

## Práctica 5.1: Firewalls de próxima generación



Práctica 5.1: Firewalls de próxima generación  
Victoria Eugenia Pérez González  
31/03/2023

# ÍNDICE

<b>Introducción pfBlockerNG:</b>	<b>4</b>
Historia:	4
Motivación:	4
Funcionalidades:	4
Alternativas:	5
Principales características:	5
<b>Instalación DNS Resolver:</b>	<b>7</b>
Historia:	7
Motivación:	7
Funcionalidades:	7
Alternativas:	8
Principales características:	8
<b>Configuración pfBlockerNG :</b>	<b>10</b>
<b>Suricata</b>	<b>17</b>
Historia:	17
Motivación:	17
Funcionalidades:	17
Alternativas:	18
Principales características:	18
<b>Empezaremos configurando una entidad certificadora CA.</b>	<b>27</b>
Historia:	27
Motivación:	27
Funcionalidades:	27
Alternativas:	28
Principales características:	28
<b>Squid</b>	<b>29</b>
Historia:	29
Motivación:	30
Funcionalidades:	30
Alternativas:	30
Principales características:	30
<b>Lightsquid</b>	<b>51</b>
Historia:	51
Motivación:	51
Funcionalidades:	51
Alternativas:	52
Principales características:	52

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.

### Introducción pfBlockerNG:

pfBlockerNG es un paquete de seguridad para pfSense que se utiliza para bloquear el tráfico de redes no deseadas y mantener la seguridad de la red. Es una herramienta útil para prevenir el spam, el malware, el phishing y otros ataques cibernéticos. pfBlockerNG utiliza listas de bloqueo públicas para filtrar el tráfico y proporciona una configuración flexible para ajustar el nivel de protección de la red.

### Instalación:

Para instalar pfBlockerNG en pfSense, siga los siguientes pasos:

Inicie sesión en su pfSense e ingrese al menú "System" y seleccione "Package Manager".

Seleccione la pestaña "Available Packages" y busque "pfBlockerNG".

Seleccione "Install" para instalar pfBlockerNG.

Confirme la instalación y espere a que se complete el proceso.

### Historia:

pfBlockerNG es un paquete de software de firewall de código abierto que se ejecuta en el sistema operativo pfSense. Fue creado en 2012 por BBcan177, un desarrollador independiente que buscaba una solución para bloquear el tráfico no deseado en su red doméstica. Desde entonces, el proyecto ha crecido en popularidad y cuenta con una gran comunidad de usuarios y desarrolladores.

### Motivación:

La motivación detrás de la creación de pfBlockerNG fue proporcionar a los usuarios de pfSense una solución de firewall de código abierto y gratuito que pudiera bloquear el tráfico no deseado en la red. La idea era ofrecer una herramienta que fuera fácil de usar y altamente personalizable, para que los usuarios pudieran adaptarla a sus necesidades específicas.

### Funcionalidades:

pfBlockerNG es una herramienta de firewall que proporciona una amplia gama de funcionalidades, entre ellas:

- Bloqueo de direcciones IP: pfBlockerNG puede bloquear direcciones IP específicas o rangos de direcciones IP completos.
- Bloqueo de nombres de dominio: pfBlockerNG puede bloquear nombres de dominio específicos o patrones de nombres de dominio.

- Integración con listas de bloqueo de terceros: pfBlockerNG puede integrarse con listas de bloqueo de terceros, como las listas de spam, las listas de bloqueo de anuncios y las listas de bloqueo de malware.
- Monitoreo de tráfico: pfBlockerNG puede monitorear el tráfico de red en tiempo real y alertar a los administradores sobre posibles amenazas de seguridad.
- Integración con otros sistemas de seguridad: pfBlockerNG puede integrarse con otros sistemas de seguridad de red para proporcionar una protección completa de la red.

#### Alternativas:

Existen varias alternativas a pfBlockerNG en el mercado, como Snort, Suricata, Zeek y Security Onion. Estos sistemas de seguridad de red también son de código abierto y gratuitos, y ofrecen funcionalidades similares a las de pfBlockerNG.

#### Principales características:

Las principales características de pfBlockerNG incluyen:

- Código abierto y gratuito
- Bloqueo de direcciones IP y nombres de dominio
- Integración con listas de bloqueo de terceros
- Monitoreo de tráfico en tiempo real
- Integración con otros sistemas de seguridad de red
- Posibilidad de personalización y extensibilidad mediante el uso de reglas personalizadas y complementos.

**pfSense** COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

**WARNING:** The 'admin' account password is set to the default value. Change the password in the User Manager.

System / Package Manager / Available Packages

Installed Packages Available Packages

**Search**

Search term:  Both

Enter a search string or \*nix regular expression to search package names and descriptions.

**Packages**

Name	Version	Description
pfBlockerNG	3.2.0_3	<p>Manage IPv4/v6 List Sources into 'Deny, Permit or Match' formats. GeoIP database by MaxMind Inc. (GeoLite2 Free version). De-Duplication, Suppression, and Reputation enhancements. Provision to download from diverse List formats. Advanced Integration for Proofpoint ET IQRisk IP Reputation Threat Sources. Domain Name (DNSBL) blocking via Unbound DNS Resolver.</p> <p>Package Dependencies:  <a href="#">lighttpd-1.4.69</a> <a href="#">jq-1.6</a> <a href="#">gnugrep-3.8</a> <a href="#">rsync-3.2.7</a> <a href="#">py-maxminddb-2.2.0_1</a> <a href="#">libmaxminddb-1.7.1</a> <a href="#">iprange-1.0.4</a> <a href="#">grepclidr-2.0</a> <a href="#">python311-3.11.2_2</a> <a href="#">php82-8.2.3</a> <a href="#">php82-intl-8.2.3_1</a> <a href="#">py-sqlite3-3.11.2_8</a> </p>

[+ Install](#)

Se instalan además los siguientes paquetes: squid,squidguard y suricata.

System / Package Manager / Installed Packages

Installed Packages Available Packages

**Installed Packages**

Name	Category	Version	Description	Actions
✓ pfBlockerNG-devel	net	3.2.0_3	<p>pfBlockerNG-devel is the Next Generation of pfBlockerNG. Manage IPv4/v6 List Sources into 'Deny, Permit or Match' formats. GeoIP database by MaxMind Inc. (GeoLite2 Free version). De-Duplication, Suppression, and Reputation enhancements. Provision to download from diverse List formats. Advanced Integration for Proofpoint ET IQRisk IP Reputation Threat Sources. Domain Name (DNSBL) blocking via Unbound DNS Resolver.</p> <p>Package Dependencies:  <a href="#">lighttpd-1.4.69</a> <a href="#">jq-1.6</a> <a href="#">gnugrep-3.8</a> <a href="#">rsync-3.2.7</a> <a href="#">py-maxminddb-2.2.0_1</a> <a href="#">libmaxminddb-1.7.1</a> <a href="#">iprange-1.0.4</a> <a href="#">grepclidr-2.0</a> <a href="#">python311-3.11.2_2</a> <a href="#">php82-8.2.3</a> <a href="#">php82-intl-8.2.3_1</a> <a href="#">py-sqlite3-3.11.2_8</a> </p>	
✓ squid	www	0.4.45_10	<p>High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP.</p> <p>Package Dependencies:  <a href="#">squidclamav-7.2</a> <a href="#">squid_radius_auth-1.10</a> <a href="#">squid-5.7</a> <a href="#">c-icap-modules-0.5.5_1</a> </p>	
✓ squidGuard	www	1.16.18_20	<p>High performance web proxy URL filter.</p> <p>Package Dependencies:  <a href="#">squidguard-1.4.15</a> <a href="#">pfSense-pkg-squid-0.4.45_10</a> </p>	
✓ suricata	security	6.0.10_4	<p>High Performance Network IDS, IPS and Security Monitoring engine by OISF.</p> <p>Package Dependencies:  <a href="#">suricata-6.0.10_2</a> </p>	

### Instalación DNS Resolver:

El servicio DNS Resolver en pfSense permite resolver los nombres de dominio de manera local en la red, sin necesidad de utilizar servidores DNS externos. Esto puede mejorar el rendimiento y la privacidad de la red.

### Historia:

El sistema DNS (Domain Name System) fue desarrollado en la década de 1980 como una solución para el creciente número de dispositivos conectados a Internet y la necesidad de resolver nombres de dominio de manera eficiente. El primer software de servidor DNS fue desarrollado por Paul Mockapetris en 1983 y desde entonces, ha evolucionado para convertirse en un sistema crítico para el funcionamiento de Internet.

### Motivación:

La motivación detrás del desarrollo de DNS Resolver fue proporcionar un sistema eficiente y escalable para resolver nombres de dominio. DNS Resolver es capaz de manejar grandes volúmenes de solicitudes de resolución de nombres de dominio y garantizar que los usuarios puedan acceder a los sitios web de manera rápida y confiable.

### Funcionalidades:

Las principales funcionalidades de DNS Resolver son:

- Resolución de nombres de dominio: DNS Resolver es capaz de resolver nombres de dominio en direcciones IP, lo que permite a los usuarios acceder a los sitios web mediante el uso de nombres de dominio.
- Caché de DNS: DNS Resolver mantiene una caché de las solicitudes de resolución de nombres de dominio para reducir el tiempo de respuesta y mejorar la eficiencia del sistema.
- Seguridad: DNS Resolver utiliza diversas técnicas de seguridad, como el filtrado de consultas y la autenticación, para garantizar que las respuestas de DNS sean seguras y confiables.
- Escalabilidad: DNS Resolver es capaz de manejar grandes volúmenes de solicitudes de resolución de nombres de dominio y garantizar que el sistema sea escalable para satisfacer las necesidades de los usuarios.

Alternativas:

Existen varias alternativas a DNS Resolver en el mercado, como BIND, PowerDNS, Unbound, entre otros. Cada una de ellas ofrece diferentes servicios de resolución de nombres de dominio y funcionalidades para adaptarse a las necesidades de los usuarios.

Principales características:

Las principales características de DNS Resolver son:

- Resolución rápida y confiable: DNS Resolver es capaz de resolver nombres de dominio de manera rápida y confiable, lo que garantiza que los usuarios puedan acceder a los sitios web de manera eficiente.
- Caché de DNS: DNS Resolver mantiene una caché de las solicitudes de resolución de nombres de dominio para reducir el tiempo de respuesta y mejorar la eficiencia del sistema.
- Seguridad: DNS Resolver utiliza diversas técnicas de seguridad para garantizar que las respuestas de DNS sean seguras y confiables.
- Escalabilidad: DNS Resolver es capaz de manejar grandes volúmenes de solicitudes de resolución de nombres de dominio y garantizar que el sistema sea escalable para satisfacer las necesidades de los usuarios.
- Personalización: DNS Resolver permite a los usuarios personalizar la configuración y los parámetros según sus necesidades específicas.

Para configurar el servicio DNS Resolver en pfSense, siga estos pasos:

Inicie sesión en pfSense y vaya a Services > DNS Resolver.

Asegúrese de que la casilla "Enable DNS Resolver" esté seleccionada.

En la sección "DNSSEC", seleccione "Enable DNSSEC Support" si desea habilitar la validación de DNSSEC. Esta opción aumentará la seguridad de las consultas DNS, pero puede causar problemas si los servidores DNS externos no tienen soporte para DNSSEC.



General Settings   **Advanced Settings**   Access Lists

---

### General DNS Resolver Options

<b>Enable</b>	<input checked="" type="checkbox"/> Enable DNS resolver
<b>Listen Port</b>	<input type="text" value="53"/> <small>The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.</small>
<b>Enable SSL/TLS Service</b>	<input type="checkbox"/> Respond to incoming SSL/TLS queries from local clients <small>Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.</small>
<b>SSL/TLS Certificate</b>	<input type="text" value="webConfigurator default (6418adf77a85f)"/> <small>The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.</small>
<b>SSL/TLS Listen Port</b>	<input type="text" value="853"/> <small>The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.</small>
<b>Network Interfaces</b>	<div> <input type="text" value="All"/>  <input type="text" value="WAN"/>  <input type="text" value="LAN"/>  <input type="text" value="IT"/>  <input type="text" value="WIFI-CORP"/> </div> <small>Interface IP addresses used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 addresses, both are used. Queries to addresses not selected in this list are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.</small>
<b>Outgoing Network Interfaces</b>	<div> <input type="text" value="All"/>  <input type="text" value="WAN"/>  <input type="text" value="LAN"/>  <input type="text" value="IT"/>  <input type="text" value="WIFI-CORP"/> </div> <small>Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. By default all interfaces are used.</small>
<b>Strict Outgoing Network Interface Binding</b>	<input type="checkbox"/> Do not send recursive queries if none of the selected Outgoing Network Interfaces are available. <small>By default the DNS Resolver sends recursive DNS requests over any available interfaces if none of the selected Outgoing Network Interfaces are available. This option makes the DNS Resolver refuse recursive queries.</small>
<b>System Domain Local Zone Type</b>	<input type="text" value="Transparent"/> <small>The local-zone type used for the pfSense system domain (System   General Setup   Domain). Transparent is the default.</small>

**DNSSEC**   ☒ **Enable DNSSEC Support**

En la sección "General DNS Resolver Options", seleccione la interfaz WAN o cualquier otra interfaz donde desee que el servicio DNS Resolver esté habilitado.

En la sección "Access Lists", agregue cualquier lista de acceso que desee utilizar para limitar el acceso al servidor DNS Resolver.

En la sección "Domain Overrides", agregue cualquier dominio que desee que se resuelva localmente en la red. Por ejemplo, si tiene un servidor web local con el nombre "webserver.local", puede agregar una entrada aquí para que los dispositivos en la red puedan resolver ese nombre de dominio sin necesidad de utilizar servidores DNS externos.

En la sección "Advanced DNS Resolver Options", puede ajustar opciones adicionales para el servicio DNS Resolver, como la configuración de caché, límites de consulta y más.

Haga clic en "Save" para guardar la configuración.

Configuración pfBlockerNG :

Una vez instalado pfBlockerNG, siga estos pasos para configurarlo:

Seleccione "Firewall" en el menú y luego "pfBlockerNG".

The screenshot shows the 'DNSBL' configuration page in pfBlockerNG. At the top, there's a 'DNSBL' header with links for 'Links', 'Firewall Aliases', 'Firewall Rules', and 'Firewall Logs'. Below this, the 'DNSBL' section is checked and labeled 'Enable DNSBL'. A note states: 'This will enable DNS Block List for Malicious and/or unwanted Adverts Domains. To Utilize, **Unbound DNS Resolver** must be enabled. Also ensure that pfBlockerNG is enabled.' Below this is the 'DNSBL Configuration' section. The 'Permit Firewall Rules' option is checked and labeled 'Enable'. A note explains: 'This will create 'Floating' Firewall permit rules to allow traffic from the Selected Interface(s) to access the **DNSBL Webserver**. (ICMP and Webserver ports only). This option is not designed to bypass DNSBL for the non-selected LAN segments. This option is only required for networks with multiple LAN Segments.' To the right of this section is a dropdown menu showing a list of interfaces: LAN, IT, WIFI\_CORP, WIFI\_INV, RRHH, GESTION, and DMZ.

Seleccione la pestaña "IP" y luego "DNSBL".

Seleccione "Enable DNSBL" para habilitar el filtrado de DNS.

The screenshot shows the 'pfBlockerNG DNSBL Component Configuration' page. It starts with a header 'pfBlockerNG DNSBL Component Configuration' and a sub-header 'DNSBL Webserver Configuration'. Below the sub-header, there are several configuration fields: 'VIP Address' (10.10.10.1), 'Port' (8081), 'SSL Port' (8443), 'IPv6 DNSBL' (unchecked), and 'DNSBL Whitelist' (checked). Each field has a description. At the bottom, there are 'Back' and 'Next' buttons. Below this is another section titled 'DNSBL IPs'. It contains a note: 'When IPs are found in any Domain based Feed, these IPs will be added to the **pfB\_DNSBL\_IP** Aliastable and a firewall rule will be added to block those IPs. **Note:** To utilize this feature, select the appropriate List Action and define the Inbound/Outbound Interfaces in the **IP Tab**.' Below this note is a 'List Action' dropdown menu set to 'Deny Both' and a 'Default: Disabled' label with an information icon.

Elija una fuente de lista de bloqueo en "DNSBL Feeds".

Haga clic en "Update" para descargar y actualizar la lista de bloqueo.

Seleccione la pestaña "IPv4" para habilitar el filtrado de direcciones IP.

Elija una fuente de lista de bloqueo en "IPv4 Feeds".

Haga clic en "Update" para descargar y actualizar la lista de bloqueo.

