**Firewalls de próxima generación**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **1**

[**2. Introducción**](#_g59i8ewd3ed3) **2**

[**3. pfBlockerNG**](#_49jiar3limf) **4**

[**3.1 GeoIP**](#_btjj1tws7n) **16**

[**4. Suricata**](#_u0gdky46h2d0) **19**

[**5. Squid/ClamAV/LightSquid**](#_ppljkyxhgpud) **30**

[**6. SquidGuard**](#_86410tc2y6hs) **47**

# **2. Introducción**

Para la realización de esta práctica utilizaremos nuestro firewall pfsense utilizado en el tema anterior al que le instalaremos nuevos módulos para ampliar su funcionalidad. La idea es añadir las siguientes funcionalidades de un firewall de próxima generación.

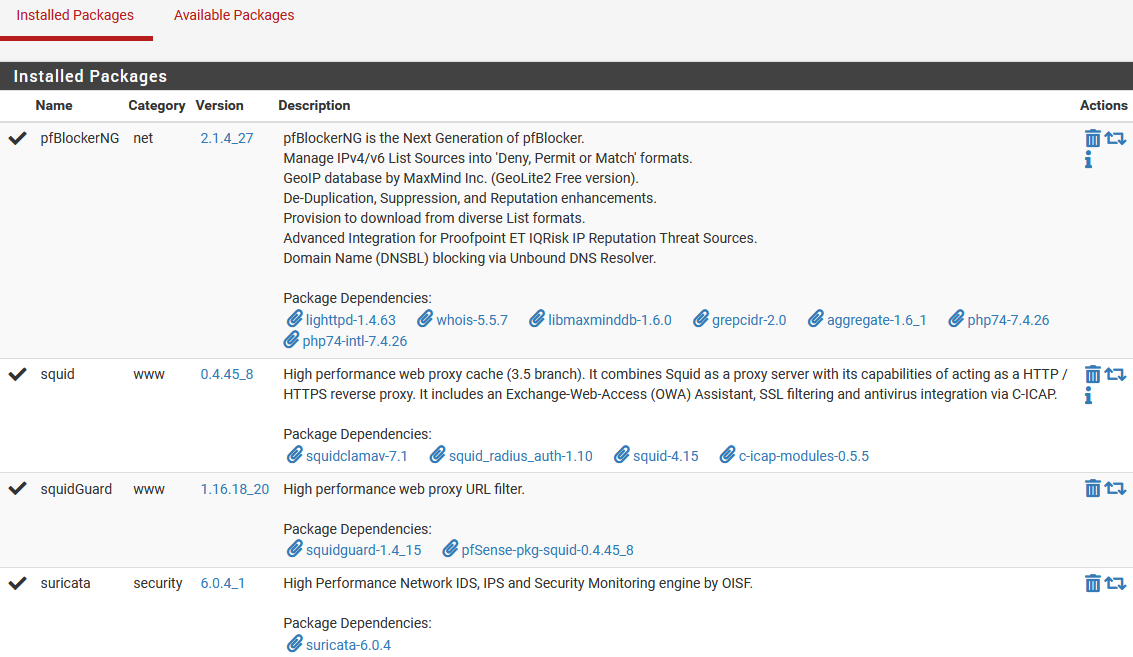
• Descifrado e inspección de SSL: El tráfico SSL actualmente supone más del 60% del tráfico de la red.

• Sistema de prevención de intrusos (IPS) con tecnología anti evasión.

• Protección contra malware y exploits basada en red.

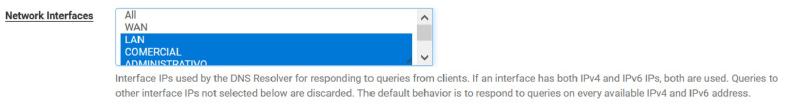
• Filtrado de contenido y control de acceso basada en la ubicación.

• Automatización: responder de manera coordinada ante una amenaza detectada.

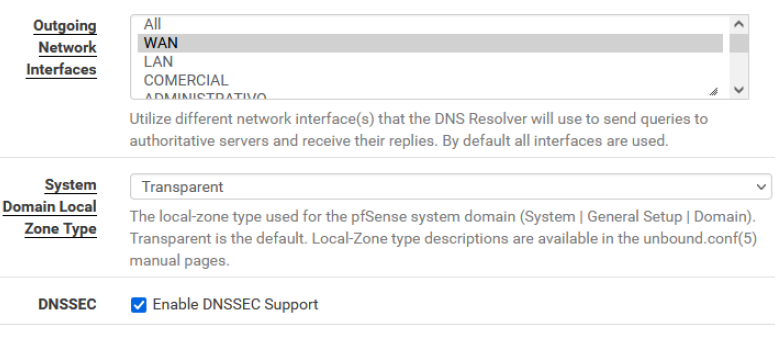


Una vez instalados, lo primero es configurar correctamente el servicio DNS en Services/DNS Resolver donde lo importante es establecer que redes son Wan y cuales Lan quedando en nuestro laboratorio de la siguiente manera, puesto que por defecto el servicio dns de pfsense está configurado para escuchar en todas las interfaces.

Seleccionaremos todas las interfaces LAN de nuestro sistema, incluido localhost (el firewall), que serán las interfaces donde el servicio podrá responder a las peticiones DNS.



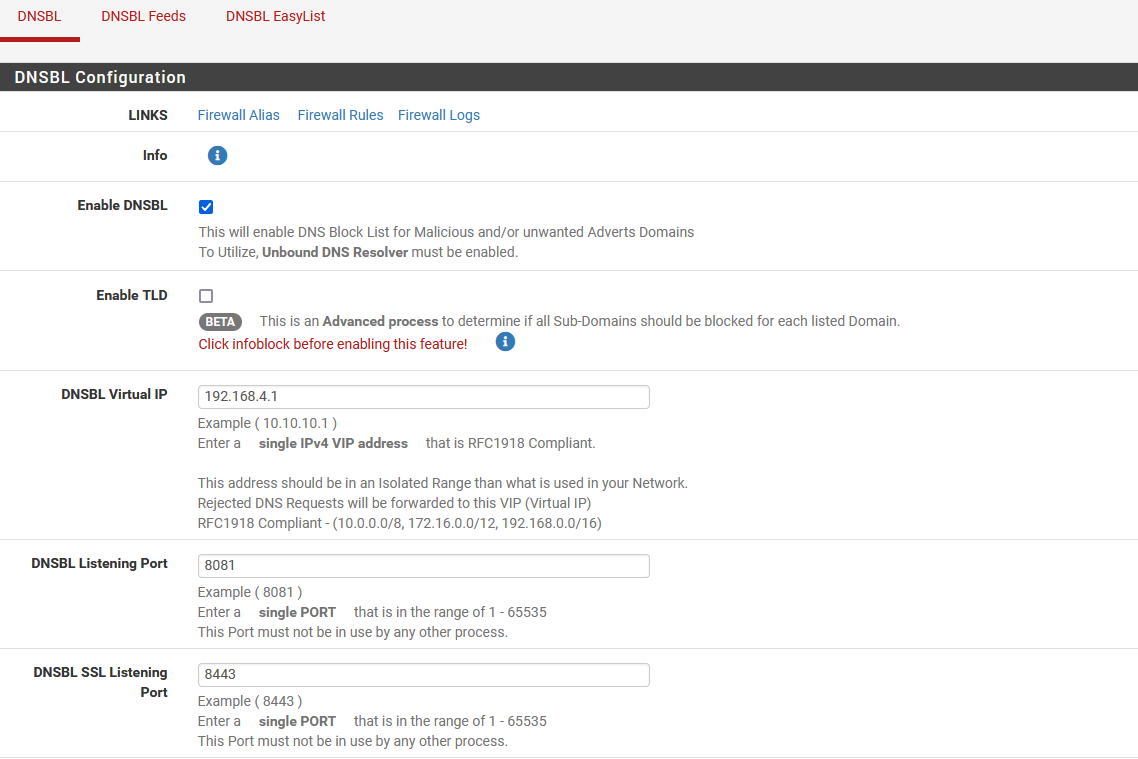
Y seleccionaremos las interfaces WAN que el firewall utilizará para realizar peticiones a otros servidores DNS.

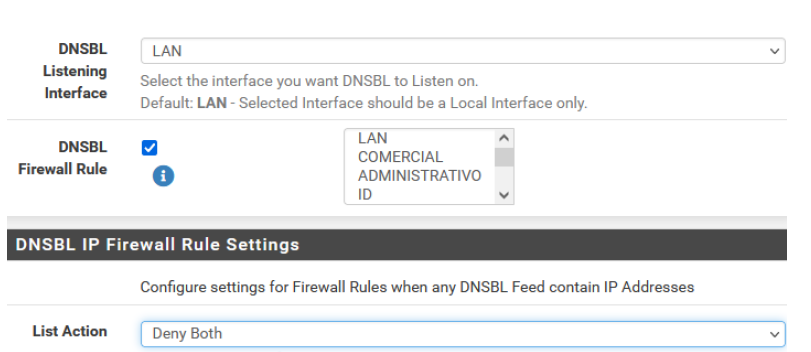


# **3. pfBlockerNG**

pfBlockerNG es un paquete que nos permitirá bloquear direcciones IP basado en listas públicas, países, dominios o listas propias, el cual podemos encontrar en pfsense.

Para proteger la parte Lan y evitar que se hagan conexiones hacia las listas de ips maliciosas lo primero sería configurar DNSBL la cual tiene muchísimas opciones por lo que no veremos todas, solamente una configuración básica

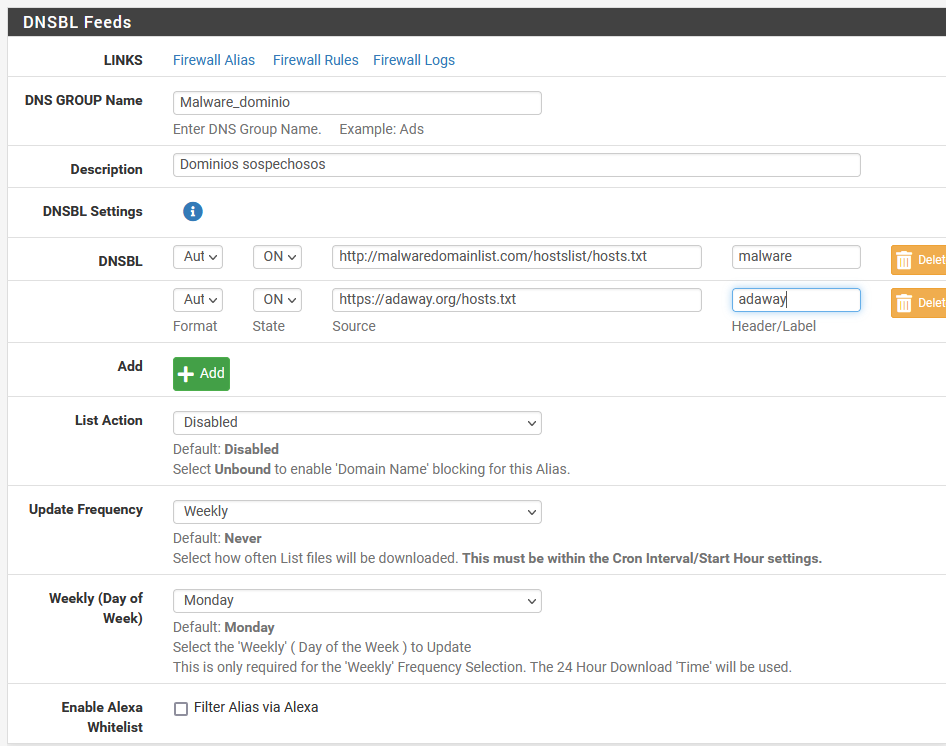




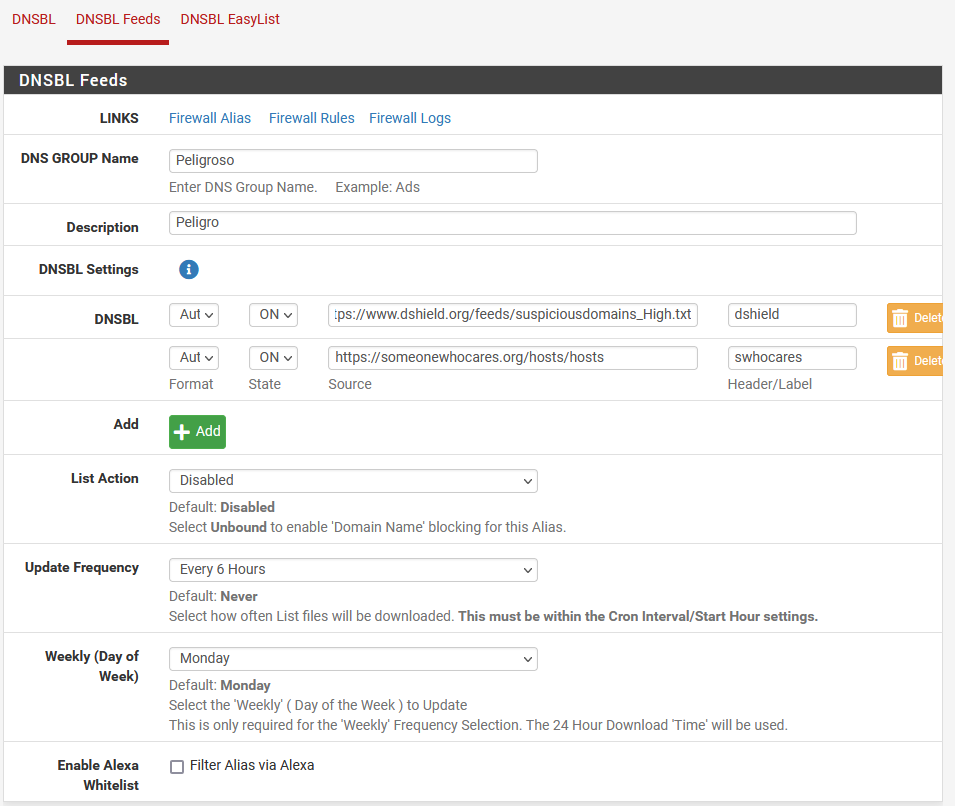
Una vez tenemos esto, las siguientes 2 pestañas nos permitirá proteger nuestra Lan en función de listas.

