

Práctica de Evaluación 13 – Pfsense con Squid



Actividad 1

¿Cuáles son los tipos de «proxy», sus características y funciones principales? **1P**

Un proxy es un servidor intermedio que actúa como intermediario para realizar consultas a Internet. Su función principal es servir como pasarela entre los clientes y los destinos en línea.

Existen diferentes tipos de proxies, cada uno con funciones distintas:

Proxy NAT: Enmascara las direcciones IP entre clientes y destinos para compartir una misma dirección de acceso a Internet.

Proxy anónimo: Oculta completamente la identidad de los clientes a los destinos. Se utiliza para evadir firewalls y medidas de seguridad impuestas por administradores de sistemas.

Proxy Web: Almacena páginas web en memorias intermedias para servir las a los clientes bajo demanda. Mejora la velocidad de obtención de información, ya que si la página está en el caché, se obtiene con la velocidad de la red local.

Proxy inverso: Utilizado entre Internet y los servidores web para mejorar la seguridad y distribuir la carga sobre los servidores recibiendo todas las peticiones y reenviándolas a los servidores web.

Proxy abierto: Acepta peticiones de cualquier equipo cliente pero puede llevar a un uso ilícito o molesto al no poder controlar quién lo utiliza.

Proxy transparente: Combinación de un proxy con NAT. Las conexiones se enrutan hacia el proxy sin necesidad de configuración en el equipo cliente, siendo útil para medidas de seguridad o para agilizar la conexión sin que el usuario sea consciente del uso del proxy.

Y estos se centran en tres funciones principales:

Filtrado de Contenidos: Es la capacidad del proxy para elegir el tipo de contenido al que las estaciones de trabajo pueden acceder.

Proxy Caché: En esta función, el proxy tiene la capacidad de almacenar las páginas web consultadas por las estaciones de trabajo en una memoria caché. Esto agiliza las conexiones posteriores y permite que el proxy sirva esas páginas incluso si se pierde temporalmente la conexión a Internet.

Firewall: Es cuando el proxy actúa como intermediario que gestiona conexiones y puede interrumpirlas o continuarlas, y este pasa a funcionar como un firewall del sistema.

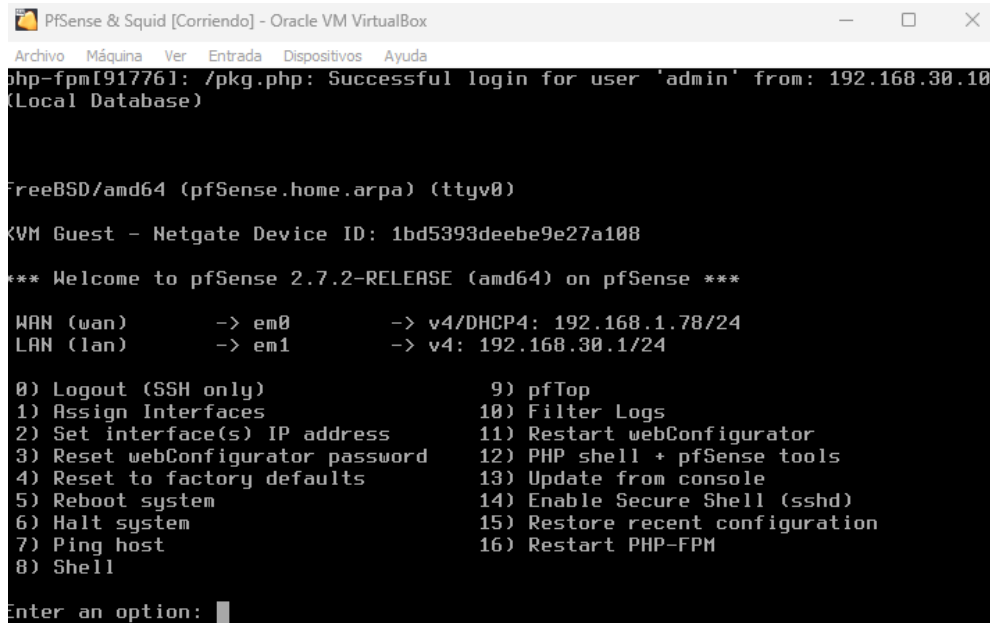
Actividad 2

Realiza un informe con capturas de pantalla del uso de pfSense con la configuración de proxy con squid.

1. Configura el escenario práctico con la siguiente arquitectura de red. 1p

Máquina con PfSense:

- Interfaz WAN
- Interfaz a LAN Interna: 192.168.30.1



```
PFsense & Squid [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
php-fpm[917761]: /pkg.php: Successful login for user 'admin' from: 192.168.30.10
(Local Database)

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
KVM Guest - Netgate Device ID: 1bd5393deebe9e27a108

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

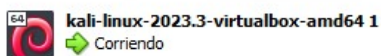
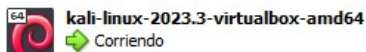
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.78/24
LAN (lan)      -> em1      -> v4: 192.168.30.1/24

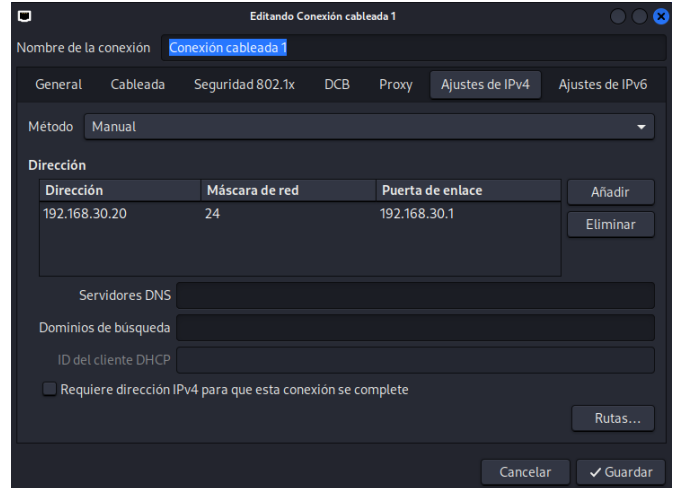
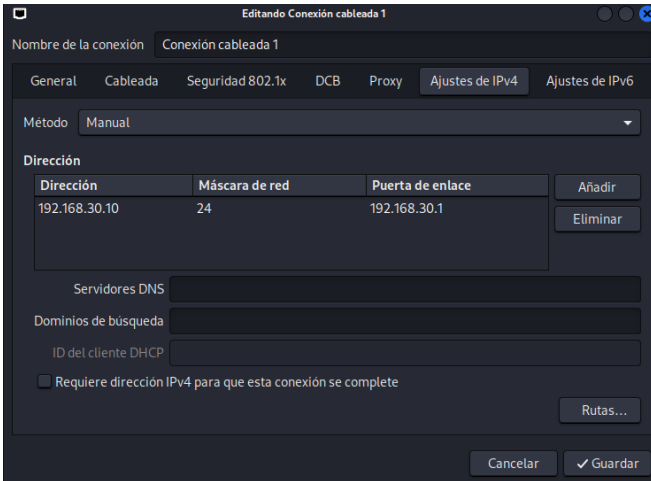
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: █
```