Configure las opciones de bloqueo en "IP Blocklist" y "DNSBL Feeds".

Configure las opciones de registro y notificación en "Logging".

Configure las opciones de actualización y sincronización en "Update".

Haga clic en "Save" para guardar la configuración.

The screenshot shows the 'DNSBL Source Definitions' section of a web interface. At the top, there are tabs for 'DNSBL Groups', 'DNSBL Category', and 'DNSBL SafeSearch'. Below these is an 'Info' section with links for 'Firewall Aliases', 'Firewall Rules', and 'Firewall Logs'. A form for adding a new source is visible, with fields for 'Name / Description' (containing 'Malware\_dominios') and 'Description'. Below this is a table of existing sources. The table has columns for 'Format', 'State', 'Source', 'Header/Label', and a 'Delete' button. Two sources are listed: one from 'http://www.malwaredomainlist.com/hostslist/hosts.txt' with header 'Malware', and another from 'https://adaway.org/hosts.txt' with header 'Adaway'. Both are set to 'Auto' format and 'OFF' state. At the bottom, there are buttons for '+ Add' and 'Enable All', and a link to 'Click here for Guidelines'.

Format	State	Source	Header/Label	Action
Auto	OFF	http://www.malwaredomainlist.com/hostslist/hosts.txt	Malware	Delete
Auto	OFF	https://adaway.org/hosts.txt	Adaway	Delete

The screenshot shows the 'Settings' section of the web interface. It contains several configuration options: 'Action' is set to 'Unbound' (Default: Disabled, with a note to select 'Unbound' to enable 'Domain Name' blocking); 'Update Frequency' is set to 'Weekly' (Default: Never, with a note to select how often list files will be downloaded); 'Weekly (Day of Week)' is set to 'Monday' (Default: Monday, with a note to select the day of the week to update); 'Auto-Sort Header field' is set to 'Enable auto-sort' (Automatic sorting of the Header/Label field grouped by the Enabled/Disabled State field setting); and 'Group Order' is set to 'Default'.

Setting	Value	Default	Notes
Action	Unbound	Disabled	Select Unbound to enable 'Domain Name' blocking for this Alias.
Update Frequency	Weekly	Never	Select how often List files will be downloaded. This must be within the Cron Interval/Start Hour settings.
Weekly (Day of Week)	Monday	Monday	Select the 'Weekly' ( Day of the Week ) to Update. This is only required for the 'Weekly' Frequency Selection. The 24 Hour Download 'Time' will be used.
Auto-Sort Header field	Enable auto-sort	-	Automatic sorting of the Header/Label field grouped by the Enabled/Disabled State field setting.
Group Order	Default	-	-

Info

Links

Firewall Aliases

Firewall Rules

Firewall Logs

Name / Description

Peligrosas

Peligrosas

Enter Name and Description. [i](#)

DNSBL Source Definitions

Auto

ON

https://www.dshield.org/feeds/suspiciousdomains\_High.txt

dshied

Delete

Auto

ON

https://someonewhocares.org/hosts/hosts

someone

Delete

Format

State

Source

Header/Label

Click here for Guidelines --> [i](#)

+ Add

Enable All

Settings

Action

Disabled

Default: Disabled

Select **Unbound** to enable 'Domain Name' blocking for this Alias.

Update Frequency

Every 6 hours

Default: Never

Info

Links

Firewall Aliases

Firewall Rules

Firewall Logs

Name / Description

Easylst

Easylst

Enter Name and Description. [i](#)

DNSBL Source Definitions

Auto

ON

https://v.firebog.net/hosts/Easylst.txt

Easylst

Delete

Auto

ON

https://v.firebog.net/hosts/Easyprivacy.txt

Easyprivacy

Delete

Format

State

Source

Header/Label

Click here for Guidelines --> [i](#)

+ Add

Enable All

Settings

Action

Unbound

Default: Disabled

Select **Unbound** to enable 'Domain Name' blocking for this Alias.

Update Frequency

Once a day

Default: Never

Select how often List files will be downloaded. This must be within the Cron Interval/Start Hour settings.

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.

Info

Links

Firewall Aliases

Firewall Rules

Firewall Logs

Name / Description

Level\_1

Level\_1

Enter Name ( Max 24 characters ) and Description. [i](#)

IPv4 Source Definitions

Auto

ON

https://rules.emergingthreats.net/blockrules/compromised-ips.txt

emerin1

Delete

Auto

ON

https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt

emerin2

Delete

Auto

ON

https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt

firehol

Delete

Format

State

Source

Header/Label

Click here for Guidelines --> [i](#)

+ Add

Enable All

Settings

Action

Deny Both

Default: Disabled

For Non-Alias type rules you must define the appropriate Firewall 'Auto' Rule Order option.

Click here for more info --> [i](#)

Update Frequency

Every 2 hours

Default: Never

Select how often List files will be downloaded. This must be within the Cron Interval/Start Hour settings.

IPv4

IPv6

GeolIP

Reputation

Info

Links

Firewall Aliases

Firewall Rules

Firewall Logs

Name / Description

Level\_2

Level\_2

Enter Name ( Max 24 characters ) and Description. [i](#)

IPv4 Source Definitions

Auto

ON

https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/firehol

firehol

Delete

Auto

ON

https://cinscore.com/list/ci-badguys.txt

cinscore

Delete

Format

State

Source

Header/Label

Click here for Guidelines --> [i](#)

+ Add

Enable All

Settings

Action

Deny Both

Default: Disabled

For Non-Alias type rules you must define the appropriate Firewall 'Auto' Rule Order option.

Click here for more info --> [i](#)

Update Frequency

Every 4 hours

Default: Never

Select how often List files will be downloaded. This must be within the Cron Interval/Start Hour settings.

Info

Links

[Firewall Aliases](#)
[Firewall Rules](#)
[Firewall Logs](#)

Name / Description

Level\_3

Level\_3

Enter Name ( Max 24 characters ) and Description.

IPv4 Source Definitions

Auto

ON

https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/firehol

filehol

Delete

Auto

ON

https://lists.blocklist.de/lists/all.txt

blocklist

Delete

Auto

OFF

http://www.sanyal.org/blocklist.txt

sanyal

Delete

Format

State

Source

Header/Label

Click here for Guidelines -->

+ Add

Enable All

Settings

Action

Deny Both

Default: Disabled

For Non-Alias type rules you must define the appropriate Firewall 'Auto' Rule Order option.

Click here for more info -->

Update Frequency

Every 8 hours

Default: Never

Select how often List files will be downloaded. This must be within the Cron Interval/Start Hour settings.

MAXMIND

[Products](#)
[Support](#)
[Developers](#)
[Company](#)
[Blog](#)
[Contact](#)

Account Summary

Account

Account Summary

Account Information

Manage License Keys

Manage Account Services

Manage Users

Account Activity

Edit My Info

Change Password

Two-Factor Authentication

Billing

Payment Method

Payment History

Purchase or Manage Databases

Query Usage Report

GeoIP2 / GeoLite2

Automatic Updates

Download Files

Download History

To comply with data privacy regulations, please monitor our [Do Not Sell My Personal Information Requests](#) page for IP addresses and networks that should not be used for advertising or marketing purposes.

Resources

Learn how to Manage your Account

MaxMind Knowledge Base

Developer Portal

minFraud Release Notes and GeoIP2 Release Notes

Database Products and Subscriptions

Download Databases

View Your Download History

Databases

Access Starts

Access Ends

GeoLite2 Country

2023-01-29

No end date

GeoLite2 City

2023-01-29

No end date

GeoLite2 ASN

2023-01-29

No end date

Purchase or manage database updates and subscriptions

La parte de IPv6 no la vamos a configurar. Respecto a GeoIP sirve para bloquear países, pero antes debemos de registrarnos en MaxMind, la versión gratuita de GeoLite2 en el siguiente enlace <https://dev.maxmind.com/geoip/geoip2/geolite2/> Ahora solo nos falta tres cosas, activar el servicio en Firewall/pfBlockerNG y revisar los parámetros a nuestro gusto por ejemplo si habéis cambiado el idioma y utilizáis MaxMind seleccionáis el mismo idioma.

IP Configuration

Links

Firewall Aliases

Firewall Rules

Firewall Logs

De-Duplication

☒ Enable
 Only used for IPv4 Deny Lists

CIDR Aggregation

☐ Enable
 Optimise CIDRs - merge contiguous CIDRs into larger CIDR blocks.

Suppression

☒ Enable
 Default enabled. This will prevent Selected IPs (and RFC1918/Loopback addresses) from being blocked. Only for IPv4 lists (/32 and /24).

Force Global IP Logging

☐ Enable
 The global logging option is only used to force logging for all IP Aliases, and not to disable the logging of all IP Aliases. This overrides any logging settings in the GeoIP/IPv4/v6 tabs.

Placeholder IP Address

Enter a single IPv4 placeholder address  
For IPv6 '::' will be prefixed to the placeholder IP.  
This address should be in an Isolated Range that is not used in your Network.  
This IP address will be used as a placeholder IP to avoid empty Feeds/Aliases.

ASN Reporting

Query for the ASN (BGPIview.io API) for each block/reject/permit/match IP entry. ASN values are cached as per the defined selection.

MaxMind GeoIP configuration

MaxMind License Key

To utilize the MaxMind GeoIP functionality, you must first register for a free MaxMind user account. Visit the following [Link to Register](#) for a free MaxMind user account. **Utilize the GeoIP Update version 3.1.1 or newer registration option.**

MaxMind Localized Language

Select the localized name data from the Language options available.  
Changes to the Locale will be executed in the background, and will take a few minutes to complete.  
Upon completion, a pfSense Notice will be generated.

IPv4

IPv6

GeoIP

Reputation

IPv4 Summary (Drag to change order)

Name	Description	Action	Frequency	Logging	
PRI1	PRI1 - Collecti...	Deny Outbound	Every hour	Enabled	
Malware_dominios	Dominios con ma...	Deny Both	Weekly	Enabled	
Peligrosas	Peligrosas	Match Inbound	Every 6 hours	Enabled	
EasyList	Easylist	Deny Outbound	Once a day	Enabled	
Level_1	Level_1	Deny Both	Every 2 hours	Enabled	
Level_2	Level_2	Deny Both	Every 4 hours	Enabled	
Level_3	Level_3	Deny Both	Every 8 hours	Enabled	

+ Add

Save

Ahora forzamos un update en Firewall/pfBlockerNG/Update y comprobamos que todas nuestras listas devuelven un 200 OK y que el proceso finaliza correctamente, si alguna lista fallara revisar la url de dicha lista o si ha sido discontinuada, este proceso se debería revisar por lo menos una vez al mes para saber que no tenemos listas discontinuadas

Firewall / pfBlockerNG / Update

General IP DNSBL Update Reports Feeds Logs Sync

### Update Settings

Links Firewall Aliases Firewall Rules Firewall Logs

Status NEXT Scheduled CRON Event will run at 17:00 with 00:09:32 time remaining.  
Refresh to update current status and time remaining.

Force Options **\*\* AVOID \*\*** Running these "Force" options - when CRON is expected to RUN! [i](#)

Select 'Force' option ☒ Update ☐ Cron ☐ Reload

[Run](#) [View](#)

### Log

Running Force Update Task

```
UPDATE PROCESS START [ v3.2.0_3 ] [ 03/22/23 16:50:28 ]

===[ DNSBL Process ]=====

===[ DNSBL Virtual IP and/or Ports are not defined. Exiting ]=====

Clearing all DNSBL Feeds.
Stopping Unbound Resolver.
Unbound stopped in 2 sec.
Starting Unbound Resolver... completed [ 03/22/23 16:50:30 ]
DNSBL update [ 0 ] PASSED ... completed
-----

===[ GeoIP Process ]=====
```

Para comprobar que está funcionando en este laboratorio basta con activar las reglas Level-1 intentar entrar al firewall por la Wan donde seréis bloqueados, y en Firewall/pfBlockerNG/Alerts en Deny veréis lo siguiente.

Unified Alerts IP Block Stats IP Permit Stats IP Match Stats DNSBL Block Stats

### Alert Settings

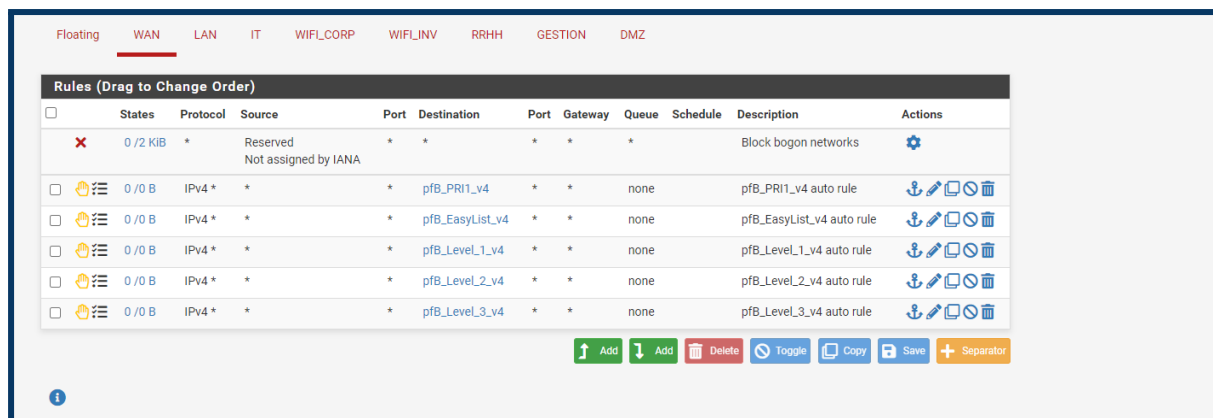
### Alert Filter

### Block- Last 25 Alert Entries

Date	IF	Rule	Proto	Source	Destination	GeoIP	Feed
Mar 24 04:00:41 [3]	WAN	pfB_Level1_v4 (1770009923)	UDP	192.168.0.1:1900 Unknown	<a href="#">i</a> 239.255.255.250:1900 Unknown	<a href="#">Q</a> Unk	Unknown Not listed! Unknown Not listed!
Mar 24 04:00:32	WAN	pfB_Level1_v4 (1770009923)	UDP	192.168.0.10:33423 Unknown	<a href="#">i</a> 224.0.0.251:5353 Unknown	<a href="#">Q</a> Unk	firehol_v4 Not listed! 224.0.0.0/3 Not listed!
Mar 24 04:00:31 [9]	WAN	pfB_Level1_v4 (1770009923)	UDP	192.168.0.1:1901 Unknown	<a href="#">i</a> 239.255.255.250:1900 Unknown	<a href="#">Q</a> Unk	Unknown Not listed! Unknown Not listed!
Mar 24 04:00:24	WAN	pfB_Level1_v4 (1770009923)	IGMP	192.168.0.13:dataLength=16 Unknown	<a href="#">i</a> 224.0.0.22: Unknown	<a href="#">Q</a> Unk	firehol_v4 Not listed! 224.0.0.0/3 Not listed!

Como podemos comprobar está trabajando perfectamente bloqueando nuestra ip en función de la lista firehol de Level1. También observareis en Firewall/Rules las reglas que ha añadido pfBlockerNG en función de nuestras categorías.





## Suricata

### Historia:

Suricata fue creado en 2008 por la Open Information Security Foundation (OISF) como un proyecto de software de seguridad de red de código abierto y gratuito. La motivación detrás de su creación fue mejorar la detección de amenazas de seguridad en redes de alta velocidad y mejorar la eficiencia de los sistemas de detección y prevención de intrusiones existentes.

### Motivación:

La motivación detrás de la creación de Suricata fue la necesidad de un sistema de detección y prevención de intrusiones de código abierto y gratuito que pudiera manejar el alto volumen de tráfico de red que se encuentra en las redes modernas. Los sistemas de detección de intrusiones existentes en ese momento no podían manejar estas cargas de tráfico de alta velocidad y no tenían la capacidad de detectar amenazas de seguridad modernas, como el malware avanzado.

### Funcionalidades:

Suricata es una herramienta de seguridad de red que proporciona una amplia gama de funcionalidades, entre ellas:

- **Detección y prevención de intrusiones:** Suricata es capaz de detectar una amplia gama de amenazas de seguridad, incluyendo intrusos en la red, malware y otros tipos de actividades maliciosas. También puede prevenir intrusiones bloqueando el tráfico malicioso.
- **Análisis de tráfico:** Suricata puede inspeccionar el tráfico de red en tiempo real y analizarlo para identificar patrones de comportamiento sospechosos.
- **Motor de detección basado en firmas:** Suricata utiliza un motor de detección basado en firmas para identificar amenazas de seguridad conocidas.
- **Análisis de protocolos de red:** Suricata puede analizar una amplia variedad de protocolos de red para detectar posibles amenazas de seguridad.
- **Soporte de múltiples plataformas:** Suricata es compatible con una amplia gama de plataformas, incluyendo Linux, Windows y macOS.