DNSBL Feeds nos permite agregar listas de terceros, cuantas más listas más recursos necesitamos en nuestro firewall. Vamos agregar las siguientes por ser listas gratis muy buenas.

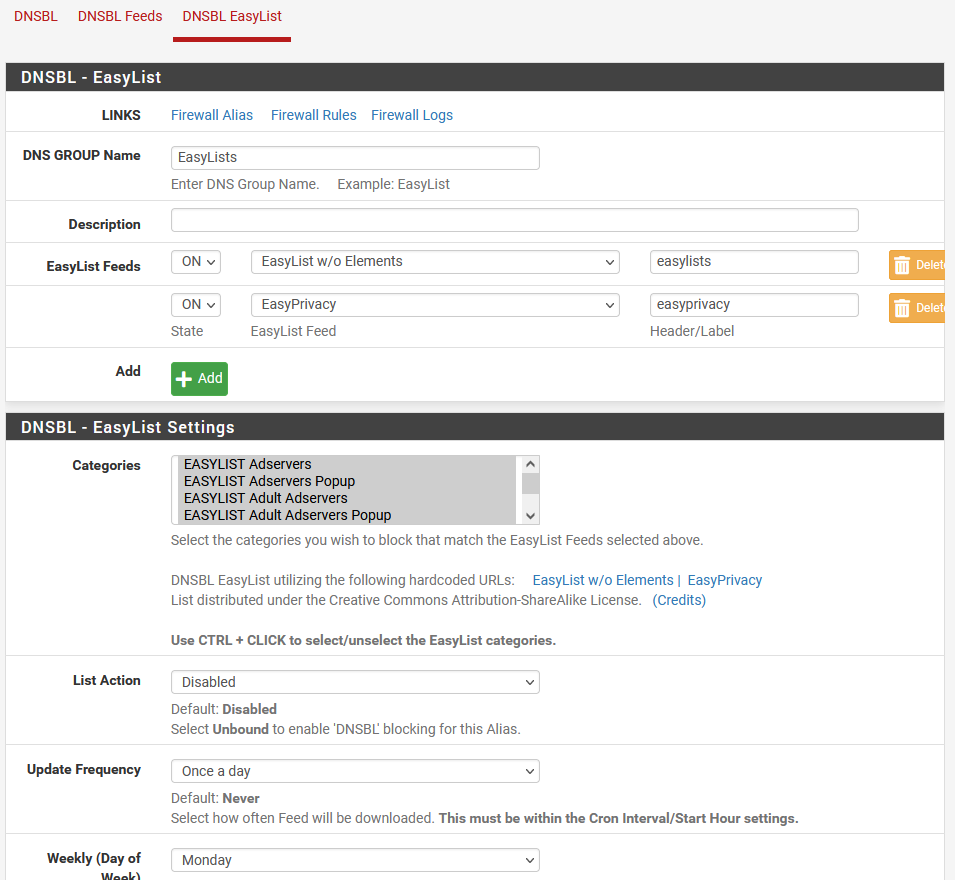
Malware\_Dominios la cual podemos actualizar una vez cada semana por ser un poco la menos peligrosa y las que menos se actualizan a nivel de origen, gastando menos recursos, con las siguientes listas:



Ahora crearemos otra que actualizaremos cada 6 horas por ejemplo siendo categoría peligrosa con las siguientes listas.



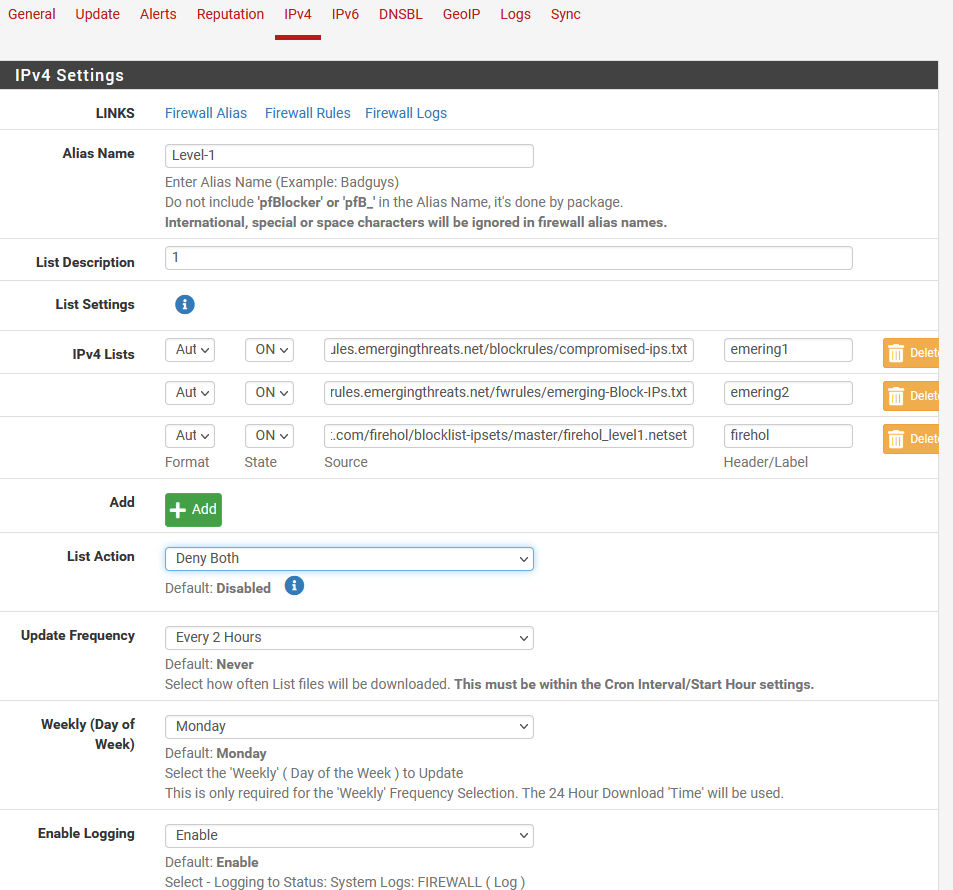
En cuanto a DNSBL EasyList son unas listas incorporadas en el propio paquete que aprovecharemos configurando de la siguiente manera:



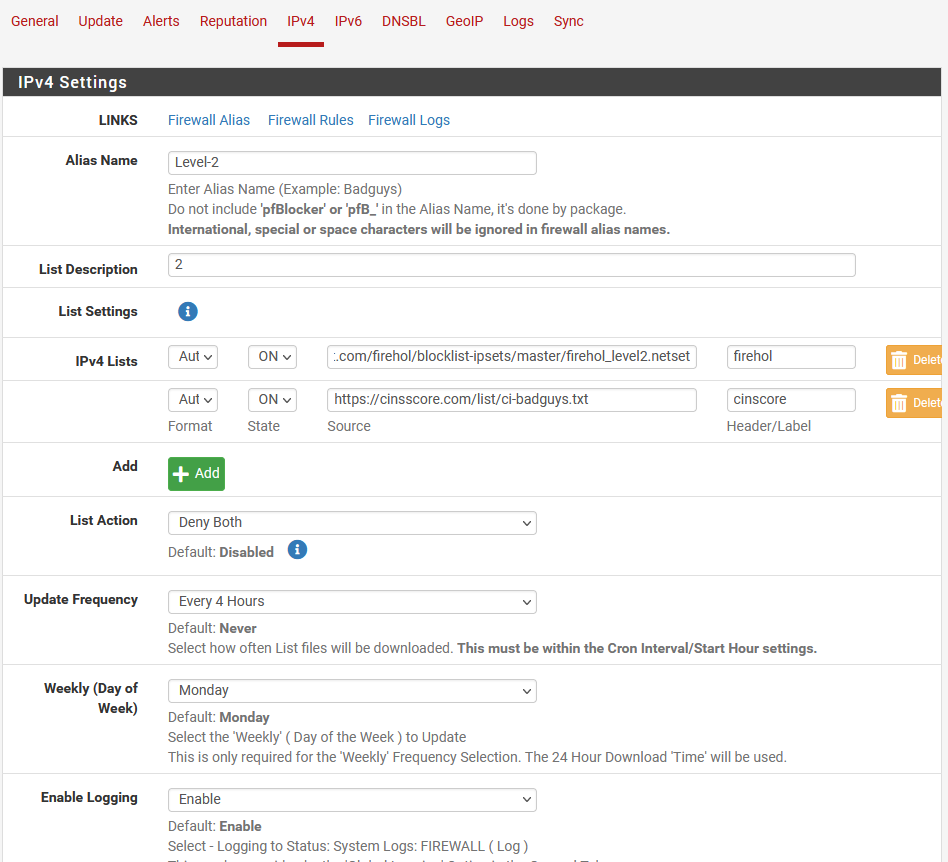
Una vez realizada esa parte vamos a proteger también la parte Wan, para ello nos dirigimos

Firewall/pfBlockerNG/IPv4 y le damos a añadir nuestra primera lista:

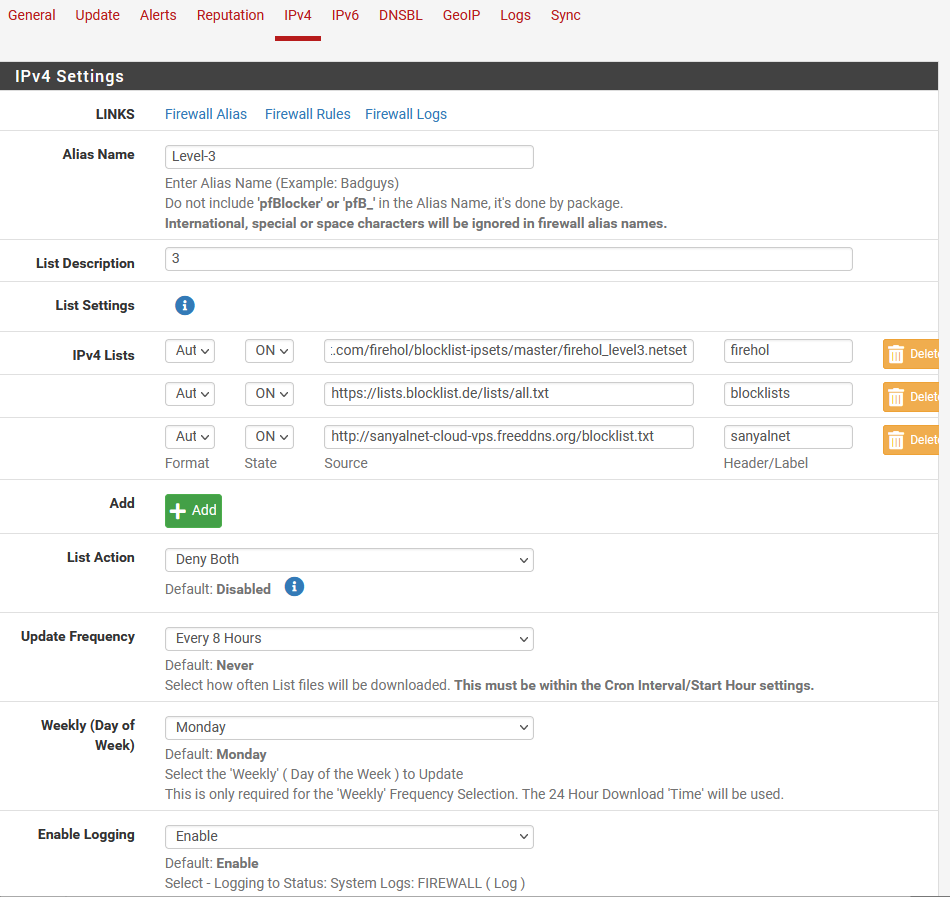
Aquí las vamos a clasificar en niveles, el primero Level-1 con las siguientes listas actualizando cada 2 horas y en ambos sentidos:



Level-2 con las siguientes listas en ambos sentidos cada 4 horas:



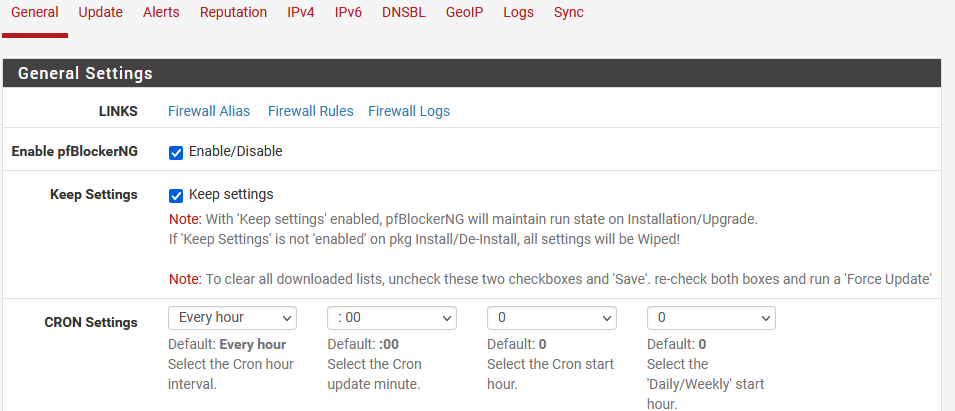
Pasamos a Level-3 cada 8 horas y en ambos sentidos:

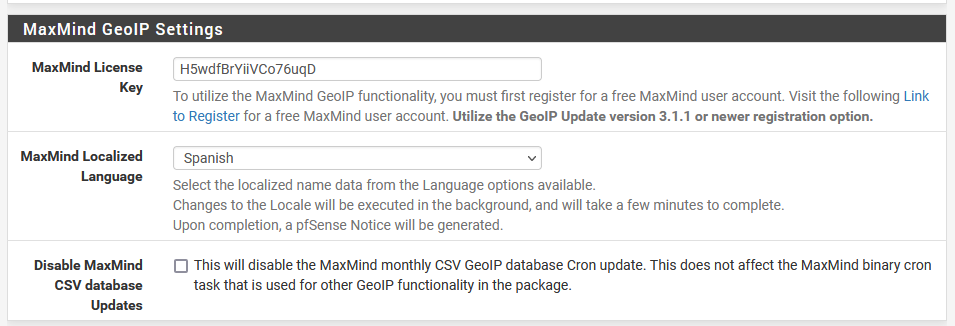
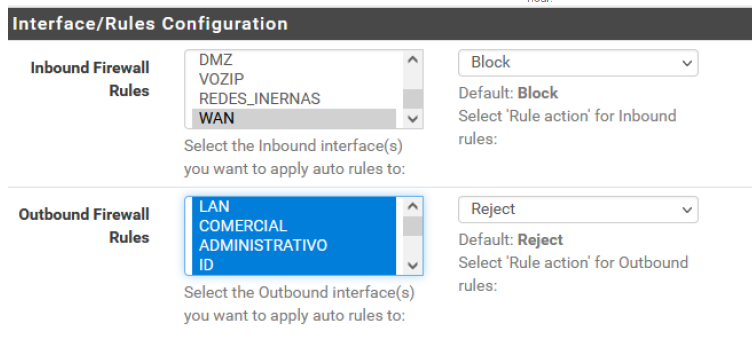


### **3.1 GeoIP**

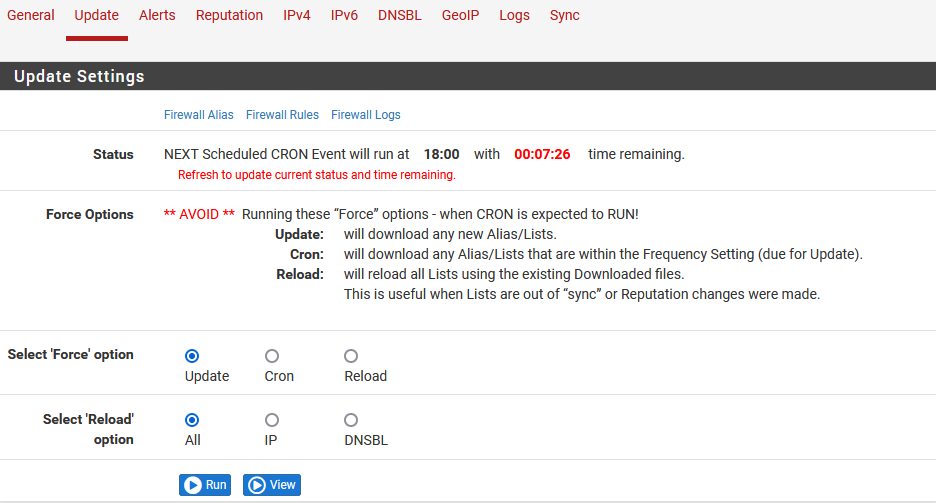
Respecto a GeoIP sirve para bloquear países, pero antes debemos de registrarnos en MaxMind, la versión gratuita de GeoLite2

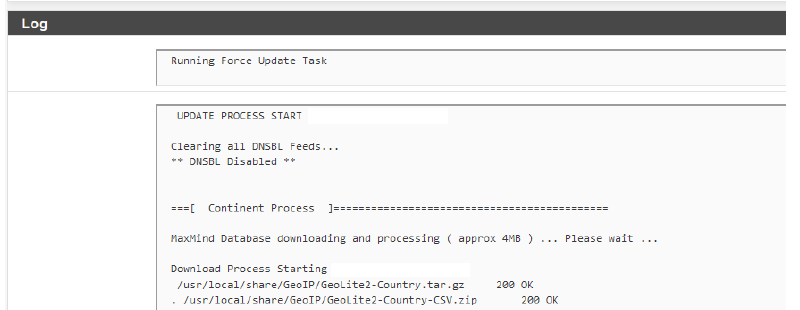
Ahora solo nos falta tres cosas, activar el servicio en Firewall/pfBlockerNG y revisar los parámetros:





Ahora forzamos un update en Firewall/pfBlockerNG/Update y comprobamos que el proceso finaliza correctamente:

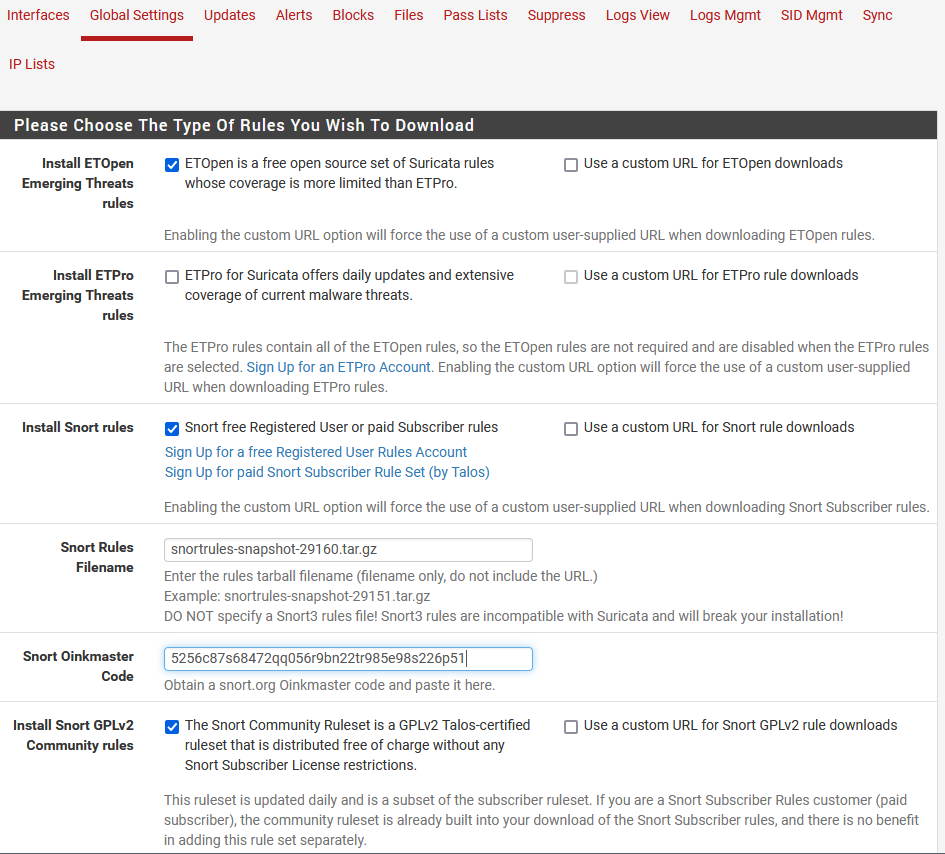




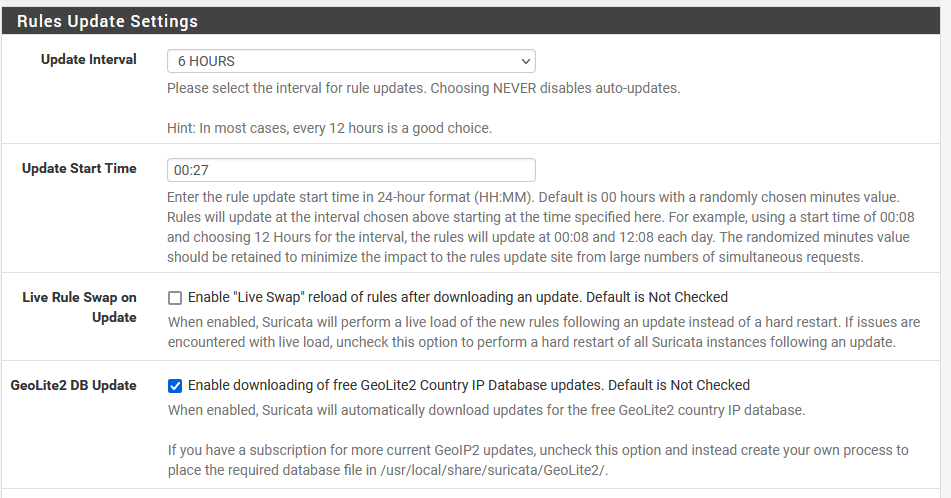
# **4. Suricata**

Suricata es un motor de red de código abierto y multiplataforma de alto rendimiento IDS, IPS y seguridad en la red.

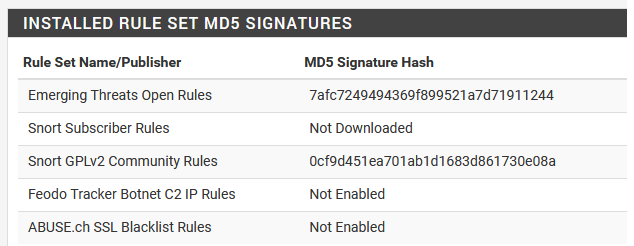
Lo primero de todo es ir a Services/Suricata/Global Settings, en este apartado lo primero que encontramos son las reglas, utilizaremos las reglas Free, quien quiera puede utilizar las Pro, para ello necesitaremos crearnos una cuenta en snort.org con suscripción free e ir al menu downloads para ver la última versión en este caso snortrules-snapshot-29160.tar.gz



Ahora cada cuanto queremos que actualice y Geolite2 donde crearemos una cuenta gratuita.