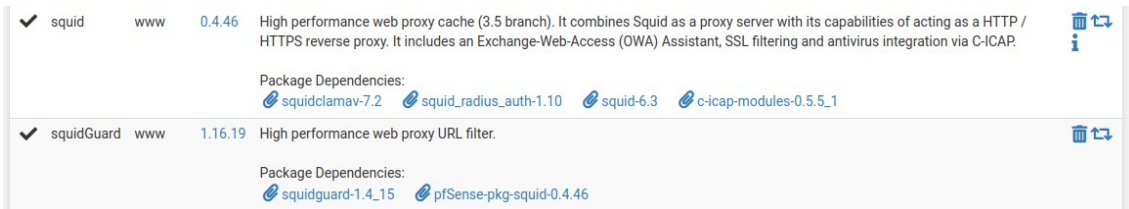
LAN Interna:

- Terminal 1: 192.168.30.10
- Terminal 2: 192.168.30.20





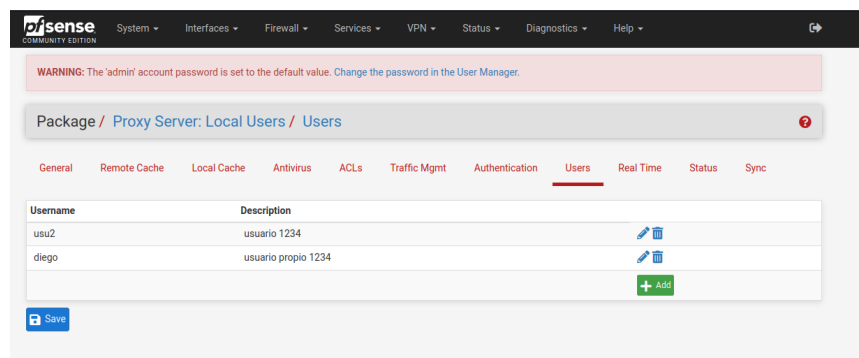
2. Configura el pfsense en modo proxy añadiendo la extensión “squid”.

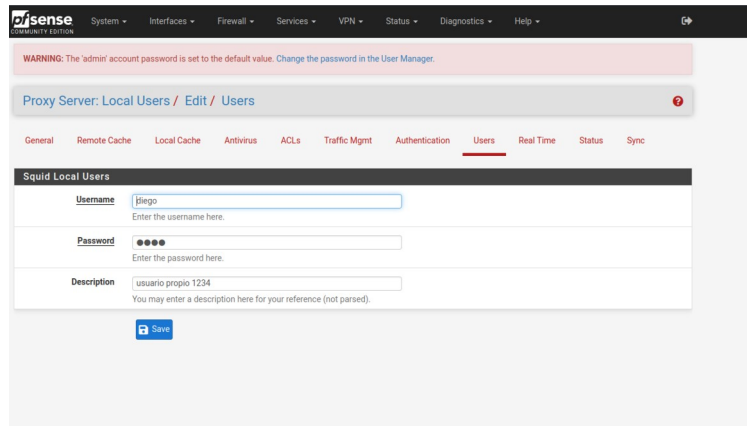


CONFIGURACIÓN DEL PROXY

1. Una lista de usuarios permitidos para su uso, los cuales tendrán que loguearse para usar el proxy.

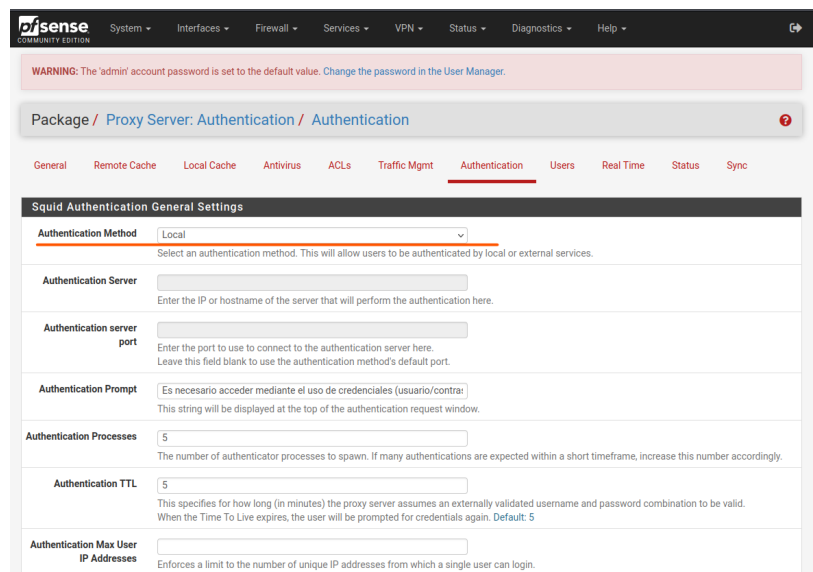
Primero vamos a crear dos usuarios desde el apartado de Users dentro de Proxy server





