

Pfsense Bandwidth Management Squid and Squidguard

Martin Njau
Systems Administrator
KENET




Componentets

- Squid
- Squidguard/Dansguardian/
- Blacklist database-
Shallalist/MESD/Urlblacklist.com – this
blacklists can also work with some firewall –
e.g Ipcop, Ipfire
- Basic configuration parameters/details

Configuration settings

- Install squid package.
- Install squidguard package.
- Enable squid service.
- Configure transparent proxy settings/interface:NB do not leave this option unselected.(open proxies)
- Configure Acl's
- Download blacklist database.
- Enable squidguard service.

Install squid/squidguard package

squid	Network	Stable 2.7.9 pkg v.4.3.1 platform: 1.2.1	No info, check the forum	High performance web proxy cache. →	
squid3	Network	DISCONTINUED on pfSense 1.2.x 3.1.14_0.1 platform: 1.2.1	No info, check the forum	DISCONTINUED on pfSense 1.2.x [EXPERIMENTAL! Not all directives are ported yet! High performance web proxy cache.]	
squidGuard	Network Management	Beta 1.4_3 pkg v.1.9 platform: 1.1	No info, check the forum	High performance web proxy URL filter. Requires proxy Squid package. →	

Cont..

1.2.3 RELEASE packages Installed packages Package Installer

Installing squid and its dependencies.

Downloading package configuration file... done.
Saving updated package information... done.
Downloading squid and its dependencies...

squid-2.7.9 30%

Confirm is package is installed



Configuring Proxy Server Package

General Upstream Proxy Cache Mgmt Access Control Traffic Mgmt Auth Settings Local Users

Proxy interface

WAN
LAN
loopback

The interface(s) the proxy server will bind to.

Allow users on interface ☐

If this field is checked, the users connected to the interface selected in the 'Proxy interface' field will be allowed to use the proxy, i.e., there will be no need to add the interface's subnet to the list of allowed subnets. This is just a shortcut.

Transparent proxy ☒

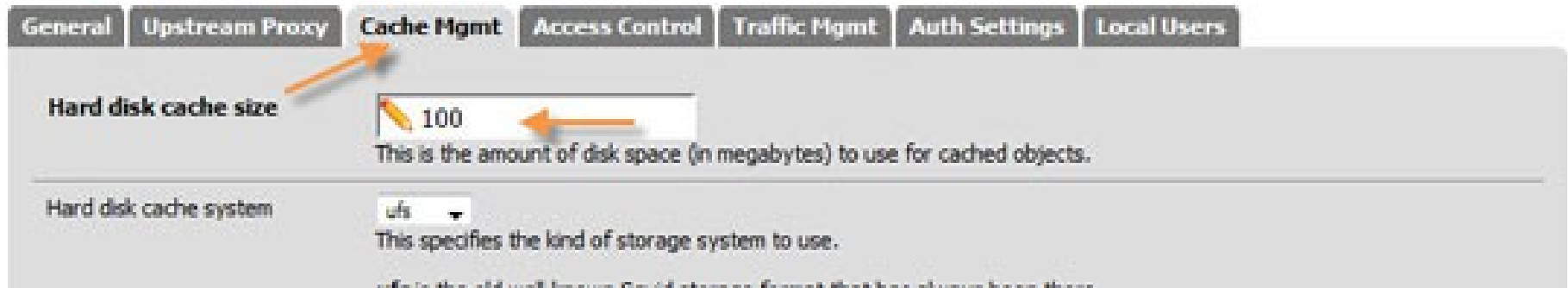
If transparent mode is enabled, all requests for destination port 80 will be forwarded to the proxy server without any additional configuration necessary.

Other Parameters

Enabled logging	<input checked="" type="checkbox"/>	This will enable the access log. Don't switch this on if you don't have much disk space left.
Log store directory	<input type="text" value="/var/squid/logs"/>	The directory where the log will be stored (note: do not end with a / mark)
Log rotate	<input type="text" value="7"/>	Defines how many days of logfiles will be kept. Rotation is disabled if left empty.
Proxy port	<input type="text" value="3128"/>	This is the port the proxy server will listen on.
ICP port	<input type="text"/>	This is the port the Proxy Server will send and receive ICP queries to and from neighbor caches. If left empty, don't want the proxy server to communicate with neighbor caches through ICP.
Visible hostname	<input type="text" value="proxy.pfsense.secure"/>	This is the URL to be displayed in proxy server error messages.
Administrator email	<input type="text" value="admin@pfsense.secure"/>	This is the email address displayed in error messages to the users.
Language	<input type="text" value="English"/>	Select the language in which the proxy server will display error messages to users.

