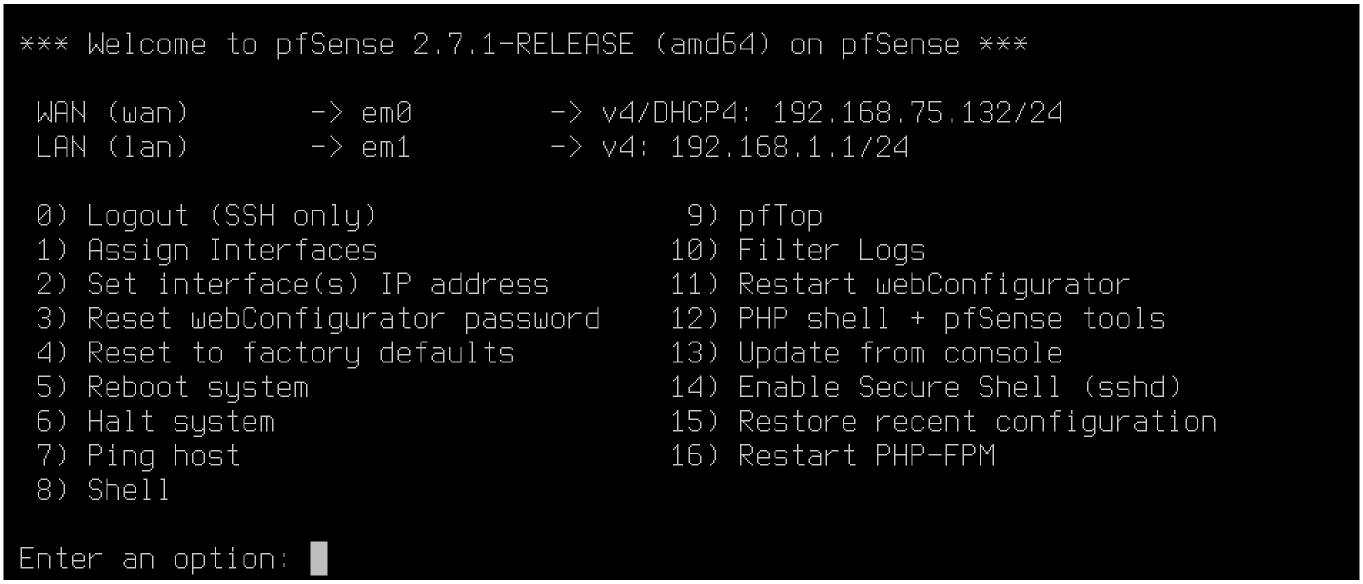
new vm --> ubuntux64 machine --> 60gb --> pfsense iso

2 adapters
nat
hostonly

if lags, settings options advanced bios UEFI ok

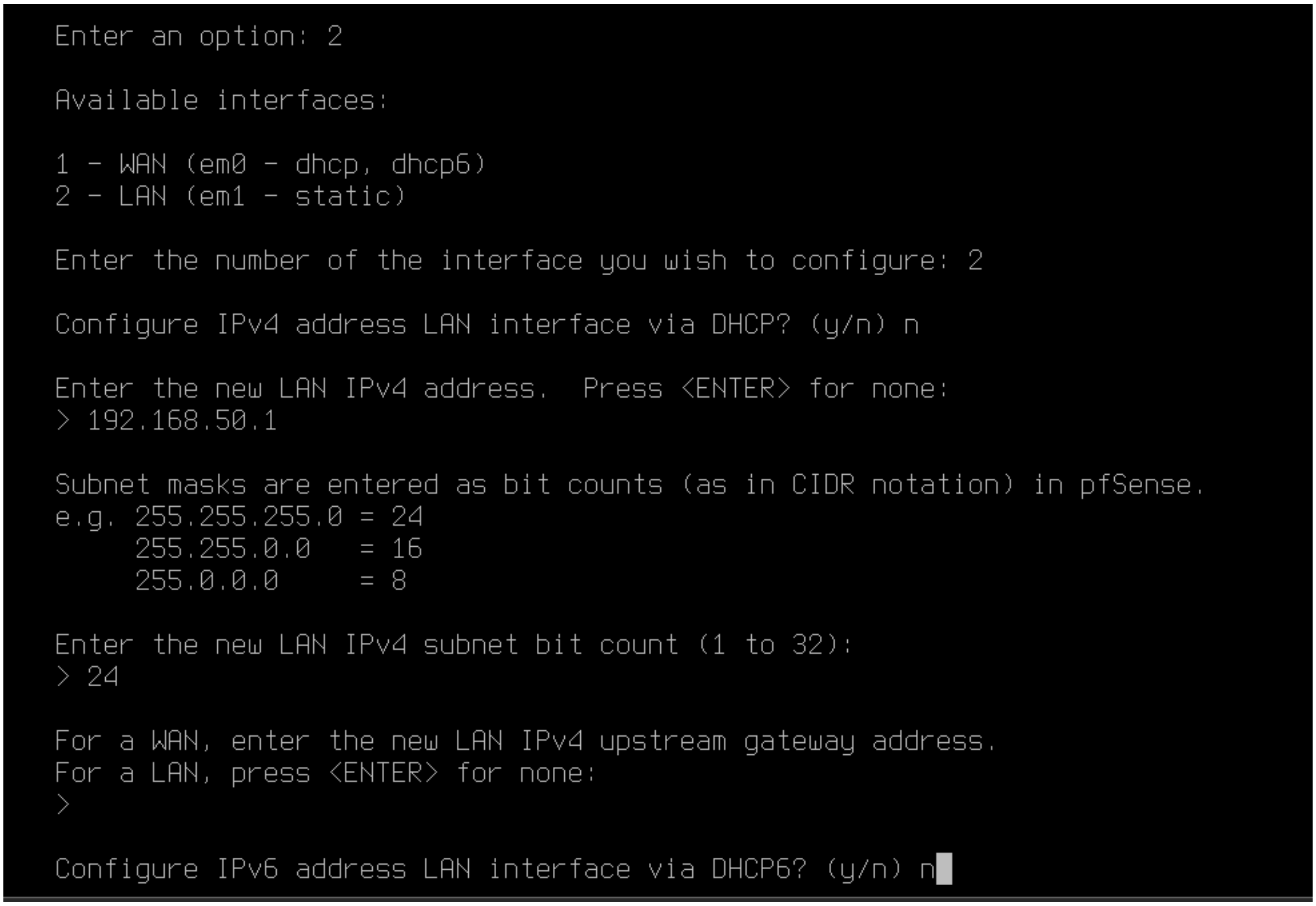
install okokok check yes destroy



```
*** Welcome to pfSense 2.7.1-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.75.132/24
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 
```

do till above steps

2



```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.50.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n
```

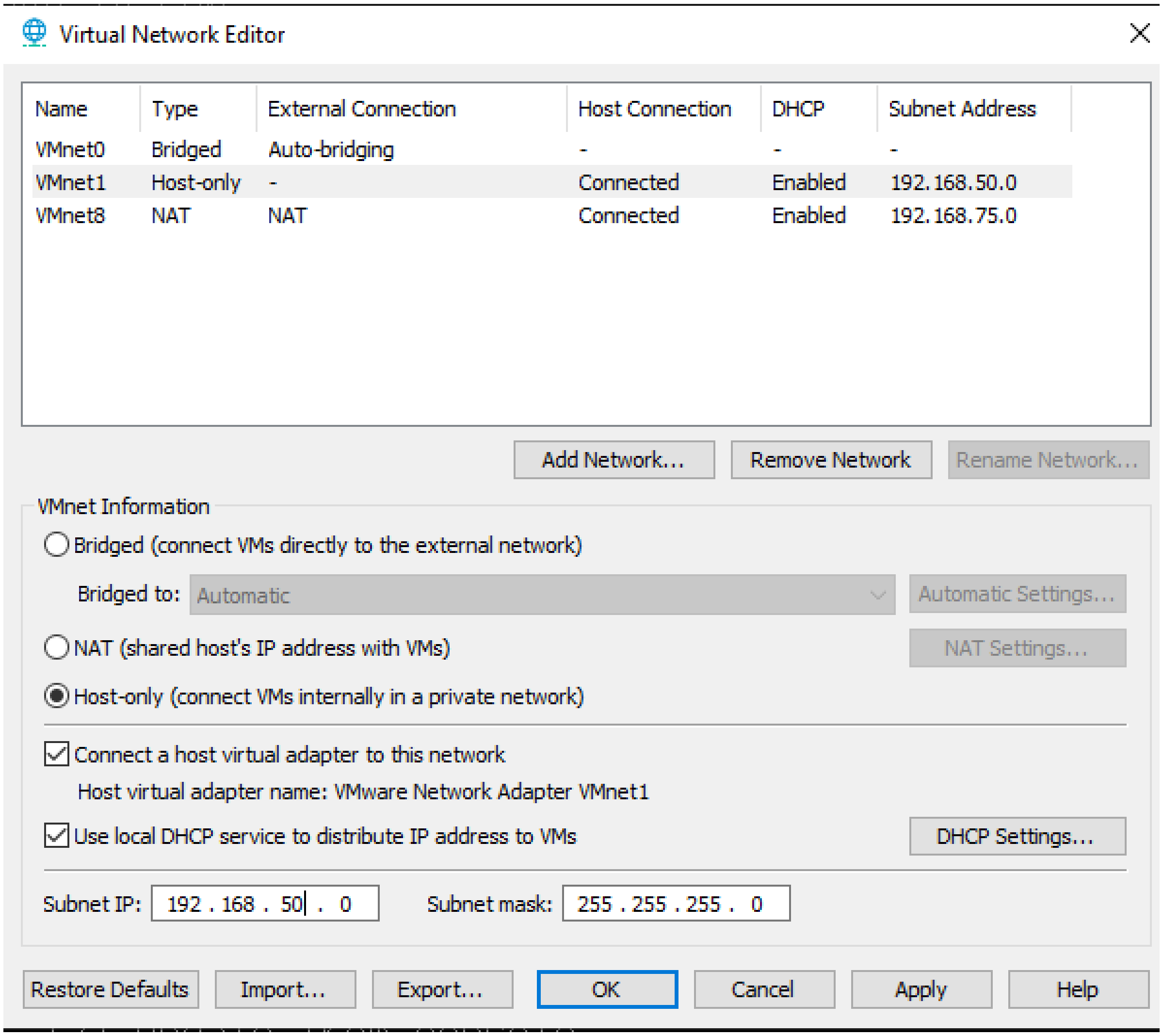
2
n
enter ip you want for that interface
mask

n
n
n

---

edit
virtual net adapter

change settings



Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.50.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.75.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

○ NAT (shared host's IP address with VMs)

● Host-only (connect VMs internally in a private network)

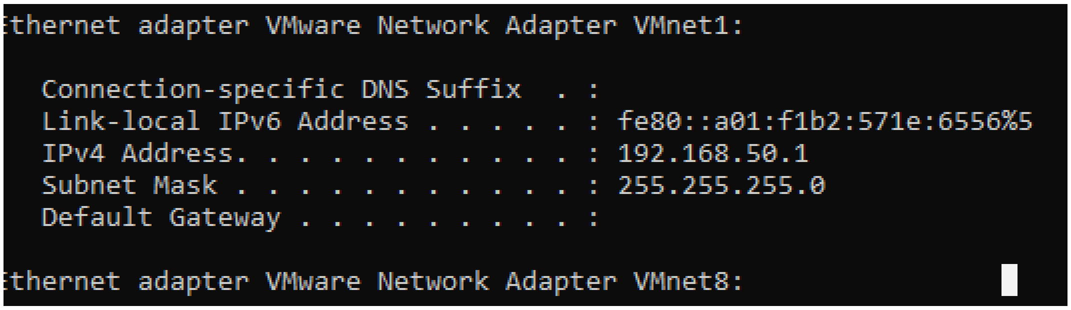
☑ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet1

☑ Use local DHCP service to distribute IP address to VMs

Subnet IP: 192 . 168 . 50 . 0 Subnet mask: 255 . 255 . 255 . 0

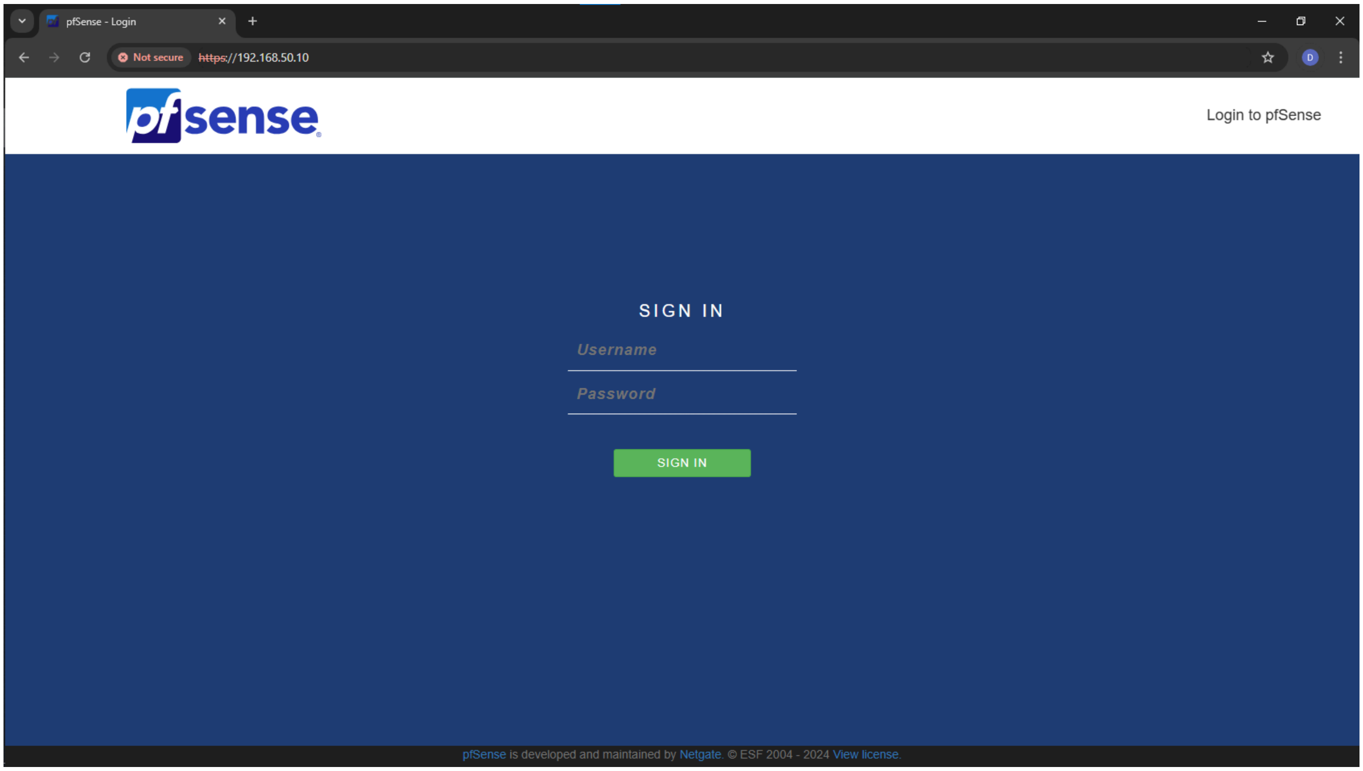
host only & chane ip to 192.168.50.0



```
thernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a01:f1b2:571e:6556%5
   IPv4 Address. . . . . . . . . . . : 192.168.50.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

thernet adapter VMware Network Adapter VMnet8:
```

