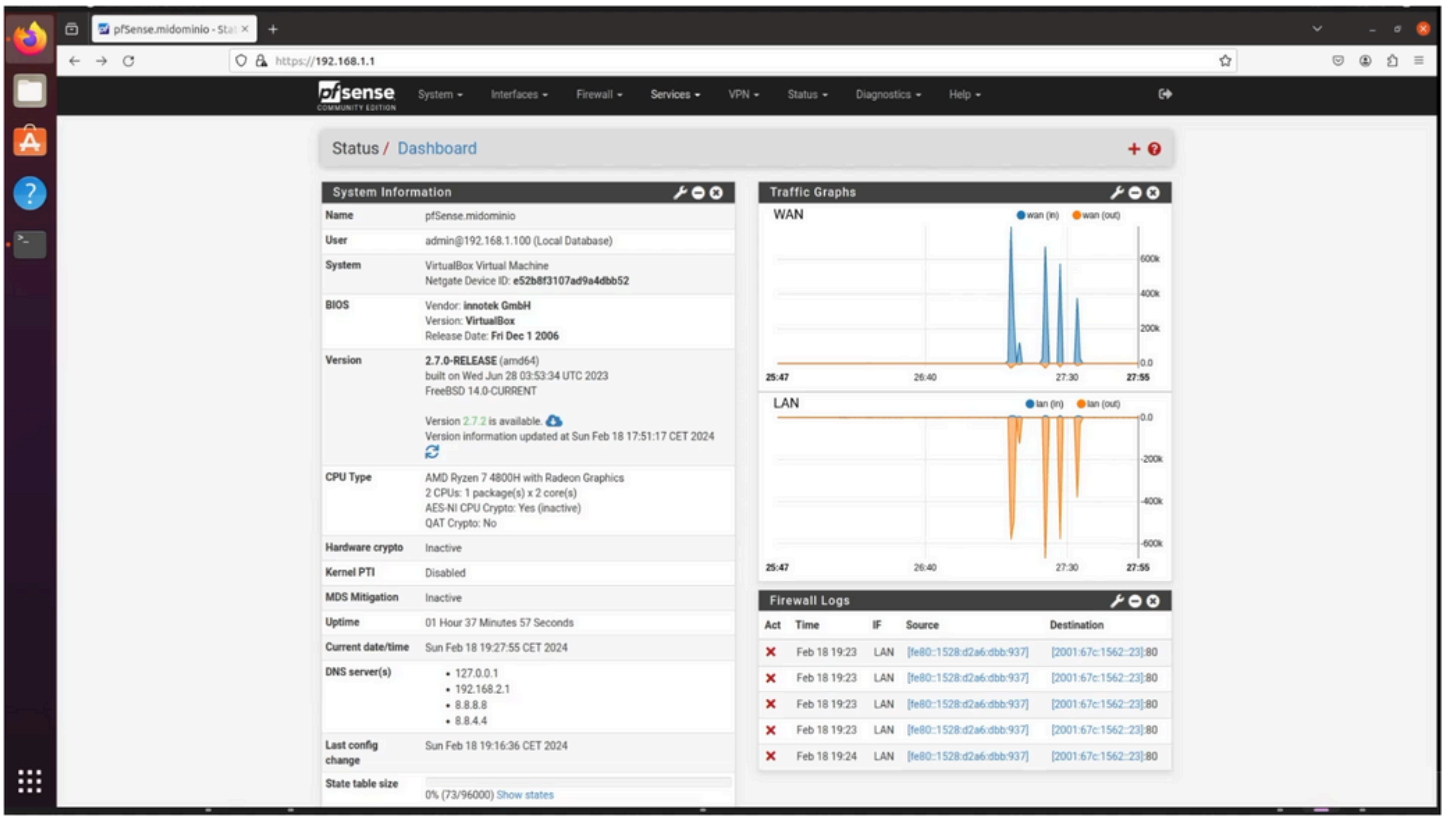
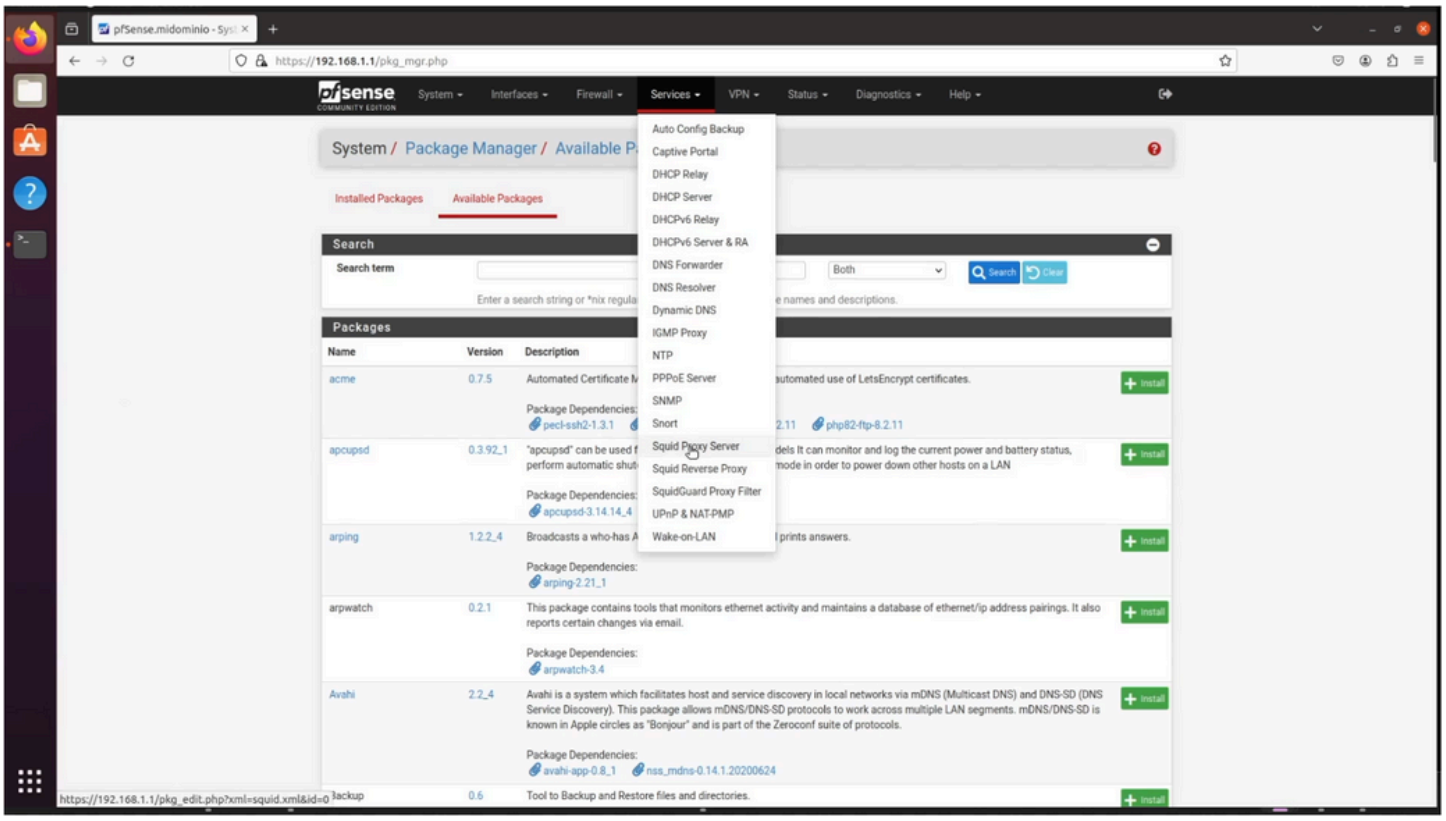
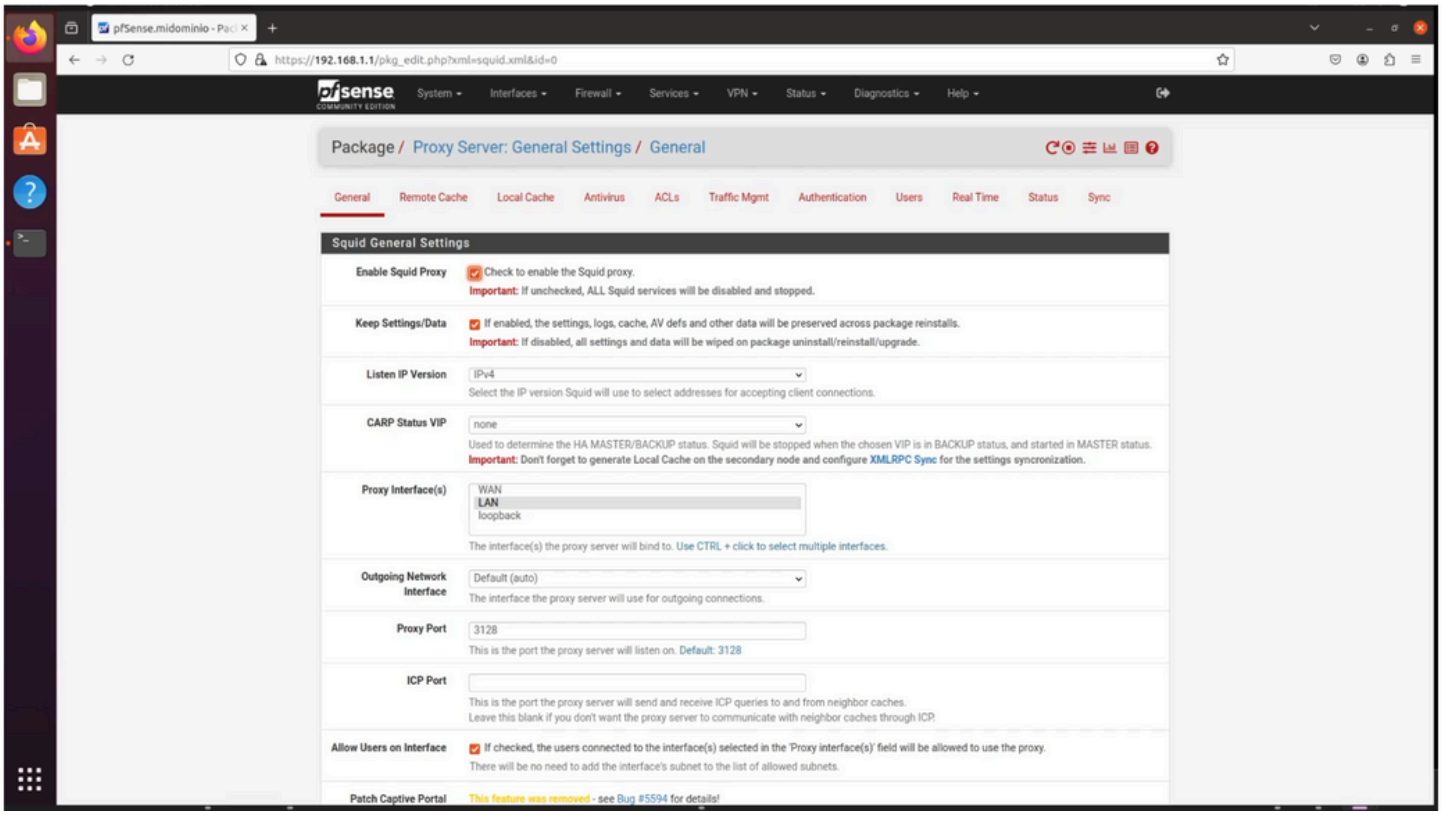