Cache Management

Proxy server: Cache management



The screenshot shows the 'Cache Mgmt' tab in a proxy server configuration interface. It features two main settings: 'Hard disk cache size' and 'Hard disk cache system'. The 'Hard disk cache size' is set to 100 MB, with a description stating it's the amount of disk space in megabytes for cached objects. The 'Hard disk cache system' is set to 'ufs', with a description stating it specifies the kind of storage system to use. A help icon is visible in the top right corner.

General Upstream Proxy **Cache Mgmt** Access Control Traffic Mgmt Auth Settings Local Users

Hard disk cache size This is the amount of disk space (in megabytes) to use for cached objects.

Hard disk cache system This specifies the kind of storage system to use.

Access Control

Proxy server: Access control



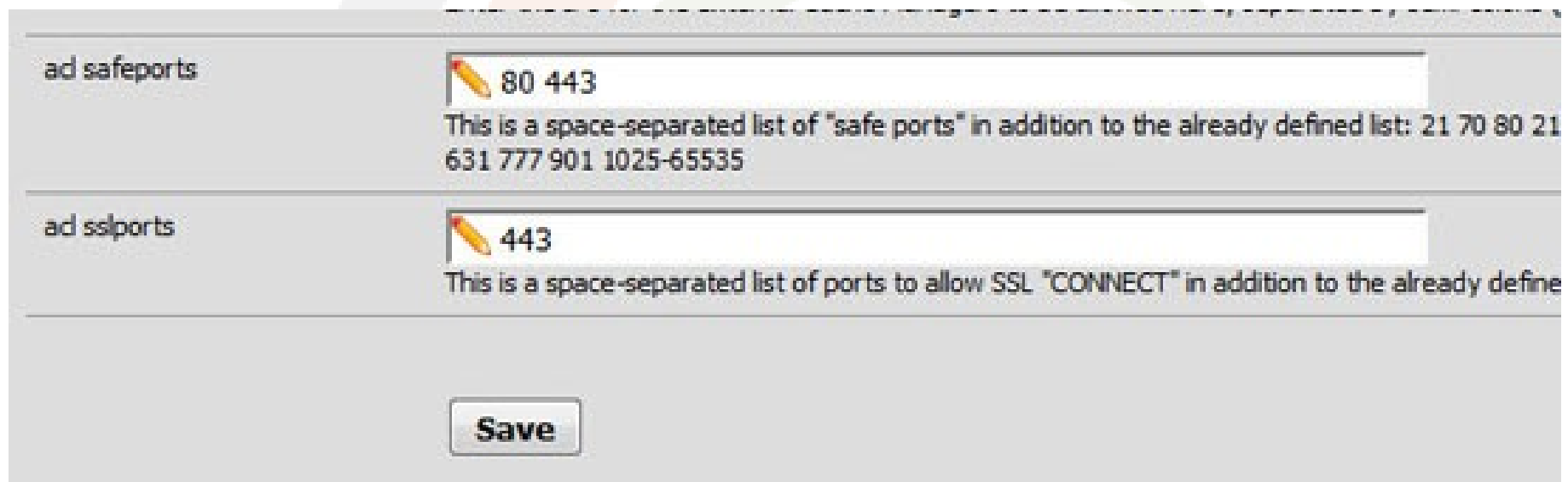
General Upstream Proxy Cache Mgmt **Access Control** Traffic Mgmt Auth Settings Local Users

Allowed subnets

```
192.168.255.0/24
192.168.254.0/24
```

Enter each subnet on a new line that is allowed to use the proxy. The subnets must be expressed as CIDR ranges (e.g.: 192.168.1.0/24). Note that the proxy interface subnet is already an allowed subnet. All the other subnets won't be able to use the proxy.

