Implementação da ferramenta PFSENSE para a empresa Associação de Médicos de hospitais privados do Distrito Federal- AMHP

INTRODUÇÃO

A empresa suporteCorp solução em tecnologia da informação apresenta a empresa Associação de Médicos de hospitais privados do Distrito Federalo- AMHP projeto de configuração da ferrameta Pfsense, implementando a melhor solução para o sistema.

OBJETIVO

Consiste na implementação e configuração de uma nova solução de firewall para atender as demandas da empresa com alta disponibilidade, Escalabilidade e Adaptabilidade.

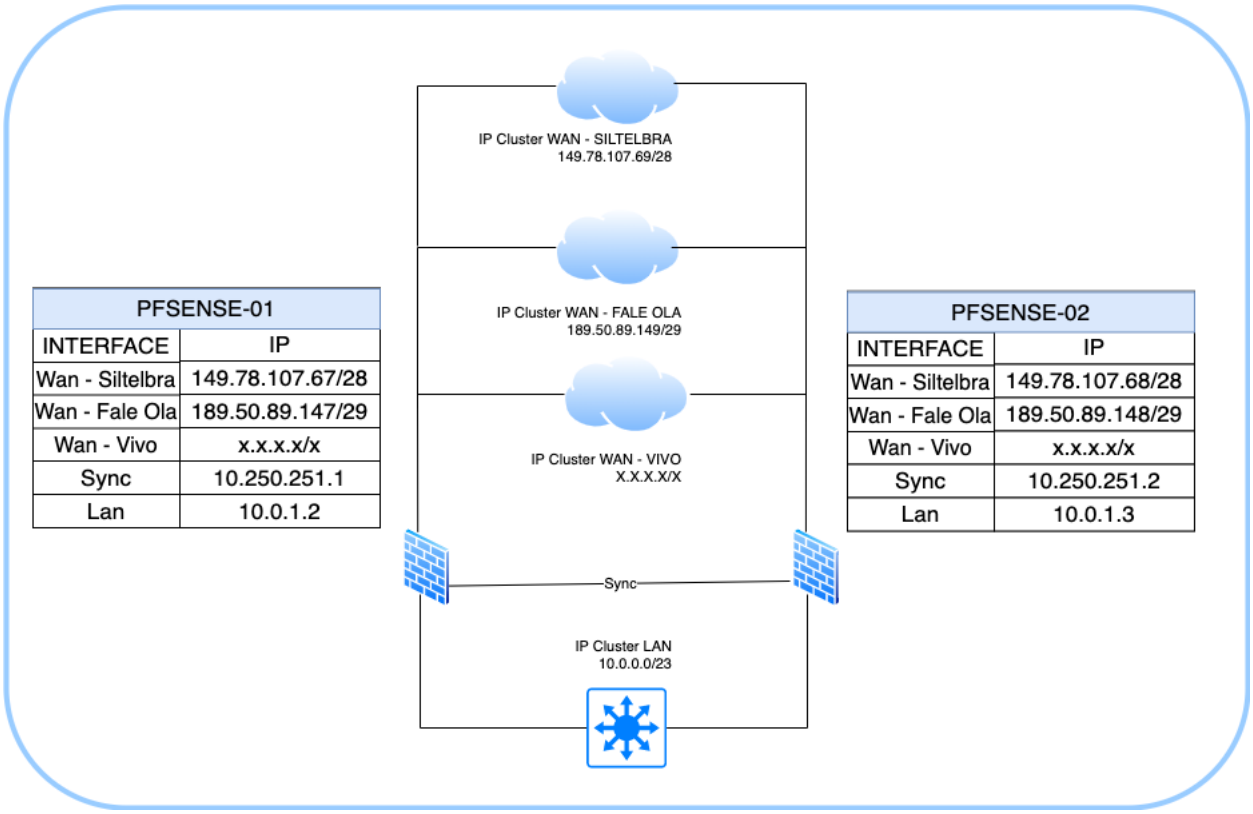
SOLUÇÃO

Foi configurados o pfsense com os seguintes itens, plugins:

1. Instalação do software pfsense em 2 servidores físico;
2. Configuração de acesso ao Pfsense via active directory “Windows”
3. Criar Loadblancer de 2 interfaces de WAN;
4. Configurar HA dos servidores de pfsense;
5. Configurar bond de 2 interfaces LAN, caso necessário;
6. Configurar VPN “OPENVPN” Client to server;
7. Criar certificado local open source para acesso VPN;
8. Ativar plugin squid ou squidGuard;
9. Fazer integração dos plugins squid ou squidguard com active directory “Windows”;
10. Definir grupos de acesso a internet via AD;
11. Criar backup da configuração do pfsense;
12. Criação das regras de firewall de acesso a internet;
13. Definir rotas para o Pfsense;

TOPOLOGIA DE REDE

Diagrama de Topologia Lógica



PFSENSE-01	
INTERFACE	IP
Wan - Siltelbra	149.78.107.67/28
Wan - Fale Ola	189.50.89.147/29
Wan - Vivo	x.x.x.x/x
Sync	10.250.251.1
Lan	10.0.1.2