50.1 is taken by vmware automatically

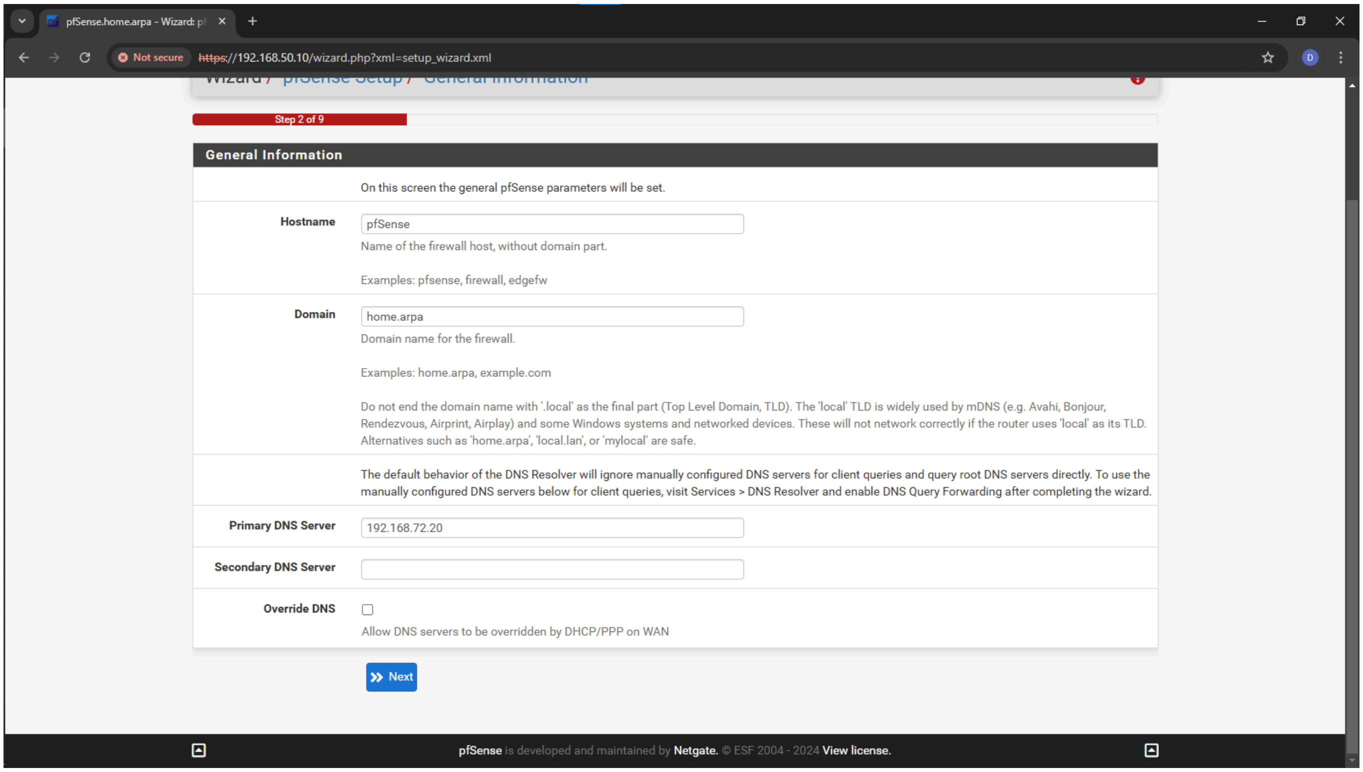
go to base machine browser



pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

admin

pfsense


pfSense.home.arpa - Wizard: pf
Not secure
https://192.168.50.10/wizard.php?xml=setup_wizard.xml
Wizard / pfSense Setup / General Information
Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname: pfSense

Name of the firewall host, without domain part.

Examples: pfsense, firewall, edgefw

Domain: home.arpa

Domain name for the firewall.

Examples: home.arpa, example.com

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server: 192.168.72.20

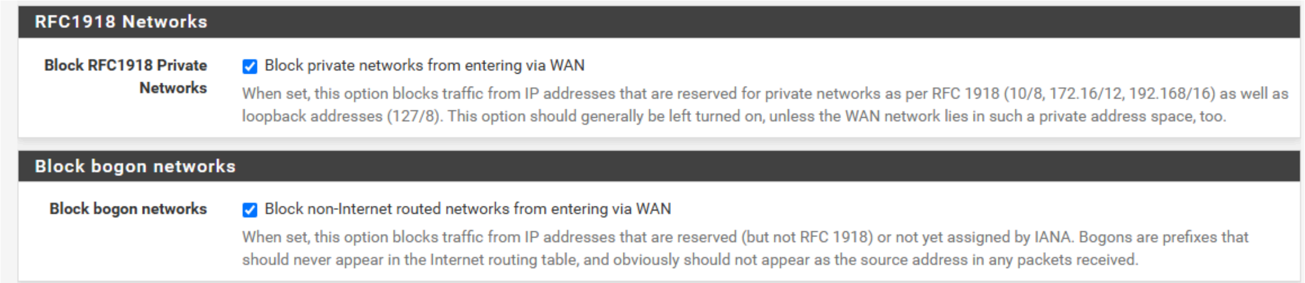
Secondary DNS Server:

Override DNS: □ Allow DNS servers to be overridden by DHCP/PPP on WAN

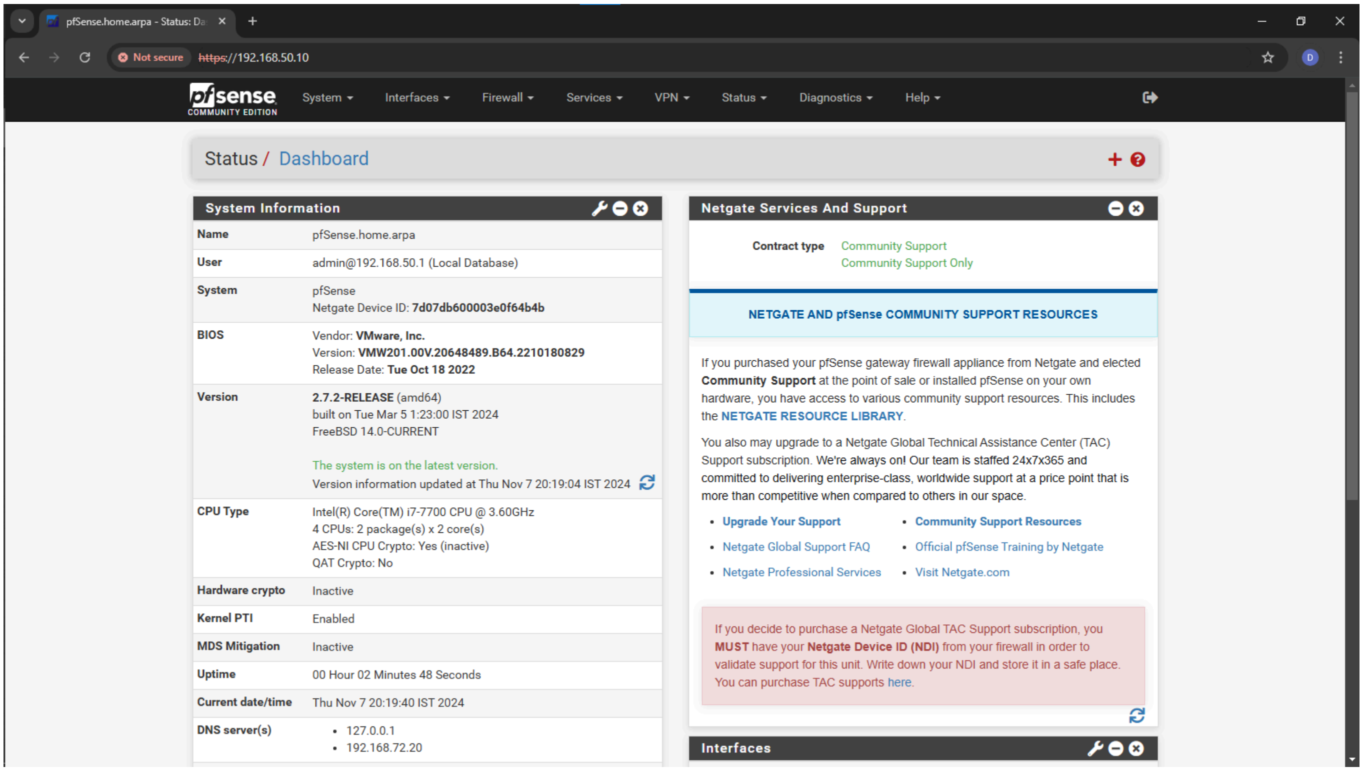
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

enter CDAC DNS & uncheck

next time zone as asia/kolkata

> 
>
> **RFC1918 Networks**
>
> **Block RFC1918 Private Networks**
>
> ☑ Block private networks from entering via WAN
>
> When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.
>
> **Block bogon networks**
>
> **Block bogon networks**
>
> ☑ Block non-Internet routed networks from entering via WAN
>
> When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.
>
> this is why private ips are not allowed and we have to do natting to conv priv ip to pub ip

n-n-give admin pwd ditiss@123
reload



Status / Dashboard

System Information

Name	pfSense.home.arpa
User	admin@192.168.50.1 (Local Database)
System	pfSense Netgate Device ID: **7d07db600003e0f64b4b**
BIOS	Vendor: **VMware, Inc.** Version: **VMW201.00V.20648489.B64.2210180829** Release Date: **Tue Oct 18 2022**
Version	**2.7.2-RELEASE** (amd64) built on Tue Mar 5 1:23:00 IST 2024 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Thu Nov 7 20:19:04 IST 2024
CPU Type	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz 4 CPUs: 2 package(s) x 2 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	00 Hour 02 Minutes 48 Seconds
Current date/time	Thu Nov 7 20:19:40 IST 2024
DNS server(s)	• 127.0.0.1 • 192.168.72.20

Netgate Services And Support

Contract type Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

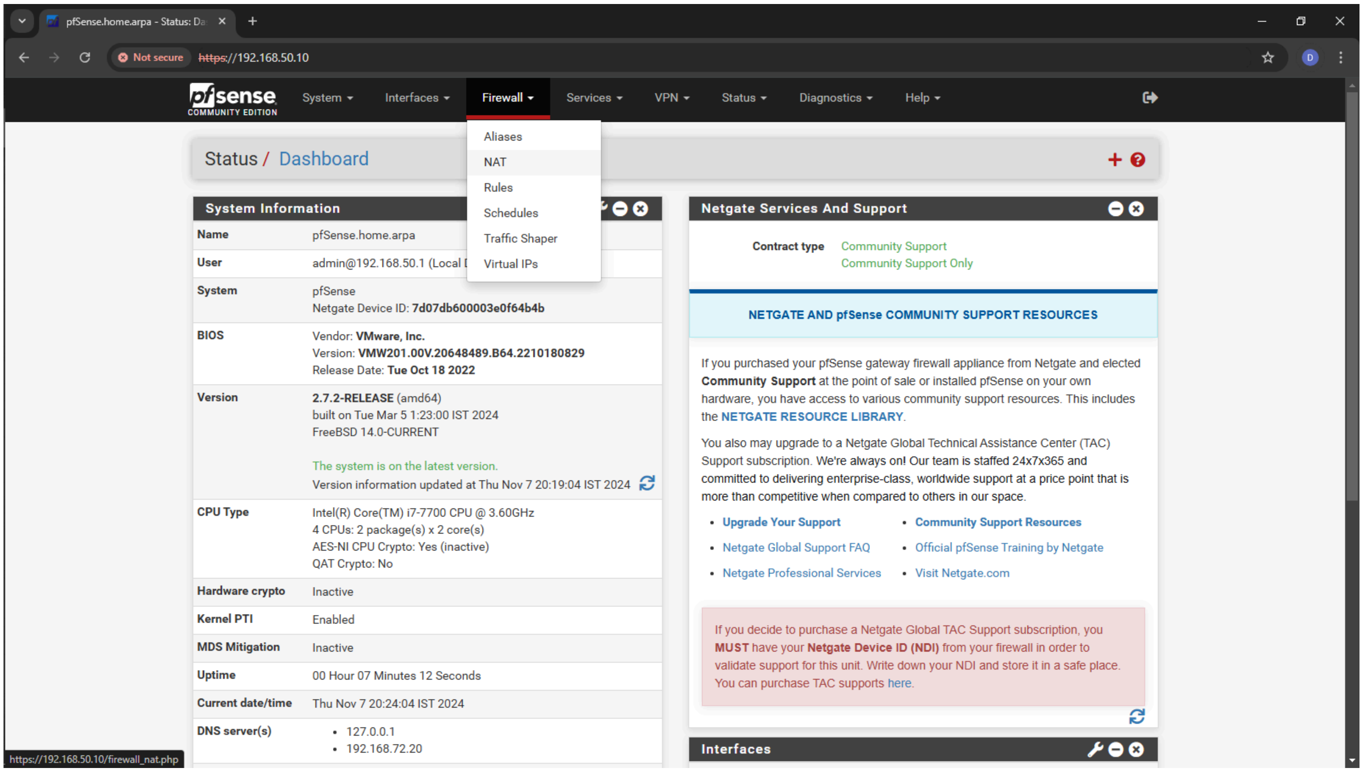
If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- **Upgrade Your Support**
- Netgate Global Support FAQ
- Netgate Professional Services
- **Community Support Resources**
- Official pfSense Training by Netgate
- Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports here.

Interfaces



Status / Dashboard

System Information

Name	pfSense.home.arpa
User	admin@192.168.50.1 (Local D
System	pfSense Netgate Device ID: **7d07db600003e0f64b4b**
BIOS	Vendor: **VMware, Inc.** Version: **VMW201.00V.20648489.B64.2210180829** Release Date: **Tue Oct 18 2022**
Version	**2.7.2-RELEASE** (amd64) built on Tue Mar 5 1:23:00 IST 2024 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Thu Nov 7 20:19:04 IST 2024
CPU Type	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz 4 CPUs: 2 package(s) x 2 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	00 Hour 07 Minutes 12 Seconds
Current date/time	Thu Nov 7 20:24:04 IST 2024
DNS server(s)	• 127.0.0.1 • 192.168.72.20

Netgate Services And Support

Contract type Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

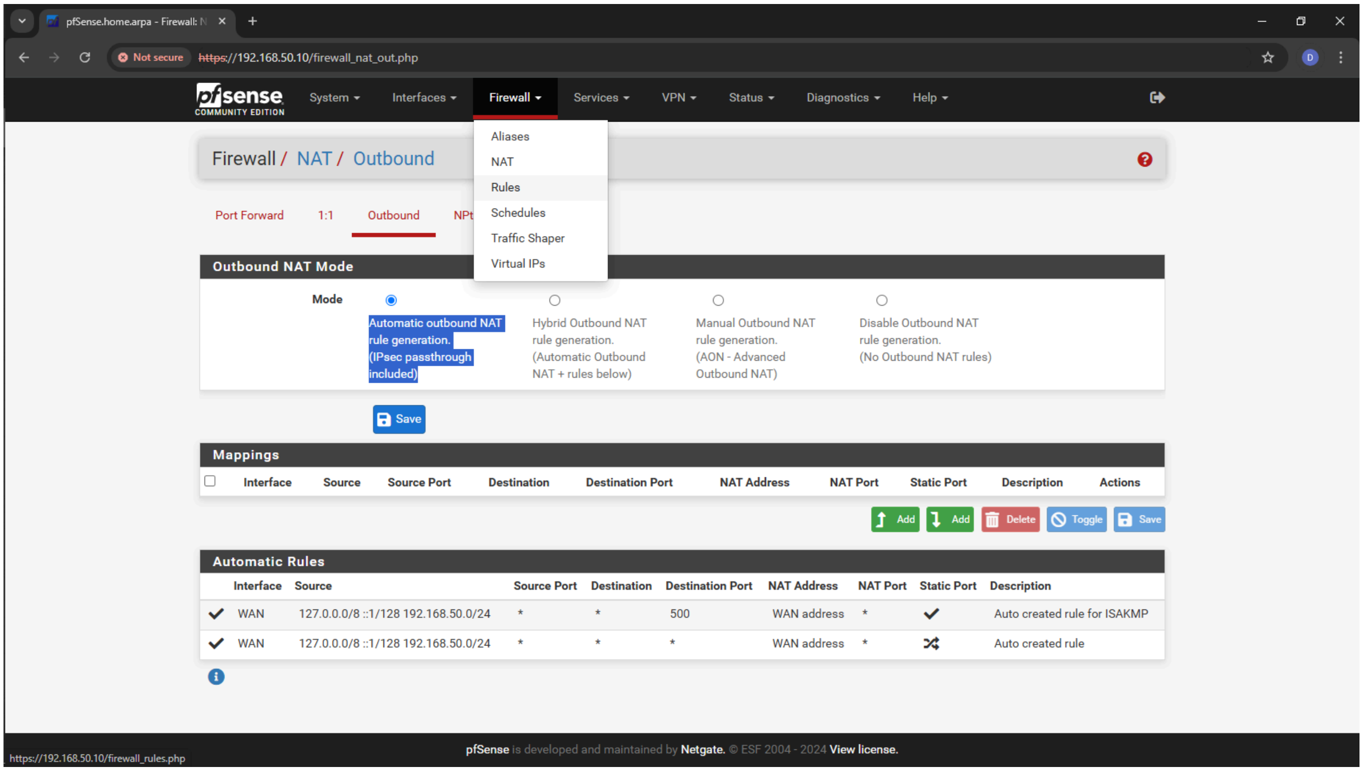
You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- **Upgrade Your Support**
- Netgate Global Support FAQ
- Netgate Professional Services
- **Community Support Resources**
- Official pfSense Training by Netgate
- Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports here.

