

Что такое squidGuard

SquidGuard это RL фильтр для прокси сервера squid. Он позволяет гибко фильтровать запрашиваемые пользователем страницы в соответствии с настроенными правилами доступа. Фильтр URL может осуществляться по ссылкам, доменам, регулярным выражениям. Имеется возможность задавать отдельные правила для групп разных пользователей.

Кроме блокирования страниц пользователь может быть перенаправлен на указанную страницу / сайт, либо его запрос может быть прозрачно заменен на нужную ссылку.

В пакете реализованы готовые настройки safeSearch (безопасный поиск) для нескольких поисковых систем

Начальные настройки

После установки squidGuard необходимо сделать начальные настройки на странице General settings.

Прежде всего включаем чекбокс Enable для разрешения запуска squidGuard и решаем,

будет ли использоваться блэклист (опции

Blacklist

) — готовая база данных разных

URL

по категориям.

При использовании блэклиста его нужно загрузить со стороннего сайта.

Proxy Content filter SquidGuard: General settings

General settings	Default	ACL	Destinations	Times	Rewrites	Log
Enable	<input type="checkbox"/>	Check this for enable squidGuard For saving configuration YOU need click button 'Save' on bottom of page After changing configuration squidGuard you must apply all changes <input type="button" value="Apply"/> SquidGuard service state: STARTED				
Blacklist	<input checked="" type="checkbox"/>	Check this for enable blacklist				
Blacklist proxy	<input type="text"/>	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	<input type="text" value="/var/tmp/_sg_blacklists.tar"/>	Enter FTP, HTTP or LOCAL (pfSense) URL blacklist archive, or leave blank. <input type="button" value="Upload Url"/> <input type="button" value="Restore last"/>				
View GUI log	<input type="checkbox"/>	Check this for view GUI log				
<input type="button" value="Save"/>						

Шаги:

Страница General Settings

- Включить опцию Enable
- Если используем Blacklist, включаем опцию Blacklist.
- Сохраняем настройки кнопкой Save

Если используем Blacklist, то загружаем базу данных со стороннего сайта

- Ввести в поле Blacklist URL адрес архива блэклиста (к примеру <http://www.shallalist.de/Downloads/shallalist.tar.gz>)
);
- Нажать кнопку Upload URL и ждать пока закончится загрузка.
- В течении следующих 10-30 минут после загрузки будет происходить перестройка

внутренней базы, поэтому придется некоторое время подождать еще. Статус будет отображаться в поле Enable.

Замечания по Blacklist:

Если вы переустановили squidGuard, который до этого работал с blacklist, то базу данных можно попытаться восстановить кнопкой

RestoreLast

, или загрузить локальную копию архива (путь

Blacklist URL

=

/

tmp/blacklist.tar.gz

).

Кстати, если вы захотите задать вопрос о функции автоматическом обновлении блэклиста, то посмотрите на время обновления базы. Эта функция не добавлена именно из-за очень долгой процедуры обработки архива программой squidGuard.

Переходим на страницу DefaultPage

Здесь содержатся общие настройки для пользователей для которых не определены особые правила фильтрации. Для базовой настройки достаточно заполнить эту страницу.

Если был включен и загружен блэклист, то Destination rules будет содержать список категорий базы данных адресов, как на рисунке ниже. Иначе, будет присутствовать только строка [all] (нижняя в списке). .

Default access самая

Proxy Content filter SquidGuard: Default

General settings Default ACL Destinations Times Rewrites Log

Default destination

Rules priority: [1]: 'white'(whitelist); [2]: 'deny'(blacklist); [3]: 'allow'; [4]: end-rule('allow' ro 'deny'). For permit of the exceptions from blacklist, use 'white' option.

Destination rules	
[blk_BL_adv]	access [dropdown]
[blk_BL_aggressive]	access [dropdown]
[blk_BL_automobile_bikes]	access [dropdown]
[blk_BL_automobile_boats]	access [dropdown]

[blk_BL_webradio]	access white [dropdown]
[blk_BL_webtv]	access white [dropdown]
Default access [all]	access allow [dropdown]

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 names, you can check this option.

Описание:

Default Destination—это поле содержит правила фильтрации адресов URL. Каждое из правил может иметь

4

состояния

:

- - -

не определено

категория адресов не будет фильтроваться

white

белый список

адреса

URL

из этой кате

allow

разрешено

разрешение адресов из этой категории. Адреса

этой катего

deny

запрещено

запрещение адресов

URL

из этой кате

Самое последнее правило Default access [all]—самое важное. Оно определяет как будут

обрабатываться все прочие адреса URL,
которые не попали не в одну из выбранных категорий. Эта опция имеет всего два
состояния

: allow

и

deny.

Можно запретить `_все_` и разрешить только некоторые категории адресов правилами
выше. А можно разрешить `_все_` и исключить некоторые нежелательные категории
адресов.

Вид страницы со свернутым набором правил:

General settings **Default** **ACL** **Destinations** **Times** **Rewrites** **Log**

Default destination

Destination ruleset (click) + x

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 names, you can check this option.

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

Spec: Use safe search engine
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. Make sure that the search engines can, and others, it is recommended to prohibit.
Note: ! This option overrides 'Rewrite' setting. !

Rewrite
Enter rewrite condition name for this rule, or leave blank.

Enable log
Check this for enable log.

На странице Destination rules задает правила для разных категорий адресов URL addresses.
Помогает избежать попадания нежелательного контента на компьютер. Например, для Low Safe Search.
тут тут