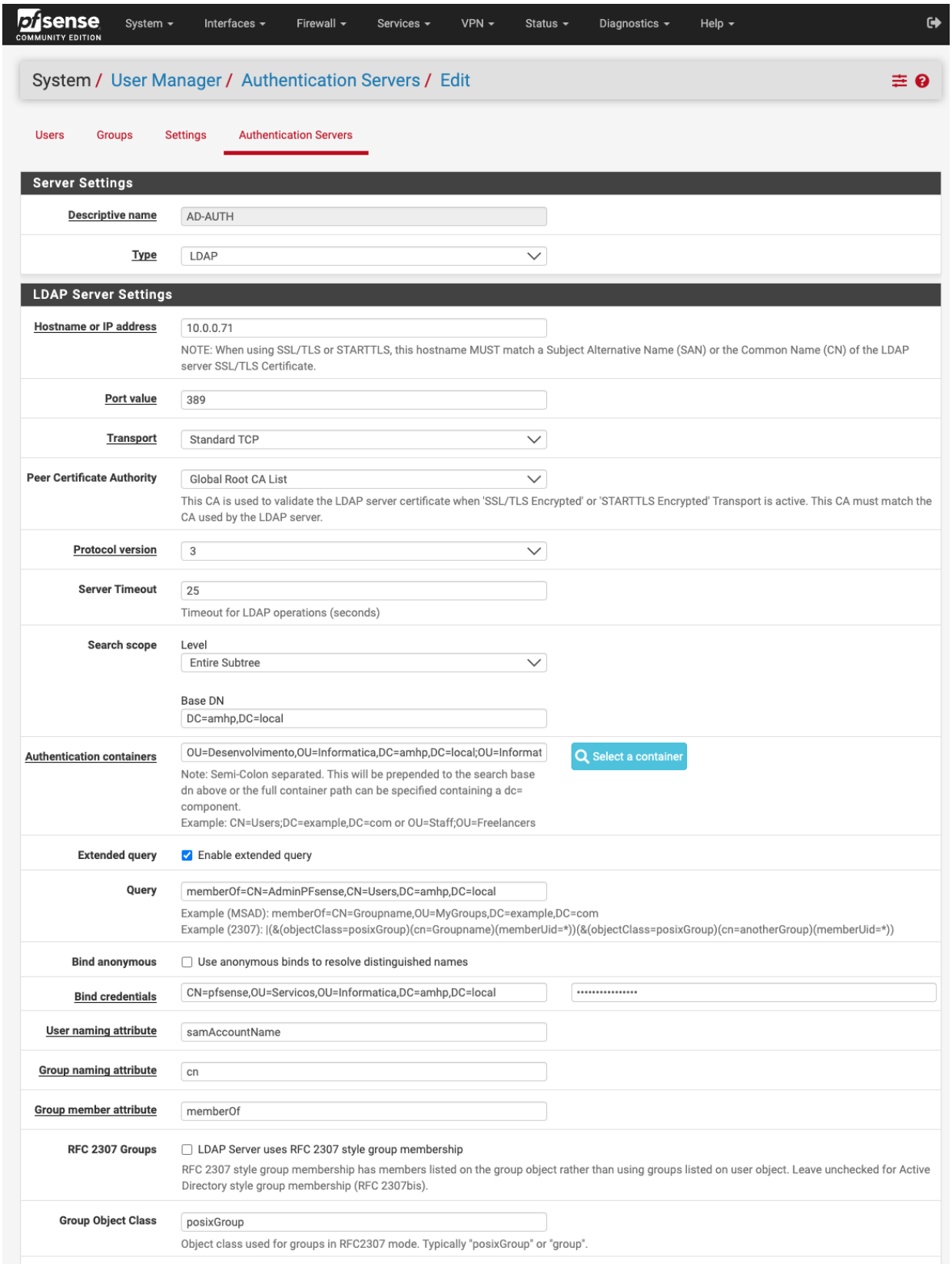
PFSENSE-02	
INTERFACE	IP
Wan - Siltelbra	149.78.107.68/28
Wan - Fale Ola	189.50.89.148/29
Wan - Vivo	x.x.x.x/x
Sync	10.250.251.2
Lan	10.0.1.3