Interfaces

POSTROUTING RULE:



Firewall / NAT / Outbound

Outbound NAT Mode

Mode

● Automatic outbound NAT rule generation. (IPsec passthrough included)
○ Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
○ Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
○ Disable Outbound NAT rule generation. (No Outbound NAT rules)

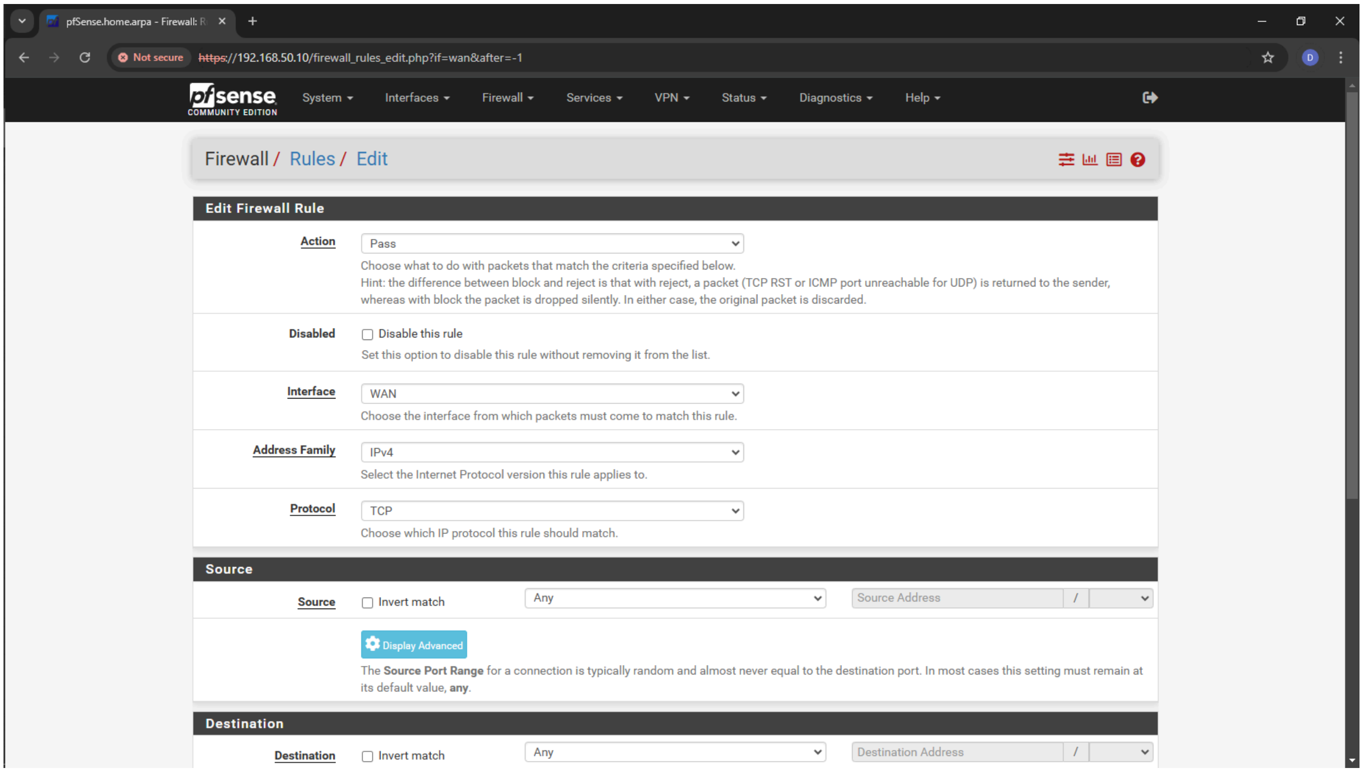
Mappings

□	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions

Automatic Rules

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✓	WAN	127.0.0.0/8 ::1/128 192.168.50.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
✓	WAN	127.0.0.0/8 ::1/128 192.168.50.0/24	*	*	*	WAN address	*	⤮	Auto created rule

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.


pfSense.home.arpa - Firewall: R
Not secure
https://192.168.50.10/firewall_rules_edit.php?if=wan&after=-1
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Display Advanced

Firewall / Rules / Edit

Edit Firewall Rule

Action: Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: □ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: WAN
Choose the interface from which packets must come to match this rule.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: TCP
Choose which IP protocol this rule should match.

Source

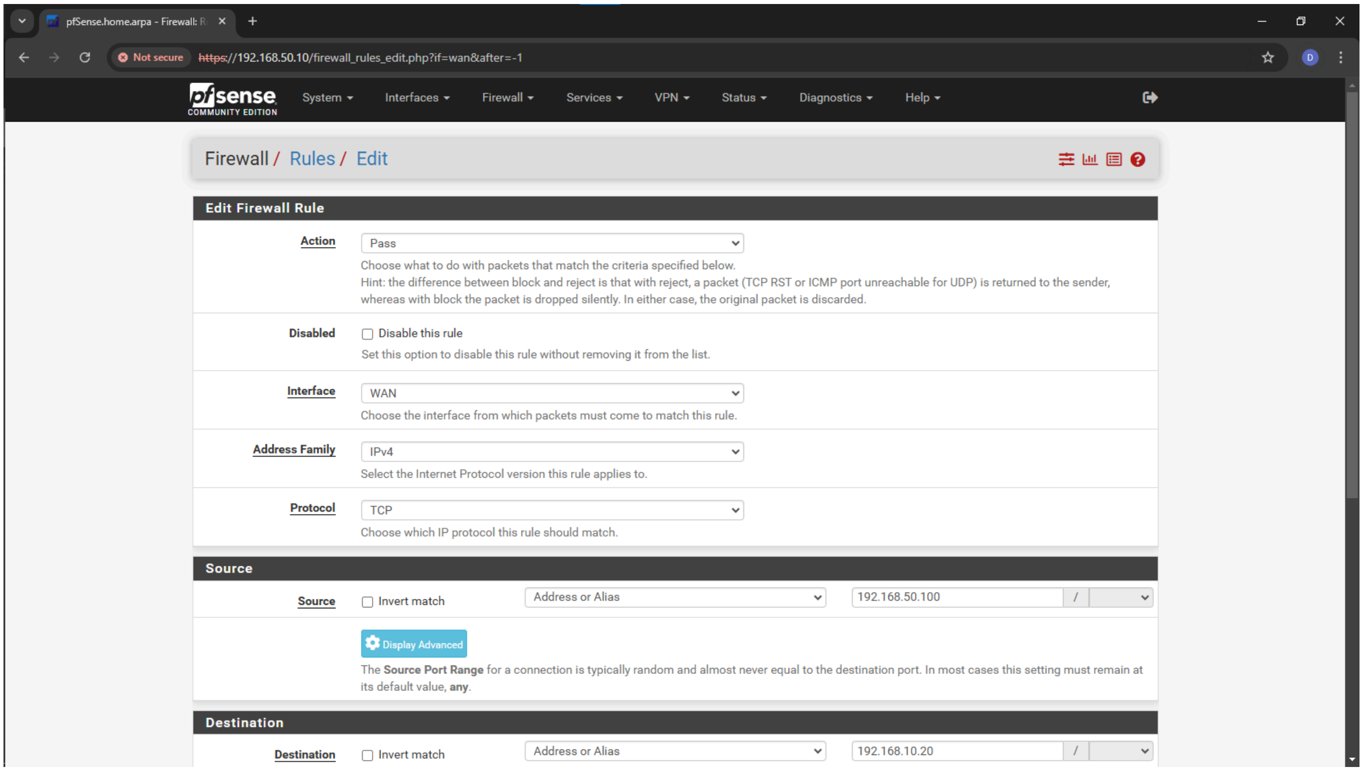
Source: □ Invert match | Any | Source Address /

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination: □ Invert match | Any | Destination Address /

pass-accpet
block-drop
reject-reject



pfSense.home.arpa - Firewall: R
Not secure
https://192.168.50.10/firewall_rules_edit.php?if=wan&after=-1
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

Firewall / Rules / Edit

Edit Firewall Rule

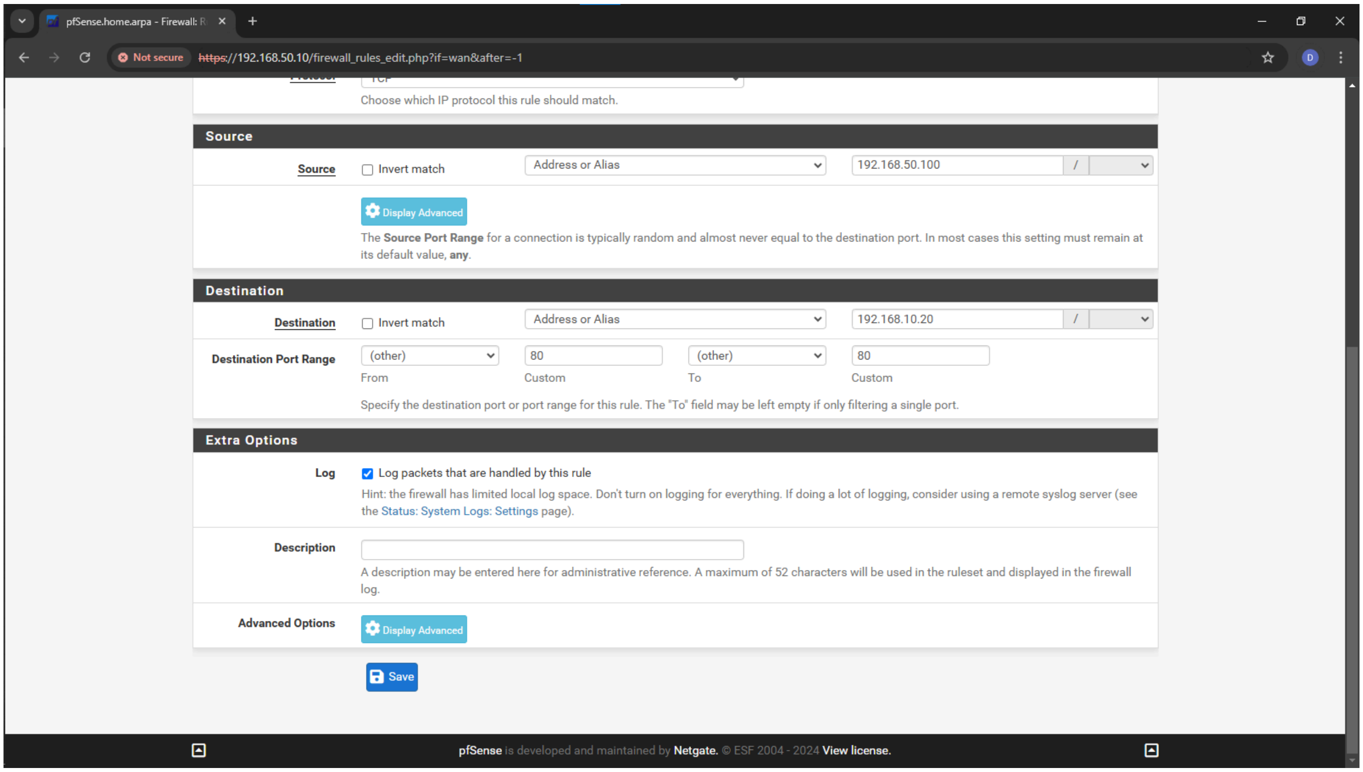
Action	Pass Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	☐ Disable this rule Set this option to disable this rule without removing it from the list.
Interface	WAN Choose the interface from which packets must come to match this rule.
Address Family	IPv4 Select the Internet Protocol version this rule applies to.
Protocol	TCP Choose which IP protocol this rule should match.

Source

Source	☐ Invert match	Address or Alias	192.168.50.100 /
	Display Advanced The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.		

Destination

Destination	☐ Invert match	Address or Alias	192.168.10.20 /



Choose which IP protocol this rule should match.

Source

Source	☐ Invert match	Address or Alias	192.168.50.100 /
	Display Advanced The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.		

Destination

Destination	☐ Invert match	Address or Alias	192.168.10.20 /	
Destination Port Range	(other) From	80 Custom	(other) To	80 Custom

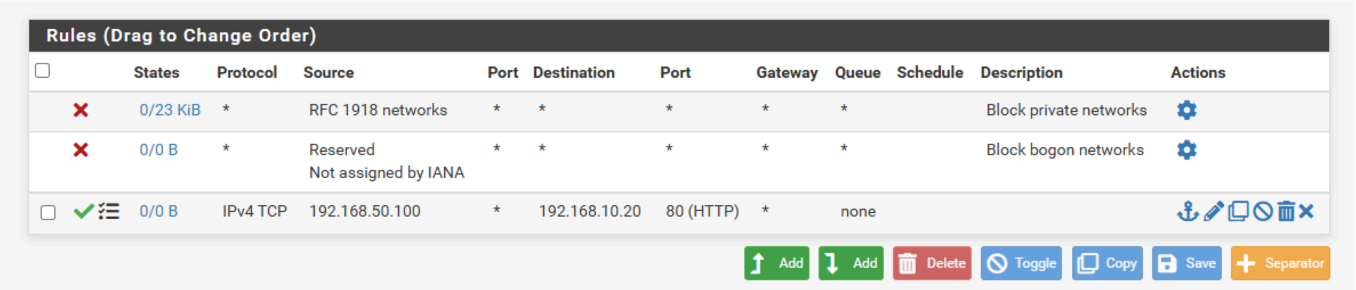
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log	☑ Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description	 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options	Display Advanced

Save

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.