Safe and SSL ports

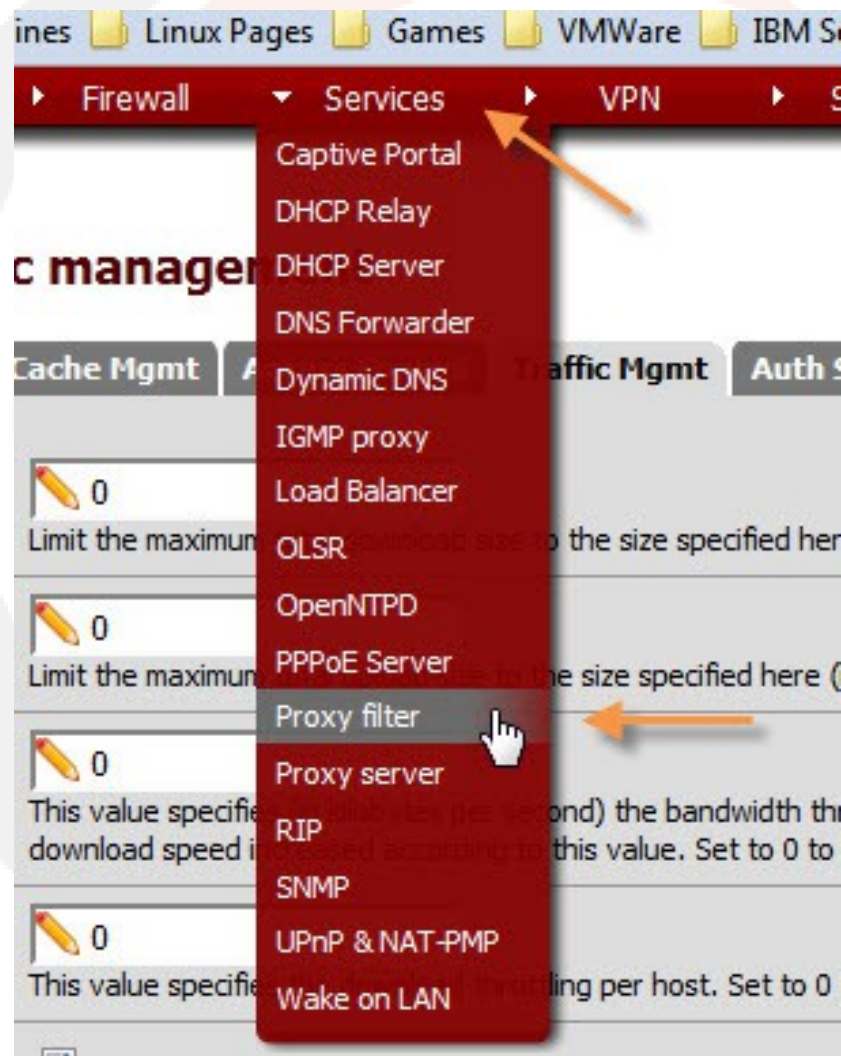


The screenshot shows a configuration window with two sections. The first section, labeled 'ad safeports', contains a text input field with the value '80 443' and a pencil icon. Below the input field is a descriptive text: 'This is a space-separated list of "safe ports" in addition to the already defined list: 21 70 80 21 631 777 901 1025-65535'. The second section, labeled 'ad sslports', contains a text input field with the value '443' and a pencil icon. Below this input field is a descriptive text: 'This is a space-separated list of ports to allow SSL "CONNECT" in addition to the already define'. At the bottom of the window is a 'Save' button.

Configuration Section	Value	Description
ad safeports	80 443	This is a space-separated list of "safe ports" in addition to the already defined list: 21 70 80 21 631 777 901 1025-65535
ad sslports	443	This is a space-separated list of ports to allow SSL "CONNECT" in addition to the already define

Save

Configuring squidguard filtering



Squidguard general settings

Proxy filter SquidGuard: General settings

General settings	Common ACL	Groups ACL	Target categories	Times	Rewrites	Blacklist	Log
Enable	<div><input checked="" type="checkbox"/></div> <p>Check this for enable squidGuard</p> <p>For saving configuration YOU need click button 'Save' on bottom of page</p> <p>After changing configuration squidGuard you must apply all changes</p> <div><input type="button" value="Apply"/></div> <p>SquidGuard service state: STARTED</p>						
Enable GUI log	<div><input checked="" type="checkbox"/></div> <p>Check this for enable GUI log.</p>						
Enable log	<div><input checked="" type="checkbox"/></div> <p>Check this for enable log of the proxy filter. Usually log used for testing filter settings.</p>						
Enable log rotation	<div><input type="checkbox"/></div> <p>Check this for enable daily rotate a log of the proxy filter. Use this option for limit log file size.</p>						
Clean Advertising	<div><input type="checkbox"/></div> <p>Check this to display a blank gif image instead the default block page. With this option you get a clear</p>						