FIREWALL

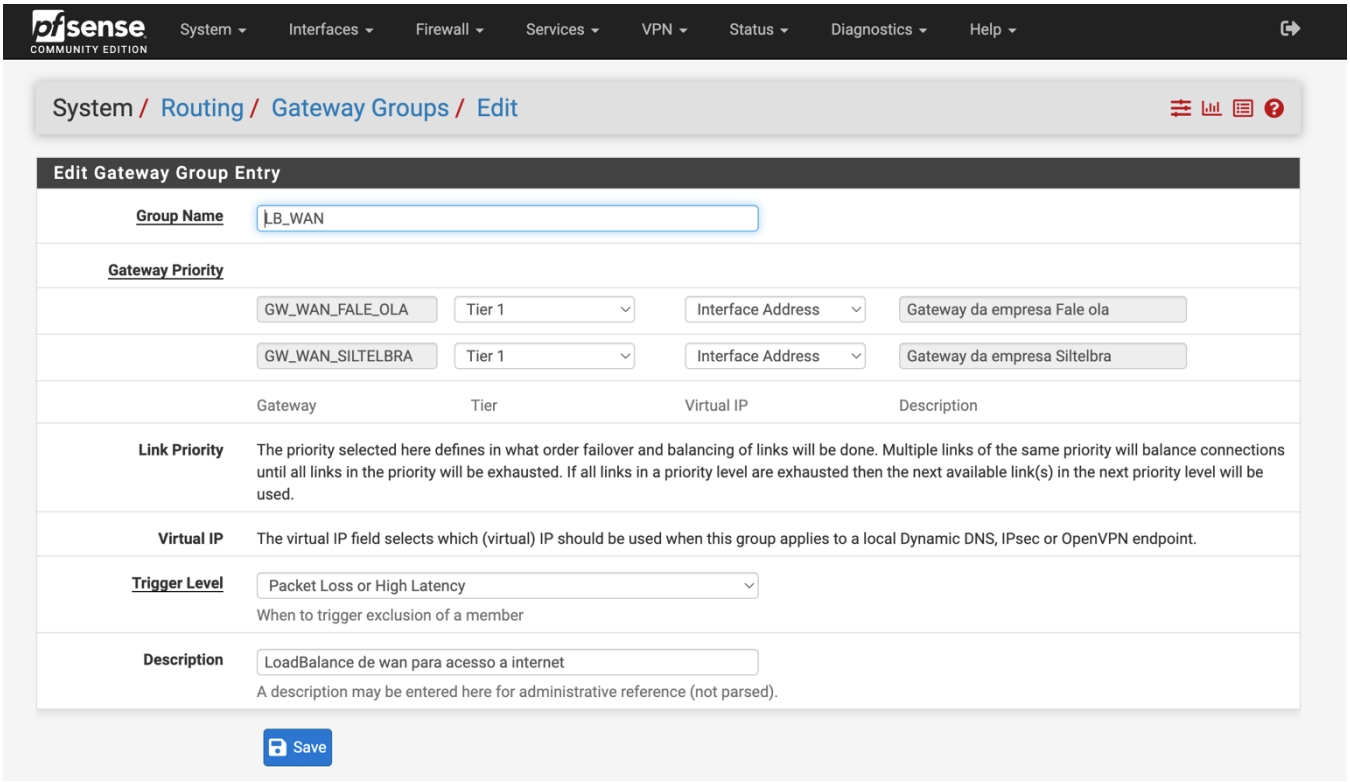
Nome	INTERFACE	IP / Mask	VIP	Localização
FW-01.AMHP.LOCAL	WAN - SILTELBRA	149.78.107.69/28	OK	Datacenter
	WAN FALE OLA	189.50.89.149/29	OK	Datacenter
	WAN VIVO	X.X.X.X/X	OK	Datacenter
	-	-	-	Datacenter
	LAN	10.0.1.1	OK	Datacenter
FW-01.AMHP.LOCAL	WAN - SILTELBRA	149.78.107.67/28	-	Datacenter
	WAN FALE OLA	189.50.89.147/29	-	Datacenter
	WAN VIVO	X.X.X.X/X	-	Datacenter
	SYNC	10.250.251.1	-	Datacenter
	LAN	10.0.1.2	-	Datacenter
FW-02.AMHP.LOCAL	WAN - SILTELBRA	149.78.107.68/28	-	Datacenter
	WAN FALE OLA	189.50.89.149/29	-	Datacenter
	WAN VIVO	X.X.X.X/X	-	Datacenter
	SYNC	10.250.251.2	-	Datacenter
	LAN	10.0.1.3	-	Datacenter