Rules (Drag to Change Order)

☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✗	0/23 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙
	✗	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
☐	✓ ☰	0/0 B	IPv4 TCP	192.168.50.100	*	192.168.10.20	80 (HTTP)	*	none			⚓ ✎ ❐ ⃠ 🗑 ✕

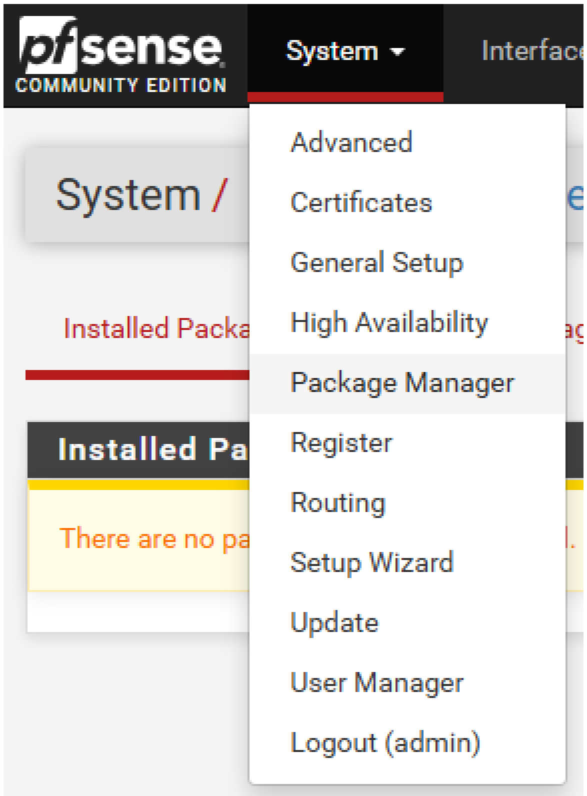
DEFAULT RULES WILL BE ALWAYS AT THE TOP

BLOCK WEBSITES---we cant as pfsense is a packet filtering firewall and can block ip's only

we can block them by installing squid---which is provided by the subscription

so while bying these firewall subscriptions, you need to compare for the product, features and price for the firewall

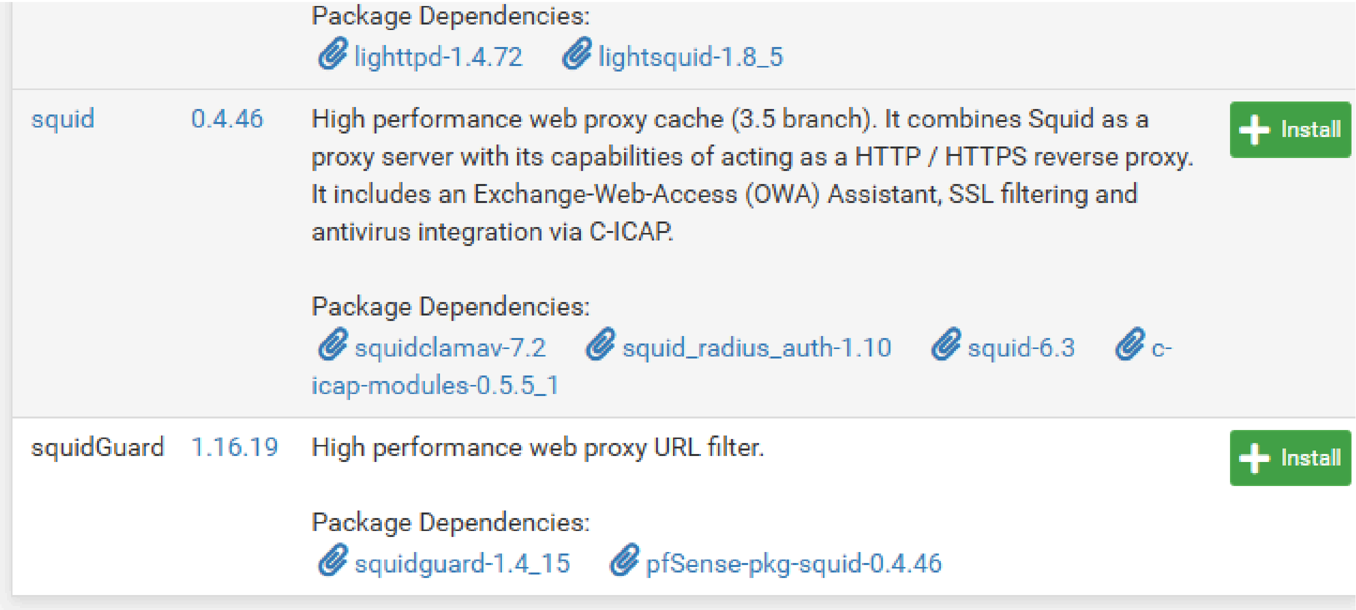
install package managers



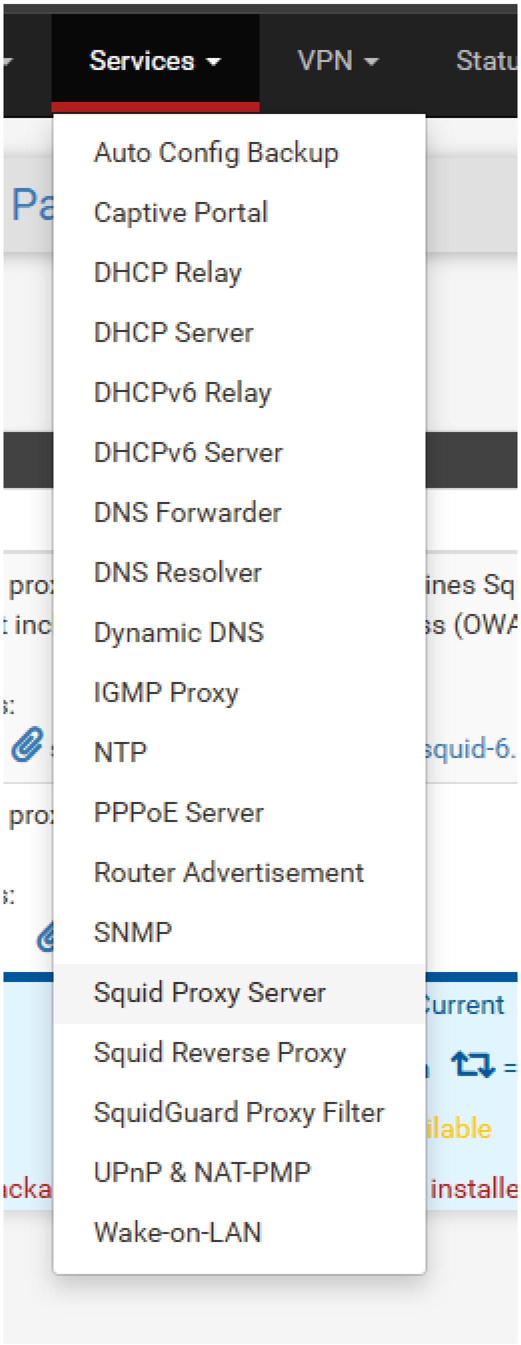
go to available packages -- search squid

squidgaurd=allows to have webbased filtering (url filter)
squid=proxy
netsquid= for reports/logging
who is using how man y websites
most visited sites ,etc

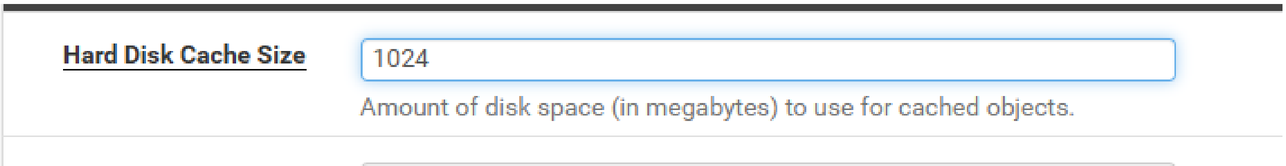
install both



		Package Dependencies: lighttpd-1.4.72 lightsquid-1.8_5	
squid	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. Package Dependencies: squidclamav-7.2 squid_radius_auth-1.10 squid-6.3 c-icap-modules-0.5.5_1	+ Install
squidGuard	1.16.19	High performance web proxy URL filter. Package Dependencies: squidguard-1.4_15 pfSense-pkg-squid-0.4.46	+ Install

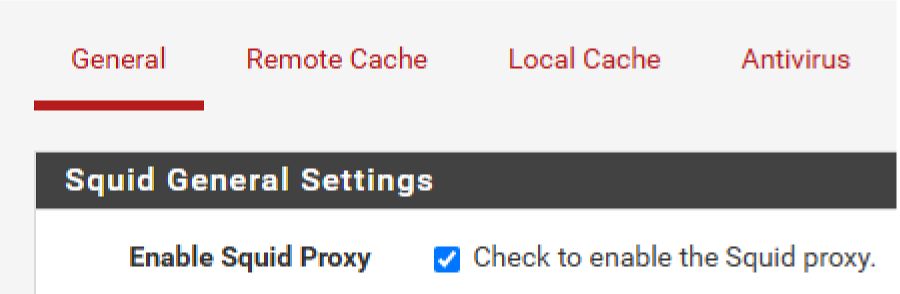


go to local cache and change to



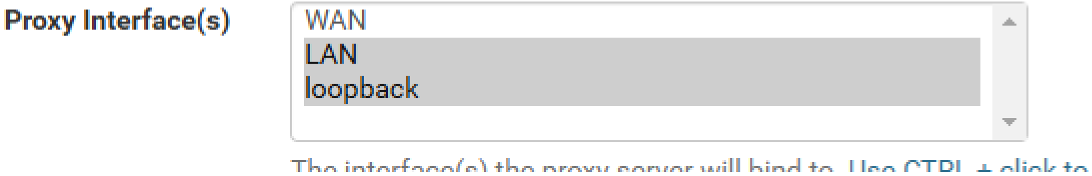
Hard Disk Cache Size 1024

Amount of disk space (in megabytes) to use for cached objects.

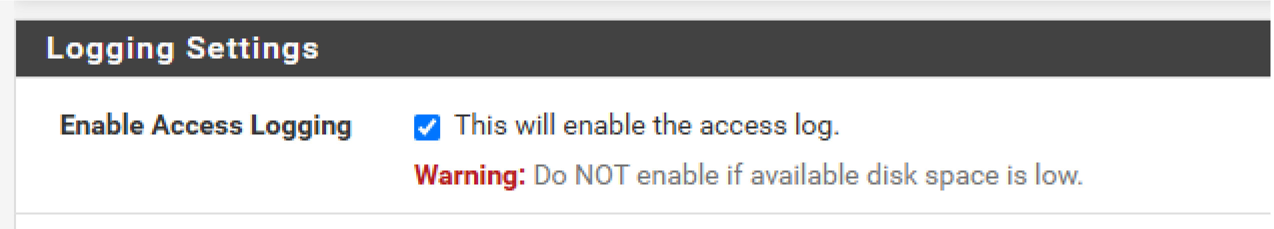
- 

Squid General Settings
Enable Squid Proxy ☑ Check to enable the Squid proxy.

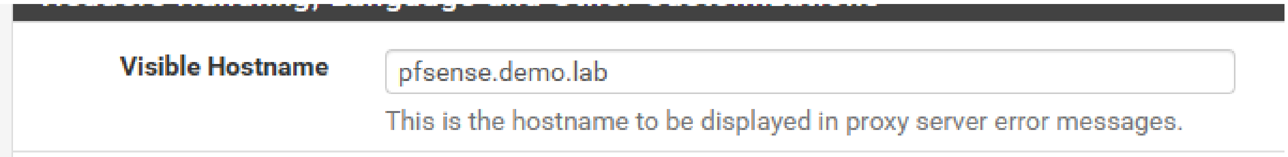
check

- 
Proxy Interface(s)
WAN
LAN
loopback
The interface(s) the proxy server will bind to. Use CTRL + click to

loopback & lan

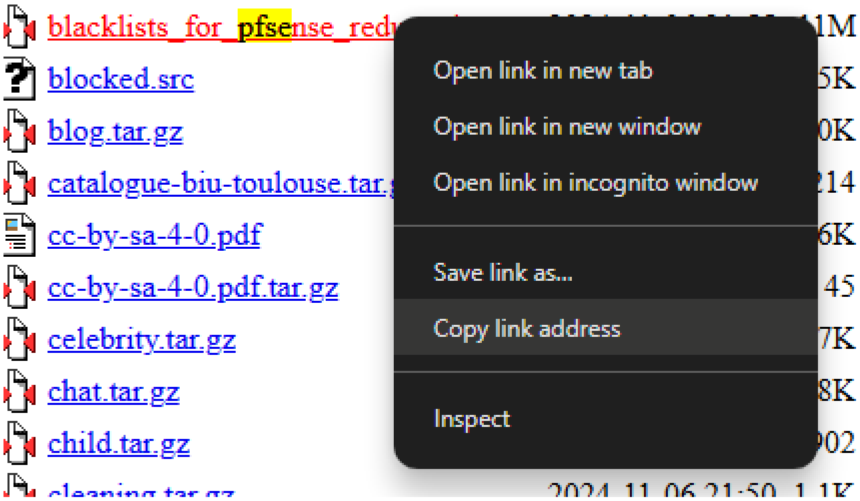
- 
Logging Settings
Enable Access Logging ☑ This will enable the access log.
Warning: Do NOT enable if available disk space is low.

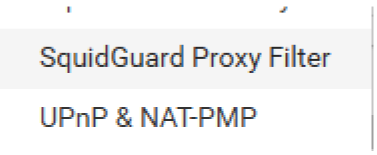
check

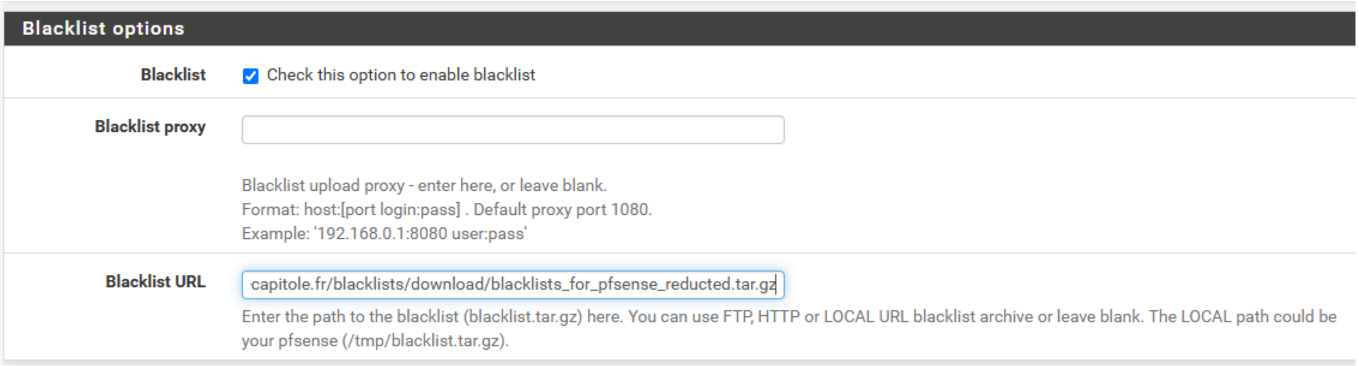
- 
Visible Hostname: pfsense.demo.lab
This is the hostname to be displayed in proxy server error messages.

---

https://dsi.ut-capitole.fr/blacklists/download/


```
blacklists_for_pfsense_redi                                  1M
blocked.src                                                  5K
blog.tar.gz                                                  0K
catalogue-biu-toulouse.tar.g                                 214
cc-by-sa-4-0.pdf                                             6K
cc-by-sa-4-0.pdf.tar.gz                                      45
celebrity.tar.gz                                             7K
chat.tar.gz                                                  8K
child.tar.gz                                                 02
cleaning.tar.gz                           2024-11-06 21:50   1.1K
```





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'

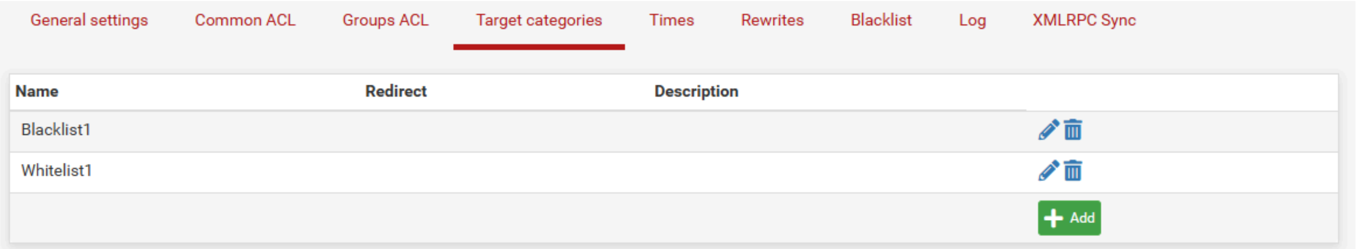
Blacklist URL capitole.fr/blacklists/download/blacklists_for_pfsense_reducted.tar.gz

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).