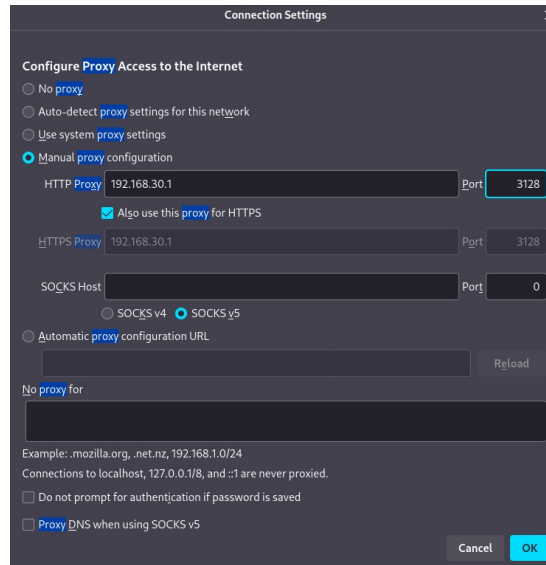
The screenshot shows the pfSense User Manager interface. At the top, there is a navigation menu with options like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message is displayed: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the breadcrumb path is "Proxy Server: Local Users / Edit / Users". The main content area is titled "Squid Local Users" and contains a form with three fields: "Username" (with the value "piego"), "Password" (masked with dots), and "Description" (with the value "usuario propio 1234"). A "Save" button is located at the bottom of the form.

Después pondremos el modo de autenticación local para que nos pida usuario y contraseña al usar cualquier servicio local

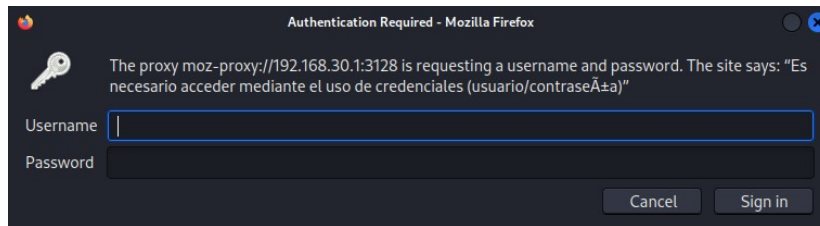


The screenshot shows the pfSense Squid Authentication General Settings interface. At the top, there is a navigation menu with options like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message is displayed: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the breadcrumb path is "Package / Proxy Server: Authentication / Authentication". The main content area is titled "Squid Authentication General Settings" and contains several configuration fields: "Authentication Method" (set to "Local"), "Authentication Server" (empty), "Authentication server port" (empty), "Authentication Prompt" (set to "Es necesario acceder mediante el uso de credenciales (usuario/contr:)", "Authentication Processes" (set to "5"), "Authentication TTL" (set to "5"), and "Authentication Max User IP Addresses" (empty). Each field has a description explaining its purpose.

Luego le especificamos al navegador la configuración de nuestro proxy especificando el puerto 3128 que es el puerto de acceso a nuestro proxy

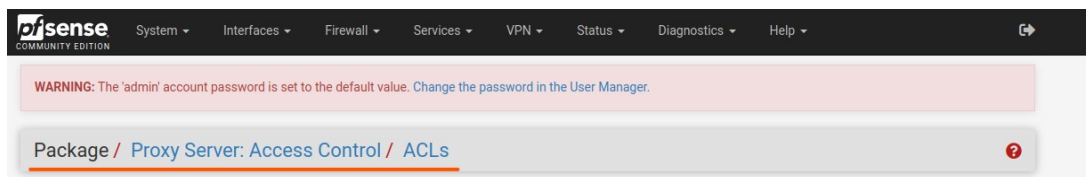


Y ahora ya al tratar de entrar a nuestro navegador ya nos pedira credenciales de usuario para poder acceder

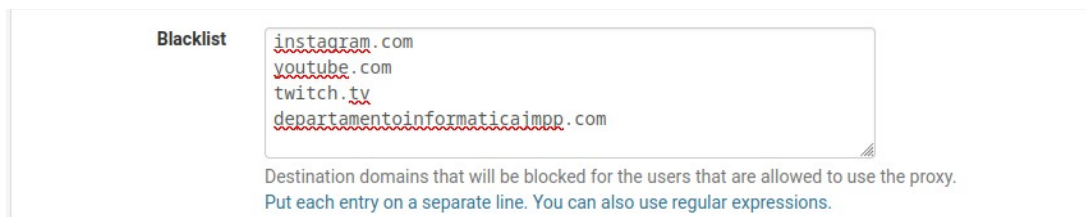


2. Un blacklist de redes sociales para que los usuarios no puedan conectarse a las mismas.

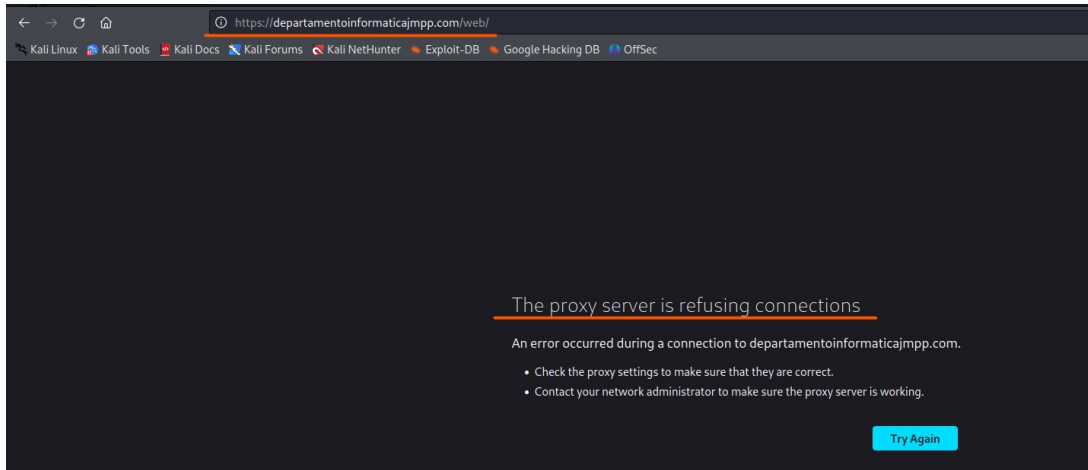
Entramos en el apartado de ACLs del servidor proxy