pfSense.midominio - Sta
https://192.168.1.1
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Status / Dashboard
System Information
Name pfSense.midominio
User admin@192.168.1.100 (Local Database)
System VirtualBox Virtual Machine
Netgate Device ID: e52b8f3107ad9a4dbb52
BIOS Vendor: innotek GmbH
Version: VirtualBox
Release Date: Fri Dec 1 2006
Version 2.7.0-RELEASE (amd64)
built on Wed Jun 28 03:53:34 UTC 2023
FreeBSD 14.0-CURRENT
Version 2.7.2 is available.
Version information updated at Sun Feb 18 17:51:17 CET 2024
CPU Type AMD Ryzen 7 4800H with Radeon Graphics
2 CPUs: 1 package(s) x 2 core(s)
AES-NI CPU Crypto: Yes (inactive)
QAT Crypto: No
Hardware crypto Inactive
Kernel PTI Disabled
MDS Mitigation Inactive
Uptime 01 Hour 37 Minutes 57 Seconds
Current date/time Sun Feb 18 19:27:55 CET 2024
DNS server(s) 127.0.0.1
192.168.2.1
8.8.8.8
8.8.4.4
Last config change Sun Feb 18 19:16:36 CET 2024
State table size 0% (73/96000) Show states
Traffic Graphs
WAN
wan (in) wan (out)
600k
400k
200k
0.0
25:47 26:40 27:30 27:55
LAN
lan (in) lan (out)
0.0
-200k
-400k
-600k
25:47 26:40 27:30 27:55
Firewall Logs
Act Time IF Source Destination
Feb 18 19:23 LAN [fe80::1528:d2a6:dbb:937] [2001:67c:1562::23]:80
Feb 18 19:23 LAN [fe80::1528:d2a6:dbb:937] [2001:67c:1562::23]:80
Feb 18 19:23 LAN [fe80::1528:d2a6:dbb:937] [2001:67c:1562::23]:80
Feb 18 19:23 LAN [fe80::1528:d2a6:dbb:937] [2001:67c:1562::23]:80
Feb 18 19:24 LAN [fe80::1528:d2a6:dbb:937] [2001:67c:1562::23]:80


pfSense.midominio - Sys
https://192.168.1.1/pkg_mgr.php
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Auto Config Backup
Captive Portal
DHCP Relay
DHCP Server
DHCPv6 Relay
DHCPv6 Server & RA
DNS Forwarder
DNS Resolver
Dynamic DNS
IGMP Proxy
NTP
PPPoE Server
SNMP
Snort
Squid Proxy Server
Squid Reverse Proxy
SquidGuard Proxy Filter
UPnP & NAT-PMP
Wake-on-LAN
System / Package Manager / Available P
Installed Packages
Available Packages
Search
Search term
Both
Search
Clear
Packages
Name Version Description
acme 0.7.5 Automated Certificate M
Package Dependencies:
pecl-ssh2-1.3.1
php82-ftp-8.2.11
apcupsd 0.3.92_1 "apcupsd" can be used f
perform automatic shut
Package Dependencies:
apcupsd-3.14.14_4
arping 1.2.2_4 Broadcasts a who-has A
Package Dependencies:
arping-2.21_1
arpwatch 0.2.1 This package contains tools that monitors ethernet activity and maintains a database of ethernet/ip address pairings. It also reports certain changes via email.
Package Dependencies:
arpwatch-3.4
Avahi 2.2_4 Avahi is a system which facilitates host and service discovery in local networks via mDNS (Multicast DNS) and DNS-SD (DNS Service Discovery). This package allows mDNS/DNS-SD protocols to work across multiple LAN segments. mDNS/DNS-SD is known in Apple circles as "Bonjour" and is part of the Zeroconf suite of protocols.
Package Dependencies:
avahi-app-0.8_1
nss_mdns-0.14.1.20200624
Backup 0.6 Tool to Backup and Restore files and directories.
Install
https://192.168.1.1/pkg_edit.php?xml=squid.xml&id=0



Transparent Proxy Settings

Transparent HTTP Proxy

☑ 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)

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 **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

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 (;)

SSL Man In the Middle Filtering

HTTPS/SSL Interception
☑ Enable SSL filtering.