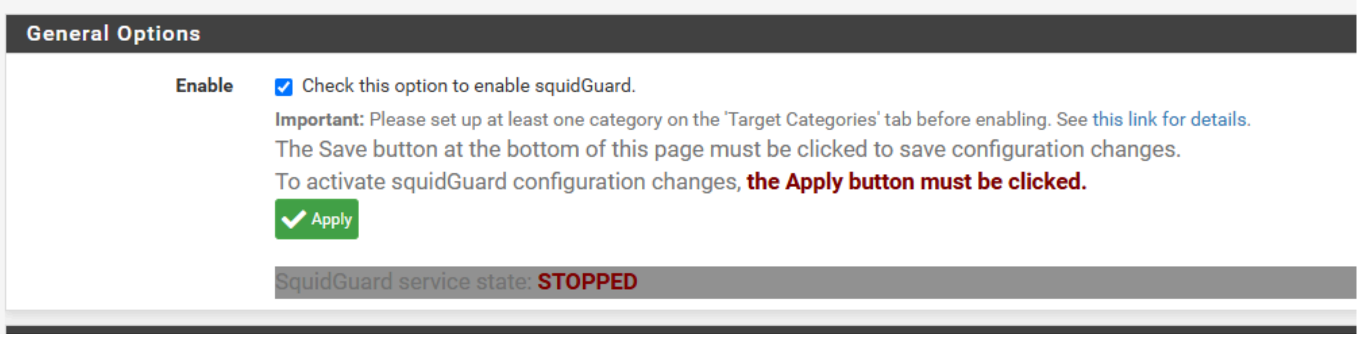
go to the blacklist tab and click on download

target categories tab
add give name, check logs save

Blacklist1 for block
whitelist1 to allow



Name	Redirect	Description
Blacklist1		
Whitelist1		



General Options

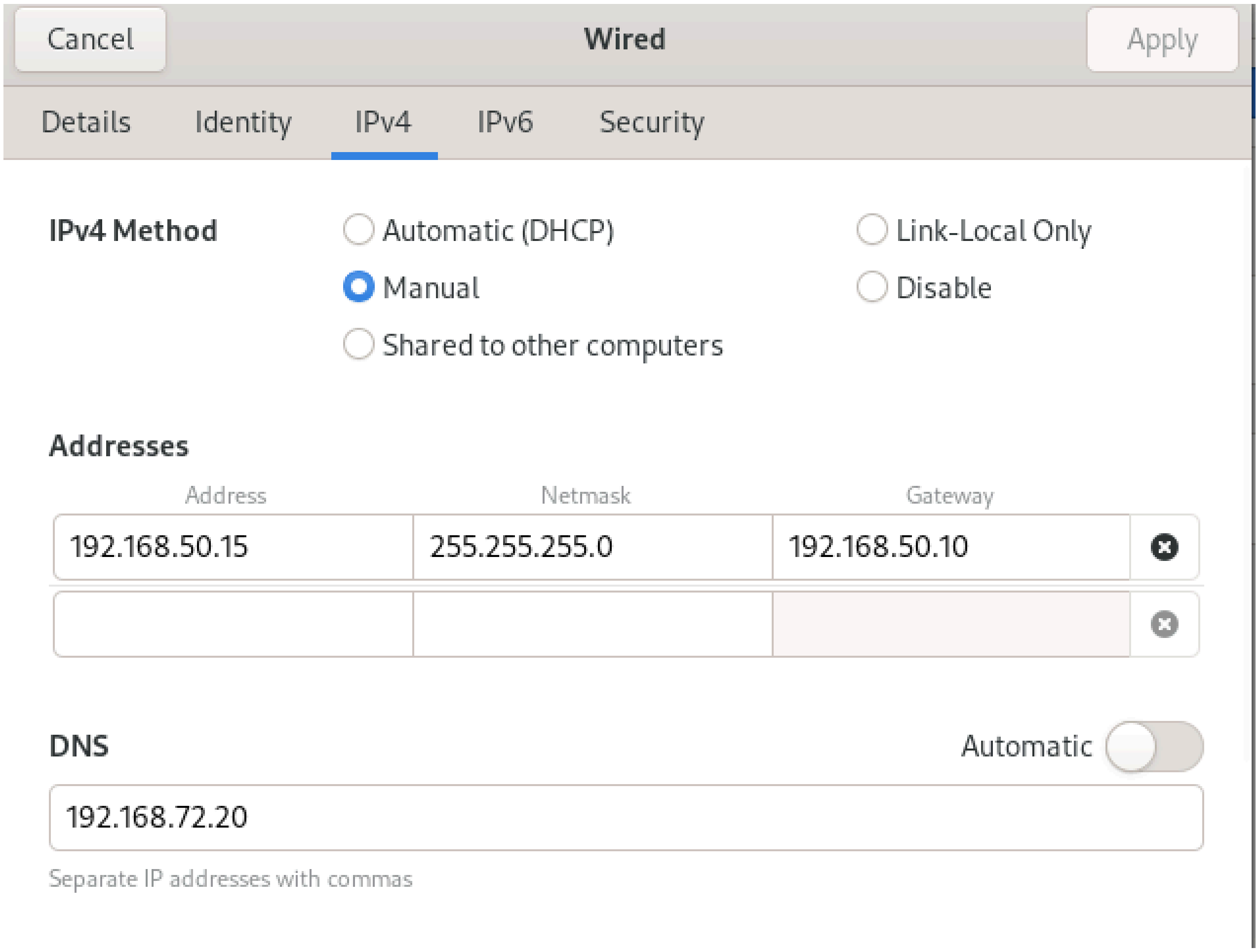
Enable ☑ Check this option to enable squidGuard.

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.**

SquidGuard service state: **STOPPED**

everything into the firewall = **UTM**
else packet filter firewall
web filter firewall

clients



IPv4 Method

○ Automatic (DHCP) ○ Link-Local Only

● Manual ○ Disable

○ Shared to other computers

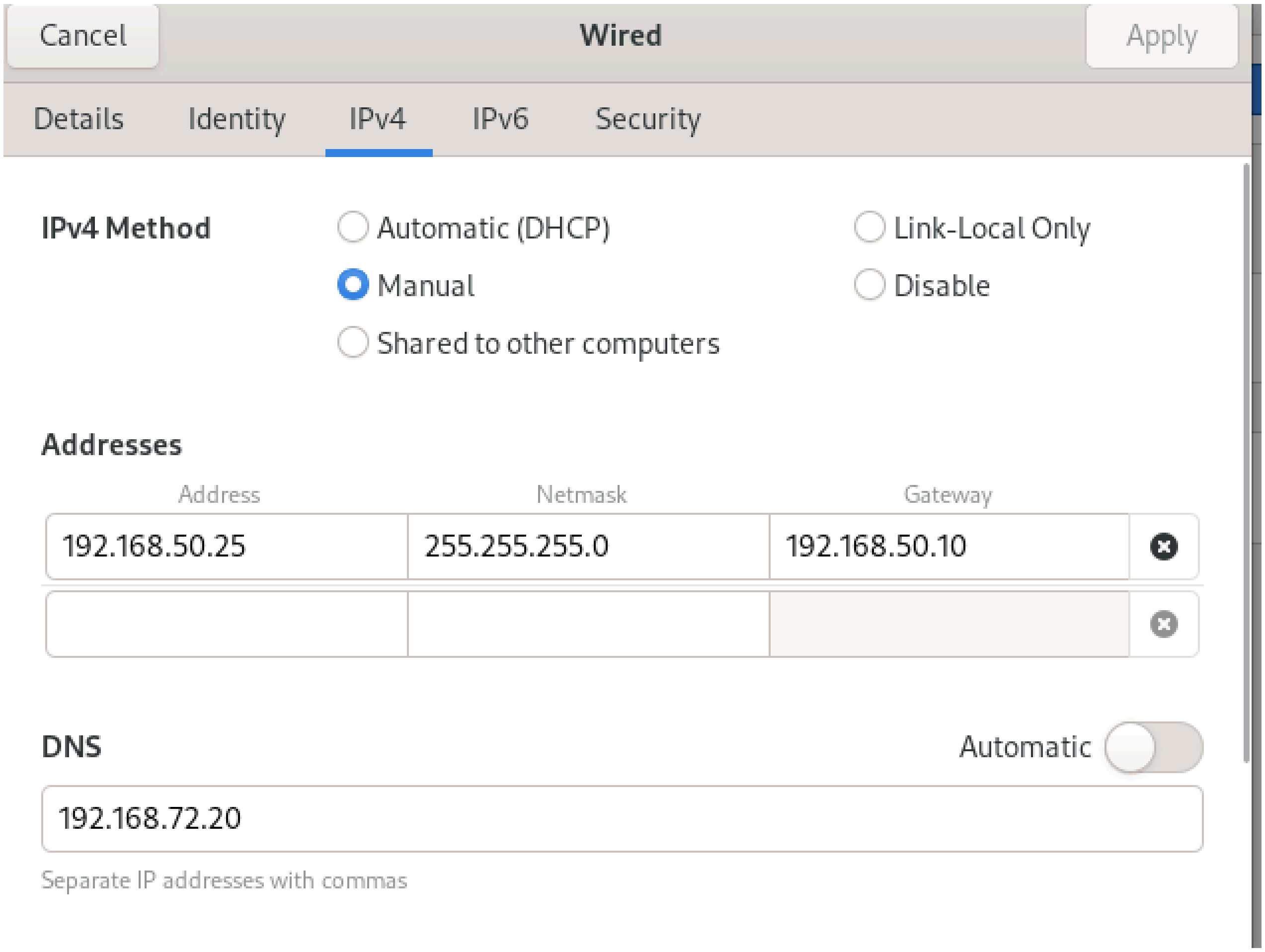
Addresses

Address	Netmask	Gateway
192.168.50.15	255.255.255.0	192.168.50.10

DNS Automatic ○

192.168.72.20

Separate IP addresses with commas



IPv4 Method

○ Automatic (DHCP) ○ Link-Local Only

● Manual ○ Disable

○ Shared to other computers

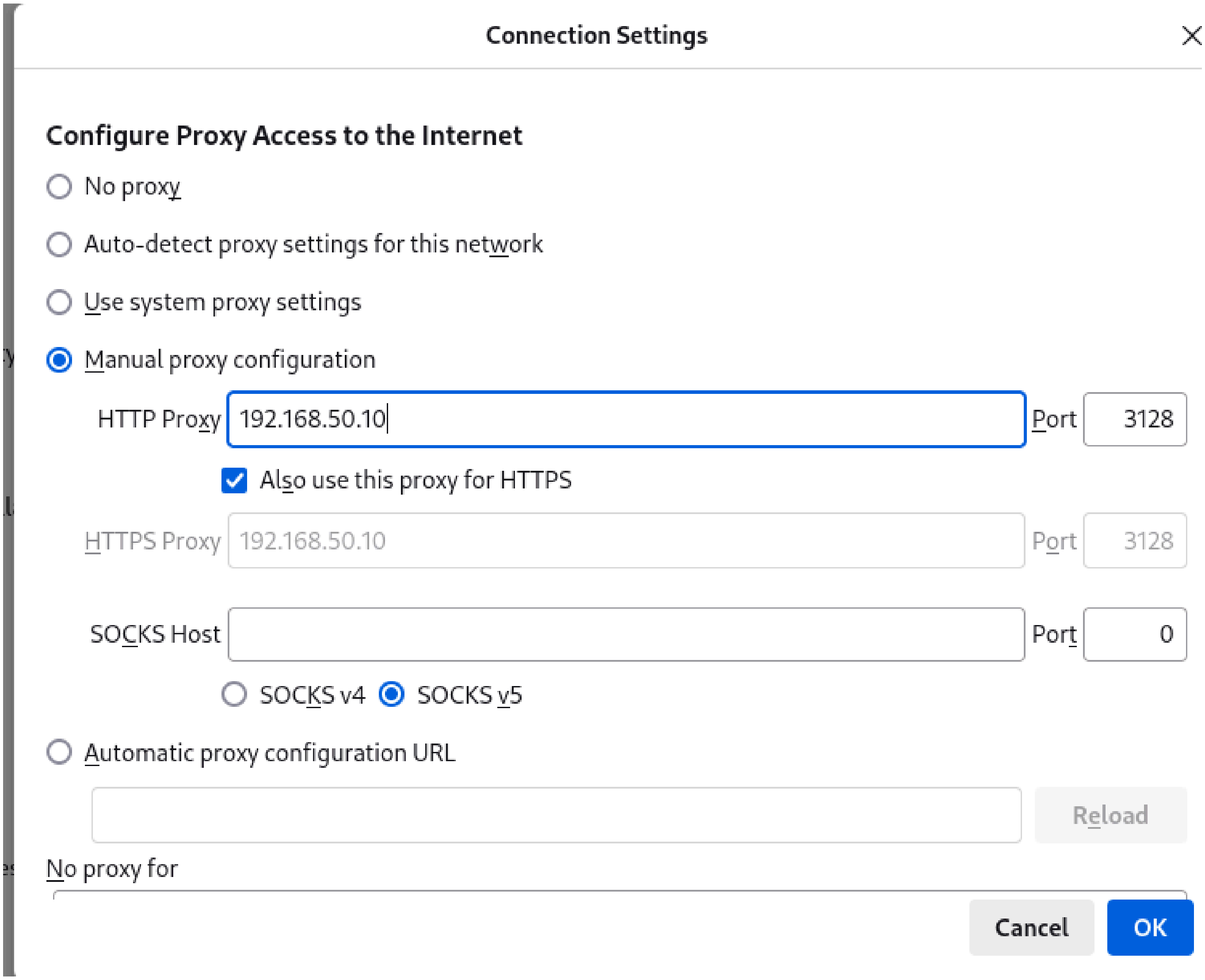
Addresses

Address	Netmask	Gateway
192.168.50.25	255.255.255.0	192.168.50.10

DNS Automatic ○

192.168.72.20

Separate IP addresses with commas



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 192.168.50.10 Port 3128

☑ Also use this proxy for HTTPS

HTTPS Proxy 192.168.50.10 Port 3128

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

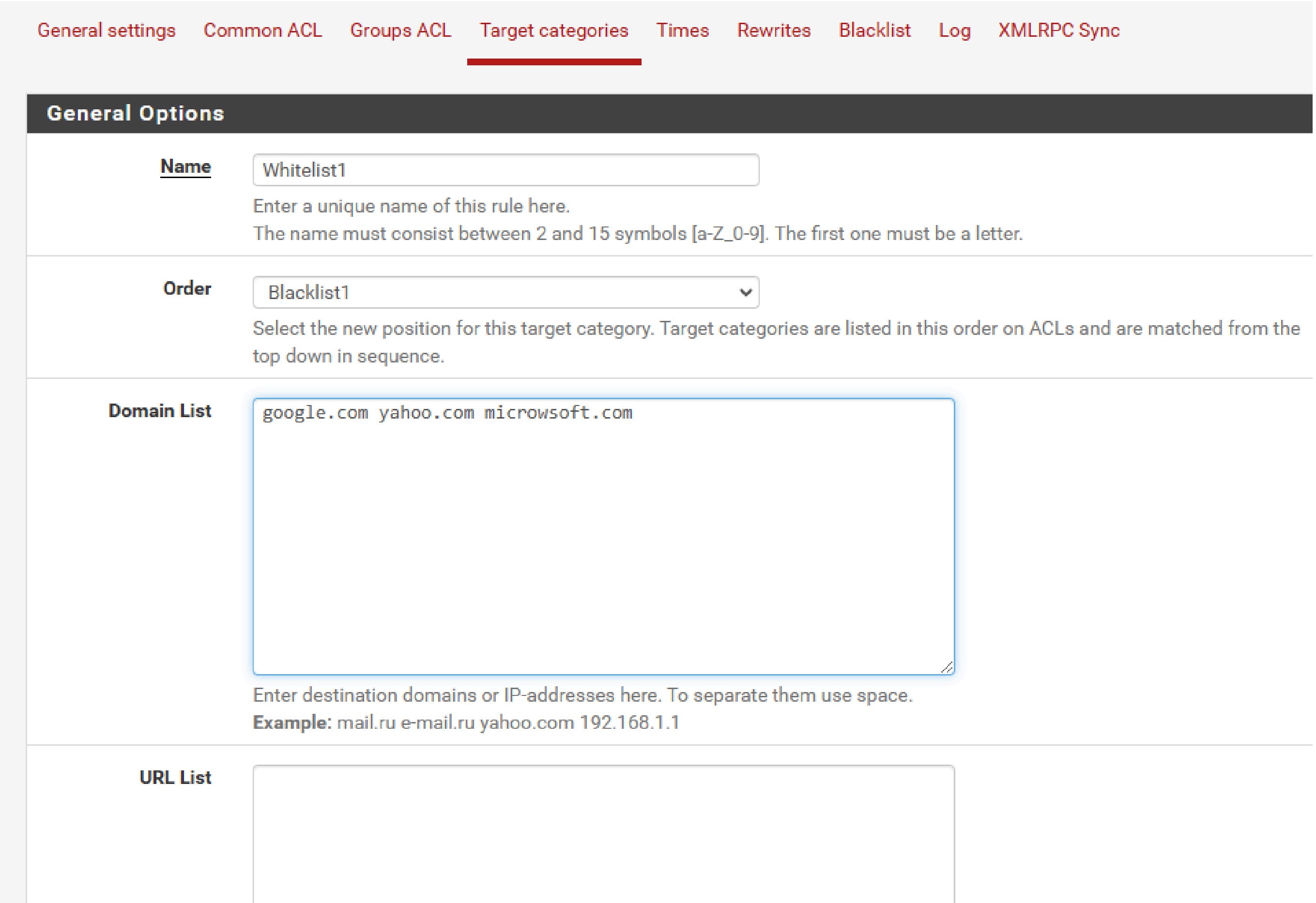
○ Automatic proxy configuration URL

default action in pfsense is deny all whixch is why any sites wont open

pfsense site:

common acl target rule +
allow whitelist1

✅ Do no allow ip address in url
✅ use safe search engine
✅ log



General Options

Name: Whitelist1

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: Blacklist1

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:

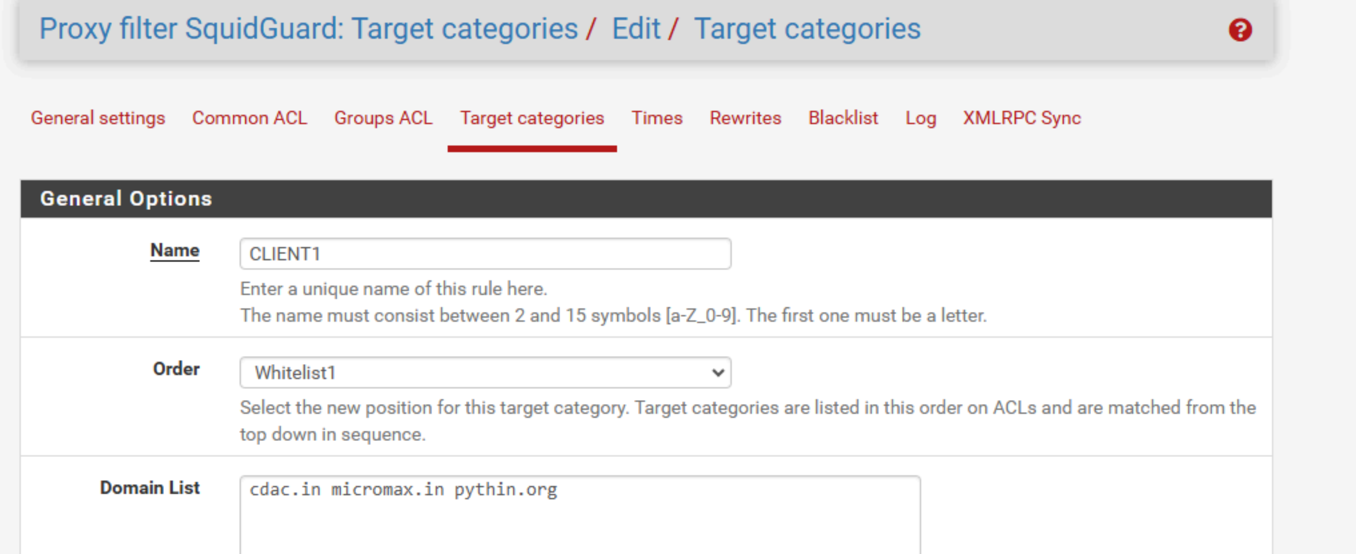
```
google.com yahoo.com microwsoft.com
```

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

URL List

whenever you make any changes, go to general settings and click on apply

GROUP ACL
WE WANT TO ALLOW MORW SITES FOR CLIENT 1


Proxy filter SquidGuard: Target categories / Edit / Target categories

General Options

Name: CLIENT1

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: Whitelist1

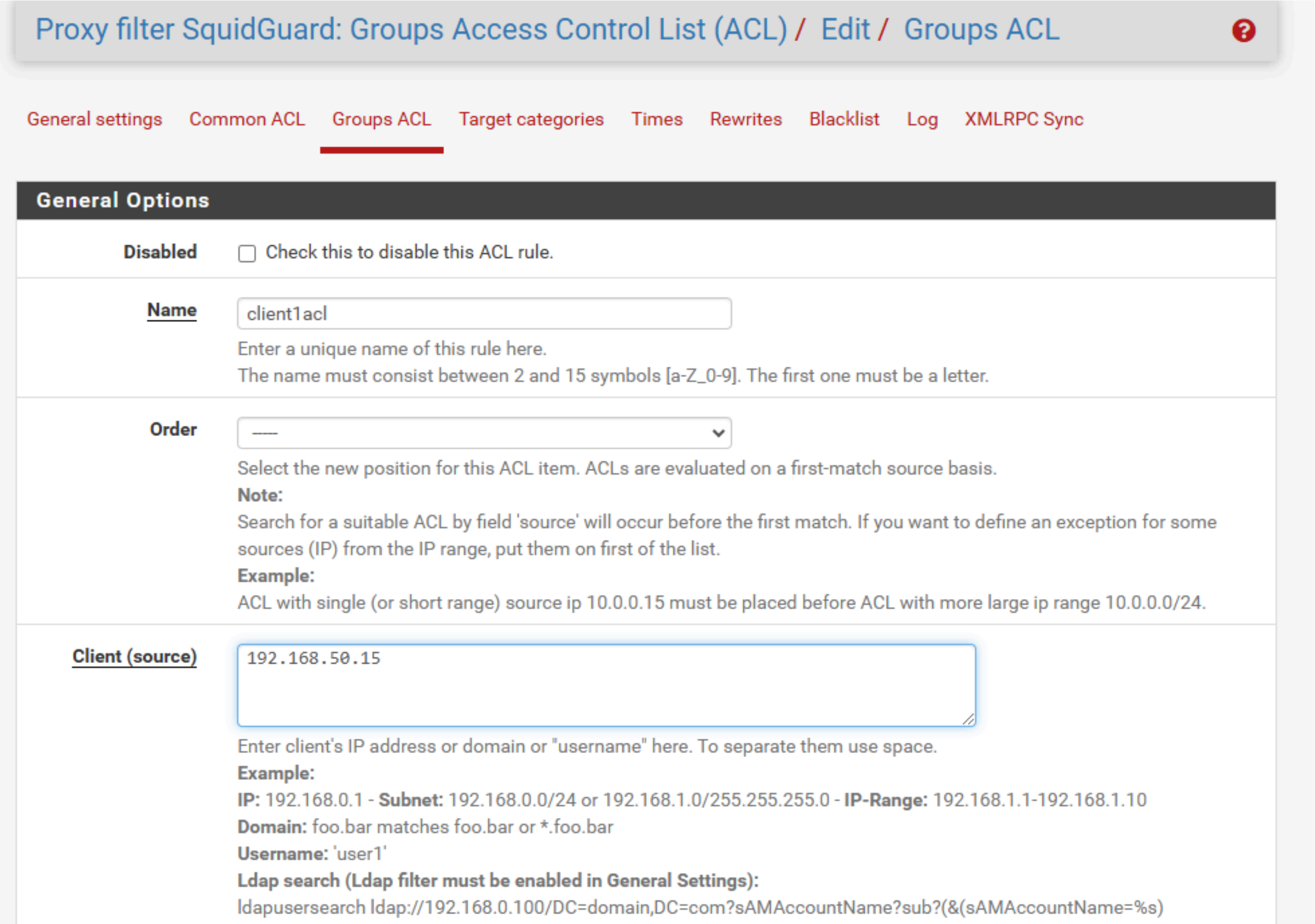
Select the new position for this target category. Target categories are listed in this order on ACLs and are matched from the top down in sequence.

Domain List:

```
cdac.in micromax.in pythin.org
```

log save

group acl --> add --> give name



Proxy filter SquidGuard: Groups Access Control List (ACL) / Edit / Groups ACL

General Options

Disabled □ Check this to disable this ACL rule.

Name client1acl

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.

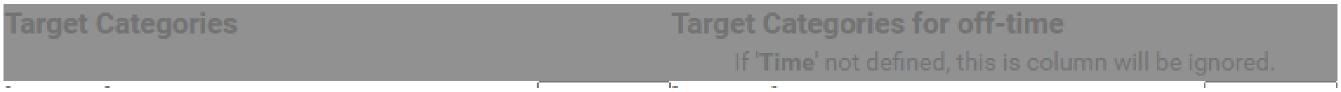
Order -----

Select the new position for this ACL item. ACLs are evaluated on a first-match source basis.
Note:
Search for a suitable ACL by field 'source' will occur before the first match. If you want to define an exception for some sources (IP) from the IP range, put them on first of the list.
Example:
ACL 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) 192.168.50.15

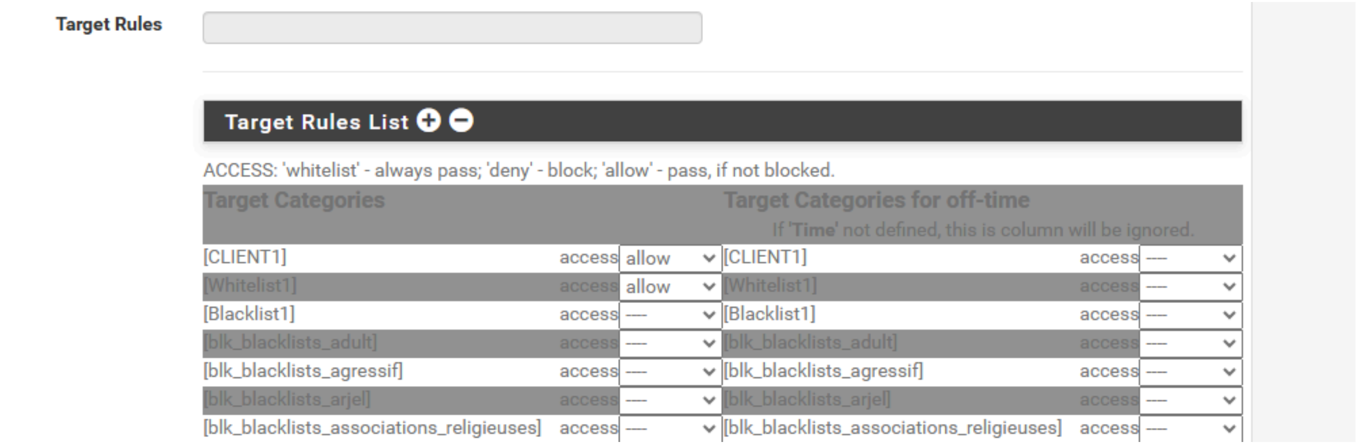
Enter client's IP address or domain or "username" here. To separate them use space.
Example:
IP: 192.168.0.1 - **Subnet:** 192.168.0.0/24 or 192.168.1.0/255.255.255.0 - **IP-Range:** 192.168.1.1-192.168.1.10
Domain: foo.bar matches foo.bar or *.foo.bar
Username: 'user1'
Ldap search (Ldap filter must be enabled in General Settings):
ldapusersearch ldap://192.168.0.100/DC=domain,DC=com?sAMAccountName?sub?(&(sAMAccountName=%s)

for any user on that machine, give his username in single quotes



Target Categories | **Target Categories for off-time**
If '**Time**' not defined, this is column will be ignored.

intime off time



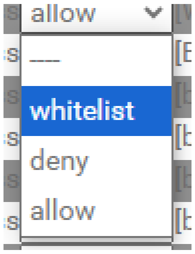
Target Rules

Target Rules List

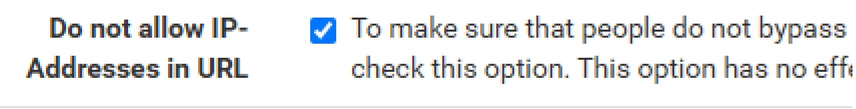
ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.

Target Categories			Target Categories for off-time If '**Time**' not defined, this is column will be ignored.		
[CLIENT1]	access	allow	[CLIENT1]	access	---
[Whitelist1]	access	allow	[Whitelist1]	access	---
[Blacklist1]	access	---	[Blacklist1]	access	---
[blk_blacklists_adult]	access	---	[blk_blacklists_adult]	access	---
[blk_blacklists_agressif]	access	---	[blk_blacklists_agressif]	access	---
[blk_blacklists_arjel]	access	---	[blk_blacklists_arjel]	access	---
[blk_blacklists_associations_religieuses]	access	---	[blk_blacklists_associations_religieuses]	access	---

last option as deny



- do not check for any rule, compulsorily allow

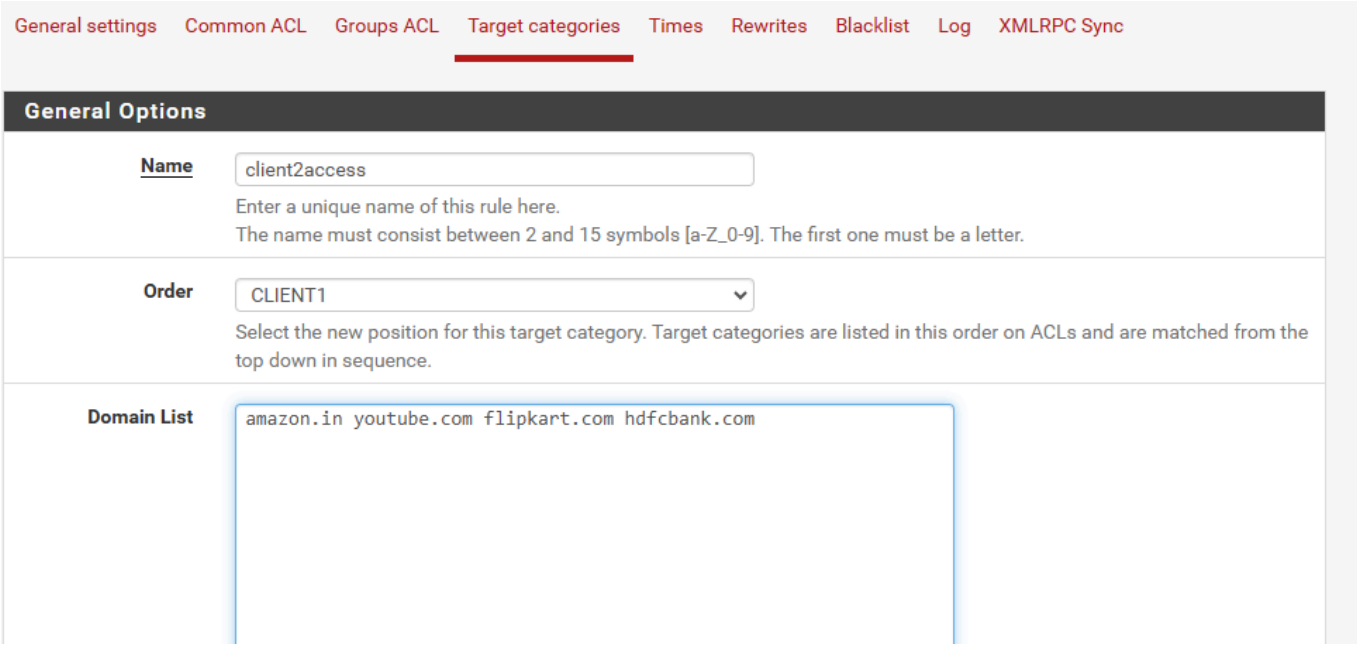


Do not allow IP-Addresses in URL ☑ To make sure that people do not bypass check this option. This option has no eff

safemode and logs as well

---

client2



General Options

Name	client2access 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	CLIENT1 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	amazon.in youtube.com flipkart.com hdfcbank.com