Blacklist Options


Blacklist options

Blacklist

☒

Check this 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

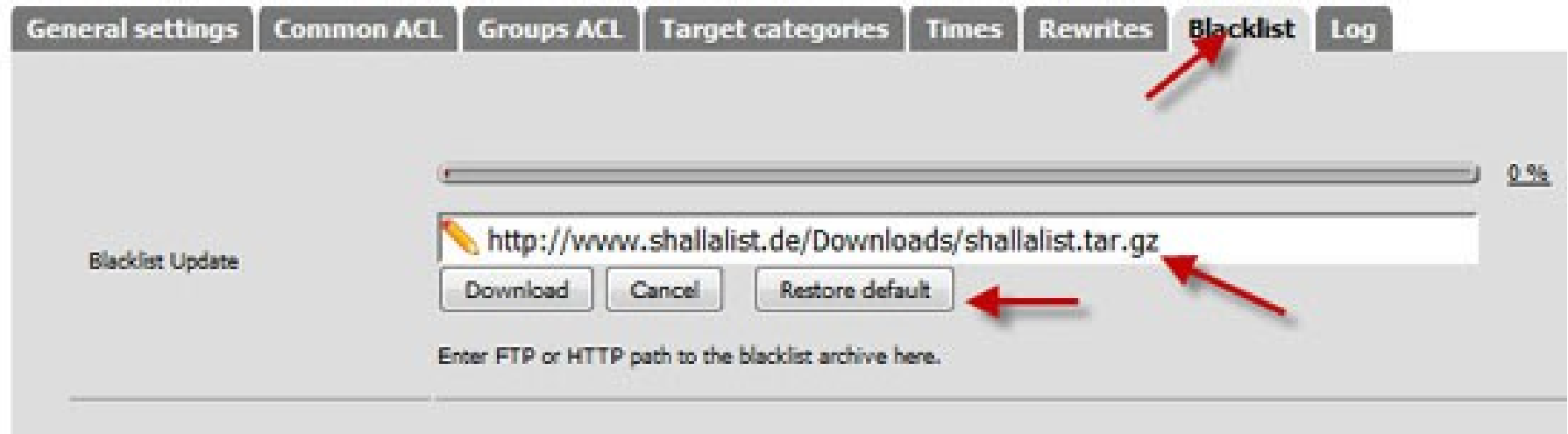


<http://www.shallist.de/Downloads/shallalist.tar.gz>
Enter FTP, HTTP or LOCAL (firewall) URL blacklist archive, or leave blank.

Save

download the database

Proxy filter SquidGuard: Blacklist page




The screenshot shows the SquidGuard web interface. At the top, there is a navigation bar with tabs: General settings, Common ACL, Groups ACL, Target categories, Times, Rewrites, Blacklist, and Log. The 'Blacklist' tab is selected and highlighted with a red arrow. Below the navigation bar, there is a progress bar at 0%. The main content area is titled 'Blacklist Update' and contains a text input field with the URL 'http://www.shallalist.de/Downloads/shallalist.tar.gz'. Below the input field are three buttons: 'Download', 'Cancel', and 'Restore default'. The 'Download' button is highlighted with a red arrow. Below the buttons, there is a text label: 'Enter FTP or HTTP path to the blacklist archive here.'

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

Blacklist Update

0 %




Enter FTP or HTTP path to the blacklist archive here.

Cont..

