# 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 servirlas 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 reenviandolas 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



LAN Interna:

- Terminal 1: 192.168.30.10
- Terminal 2: 192.168.30.20

kali-linux-2023.3-virtualbox-amd64



kali-linux-2023.3-virtualbox-amd64 1

## Administración de Sistemas informáticos en Red Seguridad y Alta Disponibilidad



•	Editando Conexión cab	leada 1	$\bigcirc \bigcirc \otimes$
Nombre de la conexión Cone	xión cableada 1		
General Cableada S	Seguridad 802.1x DCB	Proxy Ajustes de IPv4	Ajustes de IPv6
Método Manual			-
Dirección			
Dirección	Máscara de red	Puerta de enlace	Añadir
192.168.30.10	24	192.168.30.1	Eliminar
Servidores DNS			
Dominios de búsqueda			
Requiere dirección IPv4	para que esta conexión se c	omplete	
			Rutas
		Cancelar	✓ Guardar

		Editando Co	nexión cable	ada 1			$\bigcirc \bigcirc \bigotimes$
Nombre de la conexión	Cone	kión cableada 1					
General Cableac	la S	eguridad 802.1x	DCB	Proxy	Ajustes	de IPv4	Ajustes de IPv6
Método Manual							
Dirección							
Dirección		Máscara de red		Puerta	de enlace		Añadir
192.168.30.20		24		192.168.	.30.1		Eliminar
Servidores DI	NS						
Dominios de búsque	da						
ID del cliente DH							
Requiere direcci	ón IPv4	para que esta cone	xión se con	nplete			
							Rutas
						Cancelar	✓ Guardar

## 2. Configura el pfsense en modo proxy añadiendo la extensión "squid".

~	squid	www	0.4.46	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.	î≣t⊒ i
				Package Dependencies: Ø squidclamav-7.2 Ø squid_radius_auth-1.10 Ø squid-6.3 Ø c-icap-modules-0.5.5_1	
~	squidGuard	www	1.16.19	High performance web proxy URL filter.	亩口
				Package Dependencies: g squidguard-1.4_15 g pfSense-pkg-squid-0.4.46	

## **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

	System <del>-</del>	Interfaces 🗸	Firewall 👻	Services 🗸	VPN 🗸	Status 👻	Diagnostics 🗸	Help 🗸			•
WARNING: T	he 'admin' account j	bassword is set to	o the default valu	e. Change the	password in the	User Manager.					
Package	e / Proxy Ser	ver: Local l	Jsers / Us	ers							0
General	Remote Cache	Local Cache	Antivirus	ACLs	Traffic Mgmt	Authenticat	tion Users	Real Time	Status	Sync	
Username		De	scription								
usu2		u	suario 1234					Ø 🛅			
diego		us	suario propio 123	34				Ø 🛅			
								+ Add			
Sava											
Save											



WARNING: The 'admir' account password is set to the default value. Change the password in the User Manager.           Proxy Server: Local Users / Edit / Users           General         Remote Cache         Local Cache         Antivirus         ACLs         Traffic Mgmt         Authentication           Squid Local Users         Edit / Users	tion Users Real Time	e Status Sono
Proxy Server: Local Users / Edit / Users General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authenticati Squid Local Users	tion Users Real Time	Statue Sono
General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authenticati Squid Local Users	tion Users Real Time	Statue Svac
Squid Local Users		Status Sync
Username		
Enter the username here.		
Password		
Enter the password here.		
Description usuario propio 1234		
You may enter a description here for your reference (not parsed).		

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

System	<ul> <li>Interfaces - Firewa</li> </ul>	I • Services •	VPN 🗸	Status 🗸	Diagnostics 👻	Help 🗸		G
WARNING: The 'admin' acc	ount password is set to the defai	ult value. Change the j	bassword in the	e User Manager.				
Package / Proxy	Server: Authenticatic	n / Authentic	ation					0
General Remote Cac	e Local Cache Antiv	irus ACLs	Traffic Mgmt	Authenticati	on Users	Real Time	Status	Sync
Squid Authentication	General Settings							
Authentication Method	Local			~				
	Select an authentication meth	od. This will allow use	rs to be auther	nticated by local o	r external service	s.		
Authentication Server	Enter the IP or hostname of th	e server that will perfo	orm the authent	tication here.				
Authentication server port	Enter the port to use to conne Leave this field blank to use th	ct to the authenticatio e authentication meth	n server here. nod's default po	ort.				
Authentication Prompt	Es necesario acceder mediar This string will be displayed at	te el uso de credencia the top of the authen	ales (usuario/co tication reques	ontra: t window.				
authentication Processes	5 The number of authenticator p	rocesses to spawn. If	many authenti	ications are exped	ted within a shor	t timeframe, incr	rease this num	ber accordingly.
Authentication TTL	5 This specifies for how long (in When the Time To Live expires	minutes) the proxy se , the user will be pron	erver assumes anpted for crede	an externally valio ntials again. Defa	ated username a ult: 5	nd password co	mbination to b	e valid.
Authentication Max User IP Addresses	Enforces a limit to the number	of unique IP address	es from which a	a single user can	ogin			