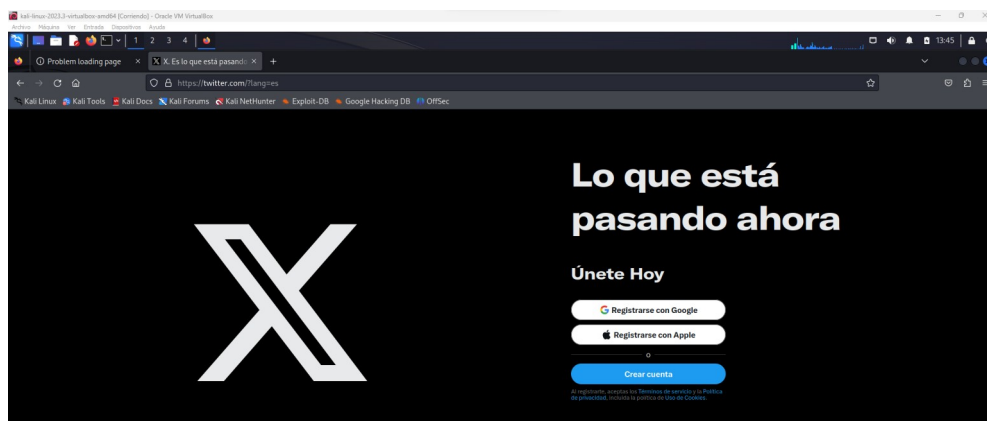
En el apartado de blacklist escribiremos las url que vamos a bloquear



Y ya podremos ver que en nuestros equipos de la Lan no nos dejara entrar a esas paginas en especifico



Pero si que nos dejara entrar a cualquier otra



3. Una franja horaria de activación de internet de 08:00 – 12:00. 1p




Primero desde el apartado de SquidGuard iremos al apartado times donde crearemos una franja horaria con las siguientes características

The screenshot shows the pfSense web interface for configuring a Proxy filter rule. At the top, there is a navigation menu with options like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the breadcrumb path is "Proxy filter SquidGuard: Times / Edit / Times". The "Times" tab is selected in the sub-menu. The "General Options" section contains the following fields:

- Name:** A text input field containing "Sin_Internet". Below it, a note says: "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:** Four dropdown menus: "Weekly" (Time type), "all" (Days), an empty field (Date or Date range), and "08:00-12:00" (Time range).
- Add:** A green "+ Add" button.
- Description:** A text input field containing "Ha hacer el desayuno y menos nintiendo". Below it, a note says: "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".

At the bottom of the form is a blue "Save" button.

The screenshot shows the "Times" tab of the Proxy filter rule configuration. The breadcrumb path is "Package / Proxy filter SquidGuard: Times / Times". The "Times" tab is selected in the sub-menu. Below the sub-menu, there is a table with the following data:

Name	Description	
Sin_Internet	Ha hacer el desayuno y menos nintiendo	 
		

At the bottom of the table is a blue "Save" button.

Ahora para crear la regla que nos deniegue el acceso a internet iremos al apartado de Groups ACL

Ya dentro de este apartado pondremos el nombre de nuestra franja horaria en las casillas remarcadas ademas de especificar la red de los clientes a los que se les aplicara y para que nos deniegue el acceso en "Target Rules List" pondremos que el acceso deba estar denegado

Proxy filter SquidGuard: Groups Access Control List (ACL) / Edit / Groups ACL

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
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: "user"
Ldap search (Ldap filter must be enabled in General Settings):
ldapsearch ldap://192.168.0.100/DC=domain,DC=com?sAMAccountName?sub?(&)(sAMAccountName=*)
(memberOf=CN=it%2CCN=Users%2cDC=domain%2cDC=com)
Attention: these line don't have break line, all on one line

Time
 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
Target Rules List
ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked
Target Categories Target Categories for off-time
Default access [all] access [deny] Default access [all] access [deny]

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 'ref' redirect mode will not accessible.
Options [set url as page](#) [set url redirect](#) [set url as 'move'](#) [set 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.

Como ahora mismo no estamos en la franja horaria definida vamos a crear una que ocupe todo el día para ver que la configuración funciona perfectamente.