SSL/MITM Mode
Splice All
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.**

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

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

SSL Proxy Compatibility Mode
Modern
The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. Click Info for details.

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
Squid-CA
Select Certificate Authority to use when SSL interception is enabled.

SSL Certificate Deamon Children
This is the number of SSL certificate deamon 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.

SSL/MITM Mode
Splice All
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.**

Splice Whitelist, Bump Otherwise:
This is the default. Destinations defined in 'Whitelist' on the 'ACLs' tab will be spliced. All other domains will be bumped.
You *need* to install the CA certificate configured below on clients.
Content filtering (such as Antivirus) *will* be available with bumped sites (but *not* for 'Whitelist').

Splice All:
This configuration is suitable if you want to use the SquidGuard package for web filtering.
All destinations will be spliced. SquidGuard can do its job of denying or allowing destinations according its rules, as it does with HTTP.
You do *not* need to install the CA certificate configured below on clients.
Content filtering (such as Antivirus) *will not* be available for SSL sites.

Custom:
Use 'Custom Options (SSL/MITM)' defined in Advanced Features. See Info there for details and examples.
Warning: Custom mode is not supported in any way!

Please see SslBump Peek and Splice wiki documentation for additional details.

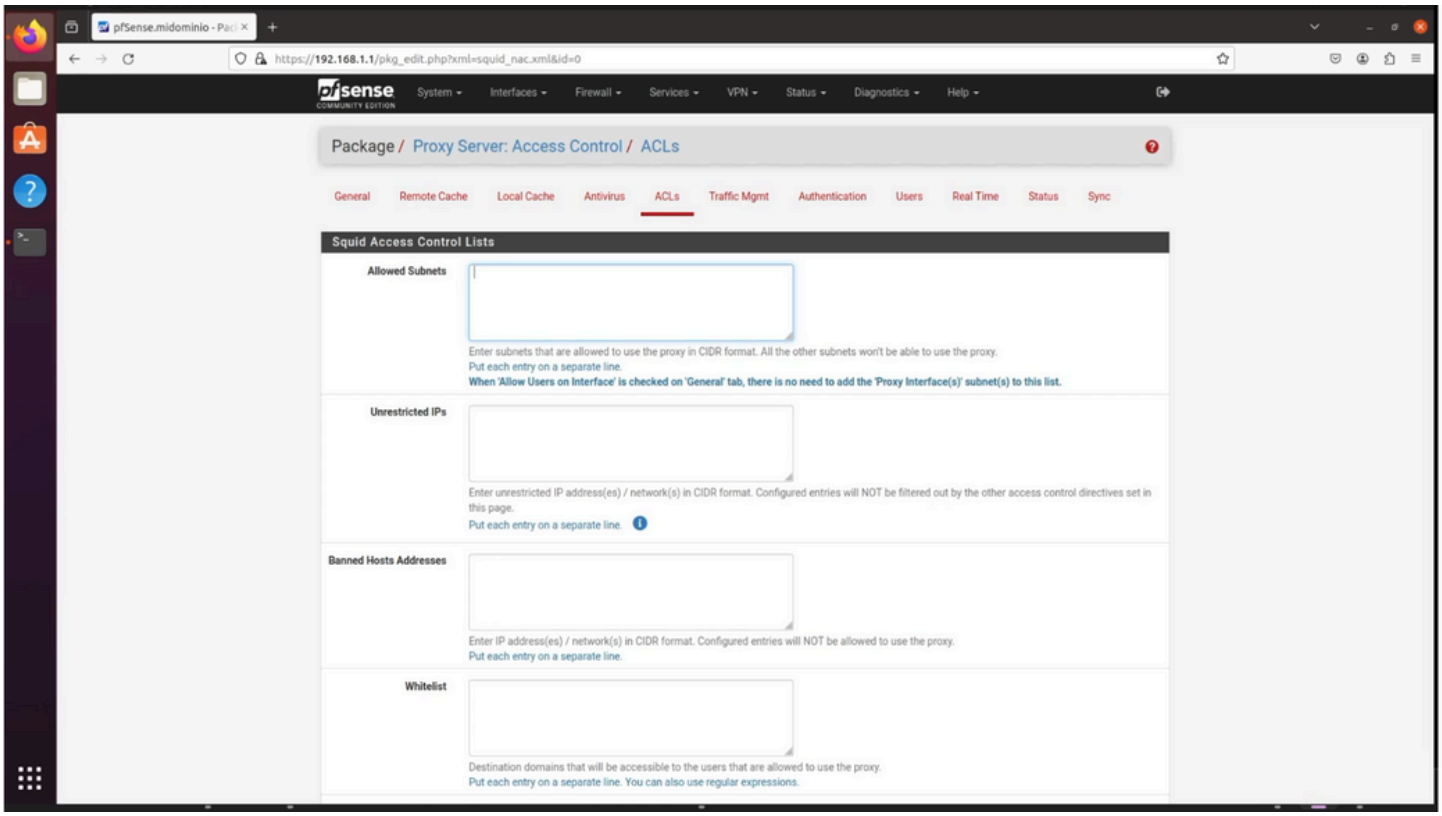
Logging Settings

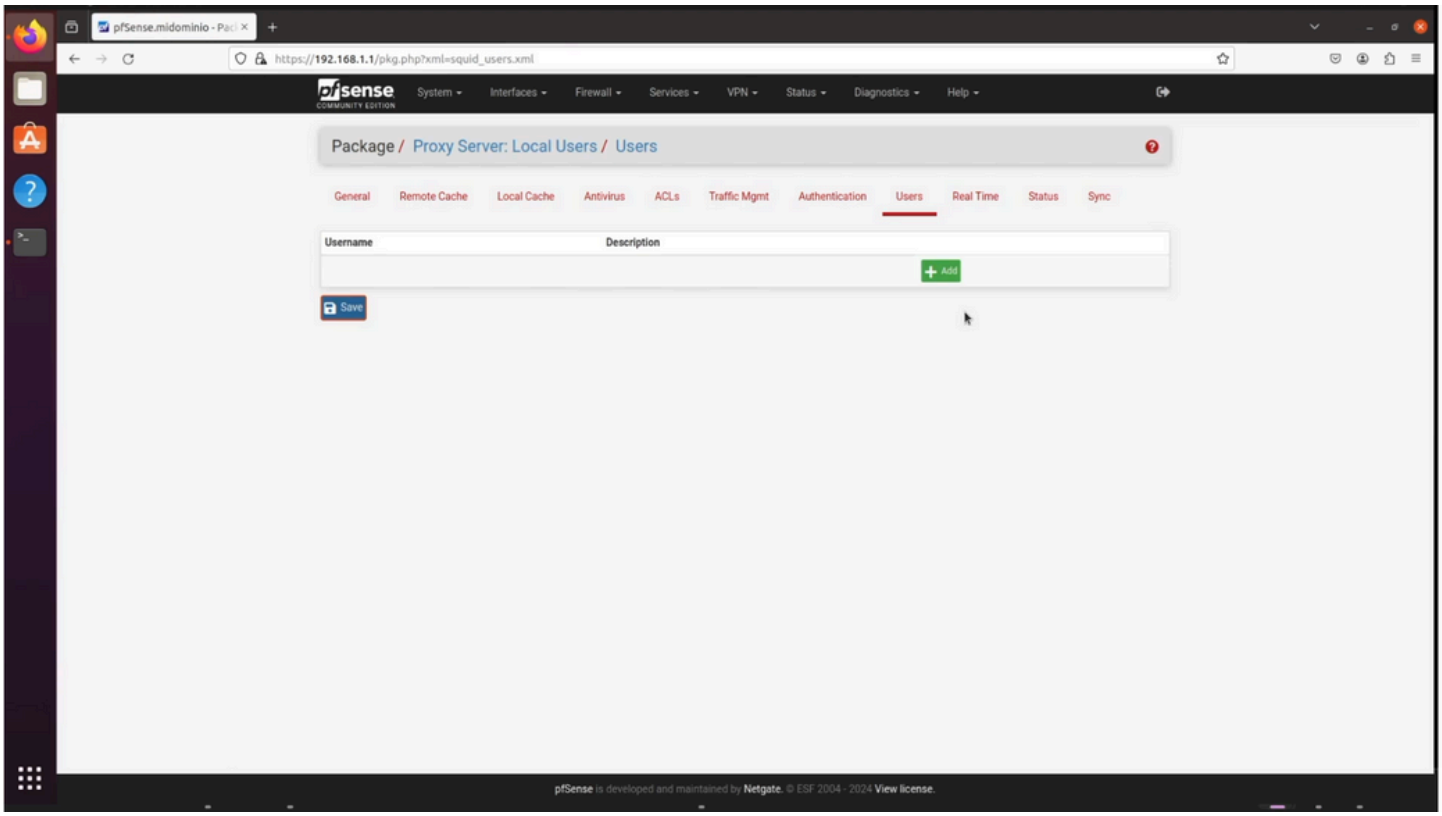
Enable Access Logging
☑ This will enable the access log.
Warning: Do NOT enable if available disk space is low.

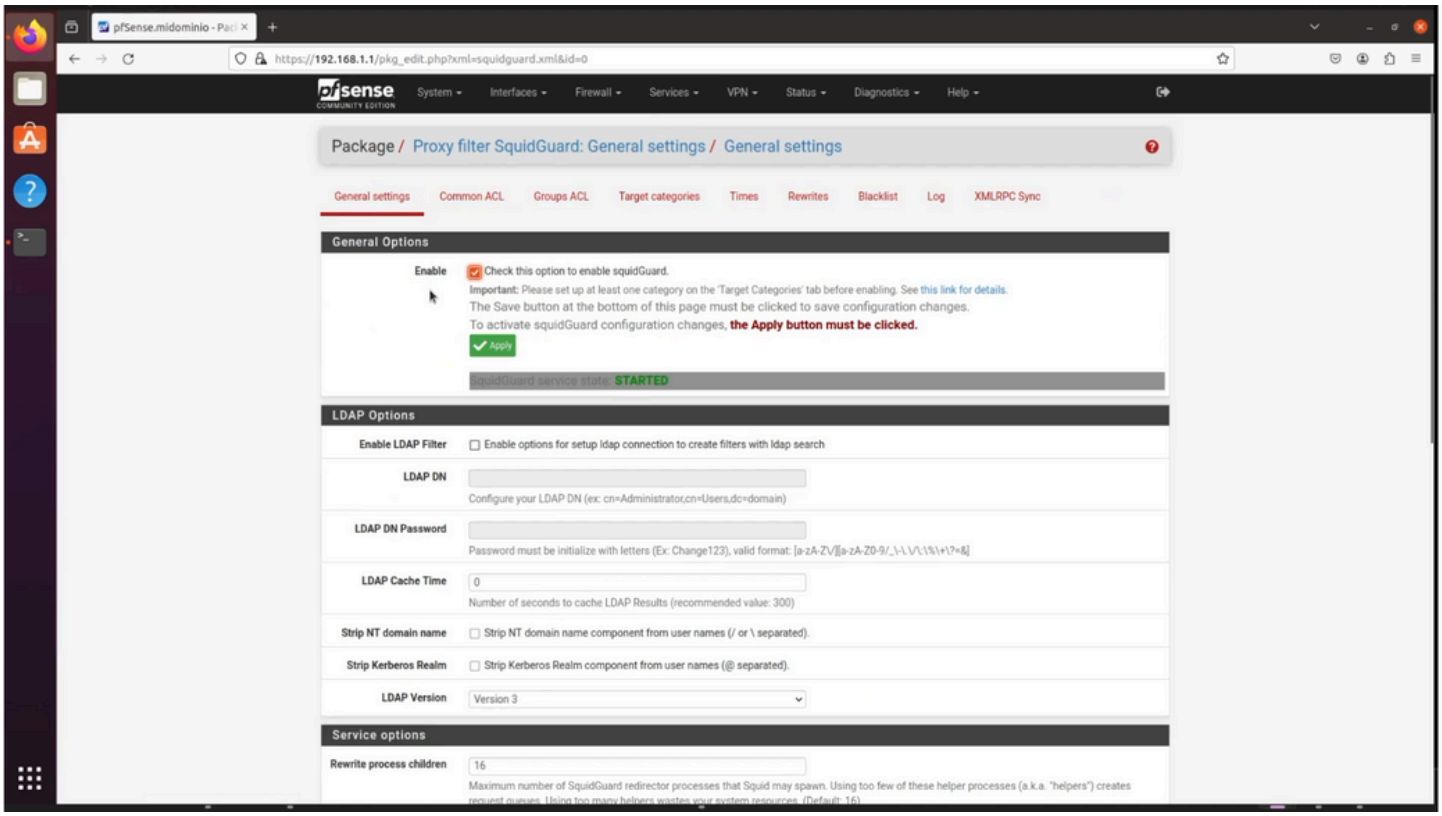
Log Store Directory
/var/squid/logs
The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs
Important: Do NOT include the trailing / when setting a custom location.