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



	Connection Settings		
Configure Pro	xy Access to the Internet		
🔘 No proxy			
Auto-detect p	proxy settings for this net <u>w</u> ork		
Use system p	roxy settings		
Manual proxy	configuration		
HTTP <mark>Proxy</mark>	192.168.30.1	<u>P</u> o	rt 3128
	Also use this proxy for HTTPS		
HTTPS Proxy			
SO <u>C</u> KS Host		Po	r <u>t</u> 0
(	⊃ SOC <u>K</u> S v4 💿 SOCKS <u>v</u> 5		
Automatic pre	oxy configuration URL		
No proxy for			
Example: .mozill	a.org, .net.nz, 192.168.1.0/24		
Connections to lo	ocalhost, 127.0.0.1/8, and ::1 are never proxied.		
Do not promp	ot for authentication if password is saved		
Proxy DNS wi	nen using SOCKS v5		
		Car	ncel OK

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

•	Authentication Required - Mozilla Firefox 🛛 🔍	3
R	The proxy moz-proxy://192.168.30.1:3128 is requesting a username and password. The site says: "Es necesario acceder mediante el uso de credenciales (usuario/contraseña)"	
Username		
Password		
	Cancel Sign in	

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

Blacklist	instagram.com <u>voutube</u> .com twitch. <u>tv</u> <u>departamentoinformaticaimpp</u> .com
	Destination domains that will be blocked for the users that are allowed to use the proxy. Put each entry on a separate line. You can also use regular expressions.

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









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

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

## Administración de Sistemas informáticos en Red Seguridad y Alta Disponibilidad



COMMUNITY EDITION	ystem 🗸	Interfaces 🗸	Firewall 🗕	Services 🗸	VPN -	Status 🗸	Diagnostics	← Help ←	¢
WARNING: The 'adm	iin' accoun	t password is set to tl	ne default value.	Change the pass	sword in the	User Manager.			
Proxy filter So	quidGu	ard: Times / I	Edit / Time	es					0
General settings	Commo	on ACL Groups /	ACL Target	categories	Times	Rewrites	Blacklist	Log XMLRPC Sync	
General Options	3								
Ni	ame ( E	βin_Internet inter a unique name o 'he name must consis	f this rule here. It between 2 and	15 symbols [a-Z	_0-9]. The fi	rst one must be	e a letter.		
Va	lues	Weekly Time type	<ul> <li>✓ all</li> <li>Days</li> </ul>		✓ Date	or Date range	 Tin	8:00-12:00	
	Add	+ Add							
Descrip	otion N E E	Ha hacer el desayuno 'ou may enter any des lote: Example for Date or Da Example for Time Ran	y menos nintien cription here for ate Range: 2007. ge: 08:00-18:00	do your reference. 12.31 or 2007.1	1.31-2007.1	2.31 or *.12.31	or 2007.*.31		
		Save							

of sense s	ystem 👻 Interf	aces 👻 🛛 Firew	vall - Services -	VPN 🗸	Status 🗸	Diagnostics		p <del>-</del>	¢	ļ
WARNING: The 'adn	nin' account passwo	rd is set to the def	fault value. Change the	password in th	ne User Manage	ır.				
Package / P	roxy filter Squ	uidGuard: T	imes / Times						0	
General settings	Common ACL	Groups ACL	Target categories	Times	Rewrites	Blacklist	Log	XMLRPC Sync		
Name	Des	scription								
Sin_Internet	Ha	a hacer el desayun	o y menos nintiendo					Ø	<b>m</b>	
								+	Add	
Save										

