

Servidor Cache Proxy HTTP/HTTPS Transparente Squid no pfSense com filtro de conteúdo SquidGuard e antivírus integrado ClamAV.

1-Criar um Certificado de Autoridade interno (Certificate Authority).
“System/ Certificate Manager/CAs” +Add

System / Certificate Manager / CAs / Edit

CAs **Certificates** **Certificate Revocation**

Create / Edit CA

Descriptive name Squid

Method Create an internal Certificate Authority

Internal Certificate Authority

Key length (bits) 2048

Digest Algorithm sha256
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

Lifetime (days) 3650

Country Code BR

State or Province e.g. Texas

City e.g. Austin

Organization e.g. My Company Inc

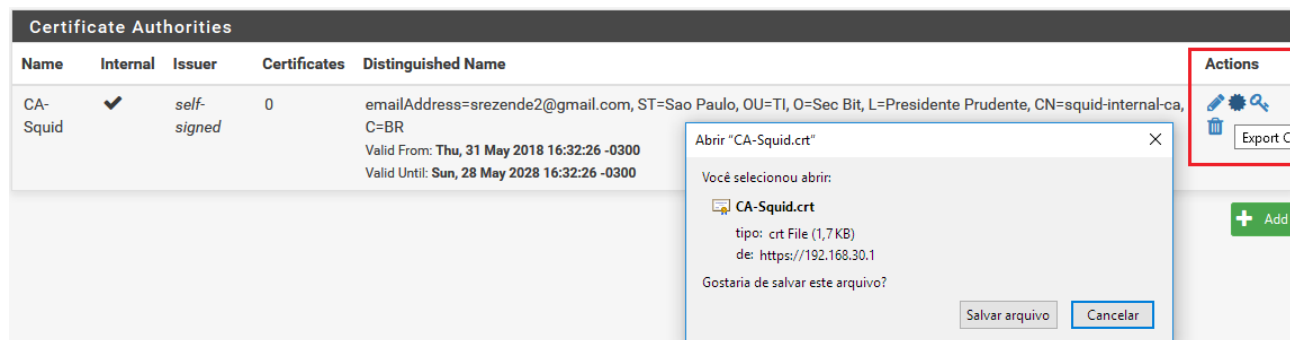
Organizational Unit e.g. My Department Name (optional)

Email Address e.g. admin@mycompany.com

Common Name squid-internal-ca

Save

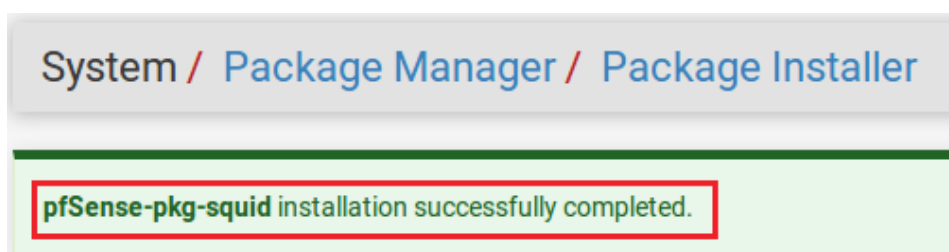
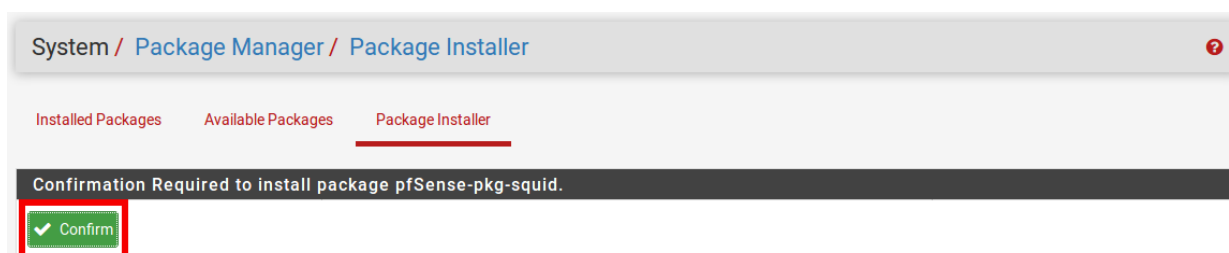
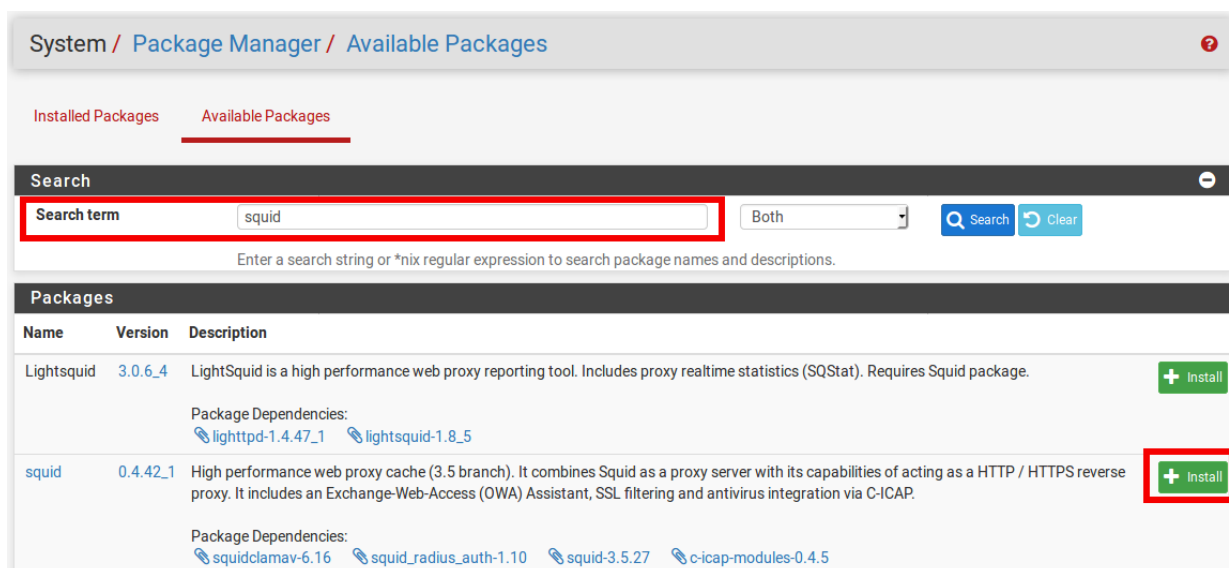
2-Importar o certificado para navegadores (IE, Firefox).