Instalação do software pfsense em 2 servidores físico

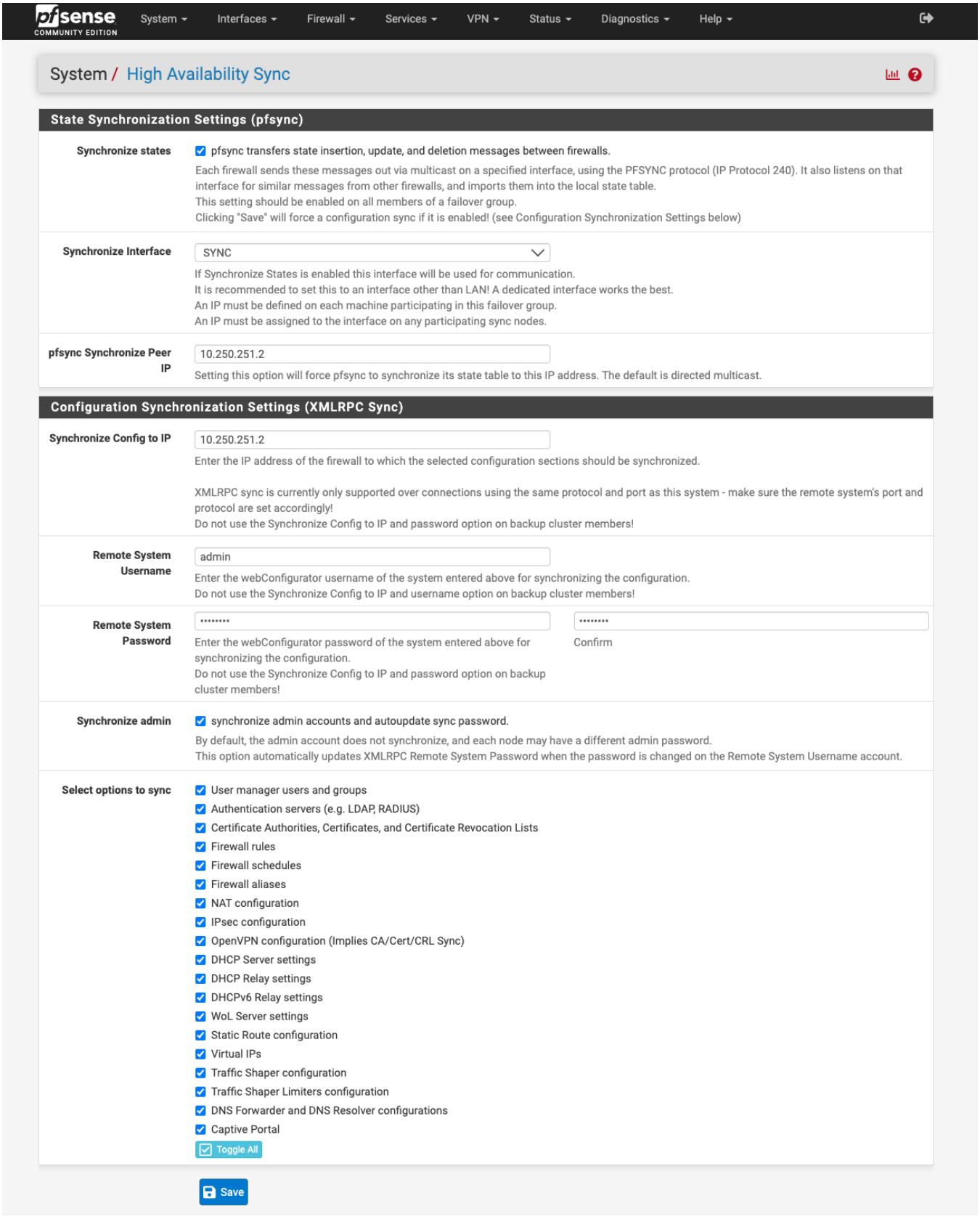
Configuração de acesso ao PFsense via active directory "Windows"