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





and another Com	anna 171 - Dennis 177 - Tempi estantea - Tempi - Bandina - Bandina - Lan - VIII 1977 Tempi
na setriga - Con	mention and and an estimation time mention technic to American
eral Options	
Disabled	Check this to disable this ACL rule.
Name	Sin_Internet
	Enter a unique norme of this rule here. The norme must constant between 2 and 15 symbols [a-2 6-9]. The first one must be a letter.
Urber	Select the new position for this ACL tern. ACLs are evaluated on a first-match source basis.
	Note:
	search for a surface w.c. by two sources we occur before the time match, in you want to denne an exception for some sources (P) from the P to put them on fact of the list.
	Example: ADL 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)	107 146 18 8/34
	III.
	Example:
	IP: 192.168.0.1 - Subret: 192.168.0.0/24 or 192.168.1.0/255.255.255.0 - IP-Range: 192.168.1.3 - 192.168.1.10 Domain: foo bar matches foo bar or *foo bar
	Username: 'user'' Ldas search (Ldas filter must be enabled in General Settings):
	Idapusersearch Idap.//192.168.0.100/DC=domain.DC=com?xAMAccountName?sub?(M/xAMAccountName=%x)
	(member 0+0x44 subt x+0xet x-xbt 0+0om an subt 0+0om)) Attention these line don't have break line, all on one line
Time	Sin Internet v
	which 'Target Rules' will operate or lasse 'how' for rales without time restriction. If this option is set then in off-time the second
	ruleset will operate.
Target Rules	tati (tati)
	Target Rules List
	Target Rules List 🔿 🔿 ACCESS: whitelist - always pass; Very' - block; 'allow' - pass, if not blocked.
	Target Rules List 🔿 🔿 ADCESS: 'whitefarf - always pass; 'deny' - block; 'allow' - pass, if not blocked. Target: Categories for off-time If These not served to success of the served
	Target Rules List • •       •         ADCESS: "whitelar - always pase, 'dery' - block,' tallow' - pase, if not blocked.       Target Categories for off-time         Target Categories       Target Categories for off-time         Default access [st]       access [dery • ]
Do not allow IP-	Target Rules List O O         ACCESS: 'white/of - sheavy pass, 'kery'-block; 'block; 'block' - pass, if not blocked         Target Categories for off-time         If Default access [at]         access [ati]
Do not allow IP- Addresses in UBL	Target Rules List O       O         ACCESS: 'whiteful - sheavy pass, 'kery' - block, 'allow' - pass, if not blocked.       Target. Categories for off-time         Target Categories       If Their minimum relies categories for off-time         Befault access [all]       access [all]       is categories         To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQON you can check this option. This option is no effect on the whitekst.
Do not allow IP- Addresses in URL Redirect mode	Target Rules List O O         ACCESS: 'whiteleff - sheavy pass, 'kery' - block, 'allow' - pass, if not blocked.         Target Categories for off-time         Torget Categories for off-time         0 Fault access [all]         access deny v         Default access access instead of the EQON you can check this option. This option in the whiteket.         Screet       v
Do not allow IP- Addresses in URL Redirect mode	Target Rules List C       C         ACCESS: 'whiteful - sheavy pass, 'kery' - block, 'allow' - pass, if not blocked.       Target Categories for off-time         Target Categories       If the model of the second off-time         If the model access [all]       access (deny v) Default access [all]         Default access [all]       access (deny v)         To make sure that people do not bypass the URL fiber by simply using the IP-Addresses instead of the EQON you can check this option. This of has no effect on the whiteket.         Incre       v)         Select redirect mode hare.         Note: 6' you can 'tarappenet proxy', then 'ter redeect mode will not accessible.
Do not allow IP- Addresses in URL Redirect mode	Target Rules List C C         ACCESS: 'whiteleff - sheavy pass, 'key' - block, 'allow' - pass, if not blocked.         Target Categories for off-time         It must construct the second device of the SQDN you can check this option. The offset not effect on the whitelet.         Increase       v         Select radiect indexid mode here.       v         Select radiect inclused interactional evicit radiese.       Notic if you can be a second with a second vicit and mode will not accessible.         Options: exist if an page, 'exist infinitive', 'exist and second evicit an found,'exist and and'exist.       Notic if you can be a second with a second will not accessible.
Do not allow IP- Addresses in URL Redirect mode Redirect	Target Rules List C C         ACCESS: 'whitefull' - sheavy pass, 'tery' - block, 'allow' - pass, if not blocked.         Target Categories         Target Categories         Cefsuit access [all]         access deny v         Default access [all]         access deny v         Select redeacd mode here.         Nets of pos us 'tarraparent prop', then 'inf redeact mode will not accessable.         Options entitient page_ ent urinedred_ ext urins frouvd_ entitient frouvd_
Do not allow IP- Addresses in URL Redirect mode Redirect	Target Rules List C C         ACCESS: 'whitefull' - sheavy pass, 'deny' - block, 'allow' - pass, if not blocked.         Target Categories       for off-time         Understand       Integer Categories         Default access [all]       access deny v         Default access for off-time       deny v         Interdeed mode here.       v         Note, fi pos tare "taraparent proy", then 'inf reduced mode will not accessable.       Cprisms esturies page, est universed and the second
Do not allow IP- Addresses in UR. Redirect mode Redirect	Target Rules List C C         ACCESS: whitelist - sheavy pass, they'-block, talow'-pass, if not blocked.         Target Categories       Target Categories for off-time         Orfset access [all       access deny v         Default access [all       access deny v         To make sure that people do not bypass the URL fiber by simply using the IP-Addresses instead of the FQDN you can check this option. The of has no effect on the wheelst.         score       v         Select reflect mode hare.         Note: if you can the first mode hare.         Options estating reduction URL, error message or size (bytes) bee.         To protect way children from addit content you can use the motioned mode of saarch enders.
Do not allow IP- Addresses in UR. Redirect mode Redirect SaleSearch engine	Target Rules List C C         ACCESS: 'whitelist' - sheary pass, 'deny' - block, 'allow' - pass, if not blocked.         Target Categories       Target Categories for off-time         Orfset access [all       access deny v         Default access [all       access deny v         In the auto effect on the wheelar.       access deny v         Select neited mode here.       v         Note: f you can 'transported proof, 'then 'trifeedeed mode will not accessible.       Cprions est unifeedeed.         Cytome estatement reduction URL, error message or size (bytes) bee.