Proxy filter SquidGuard: Times / Edit / Times

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

General Options

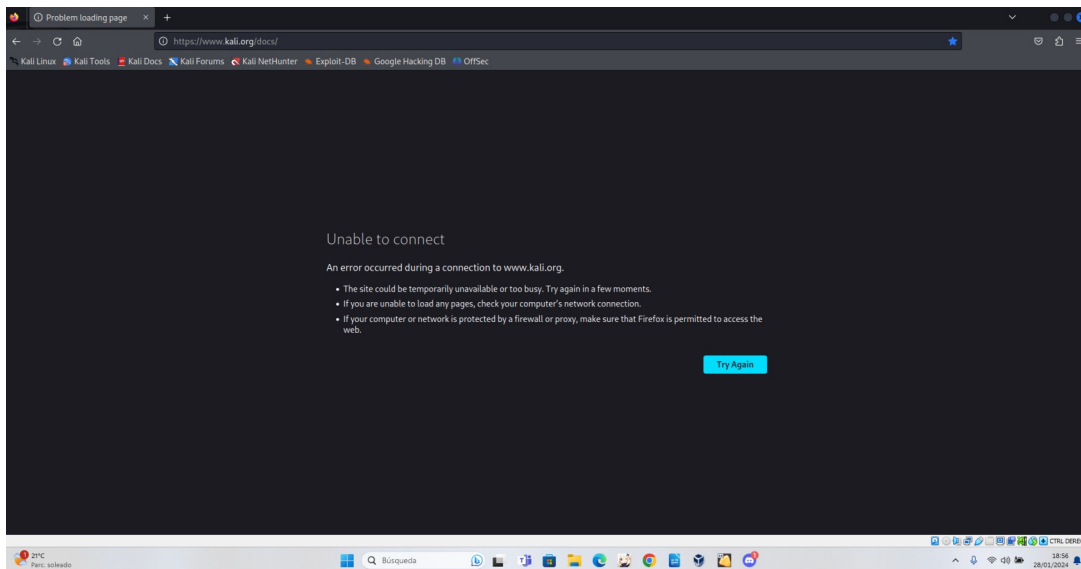
Name Comprovar
Enter a unique name of this rule here.
The name must consist between 2 and 15 symbols [a-Z_0-9]. The first one must be a letter.

Values Weekly all 00:00-23:59
Time type Days Date or Date range Time range

Add + Add

Description comprobacion
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

Y ahora ya podemos observar que el acceso esta completamente restringido



Para terminar de comprobar que las reglas están bien puestas cambiamos la configuración a allow para ver si ahora nos deja navegar con normalidad

Time Comprovar
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 !all [!all]

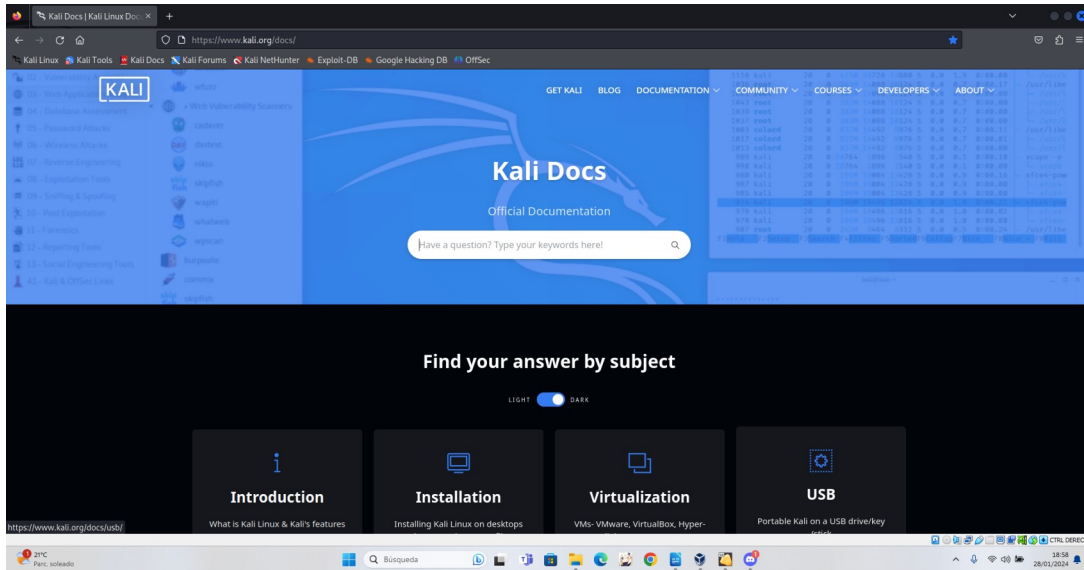
Target Rules List + -

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

Target Categories	Target Categories for off-time
Default access [all]	Default access [all]
access allow	access allow

If 'Time' not defined, this is column will be ignored.

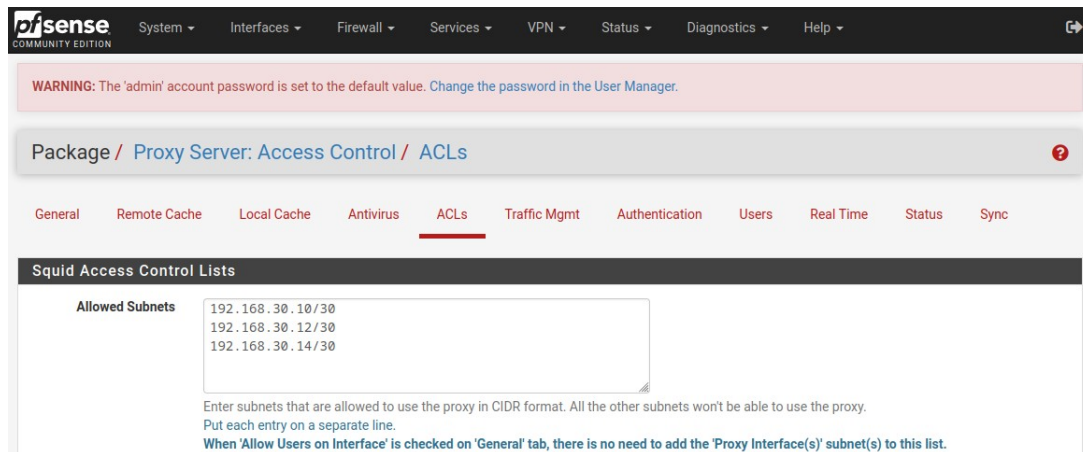
Ya después del cambio los equipos pueden navegar con completa normalidad sin ninguna restricción