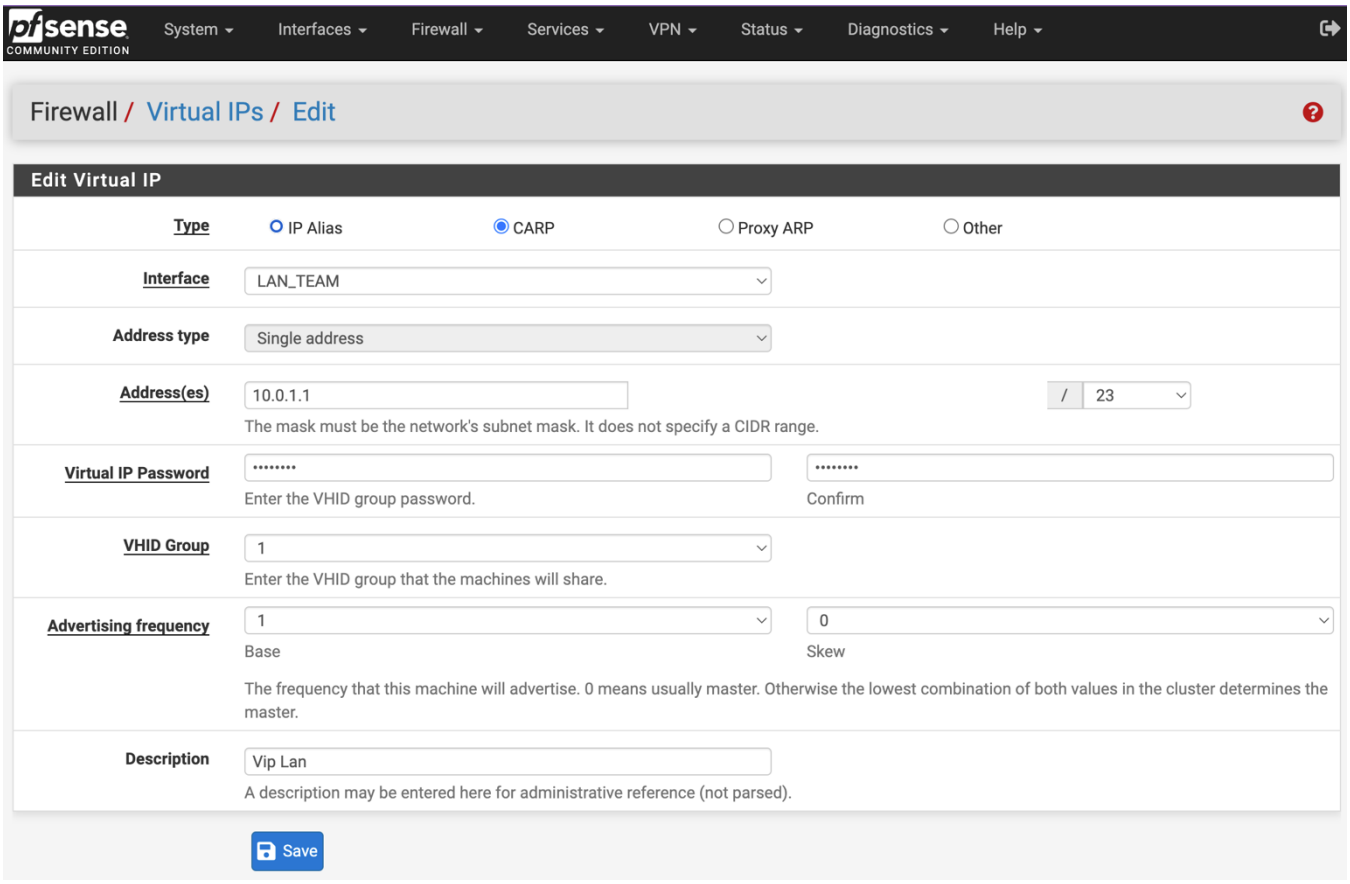


Criar Loadblancer de 2 interfaces de WAN

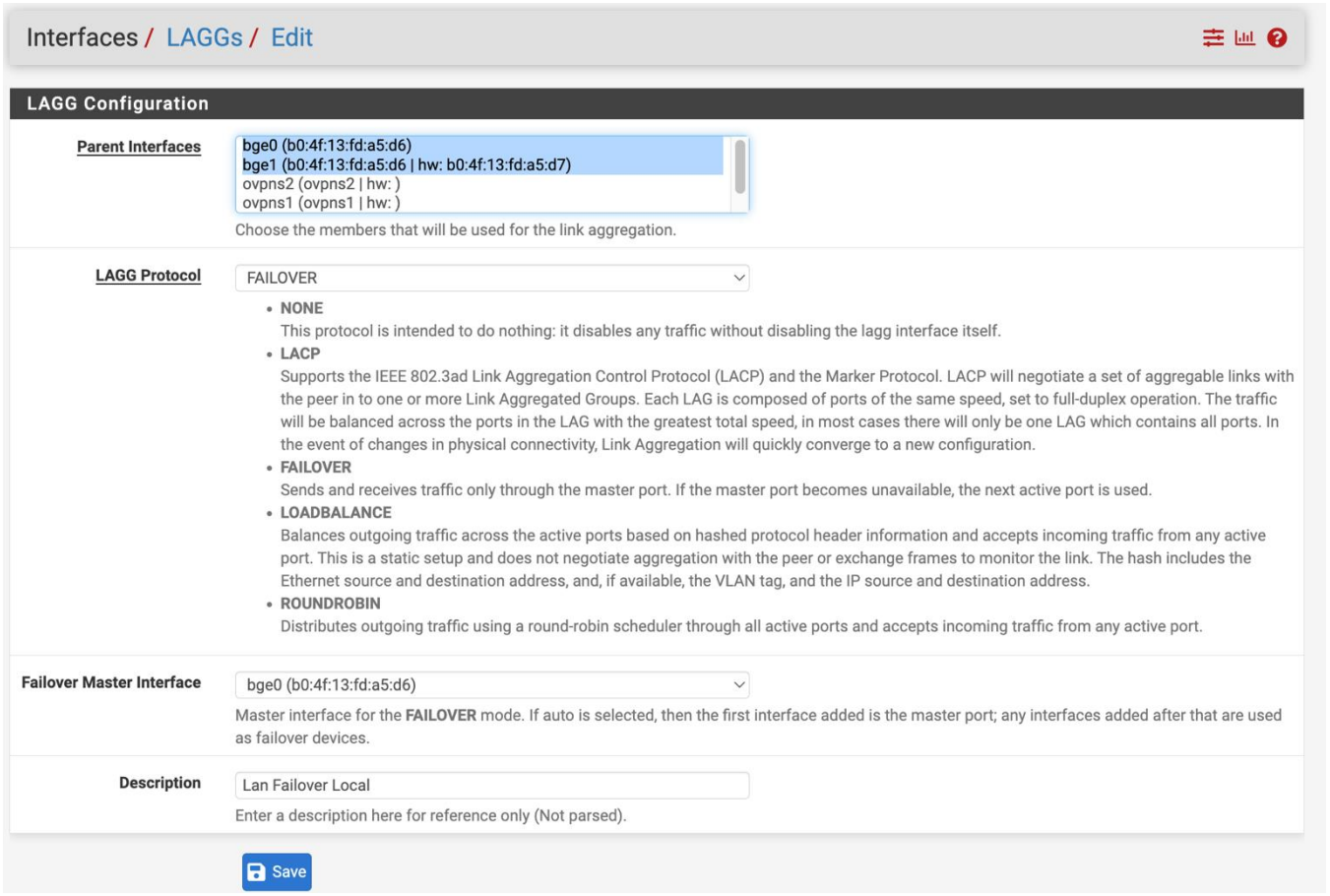


Configurar HA dos servidores de pfsense

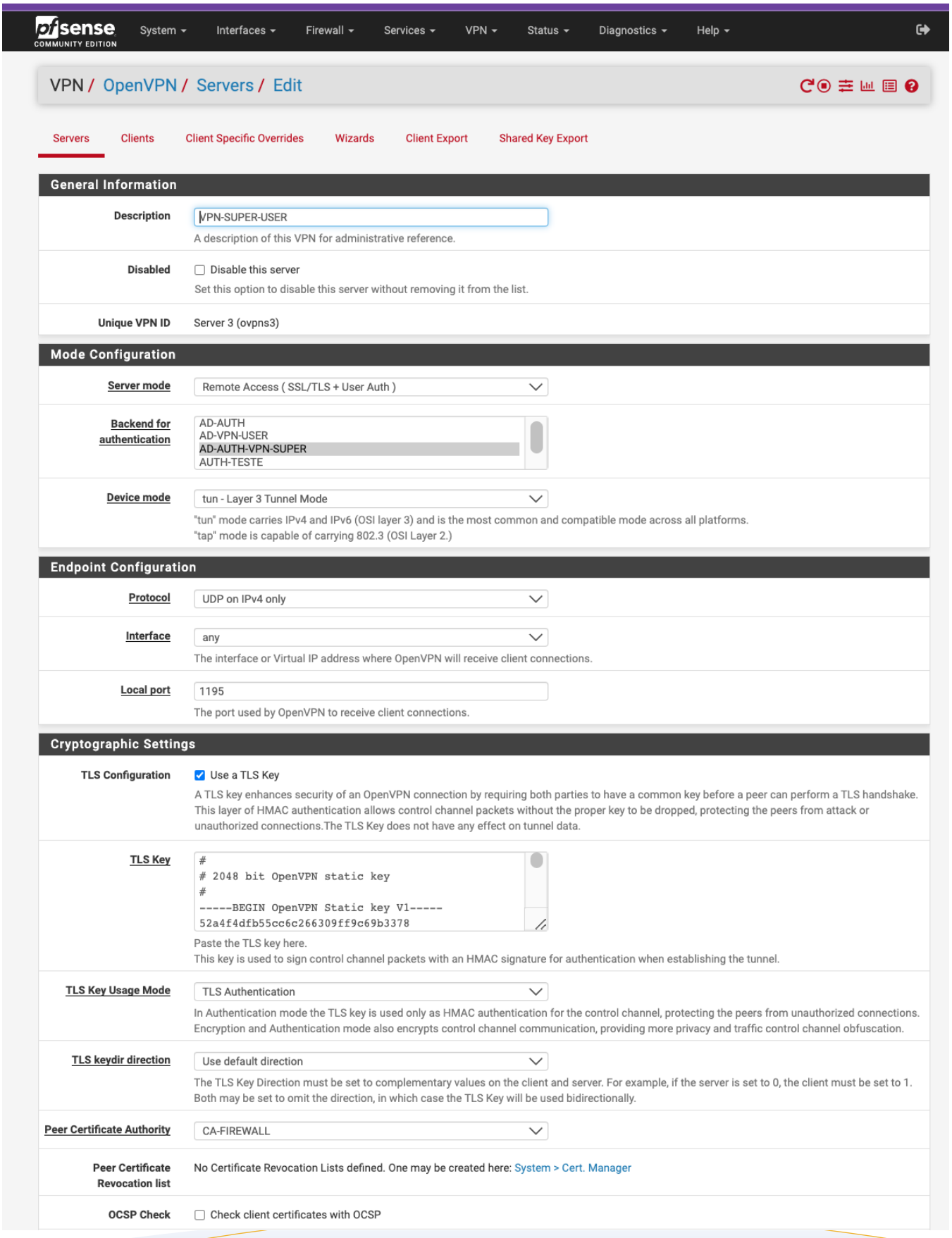



pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Virtual IPs / Edit
Edit Virtual IP
Type
IP Alias
CARP
Proxy ARP
Other
Interface
LAN_TEAM
Address type
Single address
Address(es)
10.0.1.1
/ 23
The mask must be the network's subnet mask. It does not specify a CIDR range.
Virtual IP Password
Enter the VHID group password.
Confirm
VHID Group
1
Enter the VHID group that the machines will share.
Advertising frequency
1
Base
0
Skew
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.
Description
Vip Lan
A description may be entered here for administrative reference (not parsed).
Save

