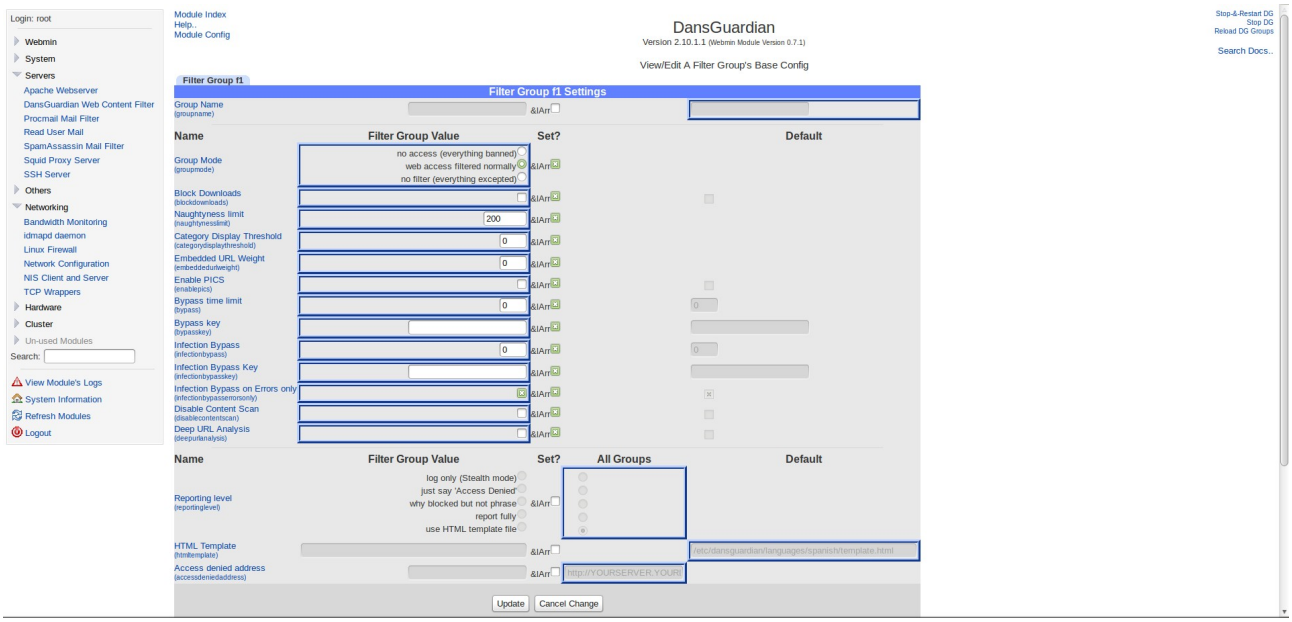


Ilustración 6: Cambio del valor del peso.

Además, Dansguardian también nos permite la consulta de estadísticas. Esta opción esta disponible en la opción del menú principal de Dansguardian (ver ilustración 5) llamada Analyze. Una vez pinchamos en esta opción, vemos la siguiente pantalla:

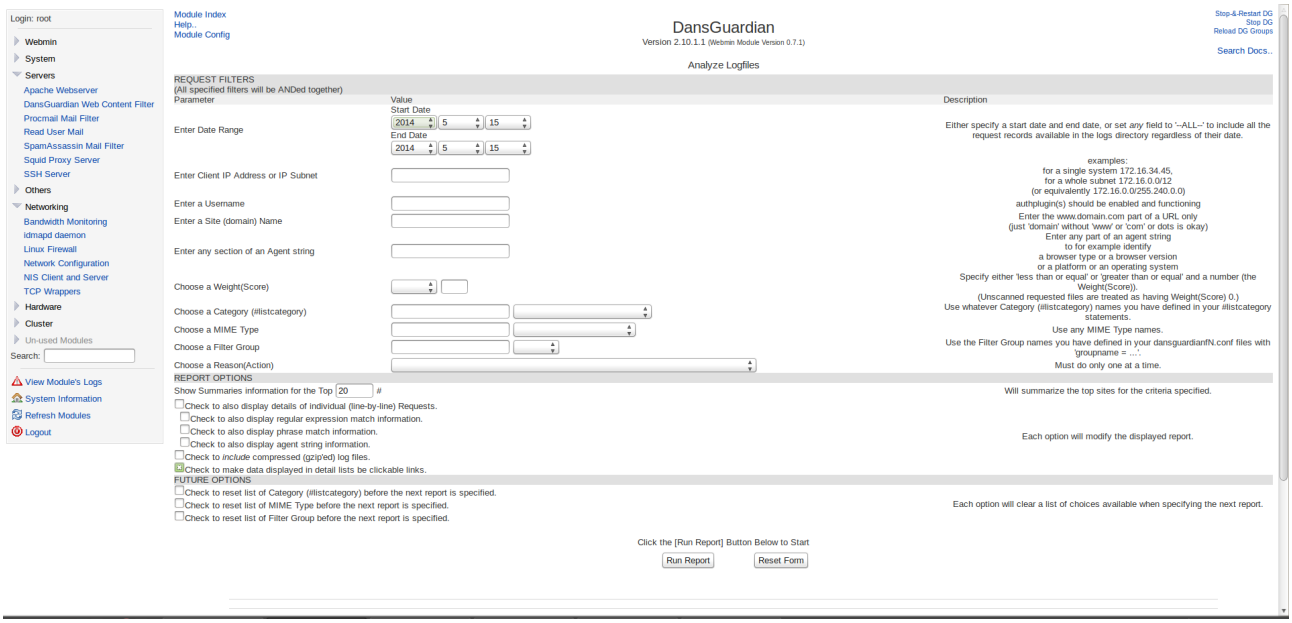


Ilustración 7: Estadísticas de Dansguardian.

Para obtener las estadísticas, seleccionamos las opciones que queramos analizar en esta pantalla y pulsamos en el botón Run Report.

4.- Configuración avanzada de Squid

Puesto que disponemos de Webmin instalado podemos tambíen 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.

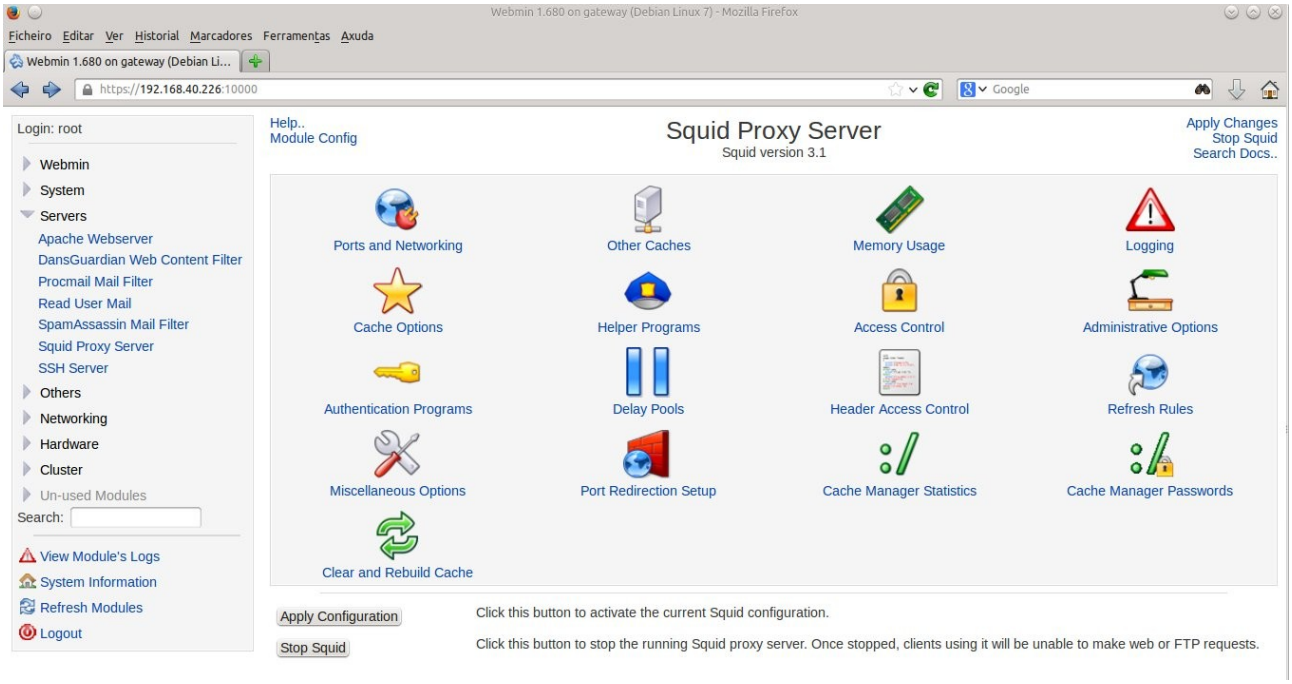


Ilustración 8: Opciones de Squid en Webmin

6.- 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.