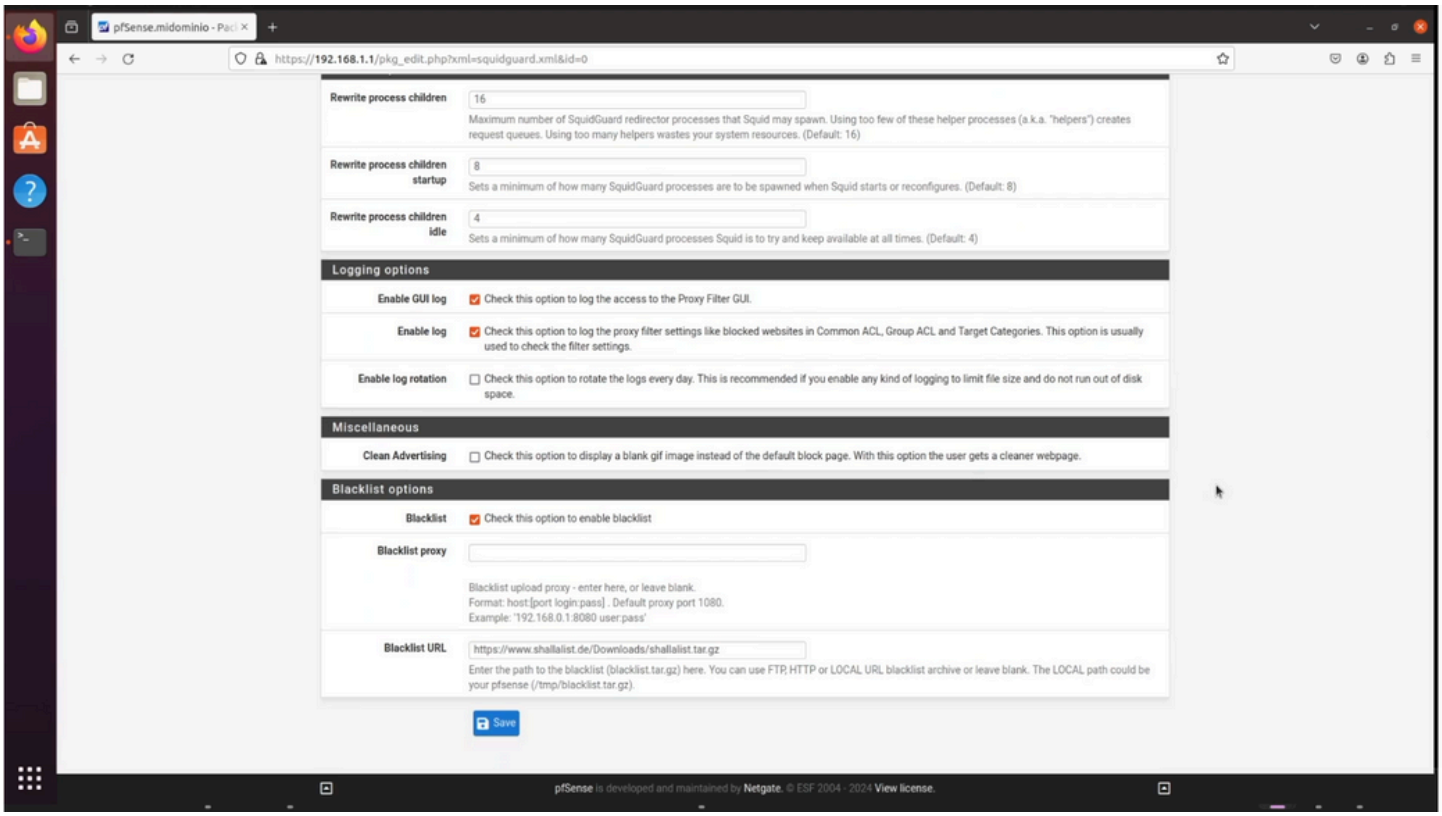
Rotate Logs
10
Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

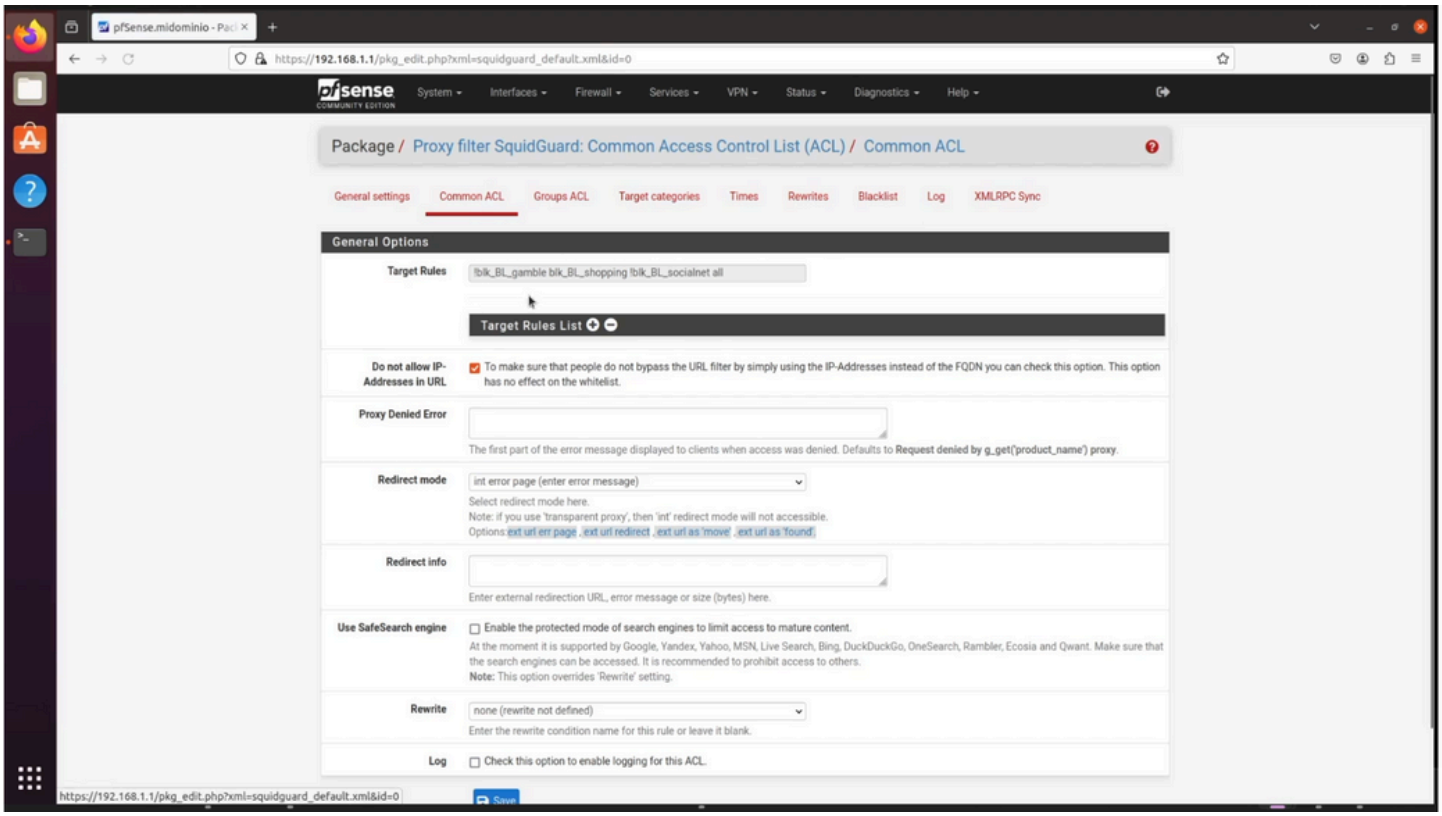
Log Pages Denied by SquidGuard
☐ Makes it possible for SquidGuard denied log to be included on Squid logs.
Click Info for detailed instructions.