- Integración con otros sistemas de seguridad: Suricata puede integrarse con otros sistemas de seguridad de red para proporcionar una protección completa de la red.

#### Alternativas:

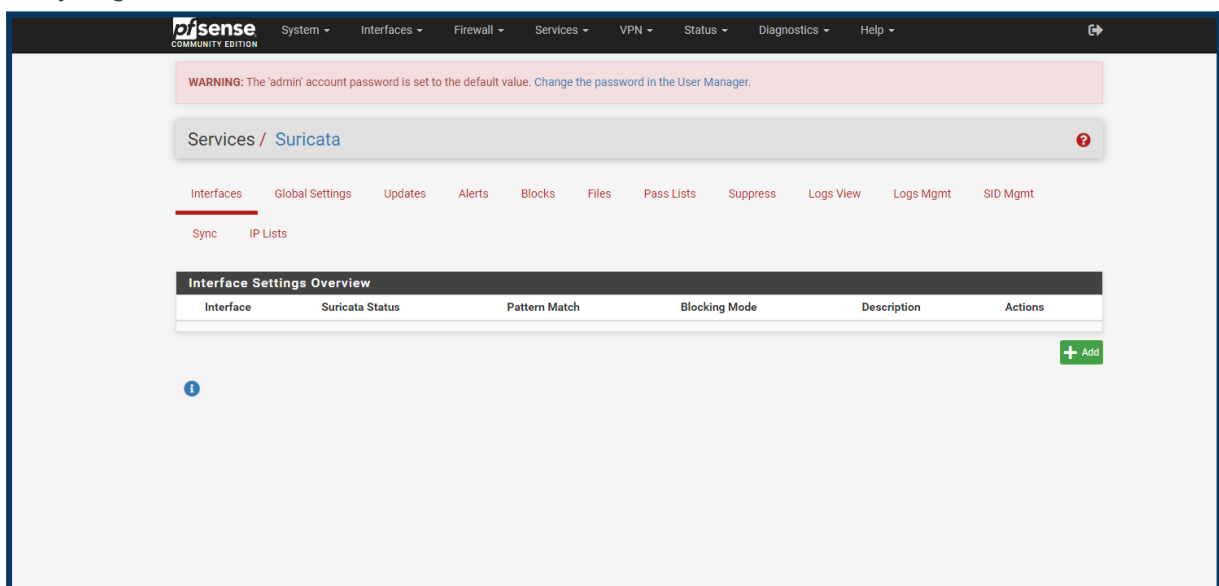
Existen varias alternativas a Suricata en el mercado, como Snort, Bro, Zeek y Security Onion. Estos sistemas de detección y prevención de intrusiones también son de código abierto y gratuitos, y ofrecen funcionalidades similares a las de Suricata.

#### Principales características:

Las principales características de Suricata incluyen:

- Código abierto y gratuito
- Detección y prevención de intrusiones
- Análisis de tráfico en tiempo real
- Motor de detección basado en firmas
- Análisis de protocolos de red
- Soporte de múltiples plataformas
- Integración con otros sistemas de seguridad de red
- Posibilidad de personalización y extensibilidad mediante el uso de reglas personalizadas y complementos.

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 menú downloads para ver la última versión en este caso snortrules-snapshot-29160.tar.gz (Importante no poner la versión 3 no es compatible) además necesitamos un Oinkcode que podéis encontrar en vuestro perfil de snort.org tras suscribiros.

Oinkcode

747bf0a4b0e69625845251ce80f7473a2788ad2a

Regenerate

Please Choose The Type Of Rules You Wish To Download

Install ETOpen Emerging Threats rules

☒ ETOpen is a free open source set of Suricata rules whose coverage is more limited than ETPro.

Use a custom URL for ETOpen downloads

Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETOpen rules.

Install ETPro Emerging Threats rules

☐ ETPro for Suricata offers daily updates and extensive coverage of current malware threats.

Use a custom URL for ETPro rule downloads

The ETPro rules contain all of the ETOpen rules, so the ETOpen rules are not required and are disabled when the ETPro rules are selected. [Sign Up for an ETPro Account](#). Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETPro rules.

Install Snort rules

☒ Snort free Registered User or paid Subscriber rules

Sign Up for a free Registered User Rules Account

Sign Up for paid Snort Subscriber Rule Set (by Talos)

Use a custom URL for Snort rule downloads

Enabling the custom URL option will force the use of a custom user-supplied URL when downloading Snort Subscriber rules.

Snort Rules Filename

Enter the rules tarball filename (filename only, do not include the URL.)  
Example: snortrules-snapshot-29151.tar.gz  
DO NOT specify a Snort3 rules file! Snort3 rules are incompatible with Suricata and will break your installation!

Snort Oinkmaster Code

Obtain a snort.org Oinkmaster code and paste it here.

Install Snort GPLv2 Community rules

☐ The Snort Community Ruleset is a GPLv2 Talos-certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions.

Use a custom URL for Snort GPLv2 rule downloads

This ruleset is updated daily and is a subset of the subscriber ruleset. If you are a Snort Subscriber Rules customer (paid subscriber), the community ruleset is already built into your download of the Snort Subscriber rules, and there is no benefit in adding this rule set separately.

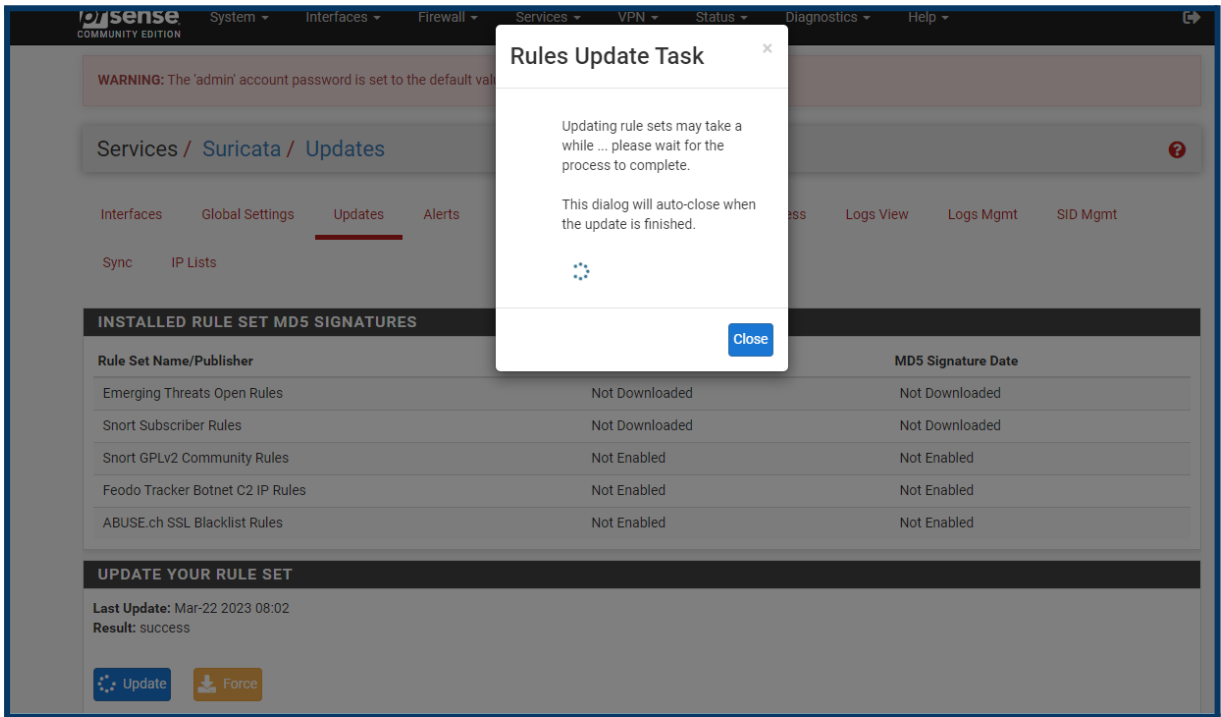
Install Feodo Tracker Botnet C2 IP rules

☐ The Feodo Botnet C2 IP Ruleset contains Dridex and Emotet/Heodo botnet command and control servers (C&Cs) tracked by Feodo Tracker.

Install ABUSE.ch SSL Blacklist rules

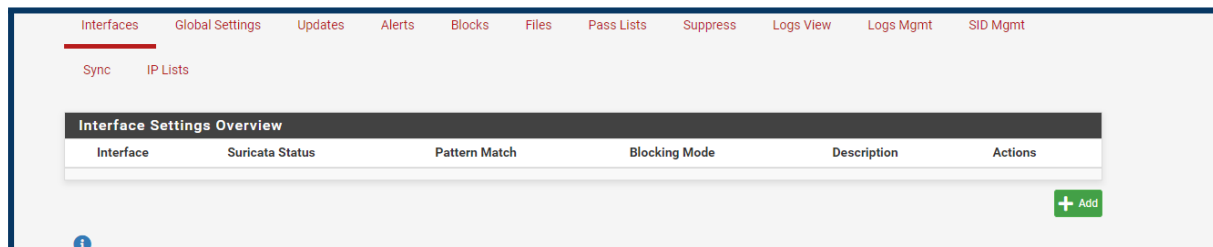
☐ The ABUSE.ch SSL Blacklist Ruleset contains the SSL cert fingerprints of all SSL certs blacklisted by ABUSE.ch.

Salvamos y nos vamos a Services/Suricata/Updates y hacemos click en updates para ver si todo está correcto quedando de la siguiente manera.

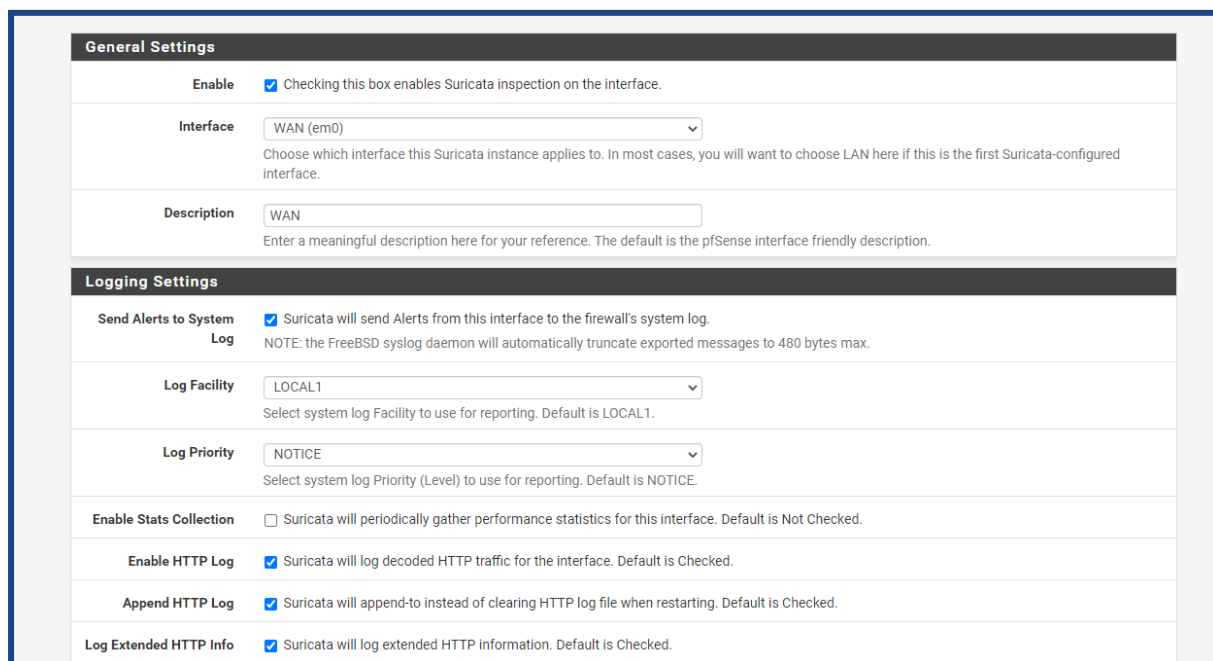


INSTALLED RULE SET MD5 SIGNATURES		
Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Emerging Threats Open Rules	a03cc561b9a6d42058cb3f0477d0587d	Thursday, 23-Mar-23 17:27:27 UTC
Snort Subscriber Rules	742204d73f86c3140d3b26d3d0c5218d	Thursday, 23-Mar-23 17:27:29 UTC
Snort GPLv2 Community Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled
ABUSE.ch SSL Blacklist Rules	Not Enabled	Not Enabled

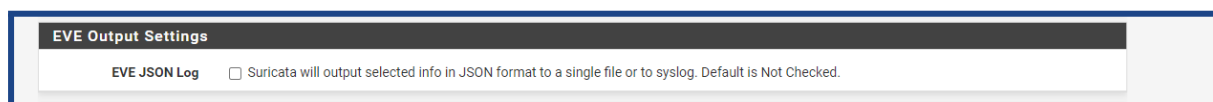
En Alerts nos mostrará las alertas que se generan y el porqué. En Blocks veremos las ips bloqueadas. Pass Lists y Suppress será explicado más adelante. La parte de Logs Mgmt echarle un vistazo y que cada uno lo configure a su gusto. En SID mgmt lo dejaremos desactivado ya que vamos a utilizar reglas de snort En IP Lists podemos utilizar las listas de IQRisk bajo suscripción o crear/subir las nuestras, no utilizaremos este apartado 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.



Una opción muy interesante para los logs si dispones de ELK(Elasticsearch Logstash y Kibana) es la opción EVE Output Settings grabándolos en json.



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.

**Alert and Block Settings**

**Block Offenders** ☒ Checking this option will automatically block hosts that generate a Suricata alert.

**IPS Mode** Legacy Mode  
Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Suricata inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.  
Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Suricata can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers include: bnxt, cc, cxgbe, cxl, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

**Kill States** ☒ Checking this option will kill firewall states for the blocked IP. Default is Checked.

**Which IP to Block** BOTH  
Select which IP extracted from the packet you wish to block. Choosing BOTH is suggested, and it is the default value.

**Block On DROP Only** ☐ Checking this option will insert blocks only when rule signatures having the DROP action are triggered. When not checked, any rule action (ALERT or DROP) will generate a block of the offending host. Default is Not Checked.

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 crear 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.

**Networks Suricata Should Inspect and Protect**

**Home Net** default [View List](#)  
Choose the Home Net you want this interface to use.  
Default Home Net adds only local networks, WAN IPs, Gateways, VPNs and VIPs.  
Create an Alias to hold a list of friendly IPs that the firewall cannot see or to customize the default Home Net.

**External Net** default [View List](#)  
Choose the External Net you want this interface to use.  
External Net is networks that are not Home Net. Most users should leave this setting at default.  
Create a Pass List and add an Alias to it, and then assign the Pass List here for custom External Net settings.

**Pass List** default [View List](#)  
Choose the Pass List you want this interface to use. Addresses in a Pass List are never blocked. Select "none" to prevent use of a Pass List.  
The default Pass List adds Gateways, DNS servers, locally-attached networks, the WAN IP, VPNs and VIPs. Create a Pass List with an alias to customize whitelisted IP addresses. This option will only be used when block offenders is on. Choosing "none" will disable Pass List generation.

Pasemos a Wan Categories donde podremos seleccionar qué categorías queremos activar de todas las que nos hemos bajado anteriormente de snort siempre y cuando NO activemos la opción Use IPS Policy ya que sería automático en función del paquete snort. Seleccionamos todas ellas para empezar en Select All y salvamos, luego cada cual puede limarlas, aunque lo suyo es afinar utilizando la Suppress List o en el siguiente apartado que veremos.

WAN Settings

WAN Categories

WAN Rules

WAN Flow/Stream

WAN App Parsers

WAN Variables

WAN IP Rep

Automatic flowbit resolution

Resolve Flowbits

☒ Auto-enable rules required for checked flowbits

Default is Checked. Suricata will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

View rules

View

Click to view auto-enabled rules required to satisfy flowbit dependencies

Note: Auto-enabled rules generating unwanted alerts should have their GID:SID added to the Suppression List for the interface.

Snort IPS Policy selection

Use IPS Policy

☐ Use rules from one of three pre-defined Snort IPS policies

Note: You must be using the Snort rules to use this option. Selecting this option disables manual selection of Snort rules categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort rules set.