6.1.- 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 busqueda 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
```

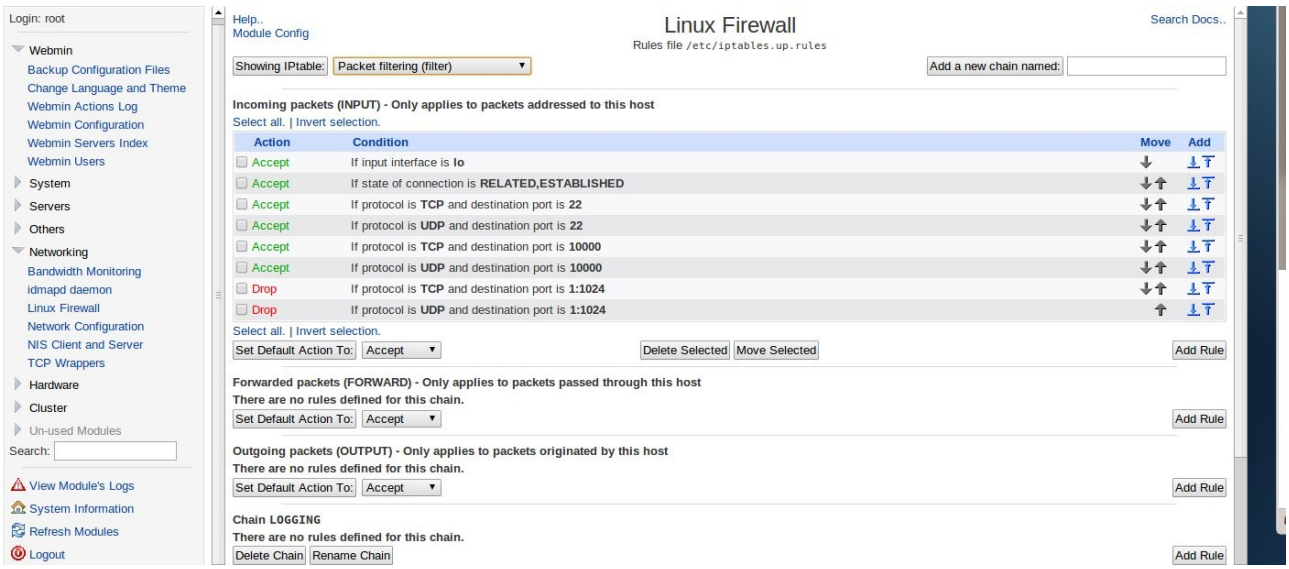
Si seguimos esta filosofía de filtrado no debemos añadir al firewall la regla vista anteriormente que bloquea todo el tráfico SSL por el puerto 443.

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 traves 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 introducciendo la regla correspondiente en Webmin

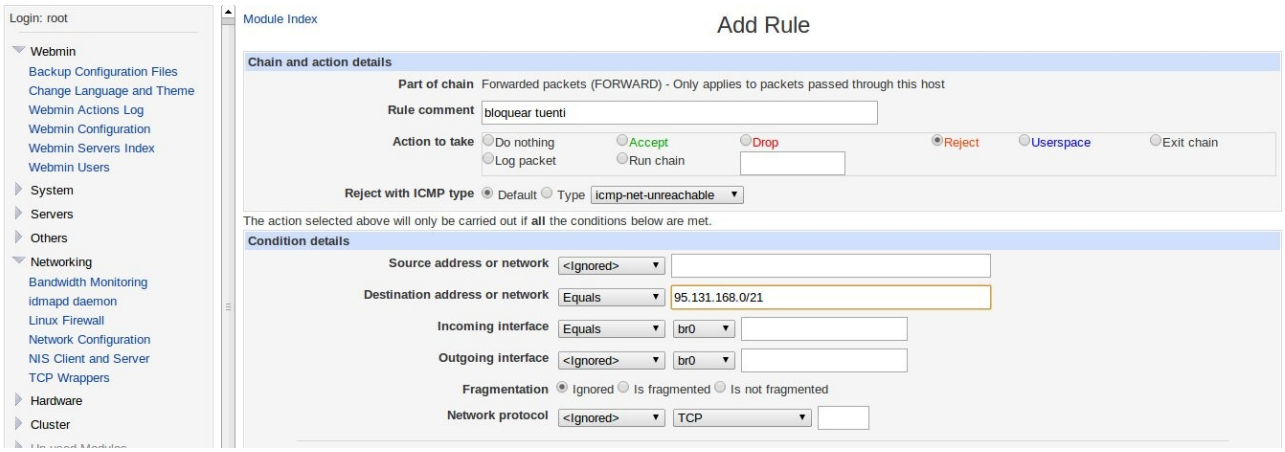
Vamos a la sección de Linux Firewall en Webmin y buscamos la sección de Forward dentro de las reglas iptables, para añadir ahí una regla que rechace todo intento de acceso a tuenti.es que pase por la interfaz br0, sería el equivalente a añadir al fichero:

```
-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.