Proxy filter SquidGuard: Blacklist page

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

Blacklist DB rebuild progress 60 %

Blacklist Update 

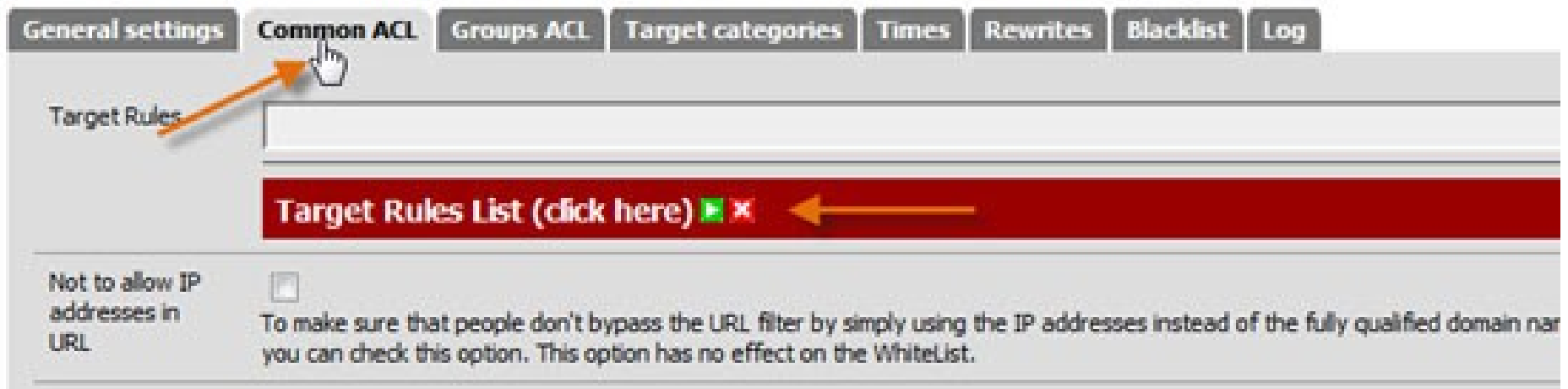
Enter FTP or HTTP path to the blacklist archive here.

Blacklist update Log

```
Begin blacklist update
Start download.
Download archive http://www.shallalist.de/Downloads
/shallalist.tar.gz
Download complete
Unpack archive
Scan blacklist categories.
Found 74 items.
Start rebuild DB.
Completed 60 %
```





Enable target rule lists

Proxy filter SquidGuard: Common Access Control List (ACL)



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

Target Rules

Target Rules List (click here)   

Not to allow IP addresses in URL ☐

To make sure that people don't bypass the URL filter by simply using the IP addresses instead of the fully qualified domain name you can check this option. This option has no effect on the WhiteList.

Cont..

Target Rules List (click here)

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

Target Categories

[blk_EI_adv]	access	deny
[blk_EI_aggressive]	access	deny
[blk_EI_alcohol]	access	---
[blk_EI_anonvpn]	access	---
[blk_EI_automobile_bikes]	access	whitelist
[blk_EI_automobile_boats]	access	whitelist
[blk_EI_automobile_cars]	access	allow
[blk_EI_automobile_planes]	access	allow
[blk_EI_chat]	access	---
[blk_EI_costtraps]	access	---
[blk_EI_dating]	access	---
[blk_EI_downloads]	access	---

Cont...

Proxy Denied Error	<input type="text" value="Request denied by \$g['product_name'] proxy"/>
	The first part of the error message displayed to clients when denied. Defaults to "Request denied by \$g['product_name'] proxy"
Redirect mode	<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: ext url err page , ext url redirect , ext url as 'move' , ext url as 'found'.
Redirect info	<input type="text"/>
	Enter external redirection URL, error message or size (bytes) here.
Use SafeSearch engine	<input type="checkbox"/>
	To protect your children from adult content, you can use the protected mode of search engines. Now it is supported by Google, Yandex, Yahoo, MSN, Live Search, Bing. Make sure that the search engines can, and others, it is recommended to prohibit. Note: ! This option overrides 'Rewrite' setting. !
Rewrite	<input type="text" value="none (rewrite not defined)"/>
	Enter rewrite condition name for this rule, or leave blank.
Log	<input checked="" type="checkbox"/>
	Check this for log this item.
<input type="button" value="Save"/>	

NB

- Ensure that you configure an implicit allow to avoid blocking all traffic.

*Transforming education
through ICT*

Thank You

www.kenet.or.ke

Jomo Kenyatta Memorial
Library, University of Nairobi
P. O Box 30244-00100, Nairobi.
0732 150 500 / 0703 044 500