Select the rulesets (Categories) Suricata will load at startup

- Category is auto-enabled by SID Mgmt conf files

- Category is auto-disabled by SID Mgmt conf files

Select All

Unselect All

Save

Enabled		Ruleset:			
Enabled	Ruleset: Default Rules	Enabled	Ruleset: ET Open Rules	Enabled	Ruleset: Snort Text Rules
<input checked="" type="checkbox"/>	app-layer-events.rules	<input checked="" type="checkbox"/>	emerging-3coresec.rules	<input checked="" type="checkbox"/>	snort_app-detect.rules
<input checked="" type="checkbox"/>	decoder-events.rules	<input checked="" type="checkbox"/>	emerging-activev.rules	<input checked="" type="checkbox"/>	snort_attack-responses.rules
<input checked="" type="checkbox"/>	dhcp-events.rules	<input checked="" type="checkbox"/>	emerging-adware_pup.rules	<input checked="" type="checkbox"/>	snort_backdoor.rules
<input checked="" type="checkbox"/>	dnp3-events.rules	<input checked="" type="checkbox"/>	emerging-attack_response.rules	<input checked="" type="checkbox"/>	snort_bad-traffic.rules
<input checked="" type="checkbox"/>	dns-events.rules	<input checked="" type="checkbox"/>	emerging-botcc.portgrouped.rules	<input checked="" type="checkbox"/>	snort_blacklist.rules
<input checked="" type="checkbox"/>	files.rules	<input checked="" type="checkbox"/>	emerging-botcc.rules	<input checked="" type="checkbox"/>	snort_botnet-cnc.rules
<input checked="" type="checkbox"/>	http-events.rules	<input checked="" type="checkbox"/>	emerging-chat.rules	<input checked="" type="checkbox"/>	snort_browser-chrome.rules
<input checked="" type="checkbox"/>	http2-events.rules	<input checked="" type="checkbox"/>	emerging-ciarmy.rules	<input checked="" type="checkbox"/>	snort_browser-firefox.rules
<input checked="" type="checkbox"/>	ipsec-events.rules	<input checked="" type="checkbox"/>	emerging-coinminer.rules	<input checked="" type="checkbox"/>	snort_browser-ie.rules
<input checked="" type="checkbox"/>	kerberos-events.rules	<input checked="" type="checkbox"/>	emerging-compromised.rules	<input checked="" type="checkbox"/>	snort_browser-other.rules
<input checked="" type="checkbox"/>	modbus-events.rules	<input checked="" type="checkbox"/>	emerging-current_events.rules	<input checked="" type="checkbox"/>	snort_browser-plugins.rules
<input checked="" type="checkbox"/>	mqtt-events.rules	<input checked="" type="checkbox"/>	emerging-deleted.rules	<input checked="" type="checkbox"/>	snort_browser-webkit.rules
<input checked="" type="checkbox"/>	nfs-events.rules	<input checked="" type="checkbox"/>	emerging-dns.rules	<input checked="" type="checkbox"/>	snort_chat.rules
<input checked="" type="checkbox"/>	ntp-events.rules	<input checked="" type="checkbox"/>	emerging-dos.rules	<input checked="" type="checkbox"/>	snort_content-replace.rules
<input checked="" type="checkbox"/>	smb-events.rules	<input checked="" type="checkbox"/>	emerging-drop.rules	<input checked="" type="checkbox"/>	snort_ddos.rules
<input checked="" type="checkbox"/>	smtp-events.rules	<input checked="" type="checkbox"/>	emerging-dshield.rules	<input checked="" type="checkbox"/>	snort_deleted.rules
<input checked="" type="checkbox"/>	ssh-events.rules	<input checked="" type="checkbox"/>	emerging-exploit.rules	<input checked="" type="checkbox"/>	snort_dns.rules
<input checked="" type="checkbox"/>	stream-events.rules	<input checked="" type="checkbox"/>	emerging-exploit_kit.rules	<input checked="" type="checkbox"/>	snort_dos.rules
<input checked="" type="checkbox"/>	tls-events.rules	<input checked="" type="checkbox"/>	emerging-ftp.rules	<input checked="" type="checkbox"/>	snort_experimental.rules
		<input checked="" type="checkbox"/>	emerging-games.rules	<input checked="" type="checkbox"/>	snort_exploit-kit.rules
		<input checked="" type="checkbox"/>	emerging-hunting.rules	<input checked="" type="checkbox"/>	snort_exploit.rules
		<input checked="" type="checkbox"/>	emerging-icmp.rules	<input checked="" type="checkbox"/>	snort_file-executable.rules
		<input checked="" type="checkbox"/>	emerging-icmp_info.rules	<input checked="" type="checkbox"/>	snort_file-flash.rules

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.

WAN Settings   WAN Categories   **WAN Rules**   WAN Flow/Stream   WAN App Parsers   WAN Variables   WAN IP Rep

**Available Rule Categories**

Category:  View All  
 Select the rule category to view and manage.

**Rule Signature ID (SID) Enable/Disable Overrides**

SID Actions: Apply Reset All Reset Current Disable All Enable All  
 When finished, click APPLY to save and send any SID state/action changes made on this tab to Suricata.

**Rules View Filter** +

**Rule Signature ID (SID) Enable/Disable Overrides**

**Legend:** ✔ Default Enabled ✔ Enabled by user ✔ Auto-enabled by SID Mgmt ⚡ Action/content modified by SID Mgmt ⚠ Rule action is alert ⚠ Rule contains noalert option  
❌ Default Disabled ❌ Disabled by user ❌ Auto-disabled by SID Mgmt 🔴 Rule action is drop

State	Action	GID	SID	Proto	Source	SPort	Destination	DPort	Message
✔	⚡	1	2260000	ip	any	any	any	any	SURICATA Applayer Mismatch protocol both directions
✔	⚡	1	2260001	ip	any	any	any	any	SURICATA Applayer Wrong direction first Data
✔	⚡	1	2260002	ip	any	any	any	any	SURICATA Applayer Detect protocol only one direction
✔	⚡	1	2260003	ip	any	any	any	any	SURICATA Applayer Protocol detection skipped
✔	⚡	1	2260004	tcp	any	any	any	any	SURICATA Applayer No TLS after STARTTLS
✔	⚡	1	2260005	tcp	any	any	any	any	SURICATA Applayer Unexpected protocol

**Category Rules Summary**

Total Rules: 6   Default Enabled: 6   Default Disabled: 0   User Enabled: 0   User Disabled: 0   Auto-Managed: 0

El resto de opciones consultar la documentación porque también son muchas opciones salvo Wan Barnyard que es un simple intérprete 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.

Interfaces   Global Settings   Updates   Alerts   Blocks   Files   Pass Lists   Suppress   Logs View   Logs Mgmt   SID Mgmt

Sync   IP Lists

**Interface Settings Overview**

Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> WAN (em0)	✔ <span>⚡</span>	AUTO	LEGACY MODE	WAN	<span>✎</span> <span>🔄</span> <span>🗑️</span>

+ Add 🗑️ Delete

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



```
(kali㉿kali)-[~]
$ nmap -Pn 192.168.0.12
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-24 04:01 WET
Nmap scan report for 192.168.0.12
Host is up.
All 1000 scanned ports on 192.168.0.12 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 214.66 seconds

(kali㉿kali)-[~]
$
```

Y podemos ver los logs de suricata como aparece el escaneo realizado.

Logs Browser Selections

Instance to View

(WAN) WAN

Choose which instance logs you want to view.

Log File to View

alerts.log

Choose which log you want to view..

Status/Result

File successfully loaded.

Log File Path: /var/log/suricata/suricata\_em02354/alerts.log

Refresh

Log Contents

[1:2200075:2] SURICATA UDPv4 invalid checksum [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 192.168.0.12:49581 -> 212.166.132.112:53

[1:2200075:2] SURICATA UDPv4 invalid checksum [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 192.168.0.12:7489 -> 212.166.132.112:53

[1:2200075:2] SURICATA UDPv4 invalid checksum [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 192.168.0.12:40274 -> 212.166.132.112:53

[1:2200075:2] SURICATA UDPv4 invalid checksum [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 192.168.0.12:123 -> 195.46.37.22:123

[1:2010937:3] ET SCAN Suspicious inbound to MySQL port 3306 [\*\*] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.13:48512 -> 192.168.0.12:3306

[1:2010937:3] ET SCAN Suspicious inbound to MySQL port 3306 [\*\*] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.13:48522 -> 192.168.0.12:3306

[1:2002911:6] ET SCAN Potential VNC Scan 5900-5920 [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.13:47676 -> 192.168.0.12:5901

[1:2010939:3] ET SCAN Suspicious inbound to PostgreSQL port 5432 [\*\*] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.13:55472 -> 192.168.0.12:543

[1:2010939:3] ET SCAN Suspicious inbound to PostgreSQL port 5432 [\*\*] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.13:55484 -> 192.168.0.12:543

[1:2010936:3] ET SCAN Suspicious inbound to Oracle SQL port 1521 [\*\*] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.13:34398 -> 192.168.0.12:152

[1:2010936:3] ET SCAN Suspicious inbound to Oracle SQL port 1521 [\*\*] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.13:34406 -> 192.168.0.12:152

[1:2200075:2] SURICATA UDPv4 invalid checksum [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 192.168.0.12:123 -> 54.39.23.64:123

[1:2002910:6] ET SCAN Potential VNC Scan 5800-5820 [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.13:40552 -> 192.168.0.12:5811

[1:2010935:3] ET SCAN Suspicious inbound to MSSQL port 1433 [\*\*] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.13:39758 -> 192.168.0.12:1433

[1:2010935:3] ET SCAN Suspicious inbound to MSSQL port 1433 [\*\*] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.13:58578 -> 192.168.0.12:1433

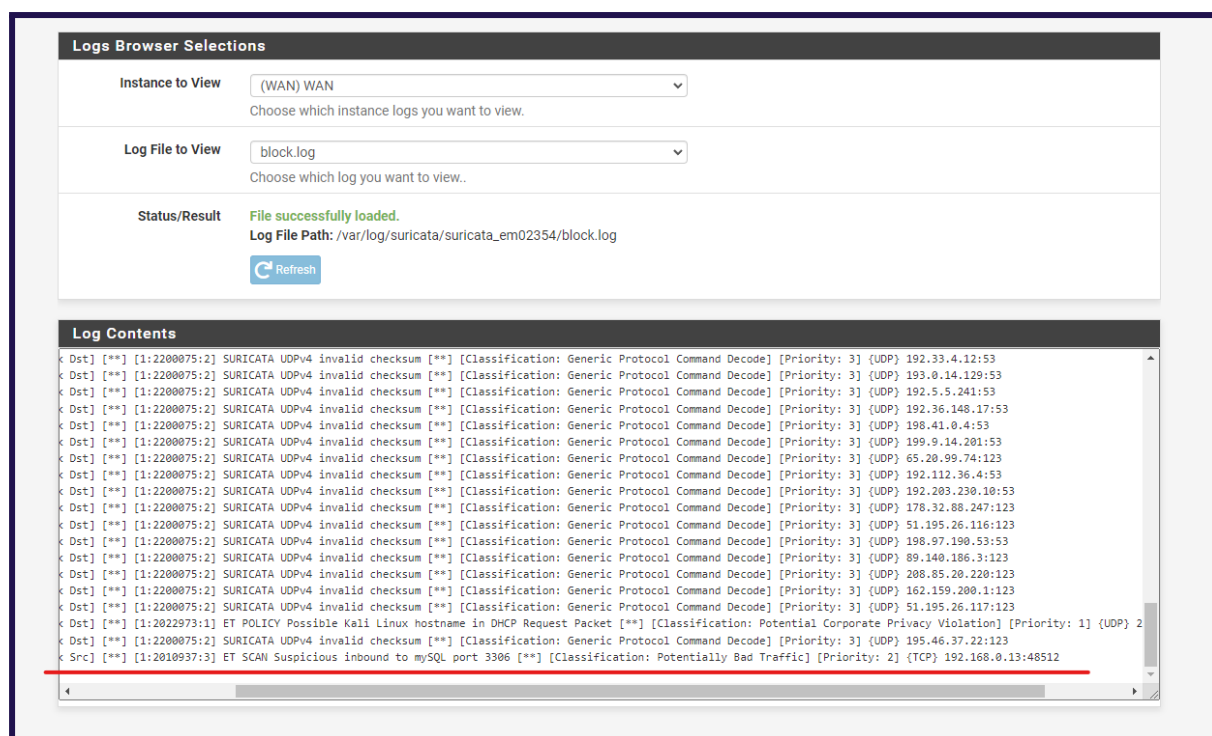
[1:2200075:2] SURICATA UDPv4 invalid checksum [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 192.168.0.12:123 -> 135.125.165.135:123

[1:2200075:2] SURICATA UDPv4 invalid checksum [\*\*] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 192.168.0.12:123 -> 185.209.85.222:123

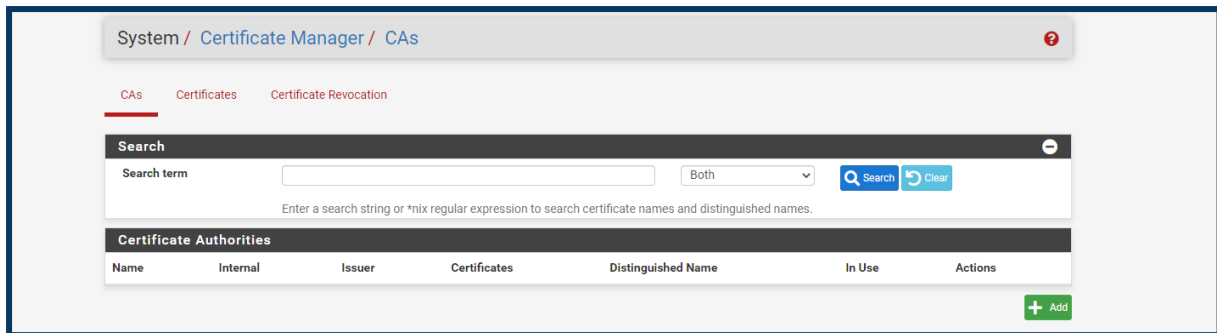
[1:2002911:6] ET SCAN Potential VNC Scan 5900-5920 [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.13:59062 -> 192.168.0.12:5910

[1:2002910:6] ET SCAN Potential VNC Scan 5800-5820 [\*\*] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.13:55328 -> 192.168.0.12:5815

Y en el log de ips bloqueadas aparecerá nuestra dirección ip



Squid + SquidGuard + Clam-AV + 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. Hay varios tipos de proxy en función de lo que necesitamos, pero no entraremos en detalle, solo aclararemos qué es eso de proxy transparente, simplemente que la máquina que pasa por el proxy no lo sabe, es decir, es transparente porque no lo ve ni necesita configuración específica, mientras que un proxy a secas necesitas configurar la máquina para que pase por el proxy. 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.

Historia:

Las Entidades Certificadoras (CA, por sus siglas en inglés) surgieron en la década de 1990 como respuesta al creciente uso de la criptografía en internet y la necesidad de garantizar la autenticidad y la integridad de la información que se transmite. La primera CA fue creada por Netscape Communications en 1994, y desde entonces han surgido numerosas empresas y organizaciones que ofrecen servicios de certificación.

Motivación:

La motivación detrás de la creación de las CAs fue proporcionar una forma segura y confiable de verificar la identidad de los usuarios y los sitios web en internet. Las CAs emiten certificados digitales que garantizan la identidad del propietario del sitio web, lo que ayuda a prevenir el fraude y el robo de identidad en línea. También permiten el cifrado de la información que se transmite entre el sitio web y el usuario, lo que aumenta la privacidad y la seguridad.

Funcionalidades:

Las principales funcionalidades de las CAs son:

- Emisión de certificados digitales: Las CAs emiten certificados digitales que garantizan la identidad del propietario del sitio web. Estos certificados se utilizan para cifrar la información que se transmite entre el sitio web y el usuario, lo que aumenta la privacidad y la seguridad.

- Verificación de identidad: Antes de emitir un certificado, las CAs verifican la identidad del propietario del sitio web mediante la verificación de documentos legales y otras medidas de seguridad.
- Revocación de certificados: Si se descubre que un certificado ha sido comprometido o que el propietario del sitio web ha cambiado, las CAs pueden revocar el certificado para garantizar la seguridad del sitio web.
- Renovación de certificados: Los certificados tienen una fecha de caducidad, por lo que las CAs deben renovarlos periódicamente para garantizar la continuidad de la seguridad del sitio web.

#### Alternativas:

Existen varias alternativas a las CAs en el mercado, como Let's Encrypt, Comodo, Symantec, GlobalSign, entre otras. Cada una de ellas ofrece diferentes servicios de certificación y funcionalidades para adaptarse a las necesidades de los usuarios.