- Windows “Painel de Controle/Rede e Internet/Opções de Internet/Conteúdo/Certificados/Autoridades de Certificação Raiz Confiáveis/Importar”
- Firefox “Abrir Menu/Opções/Privacidade e Segurança/Certificados/Ver Certificados/Autoridades/Importar”

3-Instalar o pacote do Squid.

“System/Package Manager/Available Packages” +Install



4-Configurar o cache do Servidor Proxy Squid. “Services/Squid Proxy Server/Local Cache”

Obs: Para cada 1 GB de armazenamento do cache em disco é necessário 14 MB de memória RAM.

Ex: Para 100 GB de armazenamento é necessário reservar 1.4 GB de memória RAM sem contar com a quantidade de memória RAM utilizada pelo serviço do Squid.

Squid Hard Disk Cache Settings

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

Hard Disk Cache System
This specifies the kind of storage system to use. [i](#)

Clear Disk Cache NOW Hard Disk Cache is automatically managed by swapstate_check.php script which is scheduled to run daily via cron. [i](#)
If you wish to clear cache **immediately**, click this button **once**:

Level 1 Directories
Specifies the number of Level 1 directories for the hard disk cache. [i](#)

Hard Disk Cache Location
This is the directory where the cache will be stored. Default: /var/squid/cache [i](#)

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

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

Obs: Para tamanho de memória de cache nunca ultrapasse mais de 50% da memória física instalada.

Squid Memory Cache Settings

Memory Cache Size
Specifies the ideal amount of physical RAM (in megabytes) to be used for In-Transit objects, Hot Objects and Negative-Cached objects. Minimum value: 1 (MB). Default: 64 (MB) [i](#)

Maximum Object Size in RAM
Objects greater than this size (in kilobytes) will not be attempted to kept in the memory cache. Default: 256 (KB)

Memory Replacement Policy
The memory replacement policy determines which objects are purged from memory when space is needed. Default: heap GDSF [i](#)

Dynamic and Update Content

Cache Dynamic Content ☒ Select to enable caching of dynamic content.
With **dynamic cache** enabled, you can also apply refresh_patterns to sites like Windows Updates. [i](#)

Custom refresh_patterns
Enter custom refresh_patterns for better dynamic cache usage.
Note: These refresh_patterns will only be included if 'Cache Dynamic Content' is enabled.

5-Configurar opções gerais do Servidor Proxy Squid.

“Services/Squid Proxy Server/General”

- Ativar Squid Proxy, selecionar interface (**LAN, Loopback**).