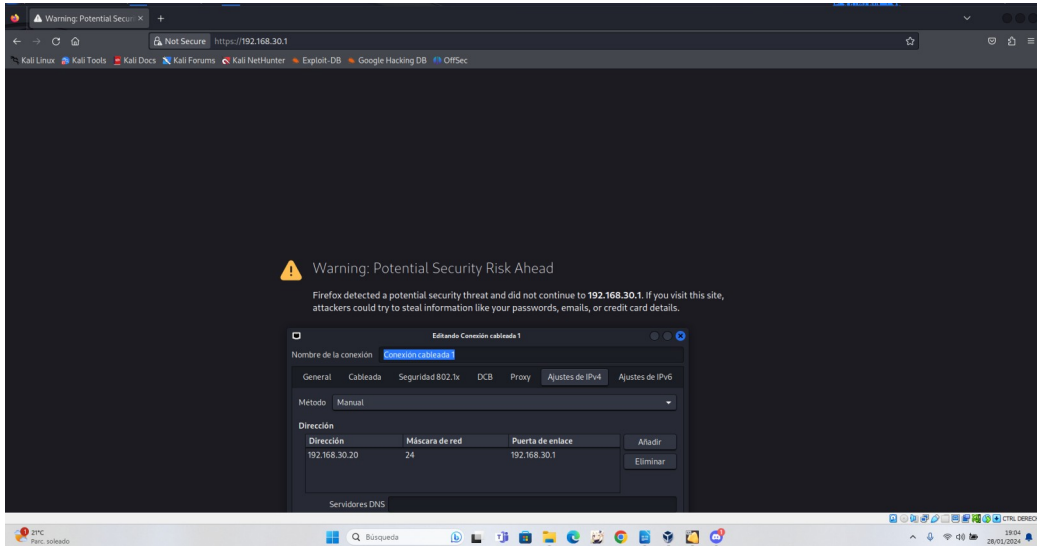
4. Solo los equipos del intervalo 192.168.30.10 - 192.168.30.15 pueden conectarse al proxy. **1P**

Para esta actividad volvemos al apartado de ACL donde al inicio debemos especificarle que subredes tendrán permitido acceder al proxy.

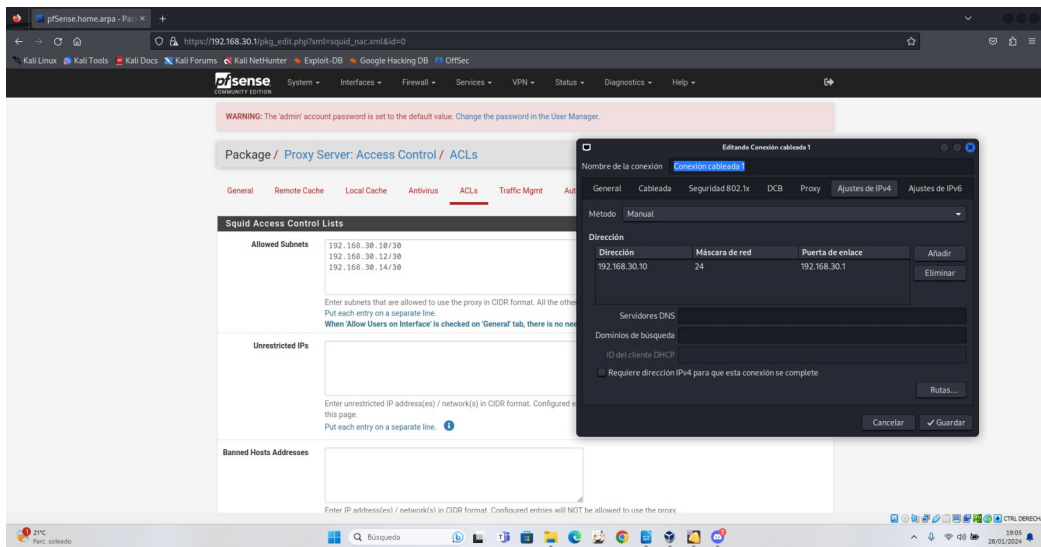
En mi caso puse 3 subredes que ocupen cada una 2 ip de las que se nos pide en la actividad.



En el cliente de la LAN con IP 192.168.30.20 podemos observar que ya al tratar de acceder al proxy nos salta directamente un error