#### Principales características:

Las principales características de las CAs son:

- Seguridad y confiabilidad: Las CAs ofrecen una forma segura y confiable de verificar la identidad de los usuarios y los sitios web en internet.
- Cifrado de la información: Los certificados emitidos por las CAs se utilizan para cifrar la información que se transmite entre el sitio web y el usuario, lo que aumenta la privacidad y la seguridad.
- Verificación de identidad: Las CAs verifican la identidad del propietario del sitio web mediante la verificación de documentos legales y otras medidas de seguridad.
- Revocación y renovación de certificados: Las CAs pueden revocar y renovar los certificados para garantizar la seguridad del sitio web en caso de compromiso o cambio de propietario.

Create / Edit CA	
<b>Descriptive name</b>	<input type="text" value="CA"/> <p>The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, &gt;, &lt;, &amp;, /, \, *, '.</p>
<b>Method</b>	<input type="text" value="Create an internal Certificate Authority"/>
<b>Trust Store</b>	<input type="checkbox"/> Add this Certificate Authority to the Operating System Trust Store When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.
<b>Randomize Serial</b>	<input type="checkbox"/> Use random serial numbers when signing certificates When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Internal Certificate Authority

Key type

RSA

2048

The length to use when generating a new RSA key, in bits.  
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm

sha256

The digest method used when the CA is signed.  
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

Lifetime (days)

3650

Common Name

internal-ca

The following certificate authority subject components are optional and may be left blank.

Country Code

ES

State or Province

tenerife

City

la laguna

Organization

cesar manrique

Organizational Unit

ciberseguridad

Save

Search

Search term

Both

Search

Clear

Enter a search string or \*nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA	✓	self-signed	0	ST=tenerife, OU=ciberseguridad, O=cesar manrique, L=la laguna, CN=internal-ca, C=ES Valid From: Thu, 23 Mar 2023 17:49:39 +0000 Valid Until: Sun, 20 Mar 2033 17:49:39 +0000		<a href="#">Info</a> <a href="#">Edit</a> <a href="#">Refresh</a> <a href="#">Delete</a>

Add

## Squid

### Historia:

Squid es un software libre de servidor proxy web y caché de páginas web que fue lanzado por primera vez en 1996. El proyecto fue iniciado por Duane Wessels como una alternativa al servidor proxy CERN. Desde entonces, Squid se ha convertido en uno de los servidores proxy más populares y ampliamente utilizados en el mundo.

### Motivación:

La motivación detrás de la creación de Squid fue mejorar el rendimiento y la velocidad de acceso a las páginas web. Squid utiliza técnicas de caché para almacenar copias de las páginas web solicitadas por los usuarios y servirlos desde la caché en lugar de solicitarlos al servidor web original. Esto reduce la latencia y el tiempo de carga de las páginas web, lo que mejora la experiencia del usuario.

### Funcionalidades:

Las principales funcionalidades de Squid son:

- Caché de páginas web: Squid almacena copias de las páginas web solicitadas por los usuarios en su caché para mejorar el rendimiento y reducir la latencia.
- Servicio proxy: Squid se utiliza como servidor proxy para interceptar y filtrar el tráfico web.
- Autenticación de usuario: Squid ofrece diversas opciones de autenticación de usuario, como la autenticación básica y la autenticación basada en certificados SSL.
- Control de acceso: Squid permite a los administradores de red establecer políticas de control de acceso para restringir el acceso a ciertos sitios web o para bloquear ciertos tipos de contenido.
- Registro de tráfico: Squid registra el tráfico web para que los administradores de red puedan monitorear y analizar el uso de la red.

### Alternativas:

Existen varias alternativas a Squid en el mercado, como Nginx, Apache Traffic Server, HAProxy, entre otros. Cada una de ellas ofrece diferentes servicios de servidor proxy y funcionalidades para adaptarse a las necesidades de los usuarios.

### Principales características:

Las principales características de Squid son:

- Rendimiento y velocidad: Squid mejora el rendimiento y la velocidad de acceso a las páginas web utilizando técnicas de caché.
- Seguridad: Squid ofrece opciones de autenticación de usuario y control de acceso para garantizar la seguridad de la red.
- Flexibilidad: Squid se puede configurar para adaptarse a las necesidades específicas de los usuarios y las redes.

- Escalabilidad: Squid es escalable y puede manejar grandes volúmenes de tráfico web.
- Comunidad de usuarios: Squid tiene una gran comunidad de usuarios y desarrolladores que proporcionan soporte y actualizaciones regulares.

Ahora pasamos a configurar Squid desde Services/ Squid Proxy Server/ Local Cache. En la primera sección nos encontramos los ajustes generales.

The screenshot shows the 'Squid General Settings' page. At the top, there's a breadcrumb trail: 'Package / Proxy Server: General Settings / General'. Below this is a horizontal menu with tabs: 'General', 'Remote Cache', 'Local Cache', 'Antivirus', 'ACLs', 'Traffic Mgmt', 'Authentication', 'Users', and 'Real Time'. The 'General' tab is selected and highlighted with a red underline. The main content area is titled 'Squid General Settings' and contains several configuration options:

- Enable Squid Proxy:** A checkbox that is currently unchecked. Below it, a red note states: 'Important: If unchecked, ALL Squid services will be disabled and stopped.'
- Keep Settings/Data:** A checkbox that is checked. Below it, a red note states: 'Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.'
- Listen IP Version:** A dropdown menu set to 'IPv4'. Below it, text says: 'Select the IP version Squid will use to select addresses for accepting client connections.'
- CARP Status VIP:** A dropdown menu set to 'none'. Below it, text says: 'Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP s'. A red note below says: 'Important: Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the se'.
- Proxy Interface(s):** A multi-select dropdown menu. The selected value is '10.10.10.1 (pfB DNSBL - DO NOT EDIT)'. Other visible options are 'WAN', 'LAN', and 'IT'. Below it, text says: 'The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.'
- Outgoing Network Interface:** A dropdown menu set to 'Default (auto)'. Below it, text says: 'The interface the proxy server will use for outgoing connections.'
- Proxy Port:** A text input field containing '3128'. Below it, text says: 'This is the port the proxy server will listen on. Default: 3128'.

La primera es la política donde se decide qué objetos permanecerán en la caché y cual se reemplazará, 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 caché independientemente de su tamaño, para empezar, es muy buena opción. Low-Water Mark in % el índice de advertencia donde empieza a liberar la cache cuando la swap está al 90%, aquí si no se utilizan discos SSD es aconsejable ponerlo al 80% High-Water Mark in % el índice crítico donde libera caché de manera más agresiva, al igual que la anterior si no utilizan SSD poner la marca a 85% Do Not Cache, en cada línea pondríamos ips o dominios que no deben ser cacheados. Enable Offline Mode no lo

utilizaremos. External Cache Managers, si utilizamos Administradores de caché externos. La siguiente sección Hard Disk cache settings.

**Squid Cache General Settings**

**Disable Caching** ☐ Disable caching completely.  
This may be required if Squid is only used as a proxy to audit website access.

**Cache Replacement Policy** Heap LFUDA  
The cache replacement policy decides which objects will remain in cache and which objects are replaced to create space for the new objects. Default heap LFUDA ⓘ

**Low-Water Mark in %** 90  
The low-water mark for AUFS/UFS/diskd cache object eviction by the cache\_replacement\_policy algorithm. ⓘ

**High-Water Mark in %** 95  
The high-water mark for AUFS/UFS/diskd cache object eviction by the cache\_replacement\_policy algorithm. ⓘ

**Do Not Cache**  
  
Enter domain(s) and/or IP address(es) that should never be cached. Put each entry on a separate line.

**Enable Offline Mode** ☐ Enable this option and the proxy server will never try to validate cached objects.  
Offline mode gives access to more cached information than normally allowed (e.g., expired cached versions where the origin server should have been contacted otherwise).

**External Cache Managers**   
Enter the IPs for the external [Cache Managers](#) to be granted access to this proxy. Separate entries by semi-colons (;)

**Squid Hard Disk Cache Settings**

**Hard Disk Cache Size** 2048  
Amount of disk space (in megabytes) to use for cached objects.

**Hard Disk Cache System** ufs  
This specifies the kind of storage system to use. ⓘ

**Clear Disk Cache NOW** Hard Disk Cache is automatically managed by swapstate\_check.php script which is scheduled to run daily via cron. ⓘ  
If you wish to clear cache **immediately**, click this button **once**: Clear Disk Cache NOW

**Level 1 Directories** 16  
Specifies the number of Level 1 directories for the hard disk cache. ⓘ

**Hard Disk Cache Location** /var/squid/cache  
This is the directory where the cache will be stored. Default: /var/squid/cache ⓘ

**Minimum Object Size** 0  
Objects smaller than the size specified (in kilobytes) will not be saved on disk. Default: 0 (meaning there is no minimum)

**Maximum Object Size** 4  
Objects larger than the size specified (in megabytes) will not be saved on disk. Default: 4 (MB) ⓘ

En esta sección definiremos en Hard Disk Cache Size el espacio de disco que utilizaremos para la cache en MB, en este caso 2 GB El tipo de sistema de cache, donde ufs es buena opción y lo dejamos por defecto. Un botón para limpiar la caché manualmente. El siguiente valor es bastante crítico para la velocidad de la caché, aquí especificaremos cuantos directorios tiene el Level-1, cada directorio tiene 256 subdirectorios de level 2 si ponemos 16 serían un total de 4096 directorios, un valor que se considera bueno para 2048 MB de



tamaño de caché. La siguiente opción es el directorio donde se almacenará, seguido del tamaño mínimo y máximo de los objetos. 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 swappear 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.

Squid General Settings	
Enable Squid Proxy	<input checked="" type="checkbox"/> Check to enable the Squid proxy. <b>Important:</b> If unchecked, ALL Squid services will be disabled and stopped.
Keep Settings/Data	<input checked="" type="checkbox"/> If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls. <b>Important:</b> If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.
Listen IP Version	IPv4 Select the IP version Squid will use to select addresses for accepting client connections.
CARP Status VIP	none Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status. <b>Important:</b> Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the settings synchronization.
Proxy Interface(s)	RRHH GESTION DMZ loopback The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.
Outgoing Network Interface	WAN The interface the proxy server will use for outgoing connections.
Proxy Port	3128 This is the port the proxy server will listen on. Default: 3128
ICP Port	 This is the port the proxy server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.
Allow Users on Interface	<input checked="" type="checkbox"/> If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy. There will be no need to add the interface's subnet to the list of allowed subnets.

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. En qué versión IP escuchará, seleccionamos IPV4. Proxy interface, en qué interface activaremos el servicio, en nuestro caso solo tenemos una LAN interna la seleccionamos y muy importante la de loopback porque sin ella no podremos activar Lightsquid. El Proxy Port, el puerto por el que escuchará squid y al que debemos conectarnos, por defecto en squid es el 3128 ICP Port, lo dejaremos en blanco, pero si utilizamos por ejemplo HA o caches remotas pondremos un número de puerto. Allow Users on interface, la marcamos para que los usuarios conectados a dicha interfaz puedan utilizar el proxy. Resolve DNS IPV4 First, como indica si tienes problemas para acceder a contenido HTTPS actívalo.

Disable ICMP, para desactivar el ping. Use Alternate DNS Servers for the Proxy Server, es decir, utilizar unos DNS diferentes a los que tenemos puestos en la configuración general del Firewall. La siguiente sección sería Transparent Proxy Settings.

**Transparent Proxy Settings**

**Transparent HTTP Proxy** ☒ Enable transparent mode to forward all requests for destination port 80 to the proxy server.

**Transparent Proxy Interface(s)**   
 WAN  
 LAN  
 IT  
 WIFI\_CORP  
 WIFI\_INV

The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.

**Bypass Proxy for Private Address Destination** ☒ Do not forward traffic to Private Address Space (RFC 1918 and IPv6 ULA) destinations.  
 Destinations in Private Address Space (RFC 1918 and IPv6 ULA) are passed directly through the firewall, not through the proxy server.

**Bypass Proxy for These Source IPs**

Do not forward traffic from these source IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall.  
**Applies only to transparent mode.** Separate entries by semi-colons (;)

**Bypass Proxy for These Destination IPs**

Do not proxy traffic going to these destination IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall.  
**Applies only to transparent mode.** Separate entries by semi-colons (;)

Activaremos el proxy transparente para no tener que configurar los equipos de los clientes. Seleccionamos las redes donde actuará el proxy transparente y marcamos el Bypass para el tráfico entre las redes internas. 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.

**SSL Man In the Middle Filtering**

**HTTPS/SSL Interception** ☒ Enable SSL filtering.

**SSL/MITM Mode**   
 The SSL/MITM mode determines how SSL interception is treated when 'SSL Man In the Middle Filtering' is enabled.  
 Default: Splice Whitelist, Bump Otherwise. [Click Info for details.](#)

**SSL Intercept Interface(s)**   
 IT  
 WIFI\_CORP  
 WIFI\_INV

The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.

**SSL Proxy Port**   
 This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129

**SSL Proxy Compatibility Mode**   
 The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. [Click Info for details.](#)

**DHParams Key Size**   
 DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.

**CA**   
 Select Certificate Authority to use when SSL interception is enabled.

Donde solo nos interesa HTTPS/SSL Interception tenerla activa, el SSL/MITM Mode Splice All ya que vamos a utilizar SquidGuard por lo tanto no necesitaremos una CA, cualquiera de las otras opciones tendrás que crear la CA primero en System/CertManager y después seleccionar en CA la entidad creada y por último seleccionar las interfaces donde estará activo, es posible aunque pone que no es necesaria que aún seleccionando Splice All te diga que necesitas instalar la CA, si es así la instalamos y la seleccionamos. Siguiendo sección logs.


See [sslproxy\\_cert\\_adapt directive documentation](#) and [Mimic original SSL server certificate wiki article](#) for details.

### Logging Settings

**Enable Access Logging** ☒ This will enable the access log.  
**Warning:** Do NOT enable if available disk space is low.

**Log Store Directory**   
 The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs  
**Important:** Do NOT include the trailing / when setting a custom location.

**Rotate Logs**   
 Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

**Log Pages Denied by SquidGuard** ☐ Makes it possible for SquidGuard denied log to be included on Squid logs.  
[Click Info for detailed instructions.](#) 


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

### Headers Handling, Language and Other Customizations


**Visible Hostname**   
 This is the hostname to be displayed in proxy server error messages.

**Administrator's Email**   
 This is the email address displayed in error messages to the users.

**Error Language**   
 Select the language in which the proxy server will display error messages to users.

**X-Forwarded Header Mode**   
 Choose how to handle X-Forwarded-For headers. Default: on 

**Disable VIA Header** ☐ If not set, Squid will include a Via header in requests and replies as required by RFC2616.

**URI Whitespace Characters Handling**   
 Choose how to handle whitespace characters in URL. Default: strip 

**Suppress Squid Version** ☐ Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.

Básicamente nombre que aparecerá ante algún error, la dirección de correo del admin que verán los usuarios, el lenguaje y ajustes sobre las cabeceras que salvo casos especiales tal y como está sería lo correcto para la mayoría de escenarios a no ser que haya páginas que no permitan proxy, en ese caso, ponemos el X-Forwarder en off y marcamos la casilla de Suppress Squid Versión. Pasamos al apartado Antivirus.

ClamAV Anti-Virus Integration Using C-ICAP

Enable AV

☒ Enable Squid antivirus check using ClamAV.

Client Forward Options

Send both client username and IP info (Default)

Select what client info to forward to ClamAV.

Enable Manual Configuration

disabled

Warning: Only enable this if you know what you are doing.
When enabled, the options below no longer have any effect. You must edit the configuration files directly in the 'Advanced Features'. After enabling manual configuration, click the button below **once** to load default configuration files. To disable manual configuration again, select 'disabled' and click 'Save'.

Load Advanced

Redirect URL

When a virus is found then redirect the user to this URL. Example: <http://proxy.example.com/blocked.html>. Leave empty to use the default Squid/pfSense WebGUI URL.

Scan Type

All (default)

What kind of data to scan:  
All: All data  
Web: Web pages, scripts, images and documents  
Applications: Executables, scripts, archives and documents

Exclude Audio/Video Streams

☒ This option disables antivirus scanning of streamed video and audio for the default scan type.

Block PUA

☐ This option enables blocking of Potentially Unwanted Applications.  
See <https://www.clamav.net/documents/potentially-unwanted-applications-pua> for details.