Configurar bond de 2 interfaces LAN, caso necessário



Configurar VPN "OPENVPN" Client to server



Peer Certificate Authority	CA-FIREWALL
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
OCSP Check	☐ Check client certificates with OCSP
Server certificate	CERT-VPN (Server: Yes, CA: CA-FIREWALL, In Use)
DH Parameter Length	4096 bit Diffie-Hellman (DH) parameter set used for key exchange.
ECDH Curve	Use Default The Elliptic Curve to use for key exchange. The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.
Data Encryption Negotiation	☑ Enable Data Encryption Negotiation This option allows OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic data encryption algorithms from those selected in the Data Encryption Algorithms list below. Disabling this feature is deprecated.
Data Encryption Algorithms	AES-128-CBC (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) AES-128-CFB1 (128 bit key, 128 bit block) AES-128-CFB8 (128 bit key, 128 bit block) AES-128-GCM (128 bit key, 128 bit block) AES-128-OFB (128 bit key, 128 bit block) AES-192-CBC (192 bit key, 128 bit block) AES-192-CFB (192 bit key, 128 bit block) AES-192-CFB1 (192 bit key, 128 bit block) AES-192-CFB8 (192 bit key, 128 bit block) Available Data Encryption Algorithms Click to add or remove an algorithm from the list AES-256-GCM Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode.
Fallback Data Encryption Algorithm	AES-256-CBC (256 bit key, 128 bit block) The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.
Auth digest algorithm	SHA256 (256-bit) The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present. When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel. The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.
Hardware Crypto	Intel RDRAND engine - RAND
Certificate Depth	One (Client+Server) When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.
Strict User-CN Matching	☐ Enforce match When authenticating users, enforce a match between the common name of the client certificate and the username given at login.
Client Certificate Key Usage Validation	☐ Enforce key usage Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").

Tunnel Settings

IPv4 Tunnel Network
10.200.220.0/26
This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

IPv6 Tunnel Network
This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

Redirect IPv4 Gateway
☐ Force all client-generated IPv4 traffic through the tunnel.

Redirect IPv6 Gateway
☐ Force all client-generated IPv6 traffic through the tunnel.

IPv4 Local network(s)
10.0.0.0/23
IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

IPv6 Local network(s)
IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

Concurrent connections
Specify the maximum number of clients allowed to concurrently connect to this server.

Allow Compression
Refuse any non-stub compression (Most secure)
Allow compression to be used with this VPN instance.
Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.

Asymmetric compression allows an easier transition when connecting with older peers.

Type-of-Service
☐ Set the TOS IP header value of tunnel packets to match the encapsulated packet value.

Inter-client communication
☐ Allow communication between clients connected to this server

Duplicate Connection
☐ Allow multiple concurrent connections from the same user
When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session.

Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.

Client Settings

Dynamic IP
☑ Allow connected clients to retain their connections if their IP address changes.

Topology
Subnet -- One IP address per client in a common subnet
Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4.
Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

Ping settings

Inactive
300
Causes OpenVPN to close a client connection after n seconds of inactivity on the TUN/TAP device.
Activity is based on the last incoming or outgoing tunnel packet.
A value of 0 disables this feature.
This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.

Ping method
keepalive -- Use keepalive helper to define ping configuration
keepalive helper uses interval and timeout parameters to define ping and ping-restart values as follows:
ping = interval
ping-restart = timeout*2
push ping = interval
push ping-restart = timeout

Interval
10

Timeout
60

Advanced Client Settings

DNS Default Domain
☑ Provide a default domain name to clients

DNS Default Domain
amhp.local

DNS Server enable
☑ Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.

DNS Server 1
10.0.0.71

DNS Server 2

DNS Server 3

DNS Server 4

Block Outside DNS
☐ Make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers.
Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.

Force DNS cache update
☐ Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation.
This is known to kick Windows into recognizing pushed DNS servers.

NTP Server enable
☑ Provide an NTP server list to clients

NTP Server 1
10.0.0.71

NTP Server 2

NetBIOS enable
☑ Enable NetBIOS over TCP/IP
If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

Node Type
m-node
Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast)

Scope ID
A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID

WINS server enable
☐ Provide a WINS server list to clients

Advanced Configuration

Custom options

Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.
EXAMPLE: push "route 10.0.0.0 255.255.255.0"

Username as Common Name

☑ Use the authenticated client username instead of the certificate common name (CN).

When a user authenticates, if this option is enabled then the username of the client will be used in place of the certificate common name for purposes such as determining Client Specific Overrides.

UDP Fast I/O

☐ Use fast I/O operations with UDP writes to tun/tap. Experimental.

Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platforms, and not compatible with OpenVPN bandwidth limiting.

Exit Notify

Reconnect to this server / Retry once

Send an explicit exit notification to connected clients/peers when restarting or shutting down, so they may immediately disconnect rather than waiting for a timeout. In SSL/TLS Server modes, clients may be directed to reconnect or use the next server. This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.

Send/Receive Buffer

Default

Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KiB and test higher and lower values.

Gateway creation

○ Both ◉ IPv4 only ○ IPv6 only

If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is 'both'.