Squid General Settings	
Enable Squid Proxy	<input checked="" type="checkbox"/> Check to enable the Squid proxy. Important: 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. Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.
Proxy Interface(s)	<div><div>LAN</div><div>WAN</div><div>loopback</div></div> <p>The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.</p>
Proxy Port	<input type="text" value="3128"/> This is the port the proxy server will listen on. Default: 3128
ICP Port	<input type="text"/> 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.
Patch Captive Portal	This feature was removed - see Bug #5594 for details!
Resolve DNS IPv4 First	<input type="checkbox"/> Enable this to force DNS IPv4 lookup first. This option is very useful if you have problems accessing HTTPS sites.
Disable ICMP	<input type="checkbox"/> Check this to disable Squid ICMP pinger helper.

- Ativar modo de Proxy transparente na interface “**LAN**”.

Transparent Proxy Settings	
Transparent HTTP Proxy	<input checked="" type="checkbox"/> Enable transparent mode to forward all requests for destination port 80 to the proxy server. 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)	<div><div>LAN</div><div>WAN</div></div> <p>The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.</p>
Bypass Proxy for Private Address Destination	<input type="checkbox"/> Do not forward traffic to Private Address Space (RFC 1918) destinations. Destinations in Private Address Space (RFC 1918) are passed directly through the firewall, not through the proxy server.
Bypass Proxy for These Source IPs	<input type="text"/> 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	<div><input type="text" value="InternetBank"/></div> <p>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 (;)</p>

Obs: Em alguns casos será necessário criar “**Alias**” para permitir que algum host definido ou liberar acessos para endereços de redes externas na Internet sem passar pelo Servidor Proxy Squid.
“**Firewall/Aliases/IP**” +Add ou Import”.

- Ativar filtro SSL “**Man In The Middle**” para interceptar trafego HTTPS.

Obs: Selecionar o Certificado de Autoridade interno criado para o Servidor Proxy Squid.

SSL Man In the Middle Filtering

HTTPS/SSL Interception ☒ Enable SSL filtering.

SSL/MITM Mode Splice Whitelist, Bump Otherwise

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.](#) [i](#)

SSL Intercept Interface(s) LAN
WAN

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

SSL Proxy Port 3129

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

SSL Proxy Compatibility Mode Intermediate

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

DHParams Key Size 2048 (default)

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

CA squidCA

Select Certificate Authority to use when SSL interception is enabled. [i](#)

SSL Certificate Daemon Children 100

This is the number of SSL certificate daemon children to start. May need to be increased in busy environments. Default: 5

Remote Cert Checks Accept remote server certificate with errors
Do not verify remote certificate

Select remote SSL certificate checks to perform. Use CTRL + click to select multiple options.

Certificate Adapt Sets the "Not After" (setValidAfter)
Sets the "Not Before" (setValidBefore)
Sets CN property (setCommonName)

See [sslproxy_cert_adapt directive documentation](#) and [Mimic original SSL server certificate wiki article](#) for details.

- Ativar e configurar a rotacionamento de “**Logs**”.

Logging Settings

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

Log Store Directory /var/squid/logs

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 7

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.](#) [i](#)

- Configurar as mensagens de erros e salvar para finalizar as configurações do Servidor Proxy Squid.

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.

6-Instalar o pacote SquidGuard para filtrar o conteúdo web. “System/Package Manager/Available Packages” +Install

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
squidGuard	1.16.4	High performance web proxy URL filter. Package Dependencies: squidguard-1.4_15

System / Package Manager / Package Installer

Installed Packages Available Packages Package Installer

Confirmation Required to install package pfSense-pkg-squidGuard.

7-Configurar uma categoria alvo para o SquidGuard.

“Services/SquidGuard Proxy Filter/Target Categories” +Add

Package / Proxy filter SquidGuard: Target categories / Target categories

General settings

Common ACL

Groups ACL

Target categories

Times

Rewrites

Blacklist

Log

XMLRPC Sync

Name	Redirect	Description
<div>+ Add</div>		

Save

General Options

Name

BlockProxySites

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 target category. Target categories are listed in this order on ACLs and are matched from the top down in sequence.

Domain List

torproject.org cometbird.com opera.com okayfreedom.com
revolucaodosbytes.pt hideman.net toolur.com hosttime.com.br
smartdnsproxy.com 10bestvpns.com expressvpn.com hsselite.com
safervpn.com safervpn.com hotvpn.com zoogvpn.com
bestproxyandvpn.com luminati.io shader.io hidemy.name
proxyservers.pro myprivateproxy.net proxydb.net hidemyass.com
proxybay.one

Enter destination domains or IP-addresses here. To separate them use space.
Example: mail.ru e-mail.ru yahoo.com 192.168.1.1

Redirect mode

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

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

Description

Block Proxy Sites

You may enter any description here for your reference.