common acl is more restrictive

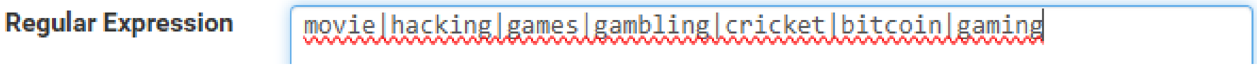
GROUP ACL HAS PRIORITY OVER COMMON ACL

---

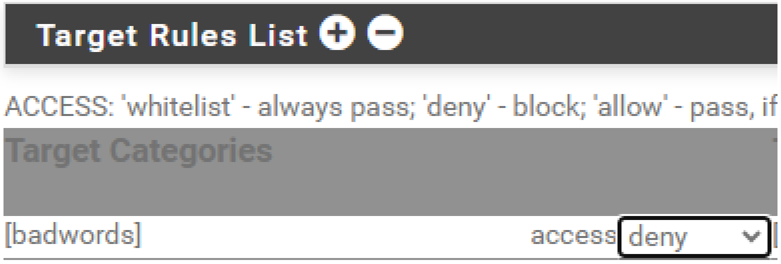
block bad words

donot start any names with allow block deny etc

target categ -> regular expressions



Regular Expression: movie|hacking|games|gambling|cricket|bitcoin|gaming



ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if

Target Categories

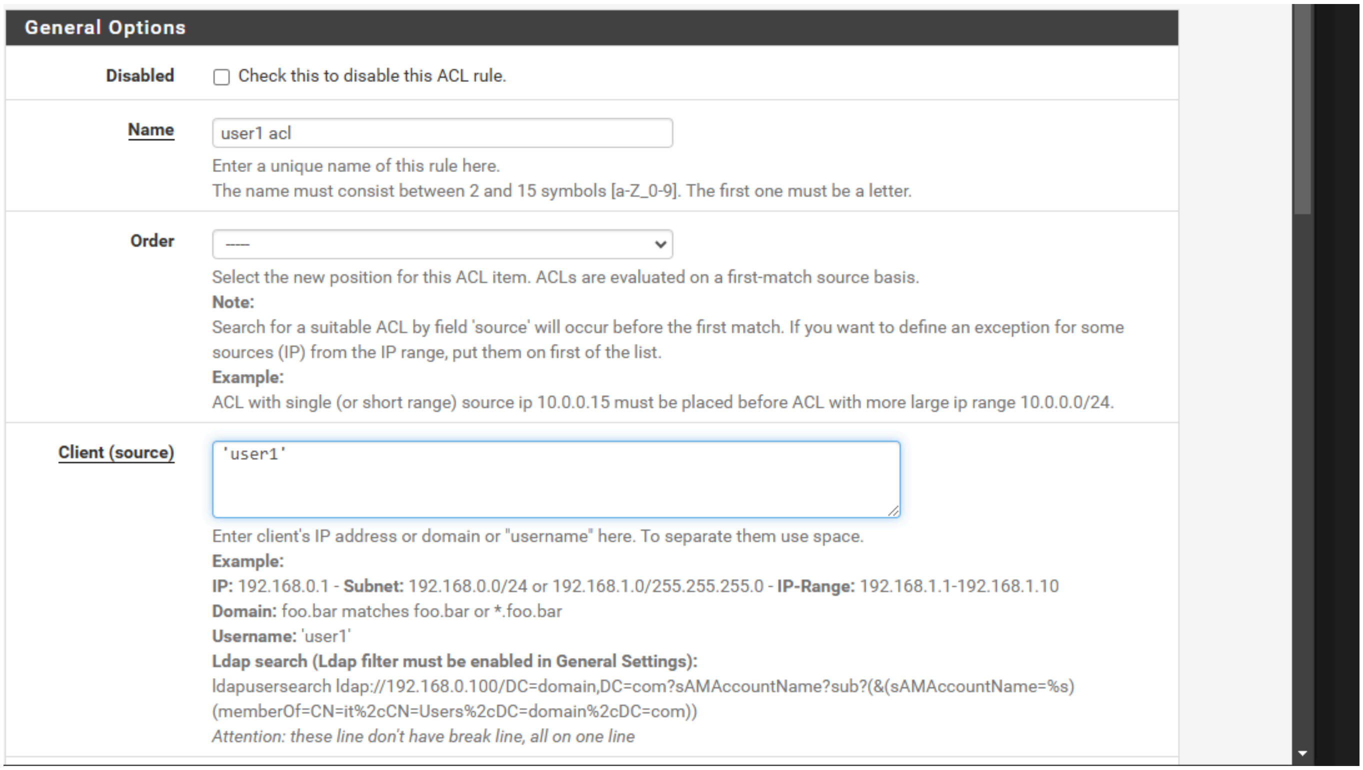
[badwords] access deny

Creating users

services --> squid proxy server --> Auth method local

users add save
general --> restart the service

services-->squidguard proxy filter



General Options

Disabled: □ Check this to disable this ACL rule.

Name: user1 acl

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: ----

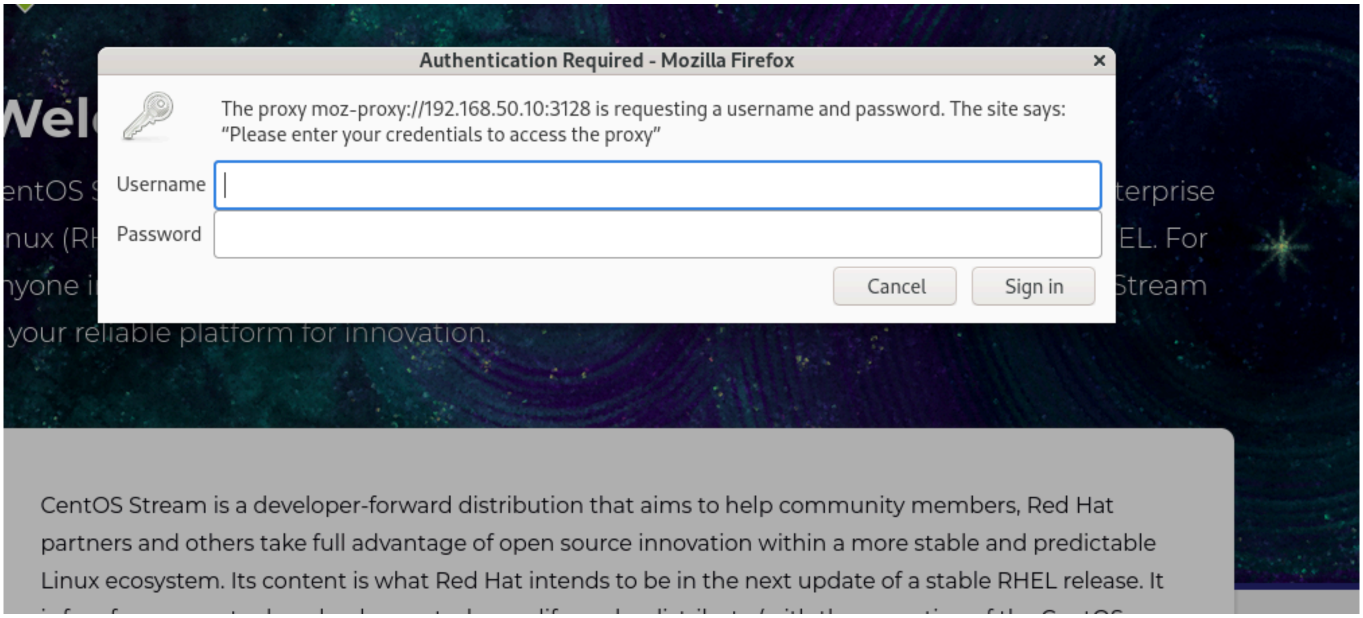
Select the new position for this ACL item. ACLs are evaluated on a first-match source basis.
Note:
Search for a suitable ACL by field 'source' will occur before the first match. If you want to define an exception for some sources (IP) from the IP range, put them on first of the list.
Example:
ACL with 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): 'user1'

Enter client's IP address or domain or "username" here. To separate them use space.
Example:
IP: 192.168.0.1 - **Subnet:** 192.168.0.0/24 or 192.168.1.0/255.255.255.0 - **IP-Range:** 192.168.1.1-192.168.1.10
Domain: foo.bar matches foo.bar or *.foo.bar
Username: 'user1'
Ldap search (Ldap filter must be enabled in General Settings):
ldapusersearch ldap://192.168.0.100/DC=domain,DC=com?sAMAccountName?sub?(&(sAMAccountName=%s)(memberOf=CN=it%2cCN=Users%2cDC=domain%2cDC=com))
Attention: these line don't have break line, all on one line

target list whitelist-alllow clienttg-allow

defaiult accesss deny



Authentication Required - Mozilla Firefox

The proxy moz-proxy://192.168.50.10:3128 is requesting a username and password. The site says: “Please enter your credentials to access the proxy”

Username

Password

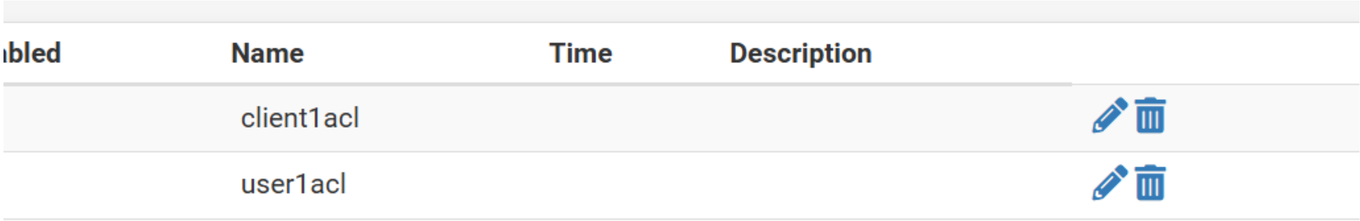
Cancel Sign in

CentOS Stream is a developer-forward distribution that aims to help community members, Red Hat partners and others take full advantage of open source innovation within a more stable and predictable Linux ecosystem. Its content is what Red Hat intends to be in the next update of a stable RHEL release. It

priority bw user and ip acl

user1--deny=whiutelist---default rule=allow

create client1acl
gieve ip
trl = allow whitelist
deny all

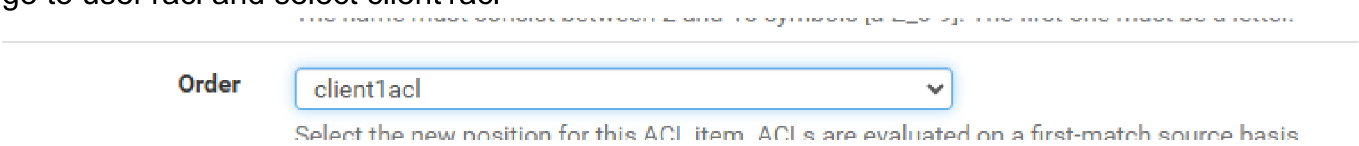


ıbled	Name	Time	Description
	client1acl		
	user1acl		

ip is given the preference

change order

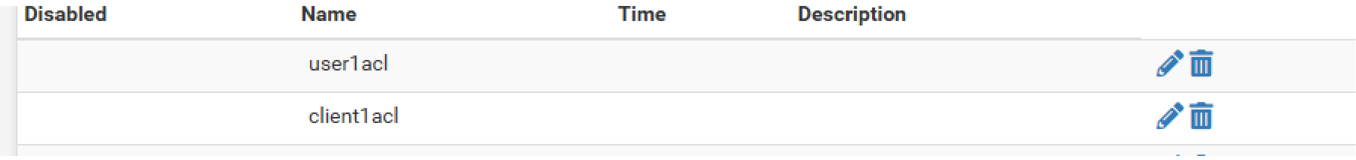
go to user1acl and select client1acl



The name must consist between 2 and 15 symbols [a-Z_0-9]. The first one must be a letter.

Order: client1acl

Select the new position for this ACL item. ACLs are evaluated on a first-match source basis.



Disabled	Name	Time	Description
	user1acl		
	client1acl		

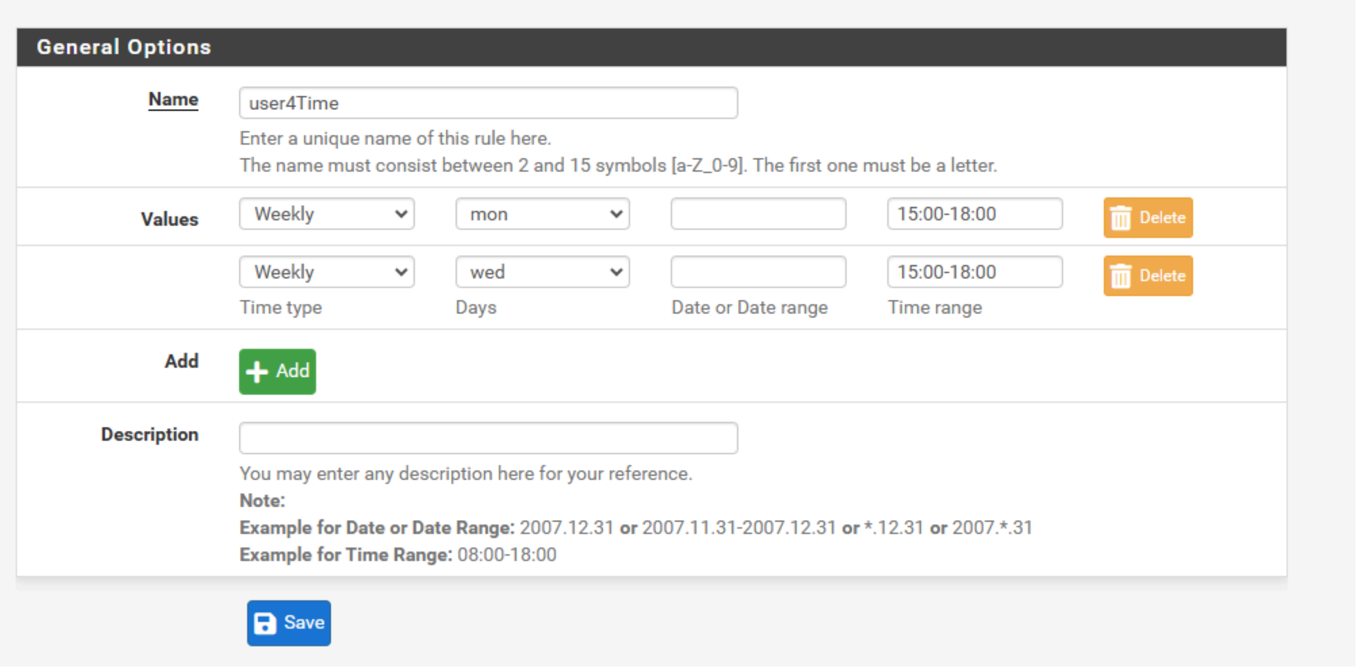
HERE USER IS GIVEN PREFERENCE

HENCE THE PREFERENCE IS DECIDED DEPENDING ON TH ORDER OF ENTRY

time based acl

guard;

timr--



General Options

Name user4Time

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.