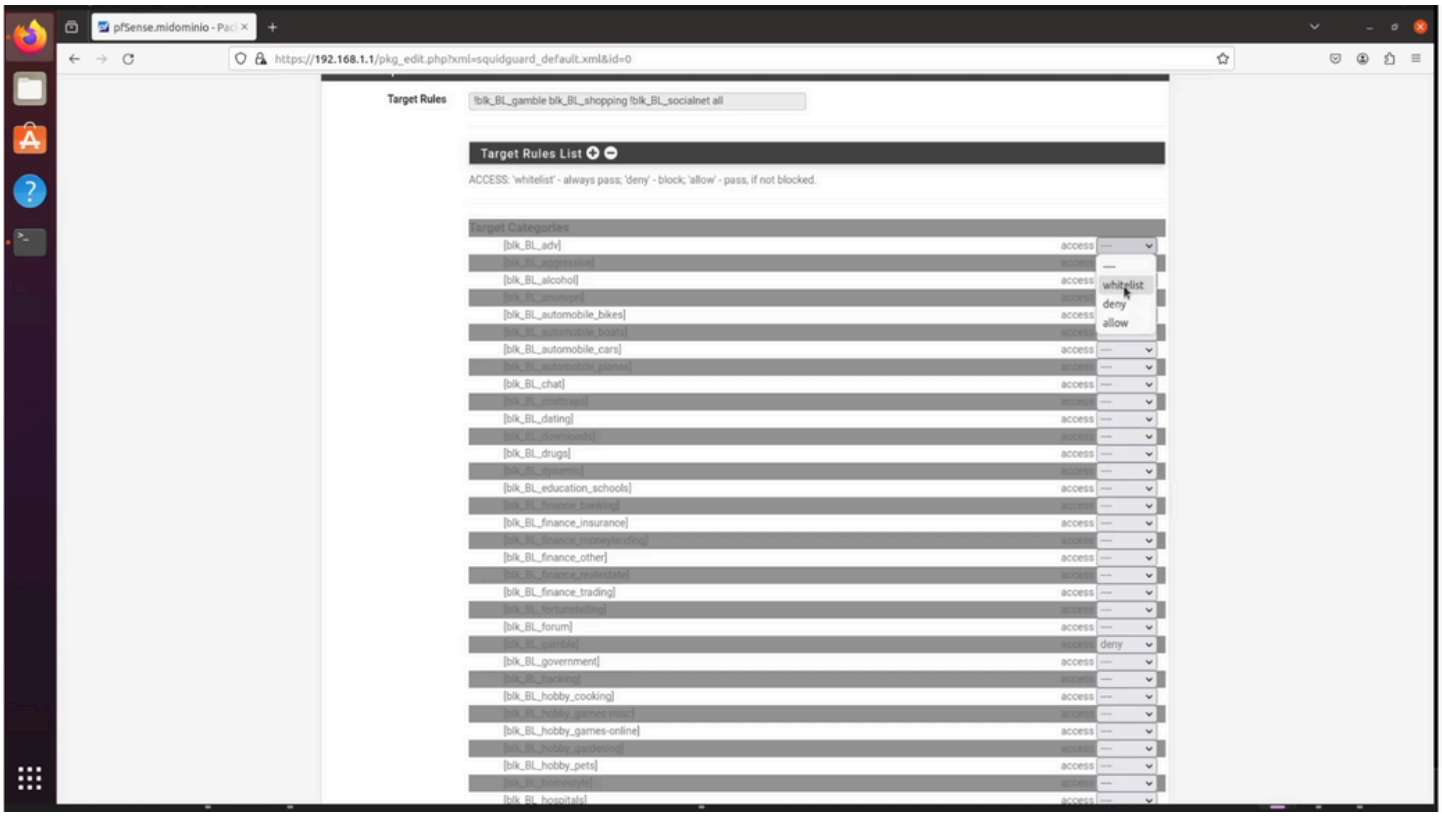

pfSense.midominio - Pac
https://192.168.1.1/pkg_edit.php?xml=squid_nac.xml&id=0
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Package / Proxy Server: Access Control / ACLs
General
Remote Cache
Local Cache
Antivirus
ACLs
Traffic Mgmt
Authentication
Users
Real Time
Status
Sync
Squid Access Control Lists
Allowed Subnets
Enter subnets that are allowed to use the proxy in CIDR format. All the other subnets won't be able to use the proxy.
Put each entry on a separate line.
When 'Allow Users on Interface' is checked on 'General' tab, there is no need to add the 'Proxy Interface(s)' subnet(s) to this list.
Unrestricted IPs
Enter unrestricted IP address(es) / network(s) in CIDR format. Configured entries will NOT be filtered out by the other access control directives set in this page.
Put each entry on a separate line.
Banned Hosts Addresses
Enter IP address(es) / network(s) in CIDR format. Configured entries will NOT be allowed to use the proxy.
Put each entry on a separate line.
Whitelist
Destination domains that will be accessible to the users that are allowed to use the proxy.
Put each entry on a separate line. You can also use regular expressions.