Do not allow IP- Addresses in UR. Redirect mode Redirect SaleSearch engine	Target Rules List C C         ACCESS: 'whitefull' - sheavy pass, 'stery' - block, 'allow' - pass, if not blocked.         Target Categories       for off-time.         If made access [all]       access deny v behad access [all]       access deny v         Import on the same that people do not bypass the URL fiber by simply using the IP-Addresses instead of the FQON you can check this option. This of has no effect on the wheelan.       w         Select network mode here.       v         Select network mode here.       v         Actes of the saternal reduction URL, error message or size (bytes) here.       interments in supported by Google, Yardes, Yahoo, MDA, Live Search, Eng. DuckDacking, DenEserch, Rambler, Ecosis and Qwarr. Make no the saternal regimes.         At the moment is in supported by Google, Vardes, Yahoo, MDA, Live Search, Eng. DuckDacking, DenEserch, Rambler, Ecosis and Qwarr. Make no the search engines.         At the moment is in supported by Google, Vardes, Yahoo, MDA, Live Search, Eng. DuckDacking, DenEserch, Rambler, Ecosis and Qwarr. Make no the search engines.         At the moment is in supported by Google, Vardes, Yahoo, MDA, Live Search, Eng. DuckDacking, DenEserch, Rambler, Ecosis and Qwarr. Make no the search engines can be accessed it to proheit access to othere.
Do not allow IP- Addresses in UR. Redirect mode Redirect SafeSearch engine	Target Rules List C         ACCESS: 'whitelist' - sheary pass, they'- block, 'allow' - pass, if not blocked.         Target Categories       Target Categories for off-time         Orfset access [all       access         Default access [all       access         To make sure that people do not bypass the URL fiber by simply using the IP-Addresses instead of the FQDN you can check this option. The of has no effect on the wheelint.         more       v         Select neitest mode hare.         Note: if you can 'transported prov', then 'trif reduct mode will not accessible.         Options existent reduction URL, error message or size (bytes) here.         To protect your children from adult cortent you can use the protected mode of search engines.         At the moment it is supported by Google, Yandes, Yahoo, MDN, Live Search, Bing, DuckDackin, DeeEserch, Rambler, Ecosis and Qwart, Make sur the search engines.         Nets: This option overlike Reverte' aetting.
Do not allow IP- Addresses Is UR: Redirect mode Redirect SaleSearch engine Rewrite	Target Rules List C C         ACCESS: Whitelist - sheary pass, they'-block, 'allow'-pass, if not blocked.         Target Categories       Intrast Categories for off-time.         Intrast Categories       Intrast Categories for off-time.         Default access [all]       access         Import on the area that people do not bypass the URL fiber by simply using the IP-Addresses instead of the FQON you can check this option. This of has no effect on the whealar.         Import access fail       access         Select reflect mode hare.       v         Select reflect mode hare.       v         Cottons external reduction URL, error message or size (bytes) here.       Import access for off-time.         Import reflection URL, error message or size (bytes) here.       Import cotton while.         To protect your children from adult cortent you can use the protected mode of search ergines.       At the moment is is supported by Googis, Yandes, Yahos, MSN, Live Search, Bing, DuckDuckGo, DreSearch, Barribler, Ecosis and Qwarr, Make surther access to other.         Nate: This option overlides Tewarts entities       access to other.         Nate: This option overlides Tewarts entity.       v         Enter the worke condition nume for this rule or lease t black.       v         Enter the restered regines can be accessed. It is recommended to probabilit access to other.       Nate: This option overlides Tewarts entities.         The moment is auto to defined. <t< td=""></t<>
Do not allow IP- Addresses In UR: Redirect mode Redirect SaleSearch engine Rewrite	Target Rules List C         ACCESS: 'whitelef' - shary pars, 'tery' - block, 'allow' - pars, if not blocked.         Target Categories       Intrast Categories for off-time         Default access [all]       access         Default access [all]       access         Imped to the whealint.       Imped to the Whealint.         Imped to the whealint.       v         Select reflect on the whealint.       v         Select reflect mode here.       v         Note if you use 'transported prov', then 'ter reduct mode will not accessible.       Coptons external reduction URE, error message or size (bytes) here.         Imped to protect your children from adult cortext you can use the protected mode of search ergines.       At the moment it is supported by Googis, Yandes, Yahos, MSN, Live Search, Bing, DuckDuckSc, DireEsearch, Barrober, Ecosis and Qwart, Make sur the sarch engines.         Nate: This option oversides Tewarts witting       v         Incre (warits not default on rane for this rule or leave it blank.       v
Do not allow IP- Addresses In UR: Redirect mode Redirect SaleSearch engine Rewrite Newrite for off-time	Target Rules List C       C         ACCESS: 'whitelef' - sharp pars, they'- block, 'allow' - pars, if not blocked.         Target Categories       In reget Categories for off-time.         Default access [all       access         Default access [all       access         In take are that people do not bypara the URL fiber by simply using the IP-Addresses instead of the FQDN you can check this option. The of has no effect on the wheelint.         Incree       v         Select reflect mode hare.       v         Note if you use 'transporet prop', then 'inf' reduct mode will not accessible.       Cptons external reduction URL, error message or size (bytes) here.         Import you children from adult cortent you can use the protected mode of search ergines.       At the moment is is supported by Googis, Yandes, Yahos, MSN, Live Search, Bing, DuckDuckGo, DesEsearch, Barrober, Ecosis and Qwart, Make surther access to other.         Nate: fils option overlides Text atting       v         Enter the reverte condition name for this rule or leave it blank.       v         Increa (warits and defined)       v)         Enter the reverte condition name for this rule or leave it blank.       v
Do not allow IP- Addresses In UR: Redirect mode Redirect SaleSearch engine Rewrite Newrite for off-time	Target Rules List C         ACCESS: 'whitelef' - shary pars, 'tery' - block, 'allow' - pars, if not blocked.         Target Categories       Intrase material categories for off-time.         Default access [all]       access         Default access [all]       access         Intrase material categories       deny v         Select reflect mode here.       v         Select reflect mode here.       v         Select reflect mode here.       v         Default accessible.       Options external redirection URL, encore message or side (bytes) here.         Inter the selection URL, encore message or side (bytes) here.       Default access to othere.         National redirection URL, encore message or side (bytes) here.       Default access to othere.         National redirection URL, encoremended to prohibit access to othere.       National access the secret actegories.         At the moment it is supp
Do not allow IP- Addresses II UR: Redirect mode Redirect SeleSearch engine Rewrite Rewrite for off-time Description	Target Rules List © ●         ACCESS: 'which ist' - sharey pars, 'they' - block, 'allow' - pars, if not blocked.         Target Categories       Intrast Categories for off-time.         These material social way pars, 'they' - block, 'allow' - pars, if not blocked.       Intrast Categories for off-time.         Default access [all   acces [all   accces [all   acces [all   acces [all   acces [all   acces [all   ac