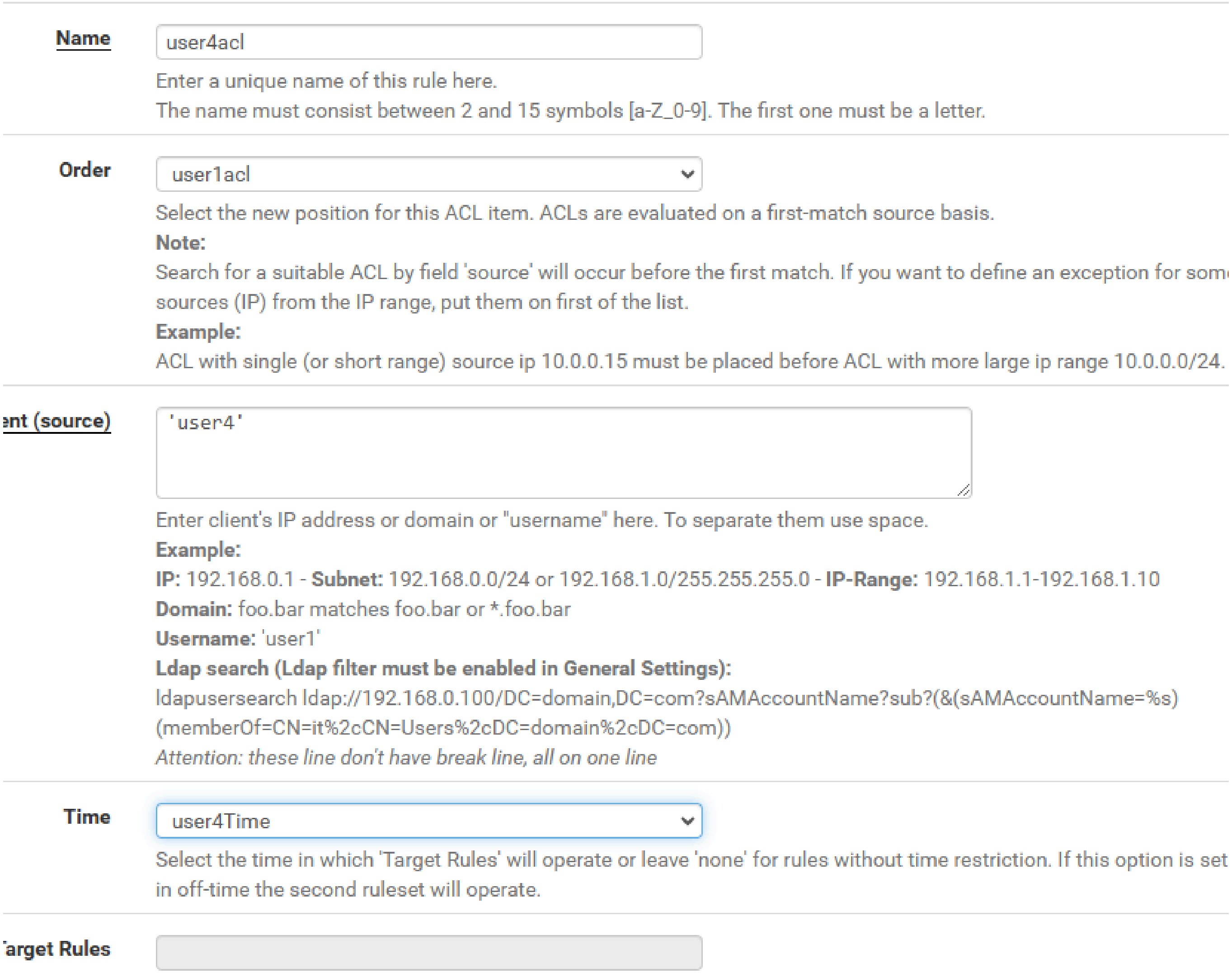
Values	Weekly	mon		15:00-18:00	Delete
	Weekly	wed		15:00-18:00	Delete
	Time type	Days	Date or Date range	Time range	

Add + Add

Description

You may enter any description here for your reference.
Note:
Example for Date or Date Range: 2007.12.31 **or** 2007.11.31-2007.12.31 **or** *.12.31 **or** 2007.*.31
Example for Time Range: 08:00-18:00

Save



Name user4acl

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 user1acl

Select the new position for this ACL item. ACLs are evaluated on a first-match source basis.
Note:
Search for a suitable ACL by field 'source' will occur before the first match. If you want to define an exception for som sources (IP) from the IP range, put them on first of the list.
Example:
ACL 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.

ent (source)

```
'user4'
```

Enter client's IP address or domain or "username" here. To separate them use space.
Example:
IP: 192.168.0.1 - **Subnet:** 192.168.0.0/24 or 192.168.1.0/255.255.255.0 - **IP-Range:** 192.168.1.1-192.168.1.10
Domain: foo.bar matches foo.bar or *.foo.bar
Username: 'user1'
Ldap search (Ldap filter must be enabled in General Settings):
ldapusersearch ldap://192.168.0.100/DC=domain,DC=com?sAMAccountName?sub?(&(sAMAccountName=%s)(memberOf=CN=it%2cCN=Users%2cDC=domain%2cDC=com))
Attention: these line don't have break line, all on one line

Time user4Time

Select the time in which 'Target Rules' will operate or leave 'none' for rules without time restriction. If this option is set in off-time the second ruleset will operate.

arget Rules

ontime offtime

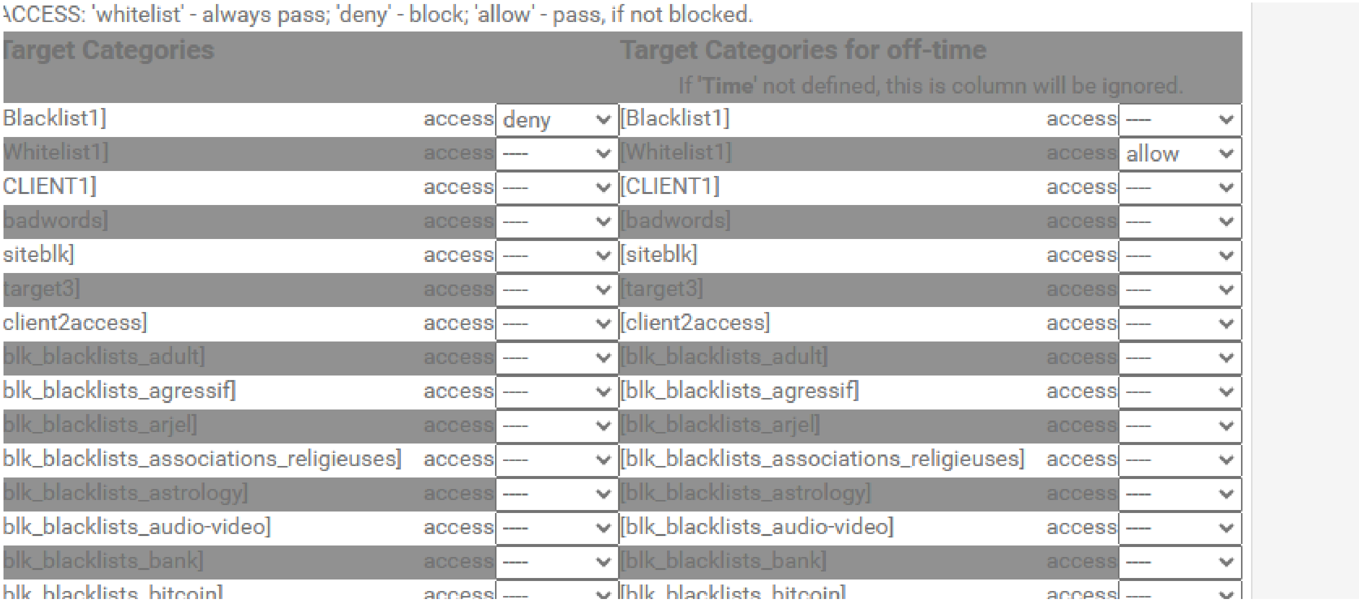
deny allow

allow all deny all

gen settings apply

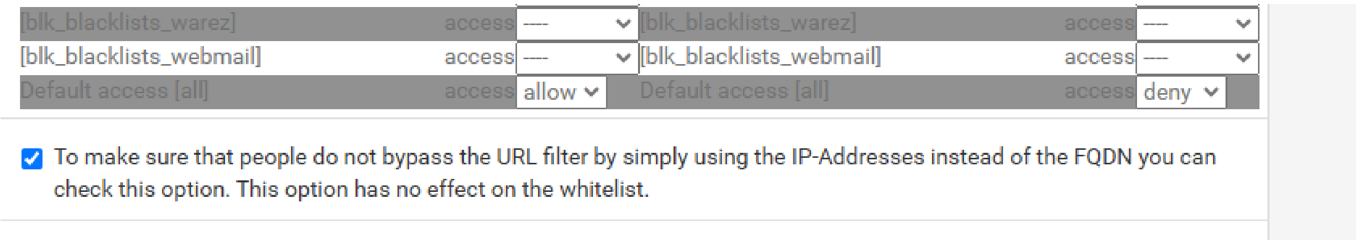
services--> squid proxy server -- creeate user

exercise:
create user10 - on all days - 9:00 to 19:00-user can access all websites except amazon.in flipkart.com myntra and after 1900 user cannot access any sites except google microsoft redhat python



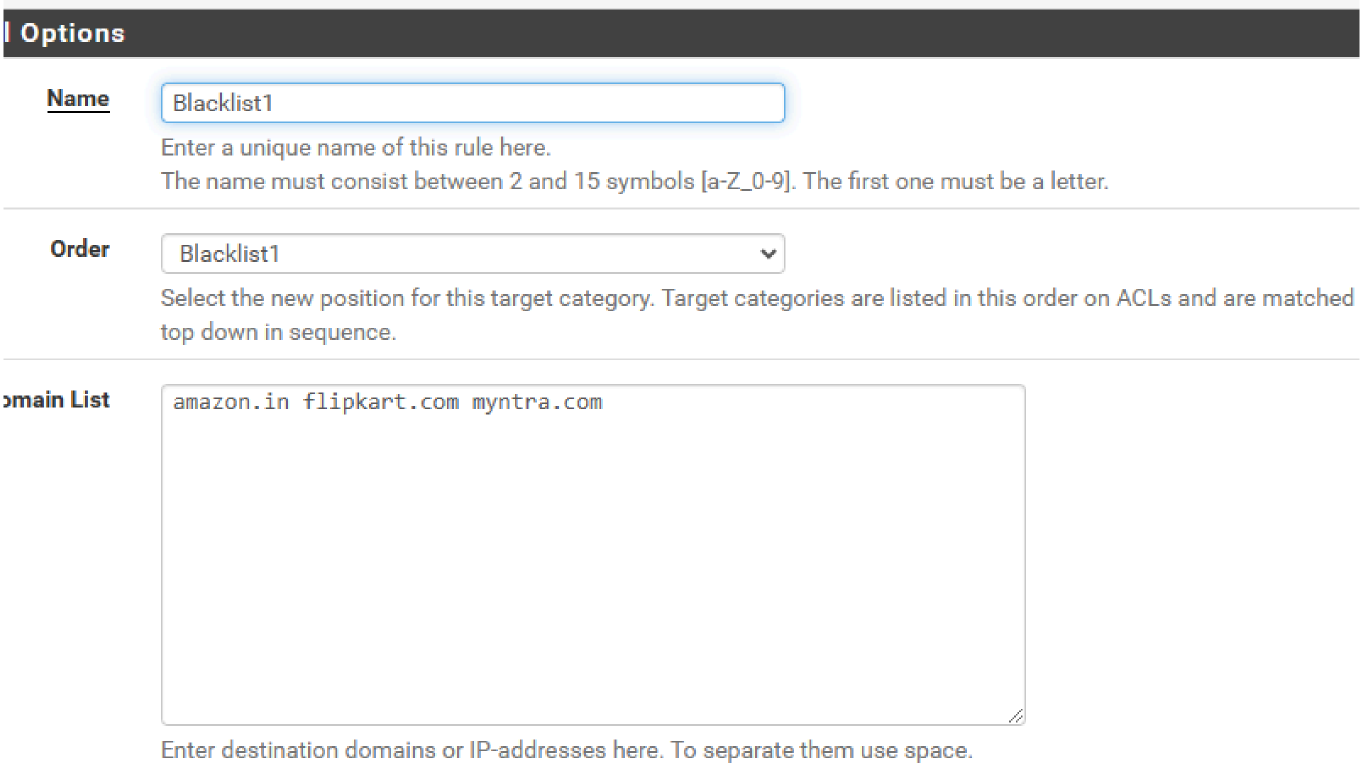
ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.

Target Categories			Target Categories for off-time If **'Time'** not defined, this is column will be ignored.		
Blacklist1]	access	deny	[Blacklist1]	access	----
Whitelist1]	access	----	[Whitelist1]	access	allow
CLIENT1]	access	----	[CLIENT1]	access	----
badwords]	access	----	[badwords]	access	----
siteblk]	access	----	[siteblk]	access	----
target3]	access	----	[target3]	access	----
client2access]	access	----	[client2access]	access	----
blk_blacklists_adult]	access	----	[blk_blacklists_adult]	access	----
blk_blacklists_agressif]	access	----	[blk_blacklists_agressif]	access	----
blk_blacklists_arjel]	access	----	[blk_blacklists_arjel]	access	----
blk_blacklists_associations_religieuses]	access	----	[blk_blacklists_associations_religieuses]	access	----
blk_blacklists_astrology]	access	----	[blk_blacklists_astrology]	access	----
blk_blacklists_audio-video]	access	----	[blk_blacklists_audio-video]	access	----
blk_blacklists_bank]	access	----	[blk_blacklists_bank]	access	----
blk_blacklists_bitcoin]	access	----	[blk_blacklists_bitcoin]	access	----



[blk_blacklists_warez]	access	----	[blk_blacklists_warez]	access	----
[blk_blacklists_webmail]	access	----	[blk_blacklists_webmail]	access	----
Default access [all]	access	allow	Default access [all]	access	deny

☑ 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.



l Options

Name	Blacklist1

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.

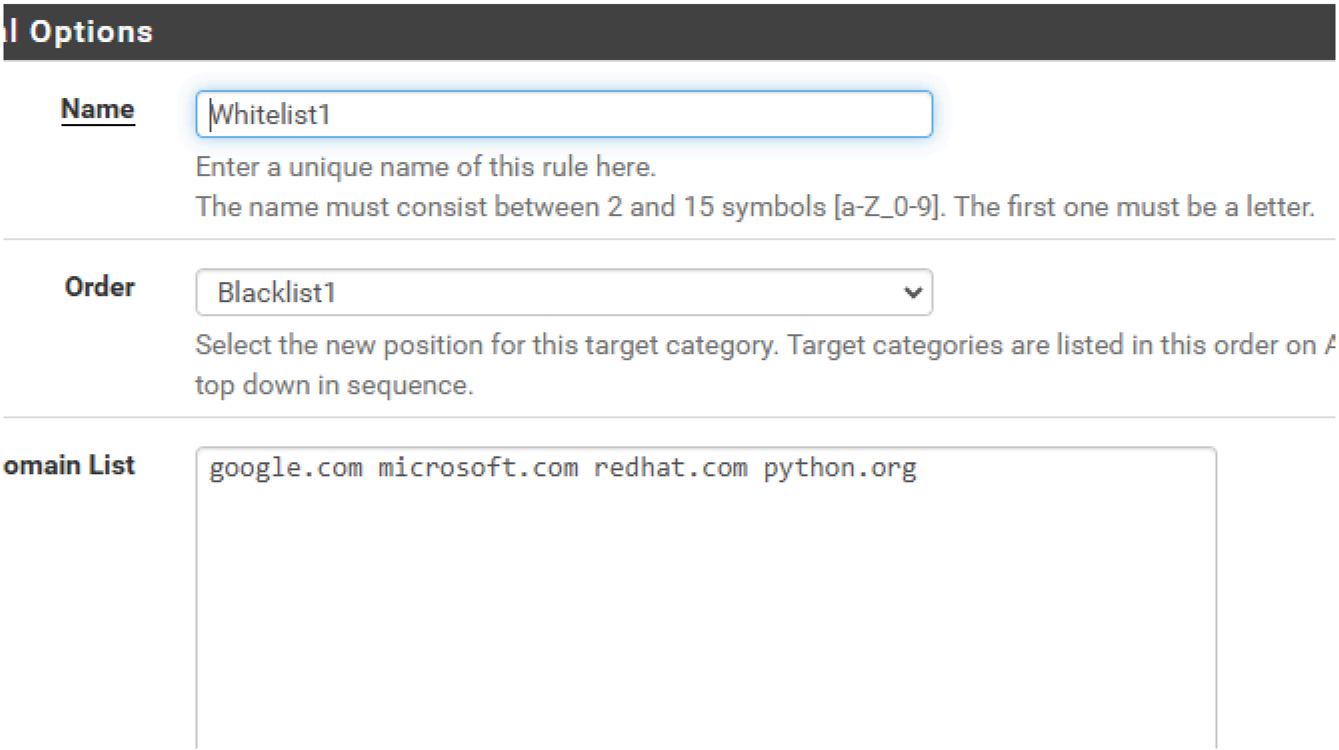
Order	Blacklist1

Select the new position for this target category. Target categories are listed in this order on ACLs and are matched top down in sequence.

omain List

```
amazon.in flipkart.com myntra.com
```

Enter destination domains or IP-addresses here. To separate them use space.



l Options

Name	Whitelist1

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	Blacklist1

Select the new position for this target category. Target categories are listed in this order on A
top down in sequence.

omain List

```
google.com microsoft.com redhat.com python.org
```