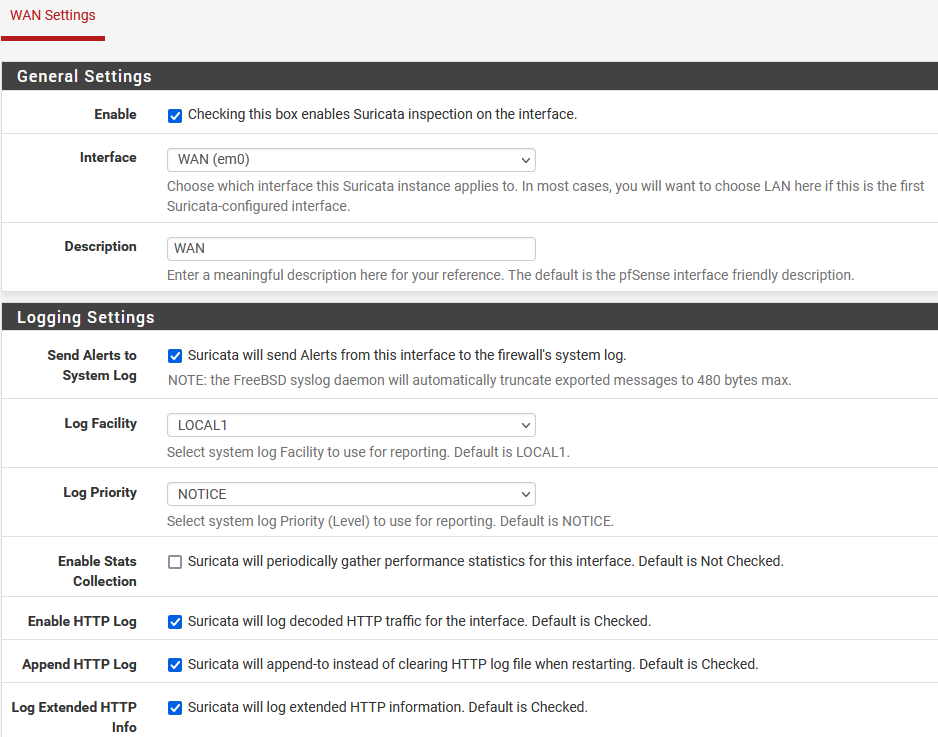
Y por último en este apartado tenemos el intervalo de tiempo para borrar la lista de ips bloqueados, donde copiamos los logs y si preservamos los setting en caso de desinstalar el paquete.



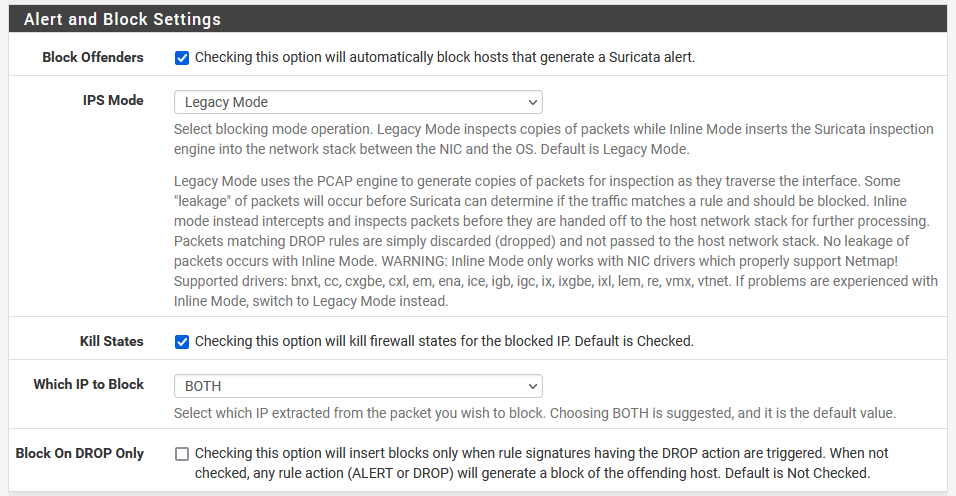
Ya tenemos lo básico, pasemos a las interfaces que queremos proteger dirigiéndonos a

Services/Suricata/Interfaces

Una vez estamos en dicho apartado le damos a Add, donde nos encontraremos muchas opciones. En la parte Wan Settings es donde seleccionaremos nuestra interfaz Wan donde queremos activar el servicio, si tenemos más Wan tendremos que activar el servicio para cada Wan.

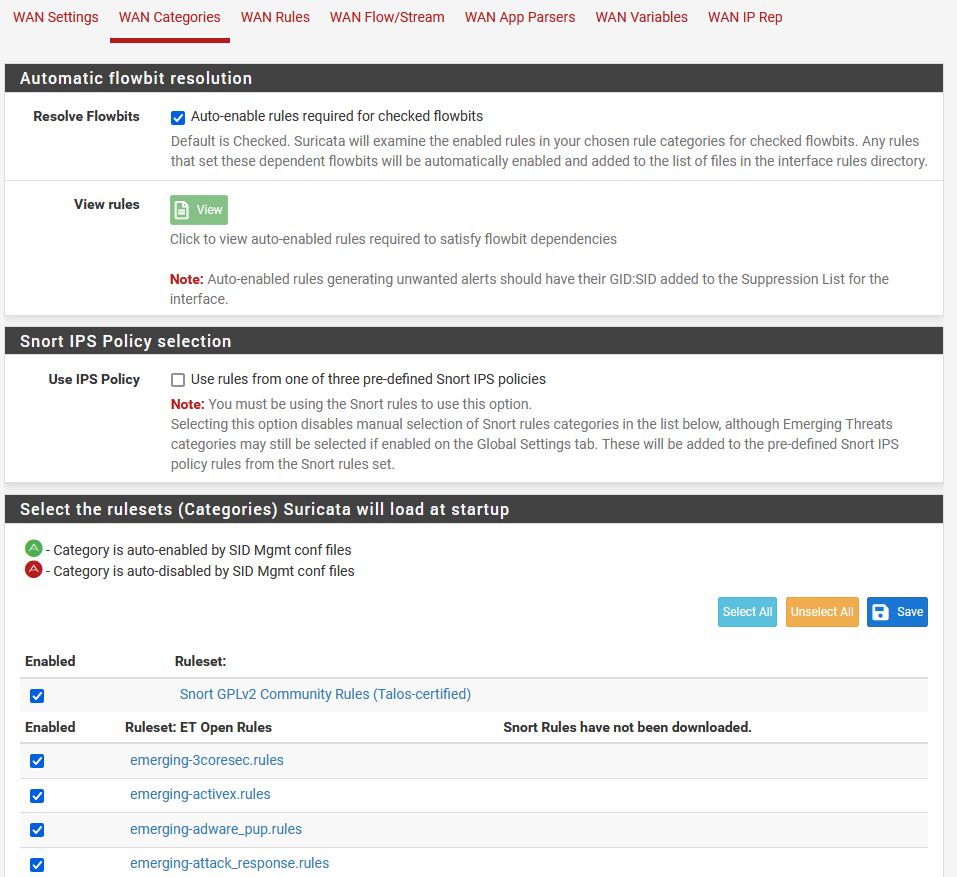


La siguiente opción es muy importante, sin ella lo único que haríamos es generar logs nada más y lo que buscamos es bloquear por lo tanto habilitamos la opción para que bloquee todos los hosts que generen una alerta de Suricata y convirtamos nuestro firewall en un IPS.



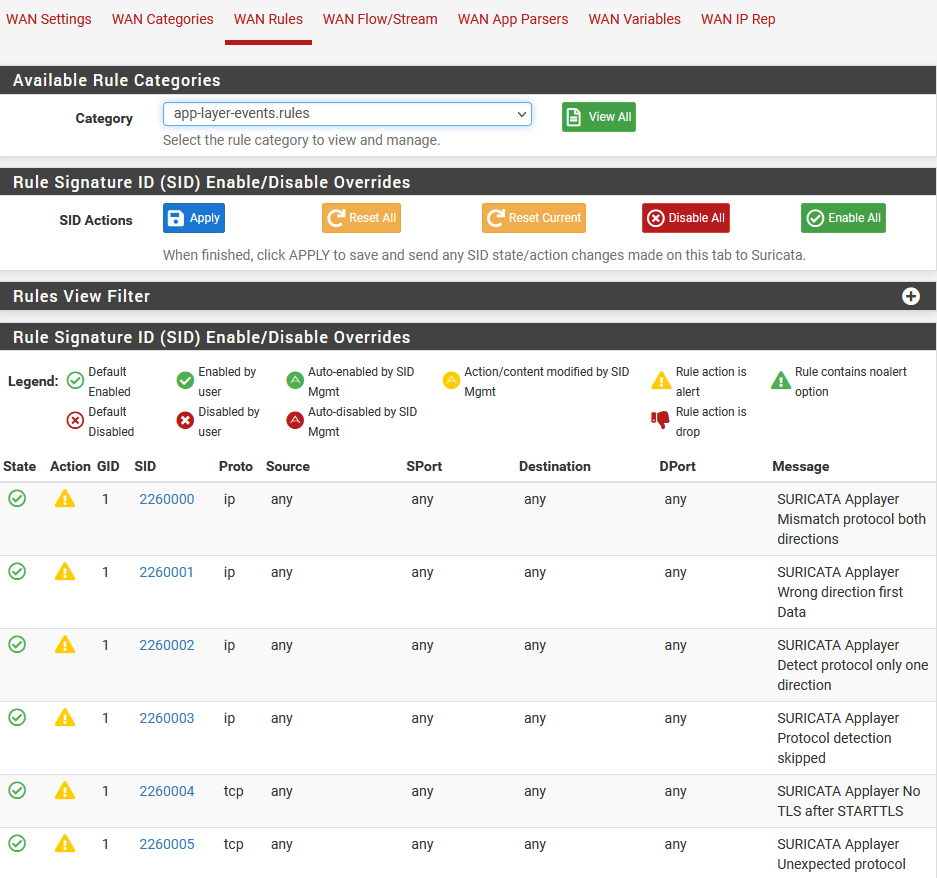
En el siguiente apartado veremos qué redes queremos proteger, la opción por defecto será válida para casi todos los usuarios, pero si tienes redes que el firewall no puede ver puedes crea un Pass List en Services/Suricata/Pass Lists con esas redes y selecciona dicha lista en cada apartado en función del tipo de red.

En la parte de Pass Lists haremos lo mismo, nos iremos a Services/Suricata/Pass Lists y creamos otra lista con todas las IPS que no deben ser bloqueadas, esto es muy recomendable para que no haya un falso positivo y te corte la comunicación de algo importante.



Dentro de cada categoría hay reglas que podremos ver en Wan Rules si las hemos activado en el paso anterior, aquí es una parte donde afinamos si tenemos reglas que por algún motivo nos da muchos quebraderos de cabeza, pero no son vitales deshabilitando o bien utilizando su SID para crear reglas en la Suppress list.

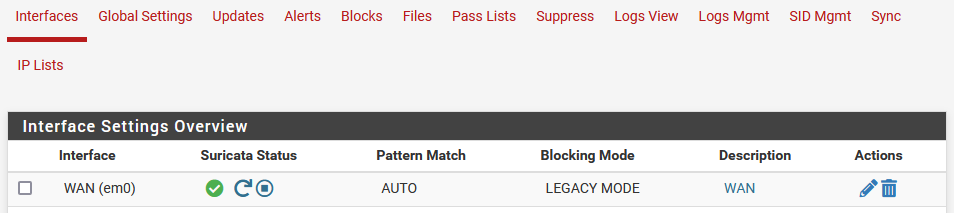
Comentar que por defecto no vienen todas activadas podéis dedicarle un buen tiempo a ver cuáles hay y que hacen.



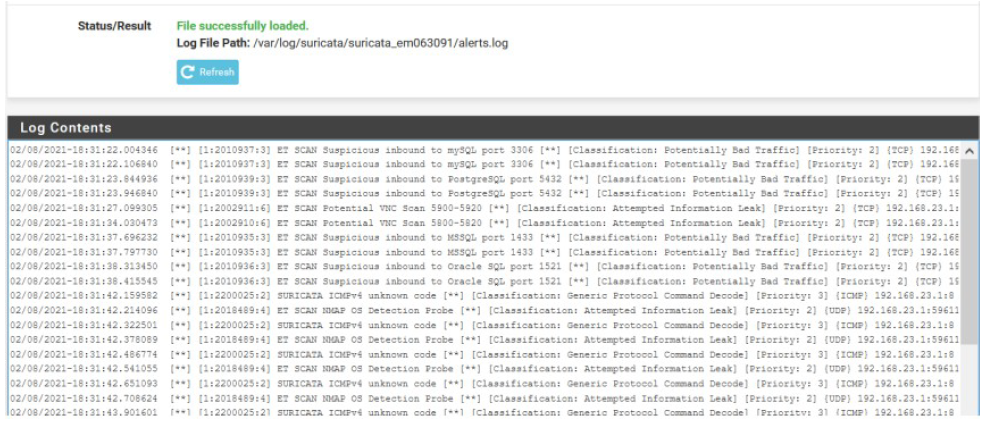
El resto de opciones consultar la documentación porque también son muchas opciones salvo Wan Barnyard que es un simple interprete que nos colocará las alertas en una base de datos Mysql para poder realizar estudios, esto gasta recursos y de momento no nos interesa y Wan IP Rep que no utilizaremos ya que utilizamos pfBlockerNG.

Una vez todo realizado y salvado solo tenemos que activar Suricata en la interfaz

Services/Suricata/Interfaces y dar al símbolo play.



Para probar el funcionamiento ejecutaremos un escáner de puertos desde nuestra máquina Windows 10 desde la que virtualizamos contra la dirección ip de la WAN del firewall.



Y en el log de ips bloqueadas aparecerá nuestra dirección ip.