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.

## Administración de Sistemas informáticos en Red Seguridad y Alta Disponibilidad



Proxy filter SquidGuard: Times / Edit / Times									0		
General settings Co	ommon ACL	Groups ACL	Target categories	Times	Rewrites	Blacklist	Log	XMLRPC Sync			
General Options											
Name	Comprovar Enter a uniq The name m	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 Time type	~	all Days	♥ Da	te or Date range		00:00-23:59 Time range				
Add	+ Add										
Description	Comprovace You may ent Note: Example for Example for	tion ter any descriptio Date or Date Rar Time Range: 08:	n here for your referen <b>1ge:</b> 2007.12.31 <b>or</b> 200 00-18:00	ce. 17.11.31-2007	.12.31 or *.12.31	or 2007.*.:	31				

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 ruleset will operate.	s' will operate or leave 'none' for rules without time restriction. If this opti	on is set then in off-time the second
Target Rules	[all [ all]		
	Target Rules List 🔂 🗢		
	Target Rules List 🔿 🗢 ACCESS: 'whitelist' - always pass; 'de	rny' - block; 'allow' - pass, if not blocked.	
	Target Rules List	ny'-block; 'allow'- pass, if not blocked. Target Categories for off-time	_
	Target Rules List ♀ ● ACCESS: 'whitelist' - always pass;'de Target Categories	eny' - block; 'allow' - pass, if not blocked. Target Categories for off-time If 'Time' not defined, thi	s is column will be ignored.