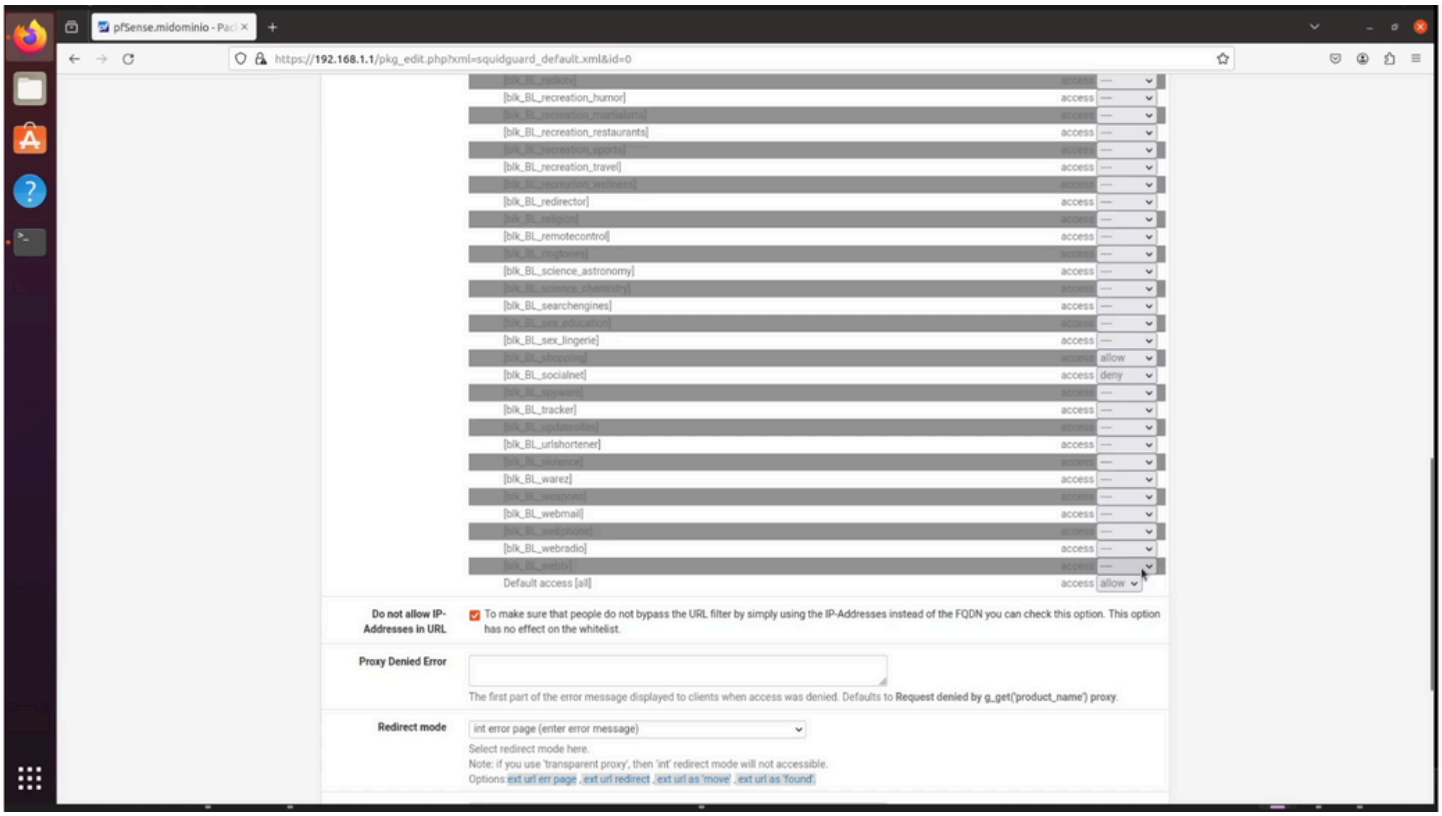

pfSense.midominio - Pac
https://192.168.1.1/pkg.php?xml=squid_users.xml
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Package / Proxy Server: Local Users / Users
General
Remote Cache
Local Cache
Antivirus
ACLs
Traffic Mgmt
Authentication
Users
Real Time
Status
Sync
Username
Description
Add
Save
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

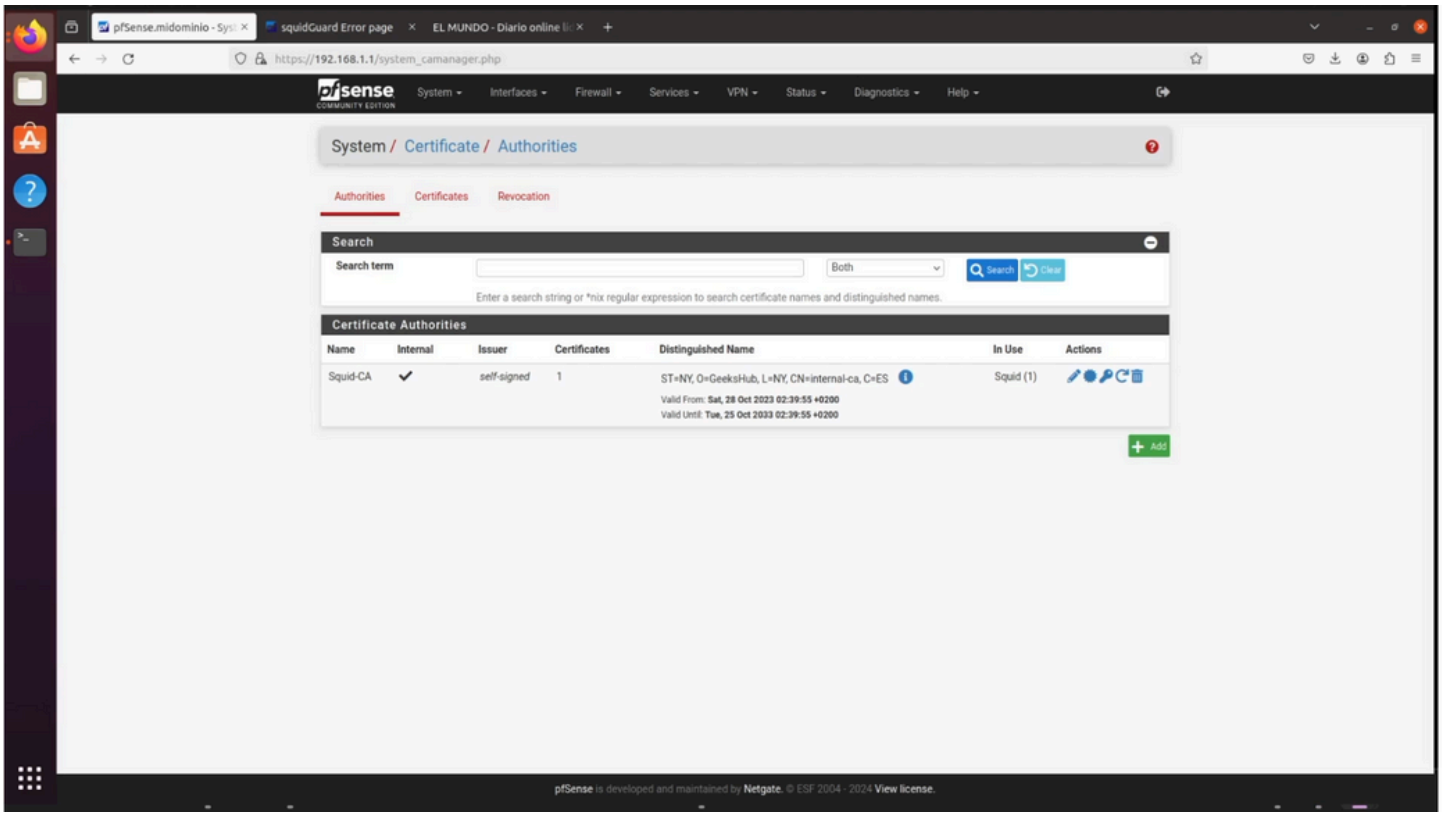

pfSense.midominio - Pac
https://192.168.1.1/pkg_edit.php?xml=squidguard.xml&id=0
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Package / Proxy filter SquidGuard: General settings / General settings
General settings
Common ACL
Groups ACL
Target categories
Times
Rewrites
Blacklist
Log
XMLRPC Sync
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
LDAP Options
Enable LDAP Filter
Enable options for setup ldap connection to create filters with ldap search
LDAP DN
Configure your LDAP DN (ex: cn=Administrator,cn=Users,dc=domain)
LDAP DN Password
Password must be initialize with letters (Ex: Change123), valid format: [a-zA-Z\][a-zA-Z0-9/_\-\.\/\;\%\+\?=&]
LDAP Cache Time
0
Number of seconds to cache LDAP Results (recommended value: 300)
Strip NT domain name
Strip NT domain name component from user names (/ or \ separated).
Strip Kerberos Realm
Strip Kerberos Realm component from user names (@ separated).
LDAP Version
Version 3
Service options
Rewrite process children
16
Maximum number of SquidGuard redirector processes that Squid may spawn. Using too few of these helper processes (a.k.a. "helpers") creates