# **5. Squid/ClamAV/LightSquid**

Squid, el servidor proxy open source más popular nacido en los 90, debido a su gran rendimiento como proxy caché, a los protocolos que soporta HTTP, HTTPS, GOPHER, FTP, IMAP, a la capacidad de limitar conexiones o ancho de banda, opción de usarse como proxy transparente y poder utilizarlo como proxy inverso.

SquidGuard, un sistema de filtrado que utiliza listas negras de contenido.

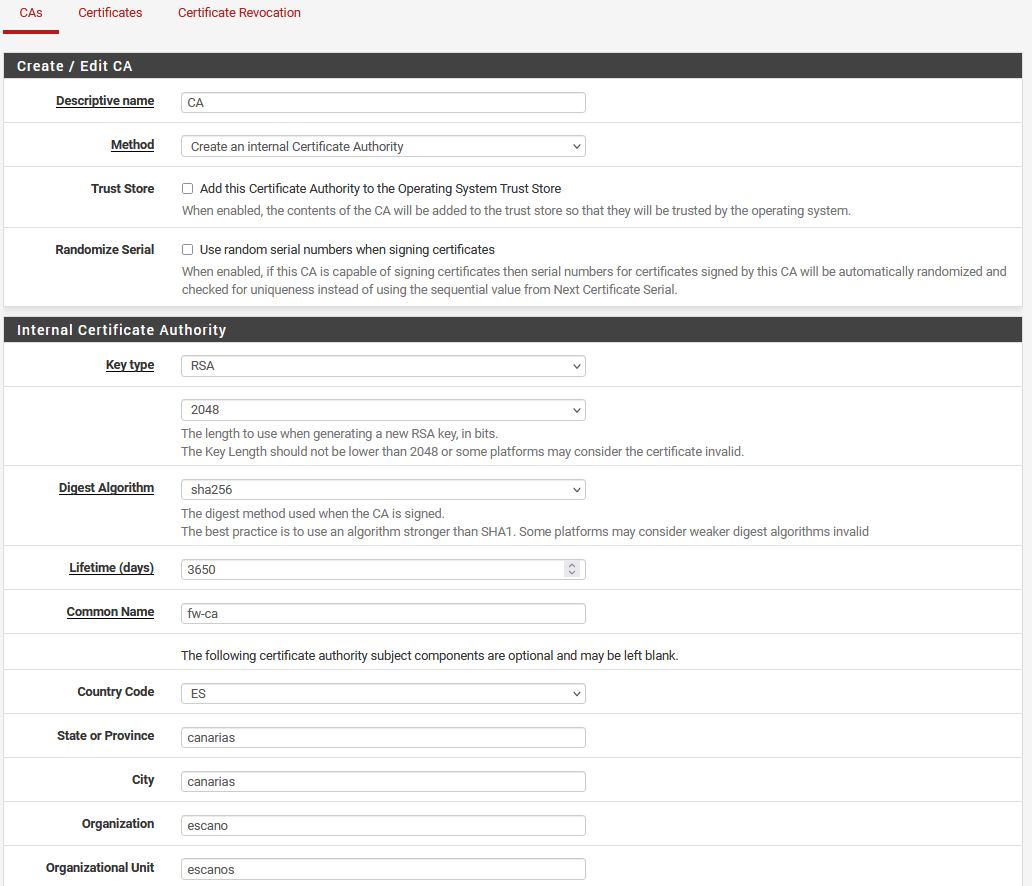
Clam-AV, antivirus open source muy bien integrado en pfSense.

Lightsquid, una aplicación vía web que a partir de los logs de Squid nos generará informes muy detallados.

Una vez instalados, en el menú Services tendremos tres nuevas opciones Squid Proxy Server, Squid Reverse Proxy (del cual no hablaremos en este curso) y SquidGuard Proxy Filter. En el menú Status tendremos Squid Proxy Reports.

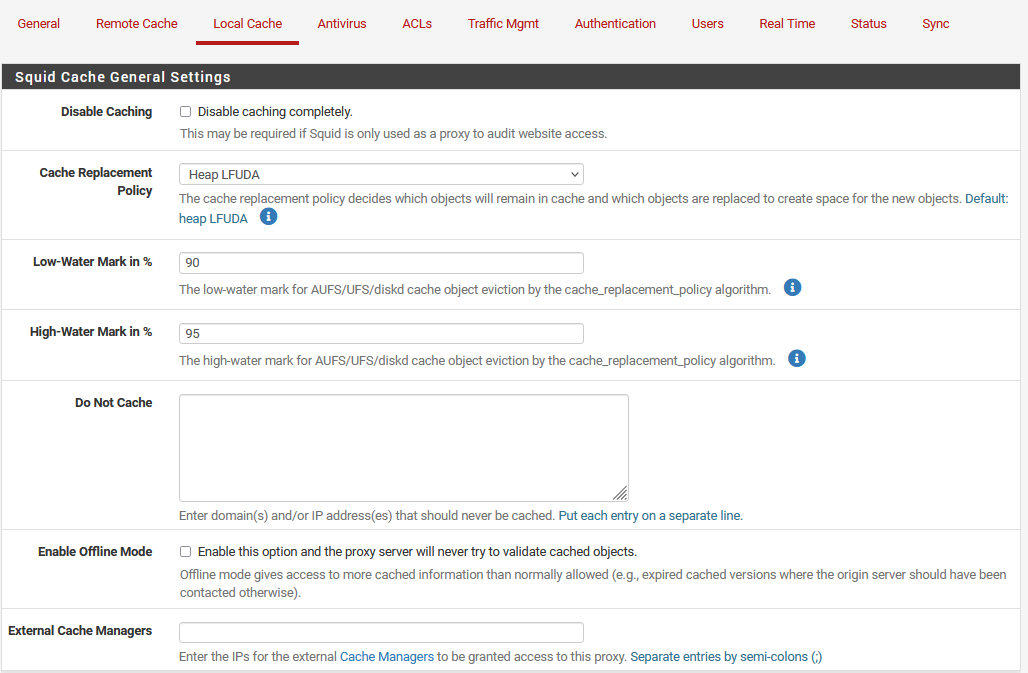
Antes de configurar el proxy, vamos a configurar certificados en el servidor ya que actualmente casi todo el tráfico en internet es https y para poner un proxy intermedio necesitamos el uso de certificados.

Empezaremos configurando una entidad certificadora CA.

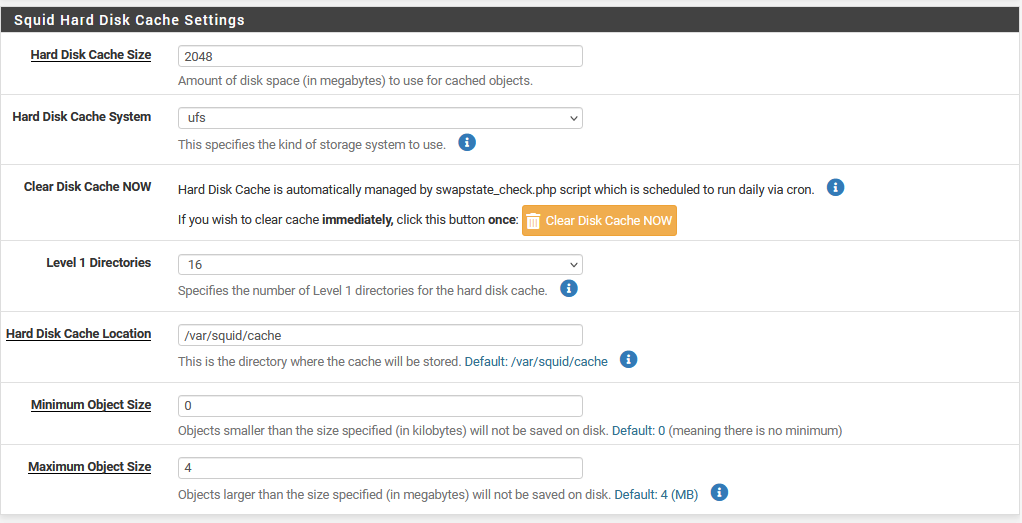


Ahora pasamos a configurar Squid desde Services/ Squid Proxy Server/ Local Cache.

En la primera sección nos encontramos los ajustes generales.



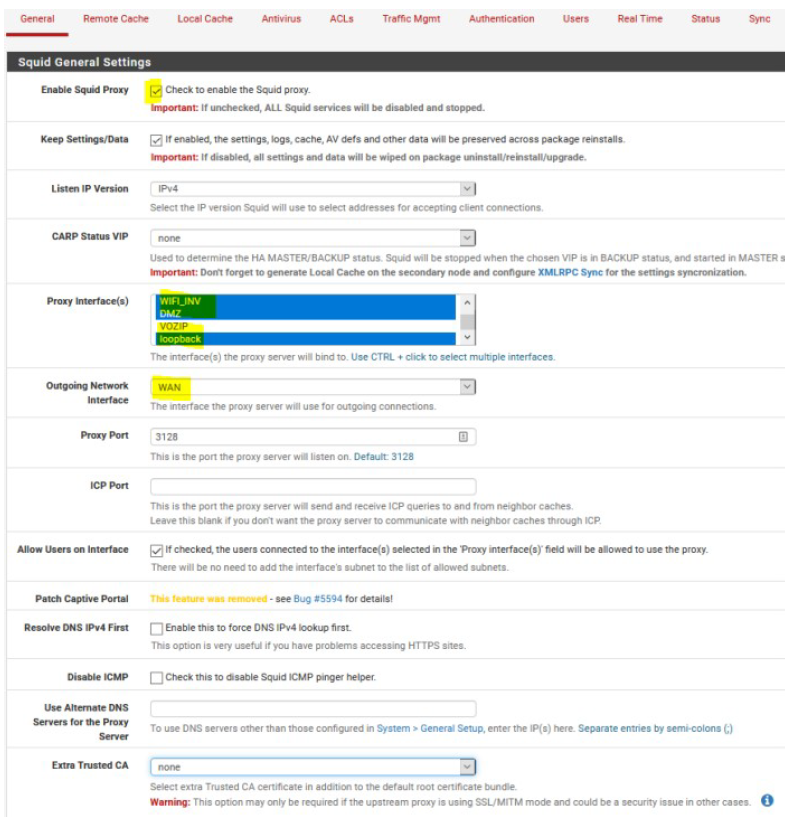
La primera es la política donde se decide que objetos permanecerán en la cache y cual se remplazará, tenemos cuatro opciones donde debemos poner la que más se ajuste a nuestras necesidades, por defecto está LFUDA donde mantiene los objetos más solicitados en cache independientemente de su tamaño, para empezar, es muy buena opción.



A continuación, la siguiente sección sería la caché en memoria mucho más rápida que la de disco, donde no asignaría más de un 25% aunque en la ayuda pone 50% porque es un parámetro que luego se olvida que está ahí empiezas a instalar servicios y tienes un problema porque te quedas sin RAM y el firewall empieza a swapear lo cual ya hace que todo vaya bastante mal.

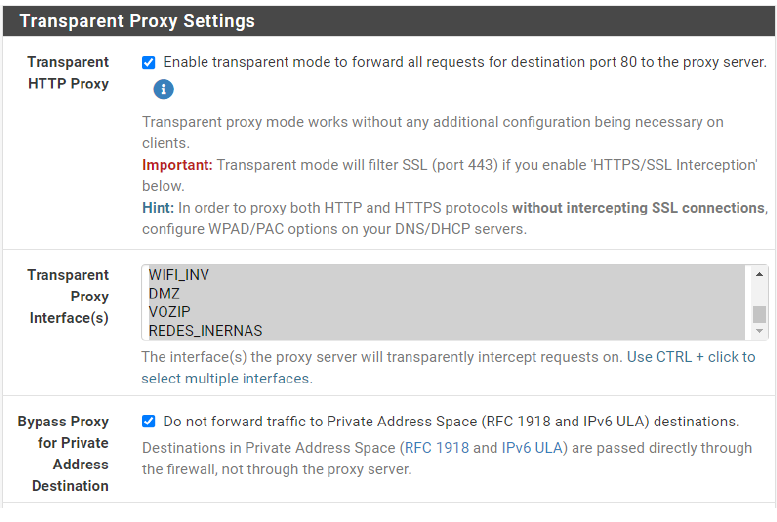
Hemos configurado primero la caché porque al configurar el servicio nos dará errores si no está definida. Con la caché preparada vamos a dirigirnos a la configuración general de Squid en la pestaña General.

Los otros dos valores para la mayoría de escenarios está correcto con 256k y política GDSF.