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



😂 🏾 🎘 Kali Docs   Kali Linux Docu 🗵					✓ ● ● ⊗
< → C @	O https://www.kali.org/docs/				★
🛰 Kali Linux 👔 Kali Tools 🧧 Kali De					
The DZ - Volner ability A	ally where			1110 kali 20 0 4258 39720 21880 S 1025 regt 20 0 1018 14055 10124 5	0.0 1.9 0:00.00 /usr/b 0.0 0.7 0:00.17 / /usr/libe
OB - Web Applead     KALI	· Web Vulnerability Scamers		ET KALL BLOG DOCUMENTATION V	COMMUNITY COURSES COURSES	S Y ABOUT Y
CA - Database Assessment					0:0 0.7 0:00.00 //usr/\ 0:0 0.7 0:00.00 //usr/\
D5 - Mireless Attacks	Gave devices				0.0 0.7 0:00.11 - /usr/libe 0.0 0.7 0:00.01 - /usr/l
10 07 - Reverse Engineering		17 - 190			0.0 0.1 0:00.10 - xcape -e
🗰 08 - Exploitation Tools		Kall I	Docs		0.0 0.9 0:00.16 - xfcc4-pow
🗯 09 - Sniffing & Spoofing	wapiti				0.0 0.9 0:00.00 - sfcet-
10 - Pest Exploitation	M whatweb	Official Docu			0.0 1.0 0100.02 - stcs4- 0.0 1.0 0100.00 - sfce4-
11 - Forensics		Have a question? Type your key	words baral	987 root 20 8 2434 9464 6312 S 1987p - 25etup 1036arch 14Ft teet 155orted 16	0.0 0.5 0:00.24 - /usr/libe
12 - Reporting Tools	burpsuite	plave a question? Type your key	words here:		
1 42 - Kall & OffSec Links	🧳 commix				2 a x
		Find your ansy	ver by subiect		
		, interspectation			
		LIGHT 🔵	🔵 dark		
				0	
	Introduction	Installation	Virtualization	USB	
	What is Kali Linux & Kali's features	Installing Kali Linux on desktops	VMs-VMware VirtualBox Hyper-	Portable Kali on a USB drive/key	
https://www.kau.org/docs/usb/	the first of the states	in the second se		letick	😰 💿 👰 🗬 🖉 🗐 🗑 🔐 🦓 💽 CTRL DERECHA
Parc soleado		Q Búsqueda 🚯 🖬 🧊	) 🖬 C 💆 O 🖺 9 🕻	3 6 <sup>9</sup>	∧ 👃 ⊚ d0 🏍 18:58 🜲
					CH, 01/2024

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.

	System 👻	Interfaces 🕶	Firewall 🗸	Services 🗸	VPN 🗸	Status 👻	Diagnostics 🕶	Help 🗸			•
WARNING: The	'admin' account	t password is set to	the default valu	ue. Change the p	assword in the	User Manager.					
Package /	Proxy Se	rver: Access	Control /	ACLs							0
General F	Remote Cache	Local Cache	Antivirus	ACLs	Traffic Mgmt	Authentica	tion Users	Real Time	Status	Sync	
Squid Acces	s Control Li	sts									
Allowed	Subnets	192.168.30.10/3 192.168.30.12/3 192.168.30.14/3	30 30 30								
	E P W	nter subnets that an ut each entry on a s /hen 'Allow Users o	e allowed to us eparate line. n Interface' is c	e the proxy in Cl hecked on 'Gene	DR format. All t eral' tab, there i	he other subnet	ts won't be able to u d the 'Proxy Interfa	ise the proxy. ce(s)' subnet(s)	to this list.		

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



۲	▲ Warning: Potential Securi ×			× 000
		A Not Secure https://192.168.30.1	ជ	ල එ ≡
°⊂, Ka		s 🕱 Kali Forums 💰 Kali NetHunter 🛸 Exploit-DB 🛸 Google Hacking DB 🌔 OffSec		
		Marping: Dotontial Socurity Dick Aboad		
		Firefox detected a potential security threat and did not continue to <b>192.168.30.1</b> . If you visit this site, attackers cauld truth staal information like your parameters amale as credit and details.		
		attackets could try to steat information like your passwords, enhans, of credit card details.		
		Editando Conexión cableada 1 0 2		
		Nombre de la conexión Conexión cableada 1		
		General Cableada Seguridad 802.1x DCB Proxy Ajustes de IPv4 Ajustes de IPv6		
		Dirección		
		Dirección Máscara de red Puerta de enlace Añadir		
		192.168.30.20 24 192.168.30.1 Eliminar		
		Servidores DNS		
				🗏 🛃 🌠 🚫 💽 CTRL DERECHA
9	21°C Parc. soleado	📕 Q. Búsqueda 🛛 🕒 🧊 💼 🐂 🕲 🖄 🧔 🗳 💆 🚭	~ \$ @	d0 🆢 19:04 🌲

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.