ClamAV Database Update

every 24 hours

Optionally, you can schedule ClamAV definitions updates via cron. Select the desired frequency here.
Important: Set to 'every 1 hour' if you want to use Google Safe Browsing feature. Click the button below **once** to force the update of AV databases immediately. Note: This will take a while. Check freshclam log on the 'Real Time' tab for progress information.

Update AV

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

Qué datos mandamos del cliente a ClamAV.

URL donde redirigir cuando se ha bloqueado por virus muy útil para educar a los usuarios en la navegación.

Si quieres excluir audio y video en Streams de los escaneos, por rendimiento los incluiría.

Cada cuanto queremos actualizar la base de datos de ClamAV y un botón para hacerlo manualmente.

La región desde donde actualizar y por último alternativa de servidores de bases de datos.

Unofficial Signatures

URLhaus

☒ Enables URLhaus active malware distribution sites DB support.  
The signature file only contains active malware distribution sites or such that have been added to URLhaus in past 48 hours. The false positive rate should be very low. See [URLhaus ClamAV signatures](#) for details.

InterServer

☐ Enables InterServer.net malware DB support.  
The signature file contains real time suspected malware list as detected by InterServer's InterShield protection system. See [InterServer Real Time Malware Detection](#) for details.

SecuriteInfo

☐ Enables SecuriteInfo.com malware DB support.  
The signature files contains more than 4.000.000 signatures. At least free registration needed. See [SecuriteInfo signatures info](#) for details.  
Warning: This option consumes significant amount of RAM.

SecuriteInfo Premium

☐ Enables SecuriteInfo.com 0-day malware DB support.  
A valid premium subscription ID required.

SecuriteInfo ID

The unique 128 character identifier from one of the download links.  
Example: [https://www.securiteinfo.com/get/signatures/your\\_unique\\_and\\_very\\_long\\_random\\_string\\_of\\_characters/securiteinfo.hdb](https://www.securiteinfo.com/get/signatures/your_unique_and_very_long_random_string_of_characters/securiteinfo.hdb)

Save

Show Advanced Options

En este apartado podemos utilizar bases de datos de internet que contienen direcciones ips de sitios con malware y virus.  
Pasemos al apartado ACLs, donde el primer apartado es simple de entender.

The screenshot shows the 'Squid Access Control Lists' configuration page. At the top, there is a navigation bar with tabs: General, Remote Cache, Local Cache, Antivirus, ACLs (selected), Traffic Mgmt, Authentication, Users, Real Time, Status, and Sync. Below the navigation bar, the page title is 'Squid Access Control Lists'. The main content area is divided into five sections, each with a text input field and instructions:

- Allowed Subnets:** Enter subnets that are allowed to use the proxy in CIDR format. All the other subnets won't be able to use the proxy. Put each entry on a separate line. When 'Allow Users on Interface' is checked on 'General' tab, there is no need to add the 'Proxy Interface(s)' subnet(s) to this list.
- Unrestricted IPs:** Enter unrestricted IP address(es) / network(s) in CIDR format. Configured entries will NOT be filtered out by the other access control directives set in this page. Put each entry on a separate line.
- Banned Hosts Addresses:** Enter IP address(es) / network(s) in CIDR format. Configured entries will NOT be allowed to use the proxy. Put each entry on a separate line.
- Whitelist:** Destination domains that will be accessible to the users that are allowed to use the proxy. Put each entry on a separate line. You can also use regular expressions.
- Blacklist:** (Empty input field)

En allowed Subnets introducimos las subredes que podrán utilizar el proxy, en nuestro caso como activamos "Allow Users on Interfaces" en el apartado General no necesitamos añadir ninguna.

Unrestricted IPS, añadiremos las redes o ips que no serán filtradas.

Banned Hosts Addresses, las subredes o ips que no tendrán permitido usar el proxy.

Whitelist, la lista blanca de dominios de destino que serán siempre accesibles para los usuarios.

Blacklist, lo contrario las que nunca podrán acceder.

Block User Agente, para bloquear ciertos navegadores.

Block MIME Types, para bloquear tipos de MIME como por ejemplo (application/javascript).

Y por último en este apartado los puertos permitidos.

Siguiente apartado Traffic Mgmt.

Squid Traffic Management Settings	
<b>Maximum Download Size</b>	<input type="text" value="0"/> <p>Limit the maximum total download size to the size specified here (in kilobytes). Set to 0 to disable. Traffic control settings mainly work with universal HTTP, so it may not work without HTTPS interception, if HTTPS is used, it can also be a problem with dynamic content (javascript).</p>
<b>Maximum Upload Size</b>	<input type="text" value="0"/> <p>Limit the maximum total upload size to the size specified here (in kilobytes). Set to 0 to disable.</p>
<b>Overall Bandwidth Throttling</b>	<input type="text" value="0"/> <p>This value specifies the bandwidth throttle for downloads (in kilobytes per second). Users will gradually have their download speed decreased according to this value. Set to 0 to disable.</p>
<b>Per-Host Throttling</b>	<input type="text" value="0"/> <p>This value specifies the download throttling per host. Set to 0 to disable.</p>
<b>Throttle Unrestricted IPs</b>	<input type="checkbox"/> If enabled, even 'Unrestricted IPs' configured on the ACLs tab are subject to throttling.

En esta primera sección el tamaño máximo de descarga y subida que no vamos a utilizar. El Overall Bandwidth disminuirá el ancho de banda de las descargas cuando el uso del ancho de banda llegué al valor especificado. Per-Host Throttling, lo mismo, pero por host, si un host llega a la velocidad indicada su descarga irá disminuyendo la velocidad. Y la última opción si queremos que dentro de estos límites de Throttling incluyamos a los Unrestricted de las ACLs.

Sección Squid Transfer Extensions Settings. No tocamos nada de esta sección.

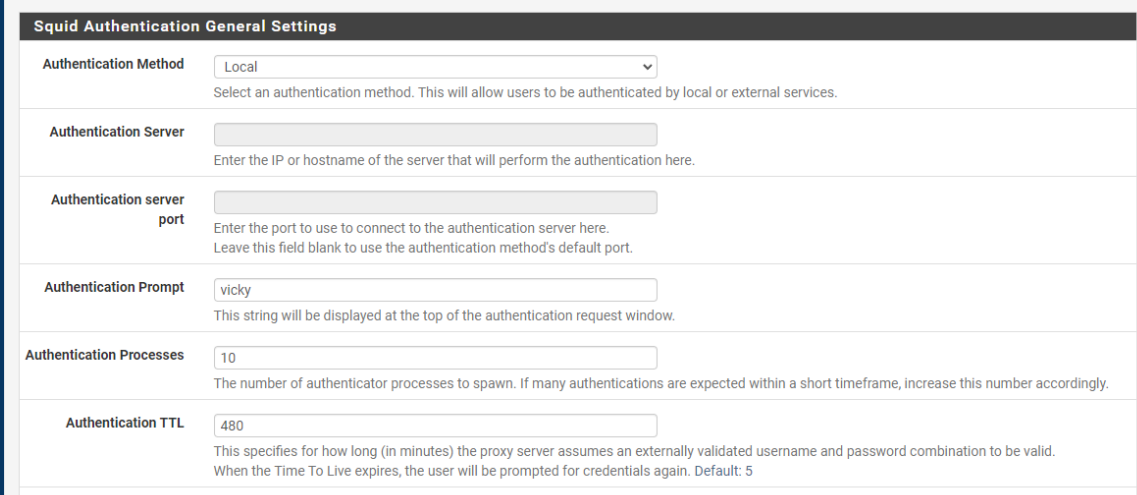
Squid Transfer Extension Settings	
<b>Throttle Only Specific Extensions</b>	<input type="checkbox"/> Leave this checked to be able to choose the extensions that throttling will be applied to. Otherwise, all files will be throttled.
<b>Throttle Binary Files</b>	<input type="checkbox"/> Check this to apply bandwidth throttle to binary files. This includes compressed archives and executables.
<b>Throttle CD/DVD Image Files</b>	<input type="checkbox"/> Check this to apply bandwidth throttle to CD/DVD image files.
<b>Throttle Multimedia Files</b>	<input type="checkbox"/> Check this to apply bandwidth throttle to multimedia files, such as movies or songs.
<b>Throttle Other Extensions</b>	<input type="text"/> <p>Comma-separated list of extensions to apply bandwidth throttle to.</p>

Y por último en este apartado Squid Transfer Abort Settings donde tampoco tocamos nada. Pasemos

Squid Transfer Quick Abort Settings	
<b>Quick Abort Settings</b>	
<b>Finish transfer if less than x KB remaining</b>	<input type="text" value="0"/> <p>If the transfer has less than x KB remaining, it will finish the retrieval.</p>
<b>Abort transfer if more than x KB remaining</b>	<input type="text" value="0"/> <p>If the transfer has more than x KB remaining, it will abort the retrieval.</p>
<b>Finish transfer if more than x % finished</b>	<input type="text" value="0"/> <p>If more than x % of the transfer has completed, it will finish the retrieval.</p>

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.



The screenshot shows the 'Squid Authentication General Settings' form. It includes fields for 'Authentication Method' (set to 'Local'), 'Authentication Server', 'Authentication server port', 'Authentication Prompt' (set to 'vicky'), 'Authentication Processes' (set to '10'), 'Authentication TTL' (set to '480'), and 'Authentication Max User'.

Squid Authentication General Settings	
Authentication Method	Local <small>Select an authentication method. This will allow users to be authenticated by local or external services.</small>
Authentication Server	<input type="text"/> <small>Enter the IP or hostname of the server that will perform the authentication here.</small>
Authentication server port	<input type="text"/> <small>Enter the port to use to connect to the authentication server here. Leave this field blank to use the authentication method's default port.</small>
Authentication Prompt	vicky <small>This string will be displayed at the top of the authentication request window.</small>
Authentication Processes	10 <small>The number of authenticator processes to spawn. If many authentications are expected within a short timeframe, increase this number accordingly.</small>
Authentication TTL	480 <small>This specifies for how long (in minutes) the proxy server assumes an externally validated username and password combination to be valid. When the Time To Live expires, the user will be prompted for credentials again. Default: 5</small>
Authentication Max User	<input type="text"/>

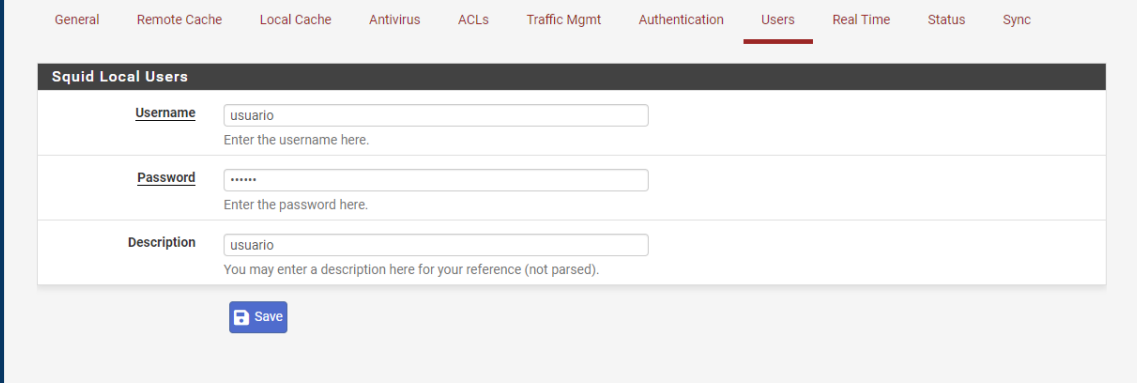
Donde se nos activa 5 opciones, la primera Authentication Prompt donde pondremos lo que verán los usuarios en la ventana que les saltará como por ejemplo “Por favor introduce tu usuario y contraseña”.

El número de procesos para autenticar, si tenemos muchos usuarios y todos entran de golpe aumentarlo porque se quejan en función de vuestro hardware.

El tiempo tras el cual una autenticación TTL será válida, hemos puesto 8 horas.

Si le requerimos autenticación a los Unrestricted IPs que tengamos en las ACLs y si queremos evitar que se tengan que autenticar ciertas ips o subredes.

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



The screenshot shows the 'Squid Local Users' form with fields for 'Username' (set to 'usuario'), 'Password' (masked with dots), and 'Description' (set to 'usuario'). A 'Save' button is at the bottom.

Squid Local Users	
Username	usuario <small>Enter the username here.</small>
Password	..... <small>Enter the password here.</small>
Description	usuario <small>You may enter a description here for your reference (not parsed).</small>
<input type="button" value="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.... SquidGuard

Package / Proxy filter SquidGuard: General settings / General settings

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync

### General Options

**Enable** ☐ Check this option to enable squidGuard.  
**Important:** Please set up at least one category on the 'Target Categories' tab before enabling. See [this link for details](#).  
 The Save button at the bottom of this page must be clicked to save configuration changes.  
 To activate squidGuard configuration changes, **the Apply button must be clicked**.

☒ Apply

SquidGuard service state: **STOPPED**

### LDAP Options

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

### Logging options

**Enable GUI log** ☒ Check this option to log the access to the Proxy Filter GUI.

**Enable log** ☒ Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings.

**Enable log rotation** ☒ Check this option to rotate the logs every day. This is recommended if you enable any kind of logging to limit file size and do not run out of disk space.

### Miscellaneous

**Clean Advertising** ☐ Check this option to display a blank gif image instead of the default block page. With this option the user gets a cleaner webpage.

### Blacklist options

**Blacklist** ☒ Check this option to enable blacklist

**Blacklist proxy**

Blacklist upload proxy - enter here, or leave blank.  
 Format: host[port login:pass] . Default proxy port 1080.  
 Example: '192.168.0.1:8080 user:pass'

**Blacklist URL**

Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or leave blank. The LOCAL path could be your pfSense (/tmp/blacklist.tar.gz).

La parte de Service options dependerá de vuestro Hardware y usuarios, deberán ser ajustados. Los valores por defecto no suelen dar problemas a priori, pero tener en cuenta en Rewrite process children que si son muy bajos creará colas de solicitud por lo tanto la navegación será menos fluida y si pones un número elevado es posible que satures el sistema, por lo tanto, hay que ir probando en cada escenario los valores adecuados.

El Rewrite process children startup es el número de procesos hijos que estarán disponibles en el arranque.

El Rewrite process children idle es el número que intentará mantener en todo momento.

Estos serán ajustados igualmente según escenarios.

En la sección Loggin options nos encontramos tres opciones:



Enable GUI log, la activamos para tener acceso a la GUI del Proxy Filter

Enable log, la activamos para poder ver qué está pasando en nuestro Proxy Filter, quien está siendo bloqueado, etc..., además de para comprobar que los filtros están funcionando.

Enable log rotation, lo activamos también para que los logs roten diariamente porque en caso contrario nos quedaremos sin espacio en disco en algún momento.

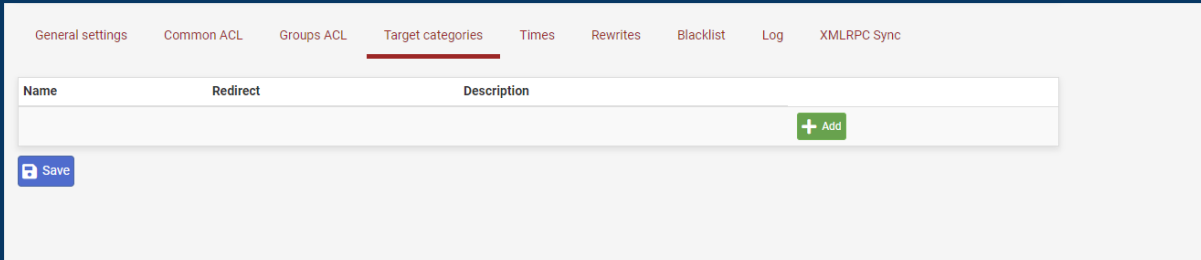
En la sección Miscellaneous nos encontramos con Clean Advertising que si la activamos los usuarios en lugar de recibir la página predeterminada que utilicemos, recibirán una página en blanco.

Y por último la sección Blacklist options que no puede faltar.

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 nanoBSD, 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. Si nos dirigimos a <http://www.squidguard.org/blacklists.html> veremos 4 opciones de listas, en nuestro caso hemos seleccionado Shalla's Blacklist añadiendo el enlace de descarga <http://www.shallalist.de/Downloads/shallalist.tar.gz> en Blacklist URL, salvamos y vamos al apartado

Target categories.