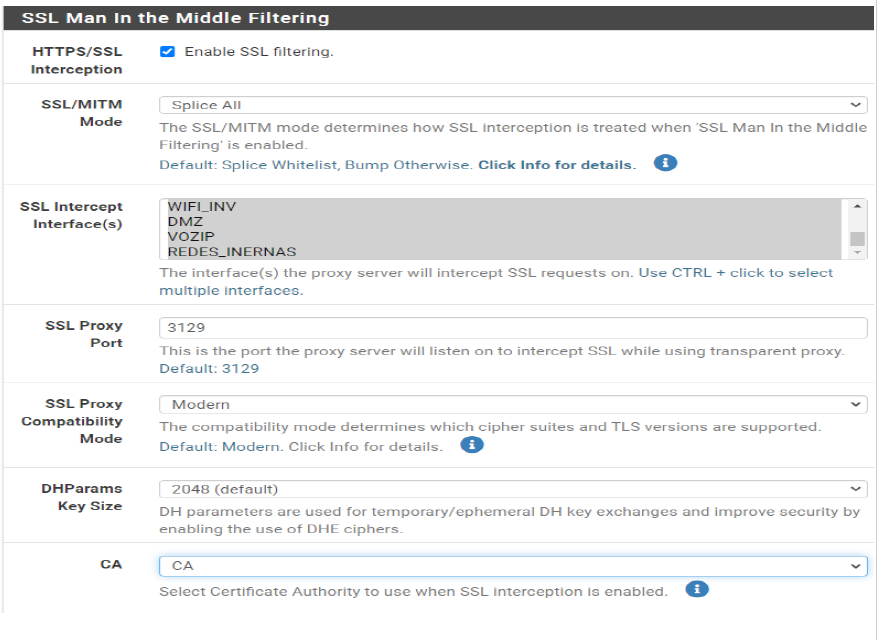


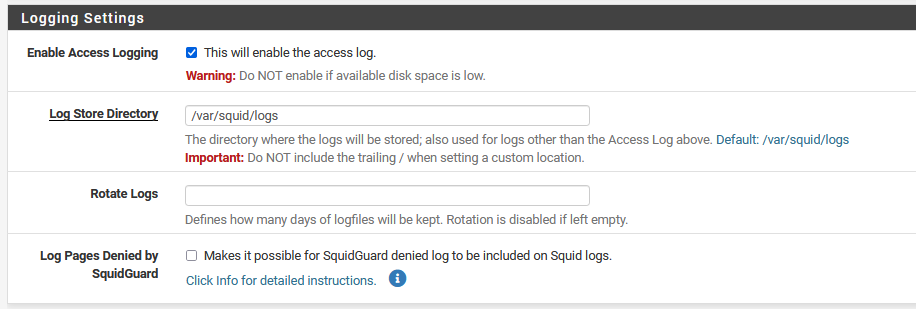
En el apartado General settings nos encontramos la opción Enable Squid Proxy y que tendremos que activar, la opción Keep Settings que como en cualquier otro paquete si está activada preservará configuraciones, logs, cache y definiciones antivirus de Squid si desinstalamos el paquete.

La siguiente sección sería Transparent Proxy Settings

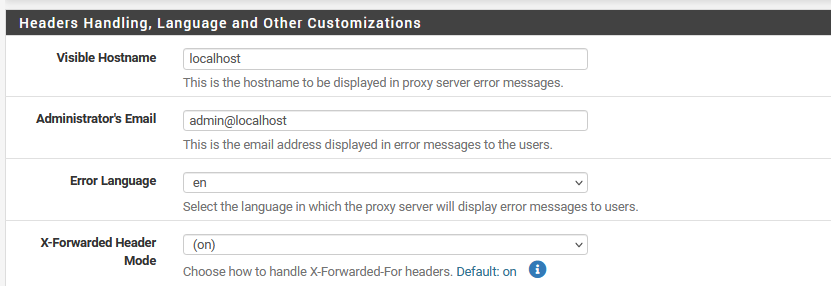


La tercera sección de este apartado es SSL Man In the Middle filtering, muy importante ya que a día de hoy la mayoría de tráfico es HTTPS.

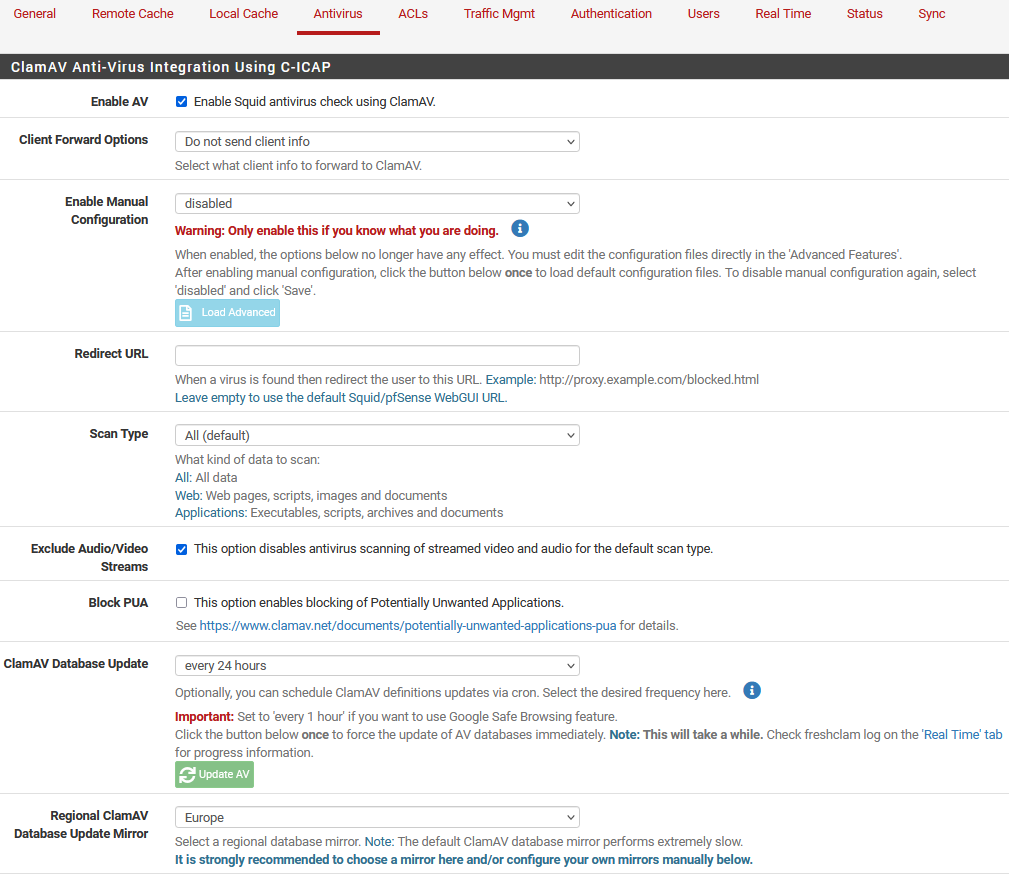




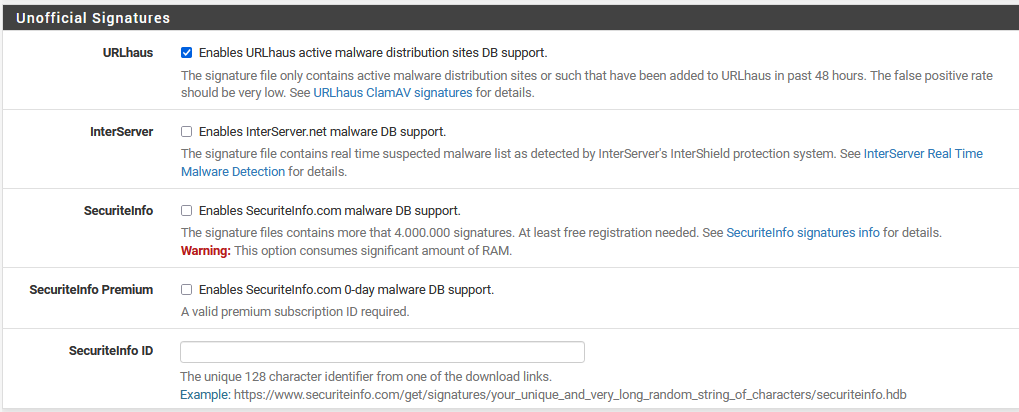
Y por último en el apartado Headers Handling, Language and Other Customizations.

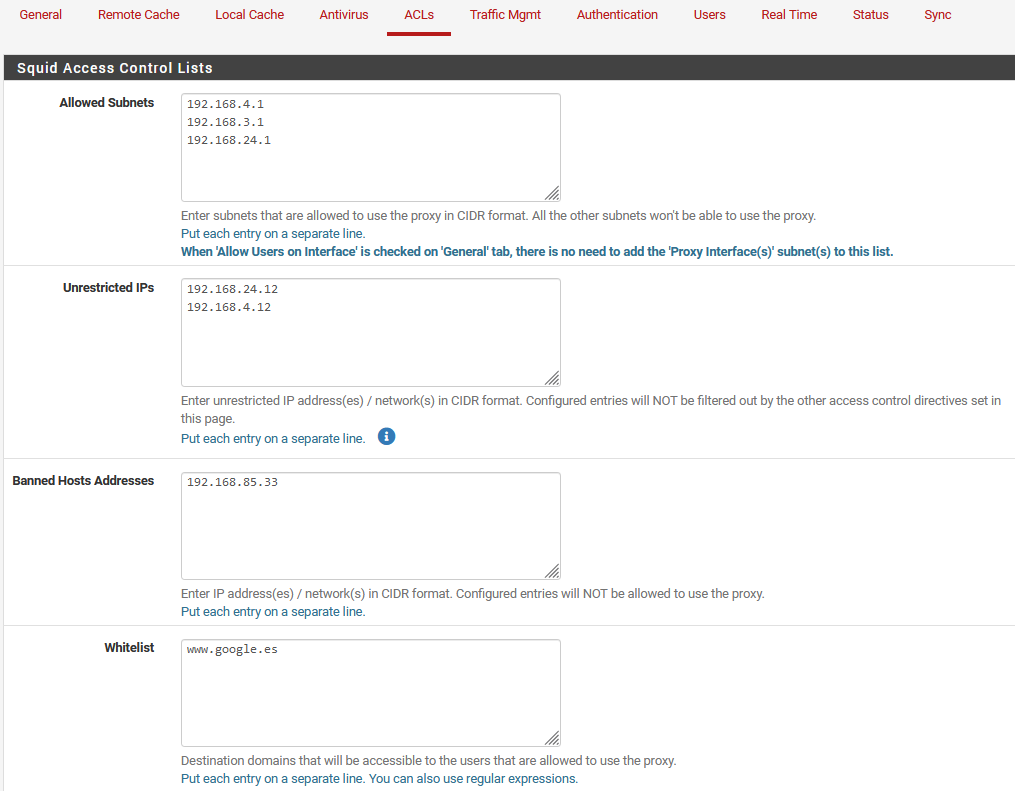


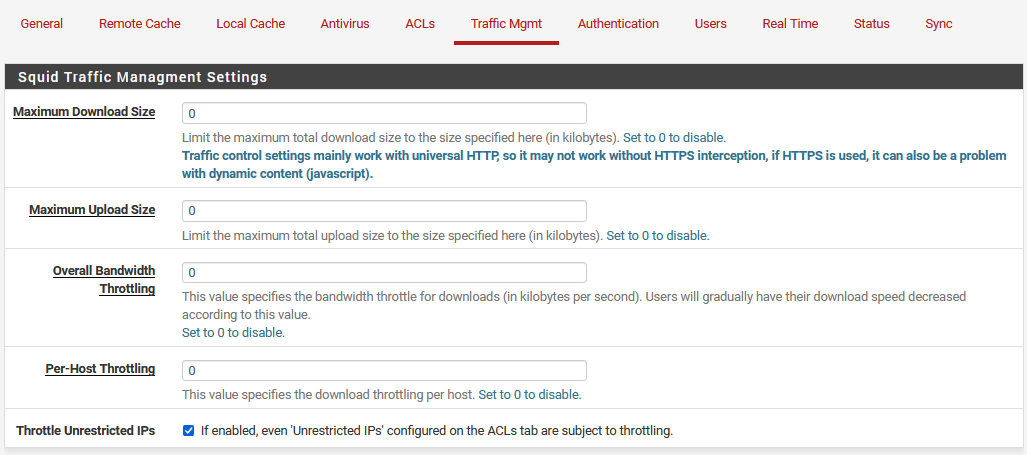
Apartado antivirus:

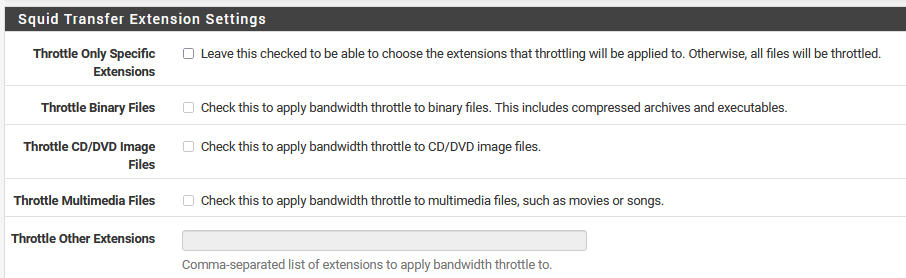


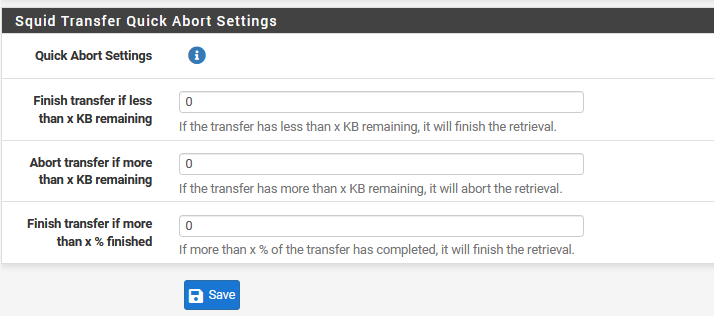
Donde nos encontramos con la primera opción para habilitar o no ClamAV.