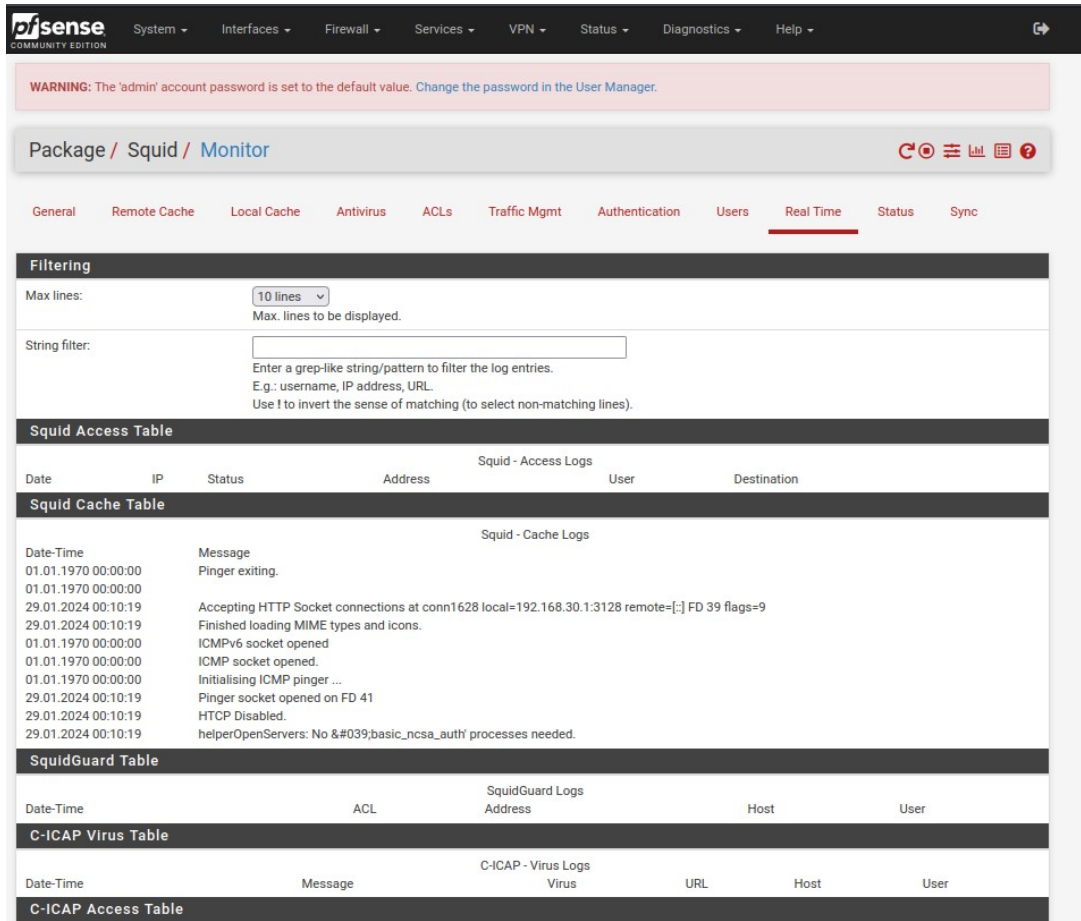


Mientras que en el equipo de IP 192.168.30.10 se puede acceder con completa normalidad sin que se nos bloquee el acceso de ninguna manera.



5. Mostrar los log del sistema proxy. **0,5p**

Los LOG del sistema proxy los podremos observar en el apartado “REAL TIME” dentro del servidor squid normal donde podremos ver algunos LOG del sistema squid como vemos en la siguiente imagen.

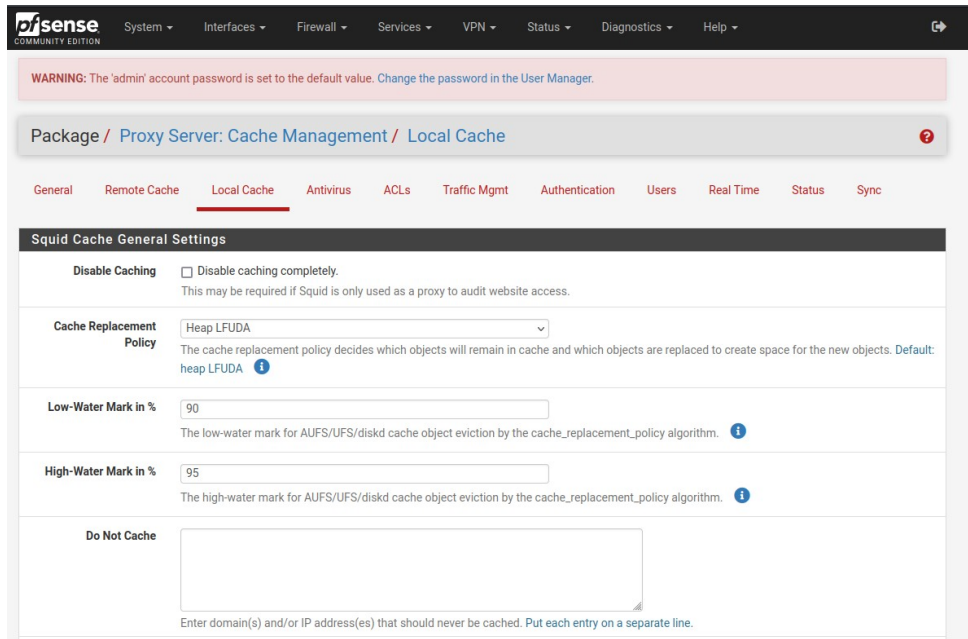


6. Mostrar si se puede configurar la caché web en squid. **1P**

Si se puede configurar y además tenemos dos métodos de hacerlo dependiendo de que manera queramos distribuirlo:

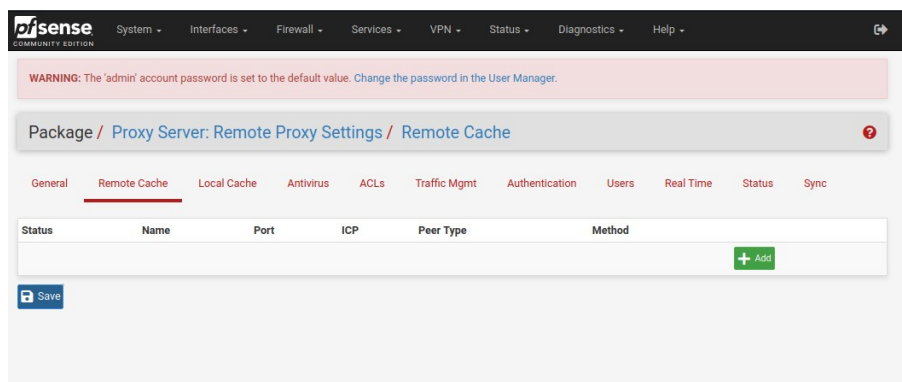
LOCAL:

Squid utiliza un espacio de almacenamiento en disco local para guardar versiones guardadas de los elementos web que los clientes solicitan. Cuando un cliente pide un recurso web a través del proxy Squid, el sistema primero verifica si ya tiene una copia almacenada de ese recurso en su caché local. Si la copia está presente y no ha caducado, Squid la entrega directamente al cliente sin necesidad de recuperarla del servidor web remoto.



REMOTO:

Squid tiene la capacidad de almacenar versiones guardadas de páginas web en servidores proxy ubicados en lugares distintos, conocido como "caché remoto". Esto es útil cuando hay varios Squid distribuidos en una red y se quiere compartir la información almacenada entre ellos. Los servidores proxy remotos pueden guardar versiones de páginas web que otros Squid en la red pueden necesitar, ayudando a reducir la carga en los servidores web.