The screenshot shows the 'Target categories' configuration page. At the top, there are several tabs: 'General settings', 'Common ACL', 'Groups ACL', 'Target categories' (which is selected and underlined), 'Times', 'Rewrites', 'Blacklist', 'Log', and 'XMLRPC Sync'. Below the tabs is a table with three columns: 'Name', 'Redirect', and 'Description'. The table is currently empty. To the right of the table is a green button with a plus sign and the text '+ Add'. At the bottom left of the table area is a blue button with a floppy disk icon and the text 'Save'.

En este laboratorio lo vamos hacer simple crearemos Bloqueadas

<b>Name</b>	<input type="text" value="Bloqueadas"/>
Enter a unique name of this rule here. The name must consist between 2 and 15 symbols [a-Z_0-9]. The first one must be a letter.	
<b>Order</b>	<input type="text" value="-- Last --"/>
Select the new position for this target category. Target categories are listed in this order on ACLs and are matched from the top down in sequence.	
<b>Domain List</b>	<div><div></div></div>
Enter destination domains or IP-addresses here. To separate them use space. <b>Example:</b> mail.ru e-mail.ru yahoo.com 192.168.1.1	
<b>URL List</b>	<div><div></div></div>
Enter destination URLs here. To separate them use space. <b>Example:</b> host.com/xxx 12.10.220.125/alisa	
<b>Regular Expression</b>	<div><div>casino games porn xxx</div></div>
Enter word fragments of the destination URL. To separate them use  . <b>Example:</b> mail[casino game]\.r sdf\$	
Enter word fragments of the destination URL. To separate them use  . <b>Example:</b> mail[casino game]\.r sdf\$	
<b>Redirect mode</b>	<input type="text" value="int error page (enter error message)"/>
Select redirect mode here. Note: if you use 'transparent proxy', then 'int' redirect mode will not accessible. Options: <a href="#">ext url err page</a> , <a href="#">ext url redirect</a> , <a href="#">ext url as 'move'</a> , <a href="#">ext url as 'found'</a> .	
<b>Redirect</b>	<div><div></div></div>
Enter the external redirection URL, error message or size (bytes) here.	
<b>Description</b>	<div><div></div></div>
You may enter any description here for your reference.	
<b>Log</b>	<input checked="" type="checkbox"/> Check this option to enable logging for this ACL.
<input type="button" value="Save"/>	

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.

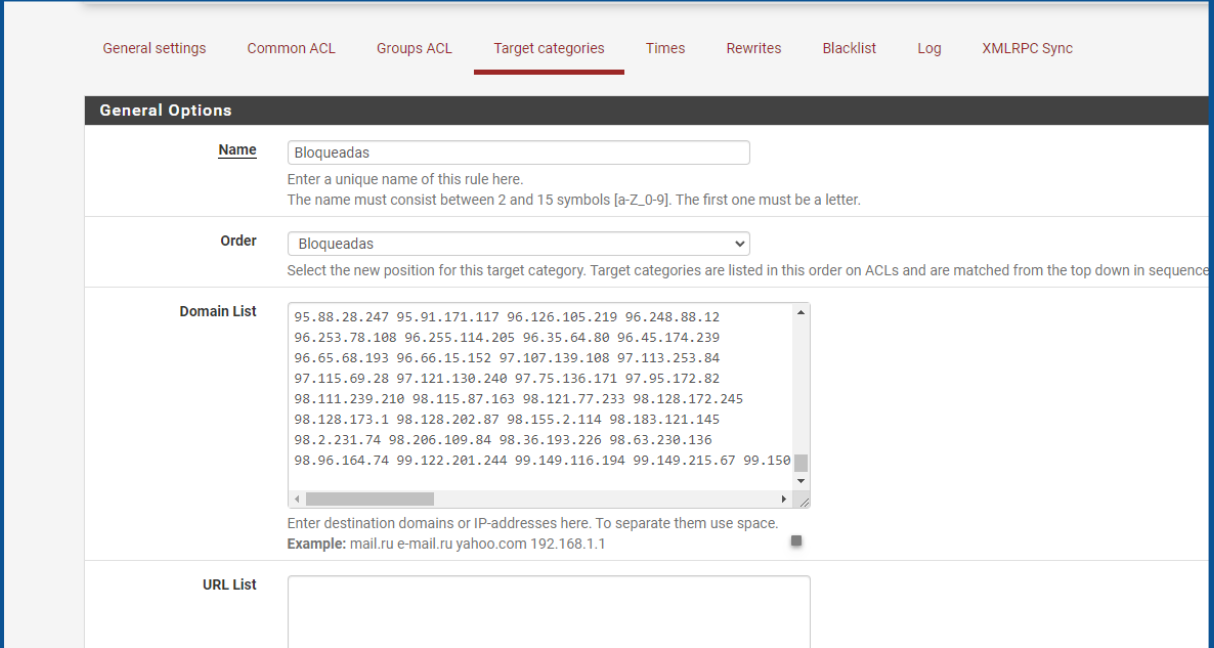
En Domain List podemos meter ips o dominios a bloquear separados por un espacio, en el ejemplo están puestas las ips de los nodos de Tor que han sido obtenidas de <https://www.dan.me.uk/torlist/>.

Aquí nos encontramos con el problema que viene una por línea y necesitamos que estén separadas por un espacio para que nos deje ponerla.

¿Cómo lo hacemos? Pues utilizando el comando “sed”, nos copiamos y pegamos la ips en un documento por ejemplo tor.tx y por consola ejecutamos:

```
sed 'a;N;$!ba;s/\n/ /g' tor.txt > torespaciado.txt
```

Ahora abrimos el fichero torespaciado.txt y copiamos y pegamos ya que lo tendremos sin salto de líneas y con un espacio entra las IPs.



The screenshot shows a web interface with a top navigation bar containing links: General settings, Common ACL, Groups ACL, Target categories (active), Times, Rewrites, Blacklist, Log, and XMLRPC Sync. Below this is a 'General Options' section. It has three main fields: 'Name' (containing 'Bloqueadas'), 'Order' (a dropdown menu with 'Bloqueadas' selected), and 'Domain List' (a text area containing a list of IP addresses separated by spaces). Below the 'Domain List' is a small text box with the instruction 'Enter destination domains or IP-addresses here. To separate them use space. Example: mail.ru e-mail.ru yahoo.com 192.168.1.1'. At the bottom is a 'URL List' field which is currently empty.

Si queremos bloquear la red Tor tener en cuenta que tendremos que actualizar este campo cada cierto tiempo.

En URL list podemos meter las URL a Bloquear.

En Regular Expression podemos poner palabras a bloquear como indica: casino|games|porno|xxx.

Ojo en esta parte si dejan espacios no funcionará ninguna, es decir, siempre separadas por “|” pero que no haya ningún espacio delante ni detrás.

En Redirect mode, redirigimos al usuario a una web externa que hayamos hecho para indicarle que está prohibido o a una página de error. Si hemos seleccionado web externa la escribiremos en el campo Redirect.

Y por último muy importante activar el log para luego poder ver que se está ejecutando correctamente y ver los bloqueos que realiza.

Hacemos lo mismo para crear permitidas con la única diferencia que en Redirect mode lo dejamos en “none” y seleccionamos que sea la primera posición “—”, teniendo las mismas opciones que en bloqueadas con la diferencia que lo que pongamos en cada apartado será permitido.

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

Blacklist Update

Blacklist download progress

0 %

http://www.shallalist.de/Downloads/sahlalist.tar.gz

Download

Cancel

Restore Default

Enter FTP or HTTP path to the blacklist archive here.

Blacklist update Log

```

Begin blacklist update
Start download.
Download archive http://www.shallalist.de/Downloads/sahlalist.tar.gz

```

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.

General Options

Name

TurnoDiurno

Enter a unique name of this rule here.  
The name must consist between 2 and 15 symbols [a-Z\_0-9]. The first one must be a letter.

Values

Weekly

mon

06:00-21:00

Time type

Days

Date or Date range

Time range

Add

+ Add

Description

TurnoDiurno

You may enter any description here for your reference.

Note:

Example for Date or Date Range: 2007.12.31 or 2007.11.31-2007.12.31 or \*.12.31 or 2007.\*.31

Example for Time Range: 08:00-18:00

Save

Para el turno Nocturno tendremos que crear dos intervalos ya que empieza a contar desde las 00:00 y nos daría un error, quedando así

General Options

Name

TurnoNocturno

Enter a unique name of this rule here.  
The name must consist between 2 and 15 symbols [a-Z\_0-9]. The first one must be a letter.

Values

Weekly

all

21:00-23:59

Delete

Weekly

all

00:00-8:00

Delete

Time type

Days

Date or Date range

Time range

Add

+ Add

Description

TurnoNocturno

You may enter any description here for your reference.

Note:

Example for Date or Date Range: 2007.12.31 or 2007.11.31-2007.12.31 or \*.12.31 or 2007.\*.31

Example for Time Range: 08:00-18:00

Save

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 entre whitelist (siempre permitida aunque la encuentre en otra categoría bloqueada), allow (permitido siempre y cuando no esté en otra categoría) o deny (no permitido) en el desplegable. En nuestro caso las permitidas las pondremos en whitelist o allow puesto que nos hemos curado en salud poniendo dicha lista la primera a comprobar, por lo tanto, ambas opciones nos valen, aunque elegiremos whitelist.

Para no extender mucho vamos a explicar Groups ACL ya que la Common ACL es prácticamente lo mismo pero común a todos los usuarios, hay que tener en cuenta que las Common ACL tienen prioridad sobre las de Grupo, es decir, si en las ACL comunes hay una categoría por ejemplo bloqueada por mucho que en grupos la permitamos seguirá estando bloqueada. En la mayoría de escenarios tendréis que utilizar solo ACL por grupos

General settings
Common ACL
Groups ACL
Target categories
Times
Rewrites
Blacklist
Log
XMLRPC Sync

General Options

Disabled
☐ Check this to disable this ACL rule.

Name

Enter a unique name of this rule here.  
The name must consist between 2 and 15 symbols [a-Z\_0-9]. The first one must be a letter.

Order

-- Last --

Select the new position for this ACL item. ACLs are evaluated on a first-match source basis.

**Note:**  
Search for a suitable ACL by field 'source' will occur before the first match. If you want to define an exception for some sources (IP) from the IP range, put them on first of the list.

**Example:**  
ACL with single (or short range) source ip 10.0.0.15 must be placed before ACL with more large ip range 10.0.0.0/24.

Client (source)

Enter client's IP address or domain or "username" here. To separate them use space.

**Example:**  
IP: 192.168.0.1 - Subnet: 192.168.0.0/24 or 192.168.1.0/255.255.255.0 - IP-Range: 192.168.1.1-192.168.1.10  
Domain: foo.bar matches foo.bar or \*.foo.bar  
Username: 'user1'  
**Ldap search (Ldap filter must be enabled in General Settings):**  
ldapusersearch ldap://192.168.0.100/DC=domain,DC=com?sAMAccountName=sub?(&(sAMAccountName=%s)(memberOf=CN=it%2cCN=Users%2cDC=domain%2cDC=com))  
*Attention: these line don't have break line, all on one line*

Time

TurnoDiurno

Select the time in which "Target Rules" will operate or leave 'none' for rules without time restriction. If this option is set then in off-time the second ruleset will operate.

Target Rules

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 e 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

<b>Do not allow IP-Addresses in URL</b>	<input type="checkbox"/> To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This has no effect on the whitelist.
<b>Redirect mode</b>	<div>int error page (enter error message) ▼</div> <p>Select redirect mode here.  Note: if you use 'transparent proxy', then 'int' redirect mode will not be accessible.  Options: <a href="#">ext url err page</a>, <a href="#">ext url redirect</a>, <a href="#">ext url as 'move'</a>, <a href="#">ext url as 'found'</a>.</p>
<b>Redirect</b>	<div></div> <p>Enter the external redirection URL, error message or size (bytes) here.</p>
<b>Use SafeSearch engine</b>	<input type="checkbox"/> To protect your children from adult content you can use the protected mode of search engines. At the moment it is supported by Google, Yandex, Yahoo, MSN, Live Search, Bing, DuckDuckGo, OneSearch, Rambler, Ecosia and Qwant. Most of the search engines can be accessed. It is recommended to prohibit access to others. <b>Note:</b> This option overrides 'Rewrite' setting.
<b>Rewrite</b>	<div>none (rewrite not defined) ▼</div> <p>Enter the rewrite condition name for this rule or leave it blank.</p>
<b>Rewrite for off-time</b>	<div>none (rewrite not defined) ▼</div> <p>Enter the rewrite condition name for this rule or leave it blank.</p>
<b>Description</b>	<div></div> <p>You may enter any description here for your reference.</p>
<b>Log</b>	<input checked="" type="checkbox"/> Check this option to enable logging for this ACL.
<div>Save</div>	

Do not allow IP-Addresses in URL si utilizáramos FQDN, activando dicha opción evitaríamos un bypass utilizando la IP en lugar del FQDN.

Redirect Mode y Redirect, lo mismo que vimos anteriormente.

Use SafeSearch engine si la activamos solo permitimos motores de búsqueda seguros donde nos indica cuales soporta, activando esta casilla las 2 siguientes quedan anuladas, ya que es lo mismo, pero para diferenciar en horario, de fuera de horario.

Y por último descripción y Log, donde claro está lo activamos.

Por último, comentaremos simplemente la pestaña Rewrite donde la utilizaremos para hacer redirecciones de URL, es decir, cuando el usuario escriba una dirección en concreta será redireccionado a donde nosotros queramos.

Y la pestaña logs donde veremos configuraciones y lo que va sucediendo en nuestro Proxy Filter.

Hecho todo esto podemos activar SquidGuard en General settings asegurando de que le damos al botón de Apply y si todo está correcto podremos salvar, si hubiera algo mal configurado nos indicaría que hay mal.

Target Rules

**Target Rules List** + -

ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.

Target Categories	Target Categories for off-time
If 'Time' not defined, this is column will be ignored.	
[Bloqueadas]	access whitelist [Bloqueadas]
Default access [all]	access allow

**Do not allow IP-** ☐ To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option

**Do not allow IP-Addresses in URL** ☐ To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.

**Redirect mode**

Select redirect mode here.  
Note: if you use 'transparent proxy', then 'int' redirect mode will not be accessible.  
Options: [ext url err page](#), [ext url redirect](#), [ext url as 'move'](#), [ext url as 'found'](#)

**Redirect**

Enter the external redirection URL, error message or size (bytes) here.

**Use SafeSearch engine** ☐ To protect your children from adult content you can use the protected mode of search engines.  
At the moment it is supported by Google, Yandex, Yahoo, MSN, Live Search, Bing, DuckDuckGo, OneSearch, Rambler, Ecosia and Qwant. Make sure that the search engines can be accessed. It is recommended to prohibit access to others.  
**Note:** This option overrides 'Rewrite' setting.

**Rewrite**

Enter the rewrite condition name for this rule or leave it blank.

**Rewrite for off-time**

Enter the rewrite condition name for this rule or leave it blank.

**Description**

You may enter any description here for your reference.

**Log** ☒ Check this option to enable logging for this ACL.

**Save**

Do not allow IP-Addresses in URL si utilizáramos FQDN, activando dicha opción evitaríamos un bypass utilizando la IP en lugar del FQDN.

Redirect Mode y Redirect, lo mismo que vimos anteriormente.

Use SafeSearch engine si la activamos solo permitimos motores de búsqueda seguros donde nos indica cuales soporta, activando esta casilla las 2 siguientes quedan anuladas, ya que es lo mismo, pero para diferenciar en horario, de fuera de horario.

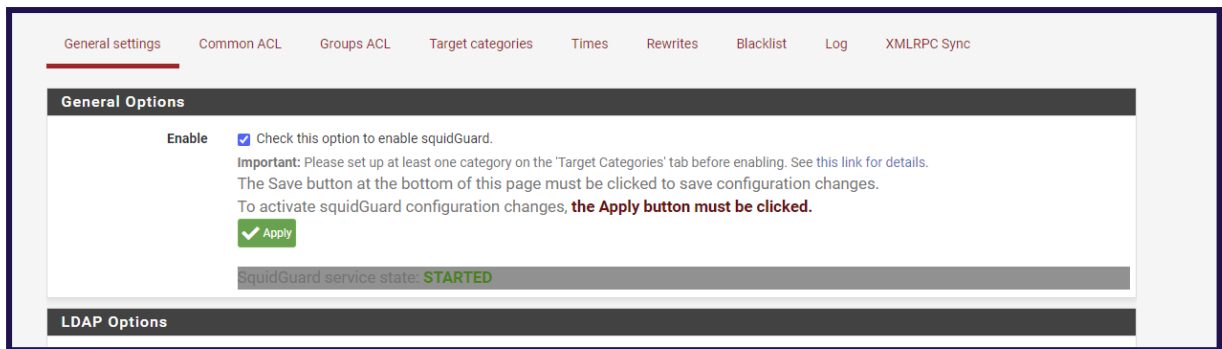
Y por último descripción y Log, donde claro está lo activamos.