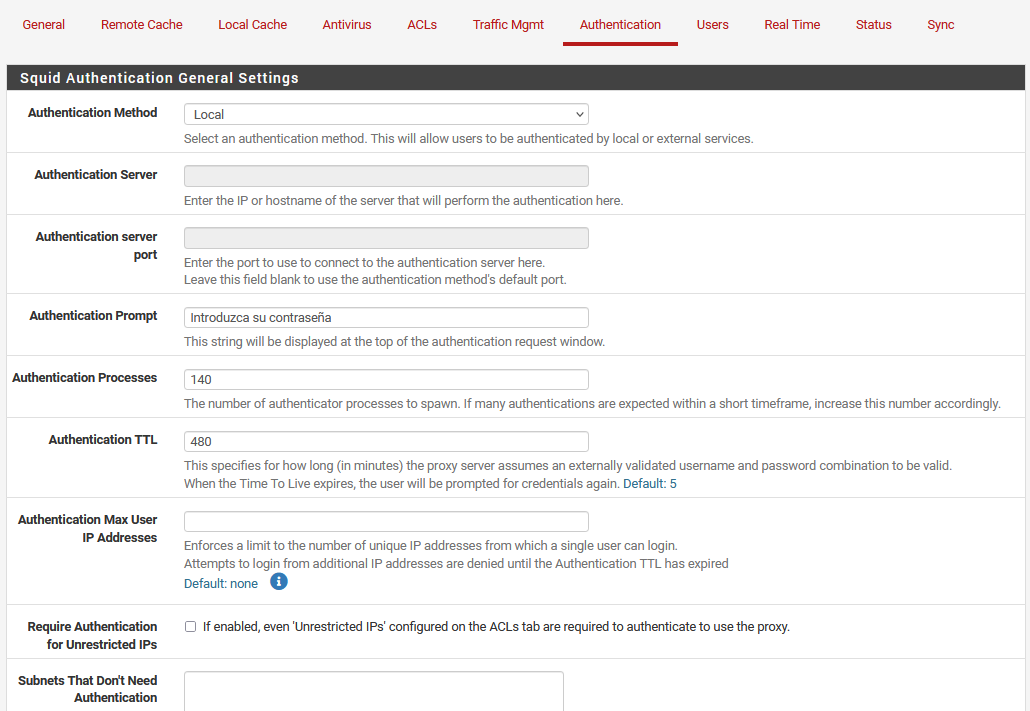




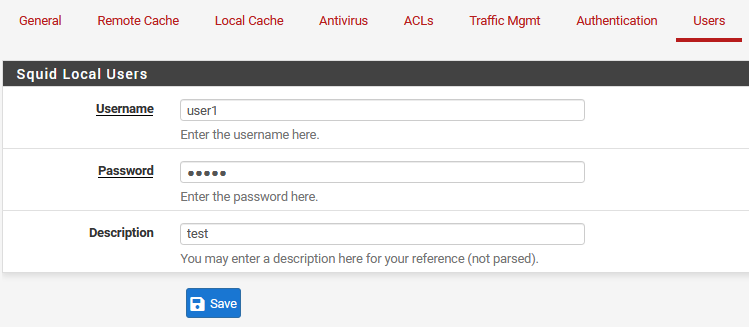




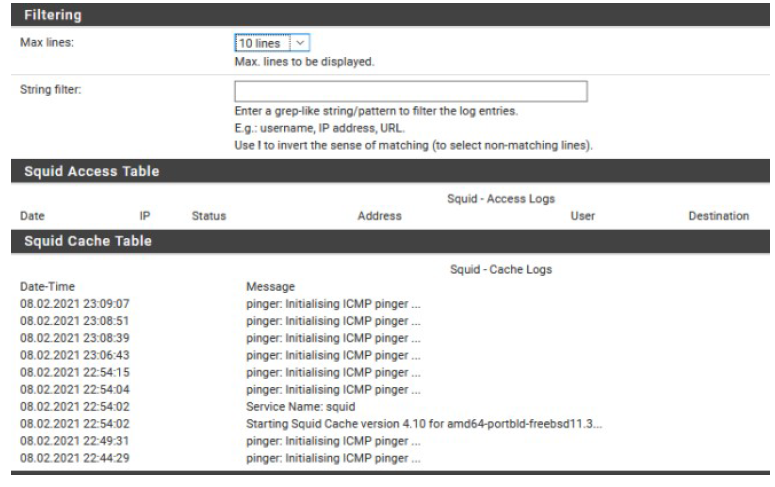
Pasemos al apartado Authentication. En todo proxy de empresas o clientes debemos tener un sistema autenticación para que nos permita crear luego reglas en función del tipo de usuario. Con squid tenemos cuatro métodos, usuarios locales que se añadirían en el apartado Users, Active Directory, Radius o Portal Cautivo, en este apartado se activarán las opciones según el método elegido, vamos a seleccionar Local.



Ahora en Users como hemos seleccionado Local vamos a introducir alguno haciendo click en Add y luego en Save.



En Real Time como su nombre indica veremos lo que está pasando por Squid en Tiempo real diferenciado en varios apartados como la tabla de caché, de SquidGuard,Virus....

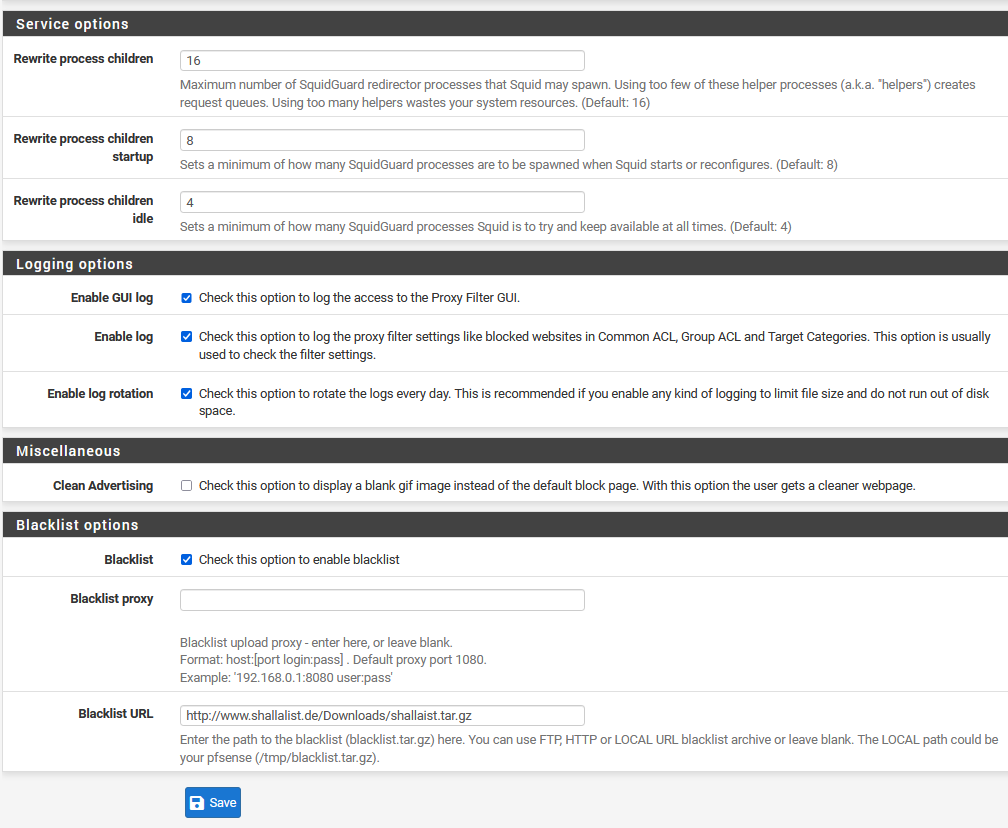


# **6. SquidGuard**

Ahora configuraremos SquidGuard dirigiéndonos a Services / SquidGuard Proxy Filter, donde nos encontramos las siguientes secciones en General Settings.

Donde nos indica que antes de activar configuremos por lo menos una Categoría y que después cualquier cambio hay que hacer click en el botón Apply, por lo tanto, lo dejaremos para el final.

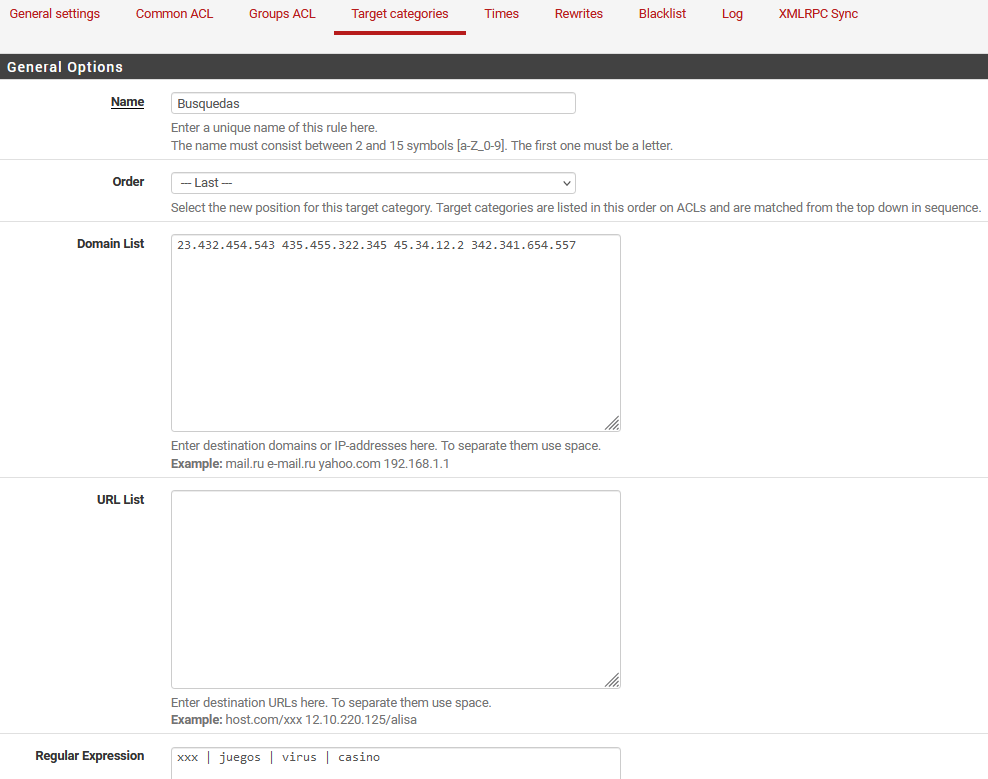
Tenemos la opción de utilizar LDAP para crear filtros, en este laboratorio no lo vamos a utilizar. Las siguientes opciones de esta pestaña general son

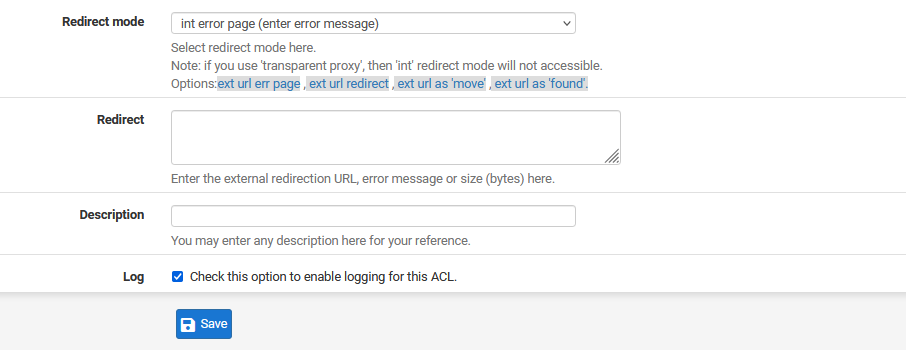


La primera opción es activar la Blacklist que por supuesto activaremos ya que la advertencia de no activarla es solo en instalaciones que se hayan realizado con la herramienta nano BSD, muy utilizada para crear imágenes de sistema.