7. S
e

puede configurar el proxy en modo transparente? Explica cómo hacerlo.

Si podemos, para poder configurar iremos al apartado general del proxy server y buscaremos el apartado “Transparent Proxy Settings”.



Transparent Proxy Settings	
Transparent HTTP Proxy	<input type="checkbox"/> Enable transparent mode to forward all requests for destination port 80 to the proxy server. i Transparent proxy mode works without any additional configuration being necessary on clients. Important: Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below. Hint: In order to proxy both HTTP and HTTPS protocols without intercepting SSL connections , configure WPAD/PAC options on your DNS/DHCP servers.
Transparent Proxy Interface(s)	<input type="text" value="WAN"/> <input type="text" value="LAN"/> <small>The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.</small>
Bypass Proxy for Private Address Destination	<input type="checkbox"/> Do not forward traffic to Private Address Space (RFC 1918 and IPv6 ULA) destinations. <small>Destinations in Private Address Space (RFC 1918 and IPv6 ULA) are passed directly through the firewall, not through the proxy server.</small>
Bypass Proxy for These Source IPs	<input type="text"/> <small>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 (;)</small>
Bypass Proxy for These Destination IPs	<input type="text"/> <small>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 (;)</small>

Donde simplemente activando no tendremos que configurar ningún cliente ya que no podrán saber que pasan por un proxy pero si que debemos configurar las interfaces por las que pasa el proxy transparente y también las redirecciones para que las conexiones vuelvan al proxy.

8. ¿Se puede configurar como proxy inverso? ¿Explica brevemente cómo se hace? **1P**
Si podremos configurar nuestro server de modo inverso de forma sencilla haciendo lo siguiente:

Vamos al apartado general de nuestro servidor proxy donde si vamos hacia abajo podremos ver dos apartados referentes al proxy inverso.

Ya desde estas opciones pondremos que la entrada de paquetes HTTP pase por el puerto 80 y la HTTPS por el 443.

Y con esto ya solo tendríamos que configurar nuestro firewall para que los paquete se reenvíen directamente a nuestro proxy y ya tendríamos nuestro proxy inverso.

[Podemos ver al apartado de configuración en la siguiente imagen:](#)

Package / Reverse Proxy Server: General / General ?

General **Web Servers** Mappings Redirects Real Time Sync

Squid Reverse Proxy General Settings

Listen IP Version v
Select the IP version Squid Reverse Proxy will use to bind to.

Reverse Proxy Interface(s) i
WAN
LAN
loopback
The interface(s) the reverse-proxy server will bind to (usually WAN). Use CTRL + click to select multiple interfaces.

User Defined Reverse Proxy IPs
Squid will additionally bind to these user-defined IPs for reverse proxy operation. Separate entries by semi-colons (;) i

External FQDN
The external fully qualified domain name of the WAN IP address.

Reset TCP Connections on Unauthorized Requests If checked, the reverse proxy will reset the TCP connection if the request is unauthorized.

Squid Reverse HTTP Settings

Enable HTTP Reverse Proxy If checked, the proxy server will act in HTTP reverse mode.
Important: You must add a proper firewall rule with destination matching the 'Reverse Proxy Interface(s)' address.

Reverse HTTP Port
This is the port the HTTP reverse proxy will listen on. Default: 80

Reverse HTTP Default Site
This is the HTTP reverse proxy default site. Leave empty to use 'External FQDN' value specified above.

Squid Reverse HTTPS Settings

Enable HTTPS Reverse Proxy If checked, the proxy server will act in HTTPS reverse mode.
Important: You must add a proper firewall rule with destination matching the 'Reverse Proxy Interface(s)' address.

Reverse HTTPS Port
This is the port the HTTPS reverse proxy will listen on. Default: 443

Reverse HTTPS Default Site i
This is the HTTPS reverse proxy default site.

9. Se puede monitorizar la actividad del proxy con herramientas gráficas? **0,5p**

Para realizarlo de esa manera instalaremos un paquete mas llamado Lightsquid que nos permitirá ver información de manera completamente grafica.

Name	Category	Version	Description	Actions
✓ Lightsquid	www	3.0.7_3	Lightsquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.	
Package Dependencies:				
lighttpd-1.4.72 lightsquid-1.8_5				

Para entra a dicha interfaz entramos en el apartado de Status en la opción “Squid Proxy Reports” y le damos a Open Lightsquid.

The screenshot shows the pfSense web interface. At the top, there is a navigation menu with options like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message is displayed: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the page title is "Package / Squid Proxy Reports: Settings". There is an "Instructions" section with an important note: "IMPORTANT: Click Info and follow the instructions below if this is initial install!". The "Web Service Settings" section contains several fields: "Lightsquid Web Port" (7445), "Lightsquid Web SSL" (checked), "Lightsquid Web User" (admin), and "Lightsquid Web Password" (masked). At the bottom, there are "Links" for "Open Lightsquid" and "Open sqstat".

Ya aquí podremos ver tablas con información de los usuarios y mas de manera grafica también pudiendo seleccionar el mes en el que se obtuvo la información.

The screenshot shows the "Squid user access report" interface. At the top, there is a "Work Period: Jan 2024" and a "Calendar" widget for 2024. Below the calendar is a row of numbers from 01 to 12. The main part of the interface is a table with columns: Date, Group, Users, Oversize, Bytes, Average, and Hit %. The data shows a single entry for "27 Jan 2024" with Group "grp", 1 user, 0 oversize, 35 595 bytes, 35 595 average, and 0.00% hit. A "Total/Average:" row is also present. To the right, there is a "Top Sites" section with a table for YEAR and MONTH, and a "Group" section with a table for YEAR and MONTH.

Date	Group	Users	Oversize	Bytes	Average	Hit %
27 Jan 2024	grp	1	0	35 595	35 595	0.00%
Total/Average:		1	0	35 595	35 595	0.00%

LightSquid v1.8 (c) Sergey Erokhin AKA ESL