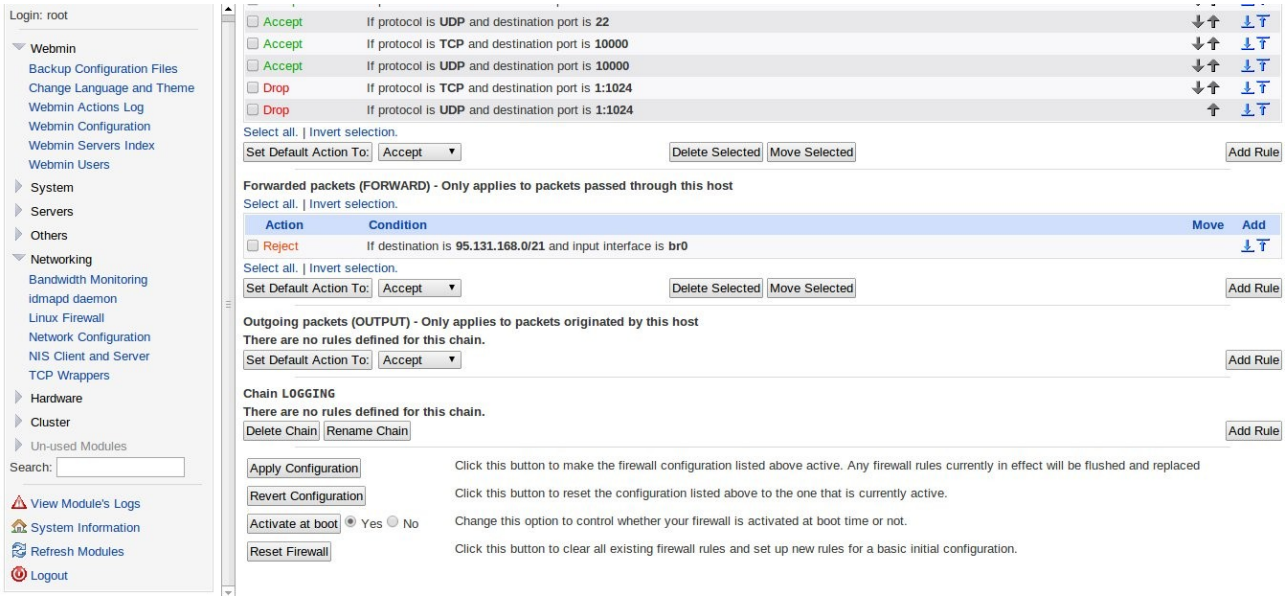


Una vez tenemos localizada la sección le damos al boton Add Rule



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.



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

6.1.- Problemática con ips dinámicas de sitios web bloqueados y solución.

Cuando configuramos el appliance para bloquear distintos sitios web, detectamos que algunos de ellos cambian sus ip's de forma dinámica por lo que tendríamos que verificar las ip's cada día para ver si habían cambiado y añadirlas a las reglas de bloqueo de iptables.

Dada la problemática que esto podría generar debido a que cada entidad que cuente con un appliance podrá desear bloquear unos sitios u otros, realizamos un proceso que realice esta funcionalidad de forma automática y transparente para el usuario.

Para la realización de este proceso es necesario que el usuario añada los sitios que quiere bloquear específicamente en un fichero concreto. Para ello, se deben realizar los siguientes pasos:

1. Conectarse por ssh a la ip del appliance con el usuario y la contraseña proporcionadas.

2. Añadir los sitios que se desean bloquear al fichero /root/baneos/sitiosProhibidos de la siguiente forma:

Ejemplo de bloqueo de la red social facebook:

$ vim /root/baneos/sitiosProhibidos

facebook.com

Guardar el fichero.

NOTA IMPORTANTE: añadir los nombre de los sitios web sin www.

7.- Procedimiento a seguir en caso de fallo del appliance.

En caso de fallo del appliance de seguridad perimetral se deberán seguir los siguientes pasos:

1. Conectarse por ssh a la ip del appliance con el usuario y la contraseña proporcionadas.

2. Ejecutar el siguiente script tal y cómo se describe.

$ ./limpiar.sh