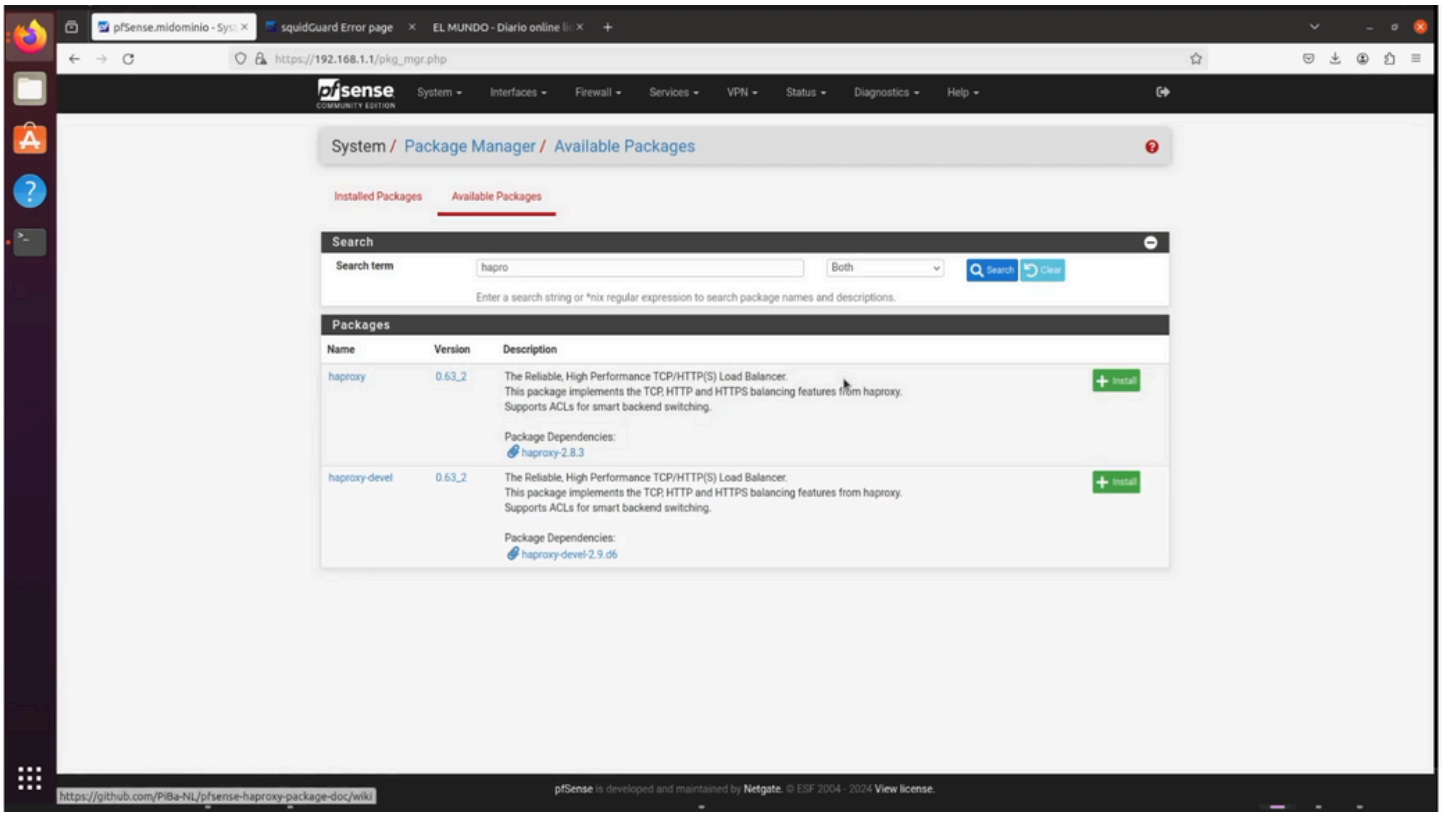

pfSense.midominio - Pac
https://192.168.1.1/pkg_edit.php?xml=squidguard.xml&id=0
Rewrite process children
16
Maximum number of SquidGuard redirector processes that Squid may spawn. Using too few of these helper processes (a.k.a. "helpers") creates request queues. Using too many helpers wastes your system resources. (Default: 16)
Rewrite process children startup
8
Sets a minimum of how many SquidGuard processes are to be spawned when Squid starts or reconfigures. (Default: 8)
Rewrite process children idle
4
Sets a minimum of how many SquidGuard processes Squid is to try and keep available at all times. (Default: 4)
Logging options
Enable GUI log
Check this option to log the access to the Proxy Filter GUI.
Enable log
Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings.
Enable log rotation
Check this option to rotate the logs every day. This is recommended if you enable any kind of logging to limit file size and do not run out of disk space.
Miscellaneous
Clean Advertising
Check this option to display a blank gif image instead of the default block page. With this option the user gets a cleaner webpage.
Blacklist options
Blacklist
Check this option 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
https://www.shallalist.de/Downloads/shallalist.tar.gz
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
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.


pfSense.midominio - Pac
https://192.168.1.1/pkg_edit.php?xml=squidguard_default.xml&id=0
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Package / Proxy filter SquidGuard: Common Access Control List (ACL) / Common ACL
General settings
Common ACL
Groups ACL
Target categories
Times
Rewrites
Blacklist
Log
XMLRPC Sync
General Options
Target Rules
!blk_BL_gamble blk_BL_shopping !blk_BL_socialnet all
Target Rules List
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.
Proxy Denied Error
The first part of the error message displayed to clients when access was denied. Defaults to Request denied by g_get('product_name') proxy.
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 info
Enter external redirection URL, error message or size (bytes) here.
Use SafeSearch engine
Enable the protected mode of search engines to limit access to mature content.
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
none (rewrite not defined)
Enter the rewrite condition name for this rule or leave it blank.
Log
Check this option to enable logging for this ACL.
https://192.168.1.1/pkg_edit.php?xml=squidguard_default.xml&id=0
Save


pfSense.midominio - Pac
https://192.168.1.1/pkg_edit.php?xml=squidguard_default.xml&id=0
Target Rules
!blk_BL_gamble blk_BL_shopping !blk_BL_socialnet all
Target Rules List
ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.
Target Categories
[blk_BL_adv]
[blk_BL_alcohol]
[blk_BL_automobile_bikes]
[blk_BL_automobile_cars]
[blk_BL_chat]
[blk_BL_dating]
[blk_BL_drugs]
[blk_BL_education_schools]
[blk_BL_finance_insurance]
[blk_BL_finance_other]
[blk_BL_finance_trading]
[blk_BL_forum]
[blk_BL_government]
[blk_BL_hobby_cooking]
[blk_BL_hobby_games-online]
[blk_BL_hobby_pets]
access
---
whitelist
deny
allow


pfSense.midominio - Pac
https://192.168.1.1/pkg_edit.php?xml=squidguard_default.xml&id=0
[blk_BL_recreation_humor] access
[blk_BL_recreation_restaurants] access
[blk_BL_recreation_travel] access
[blk_BL_redirector] access
[blk_BL_remotecontrol] access
[blk_BL_science_astronomy] access
[blk_BL_searchengines] access
[blk_BL_sex_lingerie] access
[blk_BL_shopping] access allow
[blk_BL_socialnet] access deny
[blk_BL_tracker] access
[blk_BL_urlshortener] access
[blk_BL_warez] access
[blk_BL_webmail] access
[blk_BL_webradio] access
Default access [all] access allow
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.
Proxy Denied Error
The first part of the error message displayed to clients when access was denied. Defaults to Request denied by g_get('product_name') proxy.
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'


pfSense.midominio - Syst
squidGuard Error page
EL MUNDO - Diario online li
https://192.168.1.1/system_camanager.php
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
System / Certificate / Authorities
Authorities Certificates Revocation
Search
Search term
Both
Search Clear
Enter a search string or *nix regular expression to search certificate names and distinguished names.
Certificate Authorities
Name Internal Issuer Certificates Distinguished Name In Use Actions
Squid-CA self-signed 1 ST=NY, O=GeeksHub, L=NY, CN=internal-ca, C=ES Squid (1)
Valid From: Sat, 28 Oct 2023 02:39:55 +0200
Valid Until: Tue, 25 Oct 2033 02:39:55 +0200
Add
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.



Conclusion

Squid and SquidGuard in pfSense offer enhanced web caching and filtering capabilities, boosting network performance and security. Squid optimizes internet access by caching frequently accessed content, reducing bandwidth usage. SquidGuard provides robust content filtering, allowing administrators to enforce access policies and protect against malicious websites, enhancing network safety and productivity.

Singularity Hackers 0xWORD My Public Inbox