Log

☒ Check this option to enable logging for this ACL.

Save

8-Configurar uma Blacklist para o SquidGuard. “Services/SquidGuard Proxy Filter/General settings”

<http://www.shallalist.de/Downloads/shallalist.tar.gz>

Blacklist options


Blacklist ☒ Check this option to enable blacklist
Do NOT enable this on NanoBSD installs!

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).

 Save

9-Atualizar a Blacklist do SquidGuard. “Services/SquidGuard Proxy Filter/Blacklist” Download

Blacklist Update

0 %



 Download  Cancel 

Enter FTP or HTTP path to the blacklist archive here.

10-Defina as listas de controle do SquidGuard. “Services/SquidGuard Proxy Filter/Common ACL” Target Rules List + - deny allow whitelist

General Options

Target Rules

Target Rules List  

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

Target Categories	access	deny
Block Proxy Sites [Proxy_Sites]	access	deny
[blk_BL_adv]	access	----
[blk_BL_aggressive]	access	----
[blk_BL_alcohol]	access	----
[blk_BL_anonvpn]	access	deny
[blk_BL_automobile_bikes]	access	----
[blk_BL_automobile_boats]	access	----

11-Ative o serviço do SquidGuard.

“Services/SquidGuard Proxy Filter/General settings” Enable Apply

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: **STARTED**

12-Ative o serviço de Antivírus ClamAV integrado ao Squid e salve para aplicar as configurações. “Services/Squid Proxy Server/Antivírus”.

- Ative a verificação de vírus no Servidor Proxy Squid “**Enable AV**”.

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.

Google Safe Browsing

☒ Enables Google Safe Browsing support.

Google Safe Browsing database includes information about websites that may be [phishing sites](#) or [possible sources of malware](#).
Warning: This option consumes significant amount of RAM.

Exclude Audio/Video Streams

☒ This option disables antivirus scanning of streamed video and audio.

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

Regional ClamAV Database Update Mirror

none

Select a regional database mirror. **Note:** The default ClamAV database mirror performs extremely slow.
It is strongly recommended to choose a mirror here and/or configure your own mirrors manually below.

Optional ClamAV Database Update Servers

db.br.clamav.net

Enter ClamAV update servers here, or leave empty. Separate entries by semi-colons (;)
Note: For official update mirrors, use db.XY.clamav.net format. (Replace XY with your country code.)

Save

Show Advanced Options

13-Sobre o antivírus ClamAV.

O **“ClamAV”** é um antivírus de código aberto desenvolvido especialmente para sistemas operacionais Linux/BSD atualmente mantido pela Cisco, geralmente muito utilizado para escanear e-mails em conjunto com servidores **“MTA”** como o **“Postfix”**, detecta vírus, cavalos de troia, malwares, suporta múltiplos formatos de arquivos compactados, possui atualizações automáticas e frequentes de assinaturas de antivírus. O **“ClamAV”** pode ser integrado ao servidor proxy Squid criando mais uma camada de proteção contra ameaças na Internet analisando as páginas web armazenadas no cache do servidor Proxy Squid e protegendo o usuário contra possíveis sites infectados.

Testar antivírus ClamAV: <http://www.eicar.org/download/eicar.com>, <http://www.eicar.org/85-0-Download.html>, <https://www.amtso.org/>

14-Desempenho do cache em disco do Servidor Proxy Squid.

Um fator importante a considerar ao utilizar o Squid no pfSense é a performance de leitura e escrita do disco rígido **“I/O”** que terá impacto direto na performance do armazenamento e recuperação das páginas em cache. Para ambientes com mais de 200 estações de trabalho é altamente recomendado o uso de um **“SSD”** de alta velocidade e para ambientes de pequenas empresas um disco rígido **“HDD”** comum padrão **“Sata”** de 1.5 Gbp/s com largura de banda de 150 Mbp/s é suficiente.

O tamanho do cache do Squid também requer atenção em relação a quantidade de memória **“RAM”** instalada no Firewall pfSense, o cache do Squid consome aproximadamente 14 MB de RAM para cada 1 GB de cache armazenado em disco de um sistema operacional de arquitetura 64 bits. Para cada 100 GB de cache é necessário 1.4 GB de memória RAM sem contar a quantidade de memória para executar serviço do Squid.