🧆 🧧 pfSense.home.arpa - Pacl × 🕂									000
← → ♂ @ ○ & https://1	192.168.30.1/pkg_edit.php?xr							☆	ම එ ≡
🛰 Kali Linux 👩 Kali Tools 🚊 Kali Docs 🐹 Kali Forum	s 🖪 Kali NetHunter 🔺 Expl	loit-DB 🐞 Google Hacking DB 🏼 🌗							
	of sense System -						GÞ		
	WARNING: The 'admin' acco	ount password is set to the default va	alue. Change the password in t	he User Manag	er.				
	Package / Proxy	Server: Access Control	/ ACLs	No		Editando Conexión Conexión cableada 1	n cableada 1	<b>000</b>	
	General Remote Cach	e Local Cache Antivirus	ACLs Traffic Mgm	Aut	General Cableada	Seguridad 802.1x DC	CB Proxy Ajustes de IPv4	Ajustes de IPv6	
	Squid Access Control	Lists			Método Manual				
	Allowed Subnets	192.168.30.10/30 192.168.30.12/30			Dirección	Máscara de red	Puerta de enlace		
		192.168.30.14/30			192.168.30.10		192.168.30.1	Eliminar	
		Enter subnets that are allowed to u Put each entry on a separate line.	use the proxy in CIDR format. A	li the other					
		when Allow Osers on Interface is	checked on General tab, the	e is no nee	Dominios de búsqued				
	Unrestricted IPs								
		Enter unrestricted IP address(es) / this page.	network(s) in CIDR format. Co	nfigured e					
		Put each entry on a separate line.	0				Cance	ar 🗸 Guardar	
	Banned Hosts Addresses								
		Enter IP address(es) / network(s) in	in CIDR format. Configured ent	ies will NOT be	allowed to use the pro-	ev.			
							G	◙◙₽₽₽₽₽₽	🖁 🚯 💽 CTRL DERECHA
Parc. soleado		Q Búsqueda	🕒 🖬 🤨 💼	📮 🖸	🥴 🧿 🖺 💈	) 📮 🚭		^ ↓ ⊕ d0 ₩	19:05



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.

Sense Sy	stem <del>-</del> Interfaces <del>-</del>	Firewall 🗸 🗧	Services - VPN	N + Status +	Diagnostics <del>-</del>	Help <del>-</del>		G
WARNING: The 'admi	n' account password is set	to the default value.	Change the passwor	rd in the User Manag	ger.			
Package / Sq	uid / Monitor						C.	± 💷 🗐 🚱
General Remot	e Cache Local Cache	Antivirus	ACLs Traffic I	Mgmt Authen	tication Users	Real Time	Status	Sync
Filtering								
Max lines:	10 lines Max. line	s to be displayed.						
String filter:	Enter a g E.g.: use Use ! to i	rep-like string/patter mame, IP address, UI nvert the sense of m	n to filter the log ent RL. atching (to select no	ries.				
Squid Access Ta	ble			in the test of				
	and a state		Squid - A	ccess Logs		-		
Jate Squid Cacho Tab	IP Status	Addre	SS	User	Des	tination		
oquiù oucile rui			Squid - C	ache Logs				
Date-Time 01.01.1970 00:00:00 01.01.1970 00:00:00	Message Pinger exiting.		oquiu o					
29.01.2024 00:10:19 29.01.2024 00:10:19	Accepting HTTP S Finished loading N	ocket connections at IIME types and icons	conn1628 local=19	2.168.30.1:3128 rer	mote=[::] FD 39 flags=	9		
01.01.1970 00:00:00 01.01.1970 00:00:00 01.01.1970 00:00:00	ICMPv6 socket op ICMP socket open Initialising ICMP pi	ened ed.						
29.01.2024 00:10:19 29.01.2024 00:10:19	Pinger socket oper HTCP Disabled.	ned on FD 41						
29.01.2024 00:10:19	helperOpenServers	s: No 'basic_no	sa_auth' processes	needed.				
SquidGuard Tabl	•							
SquidGuard Tabl	e		Sec.120.	uard Logo				
SquidGuard Tabl	e	ACL	SquidG Address	uard Logs	н	ost	User	
SquidGuard Tabl Date-Time C-ICAP Virus Tal	e	ACL	SquidG Address	uard Logs	н	ost	User	
SquidGuard Tabl Date-Time C-ICAP Virus Tal	e Die	ACL	SquidGo Address C-ICAP -	uard Logs	Н	ost	User	



Si se puede configurar y ademas tenemos dos métodos de hacerlo dependiendo de que manera queremos 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.