Luego tenemos 2 opciones, utilizar un proxy de listas negras o bien especificar una URL de listas negras para cargarlas, esto último es lo que haremos.

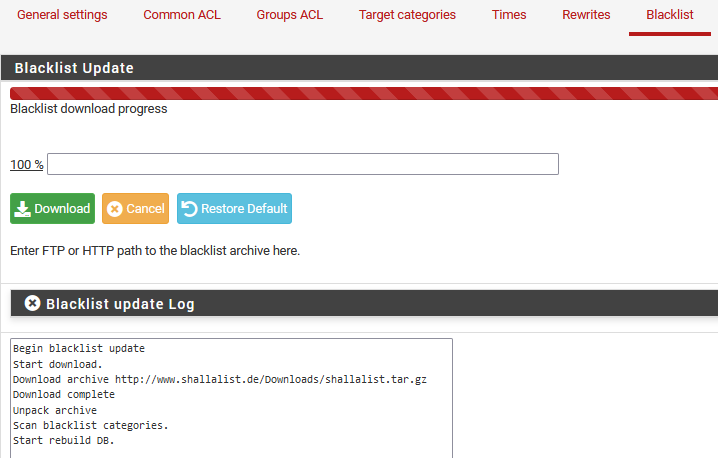
En este laboratorio lo vamos hacer simple crearemos Bloqueadas y Permitidas dando a Add.



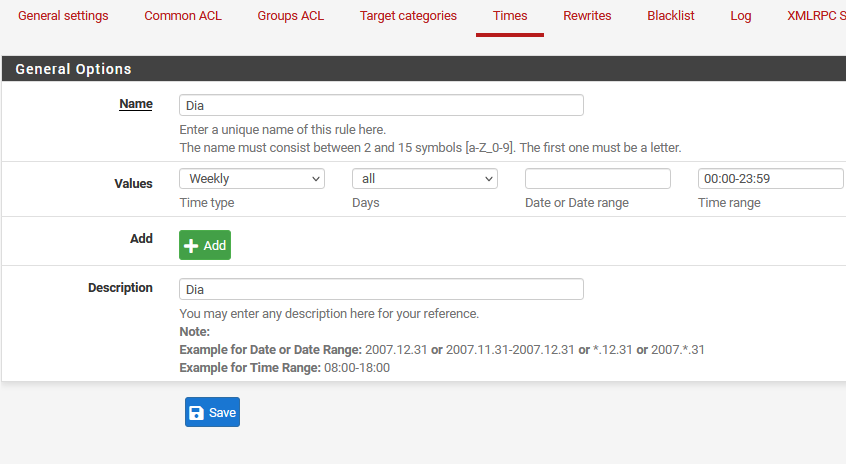


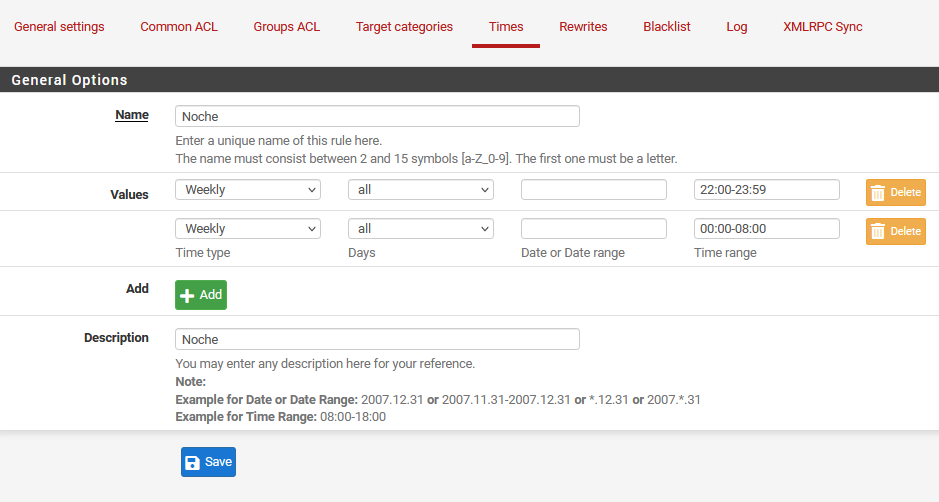
Ponemos el nombre, elegimos la posición la cual debería ser la última siempre “LAST”, ya que si fuera la primera y hay dentro de ella algo que permitimos en una lista posterior seguirá estando bloqueada.

Ahora pasaremos a descargarnos la lista que pusimos en general, vamos a la pestaña Blacklist y hacemos click en Download.

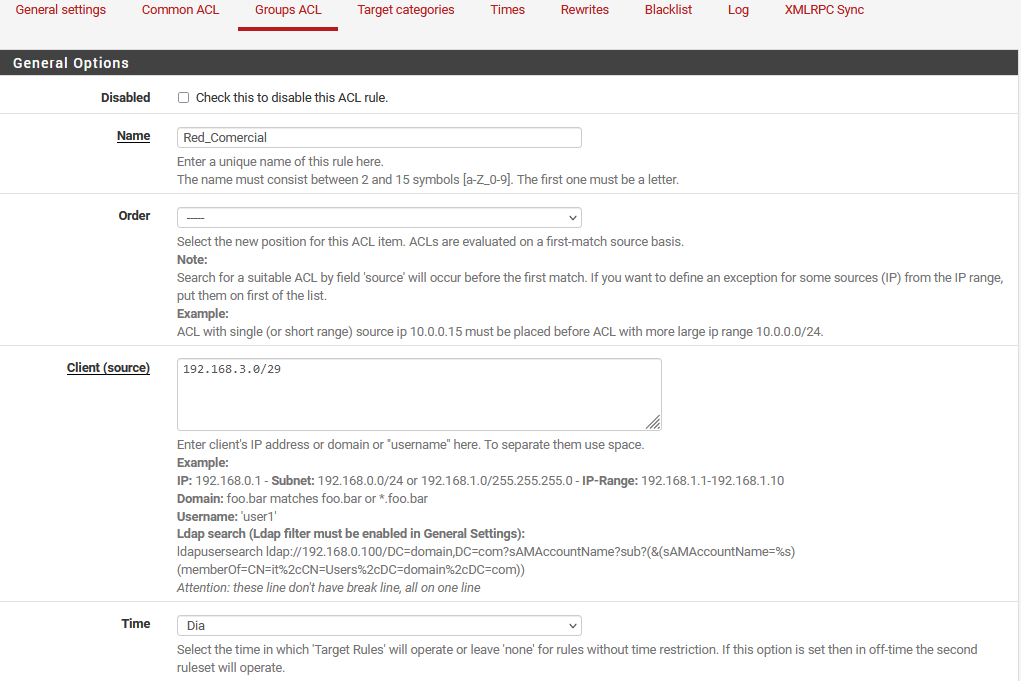


Ahora, si quisiéramos utilizar franjas horarias para las reglas porque por ejemplo para el turno nocturno somos más permisivos, lo primero sería crear esas franjas en la pestaña Times dando a Add.



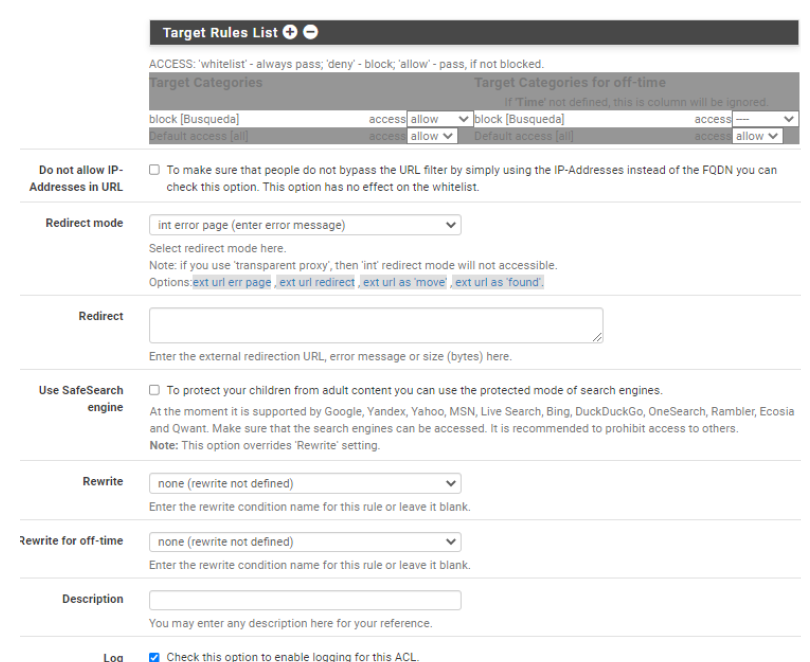


Hecho esto, podemos hacer ya ACL comunes (Common ACL) y ACL por grupos (Groups ACL), donde nos aparecerá en ambos casos en Target Rule List primero las Target categories en el orden elegido, seguido de las categorías descargadas donde debemos elegir



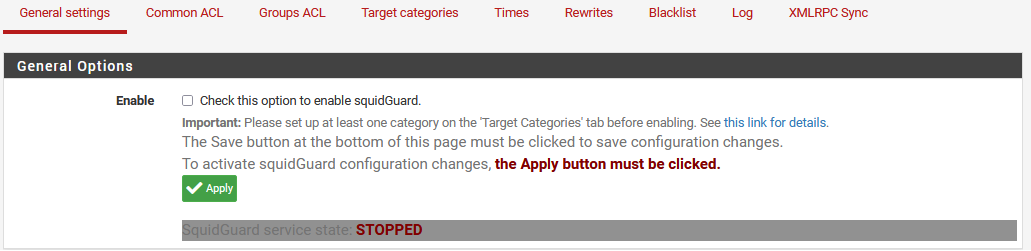
En la segunda parte elegiremos las categorías que nos hemos descargado anteriormente,

recordando que en esta parte hay una cosa importante: la última categoría Default access [all].



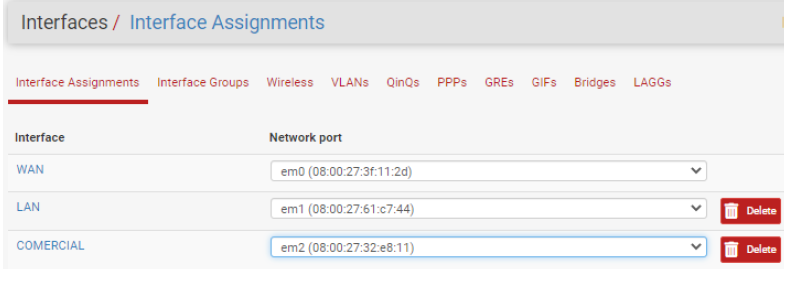
Esto definirá nuestra política, podemos bloquear todo por defecto he ir añadiendo lo permitido o permitir todo e ir denegando. en la mayoría de los casos si no te quieres complicar la vida será permitir todo e ir denegando, en otros casos te podrán pedir deniega todo menos estas 4 webs, pues ya sabéis como hacerlo.

Por último, en esta pestaña APPLY:



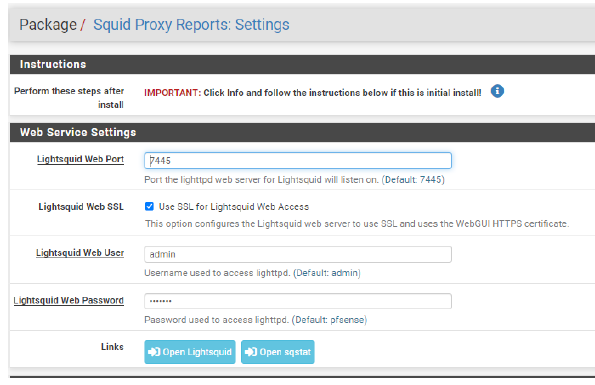
Ahora podemos empezar hacer pruebas de navegación y ver que los filtros están funcionando quedando reflejados en la pestaña Logs, recordar que si no hemos configurado proxy transparente debemos configurar los equipos con la dirección del proxy y puerto para todos los servicios.

Dentro del firewall asignamos la red comercial a la interfaz física para no marcar el tráfico con una vlan.



Configuramos una máquina virtual Windows y le asignamos la red Comercial (VMnet3) en mi caso y le asignamos una dirección ip dentro del rango de la red Comercial.

Ahora pasamos a ver Lightsquid el cual nos permite sacar estadísticas de nuestro proxy. Nos dirigimos a Status/Squid Proxy Reports y nos encontraremos con los siguientes apartados.



Una vez configurado todo esto el servicio empezará a funcionar y podemos abrirlo desde el botón azul Open Lightsquid en el apartado Web Service Setting mostrando la siguiente pantalla donde podremos elegir qué día queremos ver.