Por último, comentaremos simplemente la pestaña Rewrite donde la utilizaremos para hacer redirecciones de URL, es decir, cuando el usuario escriba una dirección en concreta será redireccionado a donde nosotros queramos.

Y la pestaña logs donde veremos configuraciones y lo que va sucediendo en nuestro Proxy Filter.

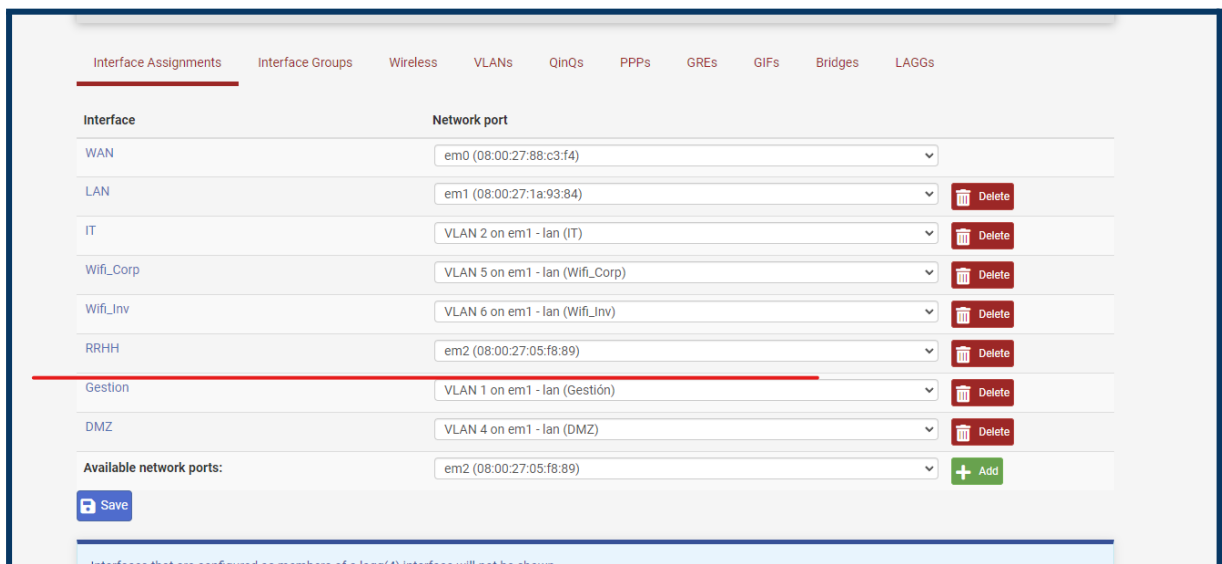
Hecho todo esto podemos activar SquidGuard en General settings asegurando de que le damos al botón de Apply y si todo está correcto podremos salvar, si hubiera algo mal configurado nos indicaría que hay mal.





Como todo estaba correcto hemos podido, aplicar, salvar y ya vemos el servicio iniciado. 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 RRHH a la interfaz física para no marcar el tráfico con una vlan.



Configuramos una máquina virtual Windows y le asignamos la red rrhh (VMnet2) en mi caso y le asignó una dirección ip dentro del rango de la red rrhh.

NOTA: Desactivamos las listas de pblock en las reglas de la red comercial para tener conexión a internet y ponemos 8.8.8.8 como servidor dns en la máquina virtual de Windows.

Floating	WAN	LAN	IT	WIFI_CORP	WIFI_LIN	RRHH	GESTION	DMZ
----------	-----	-----	----	-----------	----------	------	---------	-----

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✖	0 / 0 B	IPv4 *	pfB_Level_1_v4	*	*	*	*	none	pfB_Level_1_v4 auto rule	
<input type="checkbox"/>	✖	0 / 0 B	IPv4 *	pfB_Level_2_v4	*	*	*	*	none	pfB_Level_2_v4 auto rule	
<input type="checkbox"/>	✖	0 / 0 B	IPv4 *	pfB_Level_3_v4	*	*	*	*	none	pfB_Level_3_v4 auto rule	

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

Propiedades: Protocolo de Internet versión 4 (TCP/IPv4)

General

Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.

☐ Obtener una dirección IP automáticamente

☒ Usar la siguiente dirección IP:

Dirección IP:

Máscara de subred:

Puerta de enlace predeterminada:

☐ Obtener la dirección del servidor DNS automáticamente

☒ Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido:

Servidor DNS alternativo:

☐ Validar configuración al salir

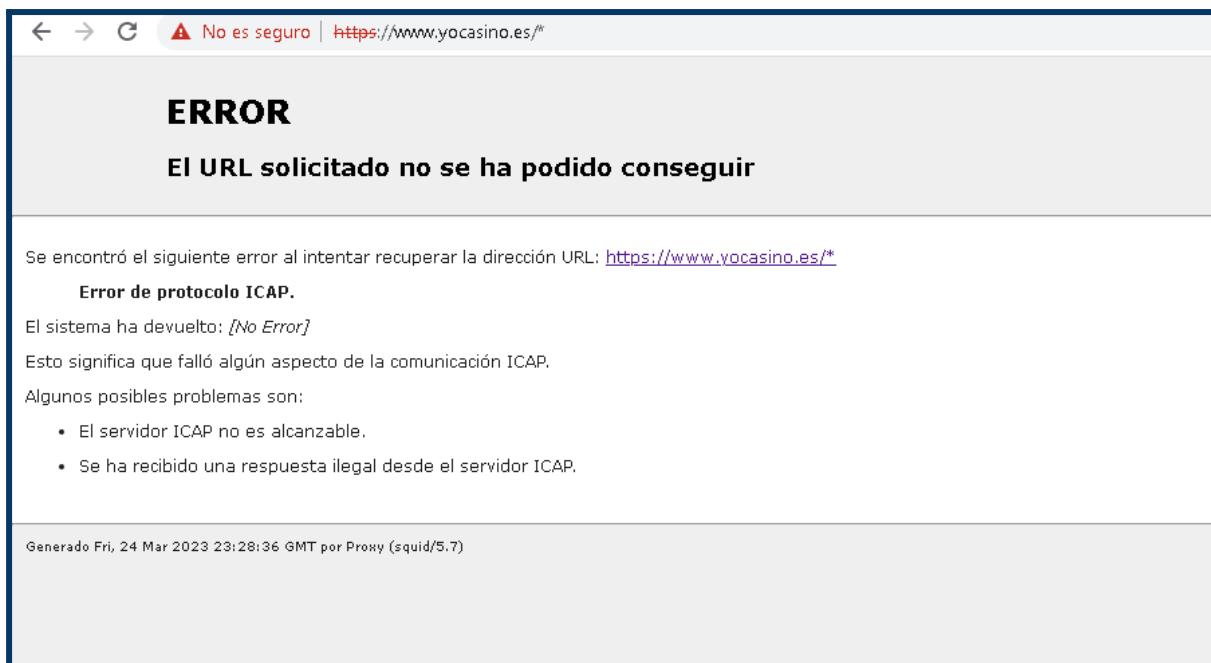
Con la configuración actual el cliente recibirá el siguiente error cuando intente acceder alguna página donde la url incluya porno o casino, ya que lo hemos metido como Regular expresion, si queremos

bloquear mejor estas categorías además de las palabras en la URL bloquearemos las categorías correspondientes, ya que solo así como está se podrá acceder a todas aquellas que no contengan en la URL las palabras.

Por ejemplo: <https://drugs.com>, [www.yocasino.es](http://www.yocasino.es)

Si en lugar de elegir int error page en la regla que nos está bloqueando en Redirect mode, hubiéramos elegido por ejemplo una url externa nos mostrará dicha url.

Si miramos los logs veremos todo lo que está bloqueando que incluya dichas palabras en la url.



## Lightsquid

### Historia:

LightSquid es un software libre de análisis y generación de informes de registro de tráfico web. Fue lanzado por primera vez en 2006 por Tomasz Kojm como una alternativa ligera al software SquidAnalyzer. Desde entonces, LightSquid se ha convertido en una herramienta popular para analizar el tráfico web en redes pequeñas y medianas.

### Motivación:

La motivación detrás de la creación de LightSquid fue proporcionar una herramienta fácil de usar y de bajo costo para analizar y generar informes sobre el tráfico web. LightSquid se integra con el servidor proxy Squid para proporcionar informes detallados sobre el uso de la red y los patrones de tráfico.

### Funcionalidades:

Las principales funcionalidades de LightSquid son:

- **Análisis de tráfico web:** LightSquid analiza los registros de tráfico web para proporcionar información detallada sobre el uso de la red, incluyendo el tráfico de entrada y salida, las páginas web más visitadas y el uso de ancho de banda.
- **Generación de informes:** LightSquid genera informes detallados en formato HTML y PDF para que los administradores de red puedan analizar y comprender el uso de la red.
- **Fácil de usar:** LightSquid es fácil de instalar y configurar, y tiene una interfaz de usuario intuitiva que permite a los usuarios navegar fácilmente por los informes generados.

- Integración con Squid: LightSquid se integra con el servidor proxy Squid para proporcionar informes detallados sobre el uso de la red.

### Alternativas:

Existen varias alternativas a LightSquid en el mercado, como SquidAnalyzer, AWStats, Piwik, entre otros. Cada una de ellas ofrece diferentes servicios de análisis de tráfico web y funcionalidades para adaptarse a las necesidades de los usuarios.

### Principales características:

Las principales características de LightSquid son:

- Análisis detallado: LightSquid proporciona un análisis detallado del tráfico web para ayudar a los administradores de red a comprender el uso de la red.
- Generación de informes: LightSquid genera informes detallados en formato HTML y PDF para que los administradores de red puedan analizar y comprender el uso de la red.
- Fácil de usar: LightSquid es fácil de instalar y configurar, y tiene una interfaz de usuario intuitiva que permite a los usuarios navegar fácilmente por los informes generados.
- Integración con Squid: LightSquid se integra con el servidor proxy Squid para proporcionar informes detallados sobre el uso de la red.
- Código abierto: LightSquid es un software libre y de código abierto, lo que significa que los usuarios pueden personalizar y modificar el código fuente según sea necesario.

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.

Package / Squid Proxy Reports: Settings

**Instructions**

Perform these steps after install **IMPORTANT:** Click Info and follow the instructions below if this is initial install! [i](#)

**Web Service Settings**

**Lightsquid Web Port**   
Port the lighttpd web server for Lightsquid will listen on. (Default: 7445)

**Lightsquid Web SSL** ☒ Use SSL for Lightsquid Web Access  
This option configures the Lightsquid web server to use SSL and uses the WebGUI HTTPS certificate.

**Lightsquid Web User**   
Username used to access lighttpd. (Default: admin)

**Lightsquid Web Password**   
Password used to access lighttpd. (Default: pfsense)

**Links** [➔ Open Lightsquid](#) [➔ Open sqstat](#)

**Report Template Settings**

Report Template Settings

Language

Spanish

Select report language.

Report Template

Base

Select report template.

Bar Color

Orange

Select bar color.

Reporting Settings and Scheduler

IP Resolve Method

DNS

Select which method(s) should be attempted (in the order listed below) to resolve IPs to hostnames. Click Info for details. (Default: DNS)

Skip URL(s)

If you want to omit some sites from statistics (e.g., a local webserver), specify the URL(s) here. Separate multiple entries by | character. **Example:** `example.com|192.168.1.|example.net`

Refresh Scheduler

20min (!)

Select data refresh period. The reporting task will be executed every XX minutes/hours.  
**Legend:** (!)(\*) Use only with fast hardware (+) Recommended values

Manual Refresh

Use these buttons to start a background refresh of the Lightsquid reports.

Refresh

Will (re)parse today's entries only in Squid's current access.log.

Refresh Full

Will (re)parse all entries in all Squid's access logs, including the rotated ones. This may take a long time to finish!

Save

La primera parte es el puerto donde levantaremos el Lightsquid, que esté con SSL usuario y password.

La segunda parte es la plantilla que más nos guste.

La tercera parte es el método de resolución donde tenemos varias opciones, por defecto viene DNS donde nos mostrará el nombre de la máquina.

Si queremos excluir alguna url de las estadísticas separadas por “|”

Cada cuanto queremos que se refresquen y el refresco manual.

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.

Informe de accesos de usuarios de Squid

Período comprendido: Mar 2023

Calendar

2023

010203040506070809101112

Sitios Top

Total

Grupo

AA O

AA O

AA O

MES

MES

MES

Fecha

Grupo

Usuarios

Excedidos

Bytes

Promedio

Hit %

24 Mar 2023

grp

1

0

27 699

27 699

0.00%

Total Promedio:

1

0

27 699

27 699

0.00%

LightSquid v1.8 (c) Sergey Erokhin AKA ESL

<div> <div> <div>←</div> <div>→</div> <div>↺</div> <div>🏠</div> </div> <div> <div>No es seguro</div> <div>https://192.168.56.101:7445/user_detail.cgi?year=2023&amp;month=03&amp;day=24&amp;user=localhost</div> </div> </div> <div> <div>Tickets bloqueados...</div> <div>New chat</div> <div>Descargar archivo (...)</div> <div>Es necesario iniciar...</div> <div>Vicky (@vicky69077...</div> <div>Inicio Gestión Online</div> <div>CAS - Gobierno de...</div> <div>Catálogo de Servicios</div> <div>Recibidos - victoria...</div> <div>Vicky PG</div> <div>Conve...</div> </div>				
<div>Informe de accesos de usuarios de Squid</div> <div> <div>Usuario: localhost (?)</div> <div>Grupo: ?</div> <div>Fecha: 24 Mar 2023</div> </div>				
Total			27 699	
#	Sitios accedidos	Conexiones	Bytes	Total %
1	http://dhcp/sgerror.php?	7 27 699	27 699	100.0%
Total			27 699	
<div>LightSquid v1.8 (c) Sergey Erokhin AKA ESL</div>				

Como última parte de este laboratorio nos queda ver como corta los virus Clam-AV. Para ello vamos a abrir una web con virus desde la máquina que está utilizando el proxy, dicha web será Wicar, una web que nos ofrece probar virus, exploits y otras amenazas todas ellas inofensivas. Por lo tanto, abrimos <https://www.wicar.org/test-malware.html> desde el navegador. El propio Google nos avisará y bloqueará el acceso, le damos a que reconocemos el riesgo y obtendremos la siguiente ventana de los diferentes test

WICAR.org - Test Your Anti-Malware Solution!

HOME TEST MALWARE! RESULTS MORE...

Select a test payload...

Each test will open up a new browser window at <http://malware.wicar.org/>. You may wish to try each test systematically. Ideally, all tests should be blocked by your anti-malware defences. If a blank window loads, then it likely was not detected/prevented.

EICAR TEST-VIRUS

[SSL] The official EICAR.COM anti-virus test file. This is a 16bit DOS COM file and cannot run on recent OSes, but should be detected.

MS14-064 XP and below

[SSL] All Windows NT/95/98/2000/XP IE3+ Internet Explorer Windows OLE Automation Array (pre XP) CVE-2014-6332

MS14-064 2003 to Windows 10

[SSL] All Windows 2003/Vista/2008/7/8/10 IE6+ Internet Explorer Windows OLE Automation Array (post XP) CVE-2014-6332

Java JRE 1.7 Applet

[SSL] win32 (Java 7 JRE/JDK) Chrome Firefox IE Java 7 Applet Remote Code Execution (Browser Independent) CVE-2012-4681

MS03-020

[SSL] win32 NT/XP/2003 IE6 MS03-020 Internet Explorer's handling of the OBJECT type attribute CVE-2003-0344

MS05-054

[SSL] win32 XP IE6 MS05-054 Microsoft Internet Explorer JavaScript OnLoad Handler CVE-2005-1790

MS09-002

[SSL] win32 XP/Vista IE7 Internet Explorer 7 CFunctionPointer Uninitialized Memory Corruption CVE-2009-0075

MS09-072

[SSL] win32 IE6 Internet Explorer Style.getElementsByTagName Memory Corruption CVE-2009-3672

MS10-090

[SSL] win32 IE6 Internet Explorer CSS SetUserClip Memory Corruption CVE-2010-3962

Firefox 5.0 - 15.0.1 exposedProps

[SSL] Windows Firefox 5.0 to 15.0.1

Embedded VLC AMV

[SSL] Windows VLC v1.1.4 to 1.1.8 Browser independent

Adobe Flash Hacking Team leak

[SSL] Hacking Team July 2015 data leak Adobe Flash 18.0.0.194