	System 🗸	Interfaces 🗸	Firewall 🗸	Services 🗸	VPN -	Status 🗸	Diagnostics 🗸	Help 🗸		•		
WARNING: The	'admin' accou	nt password is set to	the default valu	ie. Change the	password in the	User Manager.						
Package / Proxy Server: Cache Management / Local Cache												
General F	lemote Cache	Local Cache	Antivirus	ACLs	Traffic Mgmt	Authentica	tion Users	Real Time	Status	Sync		
Squid Cache	e General S	ettings										
Disable	Disable Caching Disable caching completely. This may be required if Squid is only used as a proxy to audit website access.											
Cache Rep	acement	Heap LFUDA				~						
	Policy	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 1										
Low-Water	Mark in %	90										
		The low-water mark for AUFS/UFS/diskd cache object eviction by the cache_replacement_policy algorithm. 0										
High-Water M	Mark in %	95										
		The high-water mark	for AUFS/UFS/	diskd cache ob	ject eviction by t	the cache_repla	cement_policy algo	orithm. 🕕				
Do N	ot Cache	Enter domain(s) and	/or IP address(e	s) that should	never be cached	l. Put each entry	y on a separate line					

## **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.



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 "Trasparent Proxy Settings".

Package / Proxy Server: General Settings / General

Transparent Proxy Se	ettings
Transparent HTTP Proxy	Enable transparent mode to forward all requests for destination port 80 to the proxy server.     Important: 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)	WAN LAN 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 <b>source</b> IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall. <b>Applies only to transparent mode.</b> Separate entries by semi-colons (;)
Bypass Proxy for These Destination IPs	Do not proxy traffic going to these <b>destination</b> IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall. Applies only to transparent mode. Separate entries by semi-colons (;)

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 secilla 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 / Revers	se Proxy Server: General / General	0
General Web Servers	Mappings Redirects Real Time Sync	
Squid Reverse Proxy	General Settings	
Listen IP Version	IPv4 v Select the IP version Sauid Reverse Proxy will use to bind to.	
Reverse Proxy Interface(s)	WAN LAN loopback	
User Defined Reverse Proxy IPs	Squid will additionally bind to these user-defined IPs for reverse proxy operation. Separate entries by semi-colons (;)	
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	80 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	S 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	443 This is the port the HTTPS reverse proxy will listen on. <b>Default: 443</b>	
Reverse HTTPS Default Site	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		3.0.7_3	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.	前口
				Package Dependencies: Ø lighttpd-1.4.72 Ø 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.

COMMUNITY EDITION	n → Interfaces →	Firewall 🗕	Services 🗸	VPN -	Status 🗸	Diagnostics 👻	Help 🗸	G
WARNING: The 'admin' a	ccount password is set	to the default value	e. Change the p	assword in th	e User Manage	r.		
Package / Squi	d Proxy Reports	: Settings						C® 幸 ਘ 🗉 🕄
Instructions								
Perform these steps after instal	IMPORTANT: Click	Info and follow th	e instructions t	below if this is	initial install!	0		
Web Service Settin	gs							
Lightsquid Web Port	7445 Port the lighttpd we	eb server for Lights	squid will listen	on. (Default: 7	7445)			
Lightsquid Web SSL	. Vse SSL for Ligi This option configu	htsquid Web Acces ires the Lightsquid	ss I web server to u	use SSL and u	ses the WebGl	JI HTTPS certificate.		
Lightsquid Web Use	admin Username used to	access lighttpd. (D	)efault: admin)					
Lightsquid Web Password	Password used to a	access lighttpd. (D	efault: pfsense)	)				
Links	➡) Open Lightsqu	id 🎝 Open sqst	tat					

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.

Squid user access report							Home	
			Work Perio	d: Jan 2024				
			Cale	endar				
			20	)24				
			01 02 03 04 05 06	07 08 09 10 11 12				
							Top Sites	
Date	Group	Users	Oversize	Rutes	Average	Hit %	YEAR	MONTH
27 Jan 2024	Group	1	0	25 505	25 505	0.00%	Total	
27 Jan 2024	grp	1	0	33 393	33 393	0.00%	YEAR	MONTH
Total/Average:		1	0	35 595	35 595	0.00%	Group	
							YEAR	MONTH

LightSquid v1.8 (c) Sergey Erokhin AKA ESL