Verbosity level

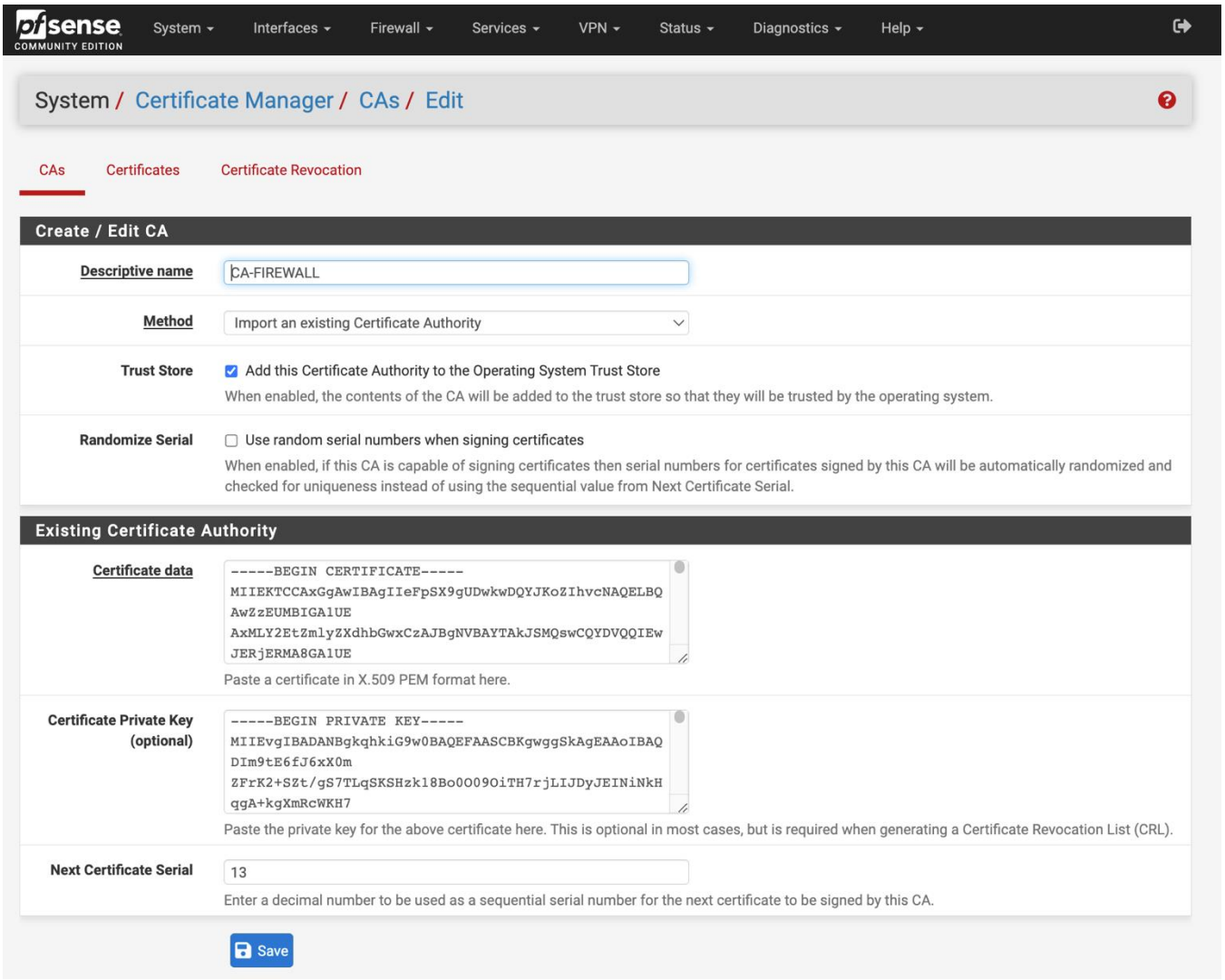
3 (recommended)

Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output.

None: Only fatal errors
Default through 4: Normal usage range
5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets.
6-11: Debug info range

Save

Criar certificado local open source para acesso VPN



System / Certificate Manager / Certificates

CAs | Certificates | Certificate Revocation

Edit an Existing Certificate

Method Edit an existing certificate

Descriptive name CERT-VPN

Subject ST=DF, OU=Tecnologia, O=AMHP, L=Brasilia, CN=fw-01.amhp.local, C=BR

Edit Certificate

Certificate Type X.509 (PEM) PKCS #12 (PFX)

Certificate data

```
-----BEGIN CERTIFICATE-----
MIIE2TCCA8GgAwIBAgIBATANBgkqhkiG9w0BAQsFADBnMRQwEg
YDVQQDEwtjYS1m
aXJld2FsbDELMAkGA1UEBhMCQlIxCzAJBgNVBAgTAkRGMREwDw
YDVQQHEwhCcmFz
```

Paste a certificate in X.509 PEM format here.

Private key data

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQ
DIEl9TWSaui75j
7RqQPUSwIZucqoM0mTydNQMhZvfQuhky9Z6tNJ4DItgbYJ6Z7D
mFJVNDVcdi57DG
```

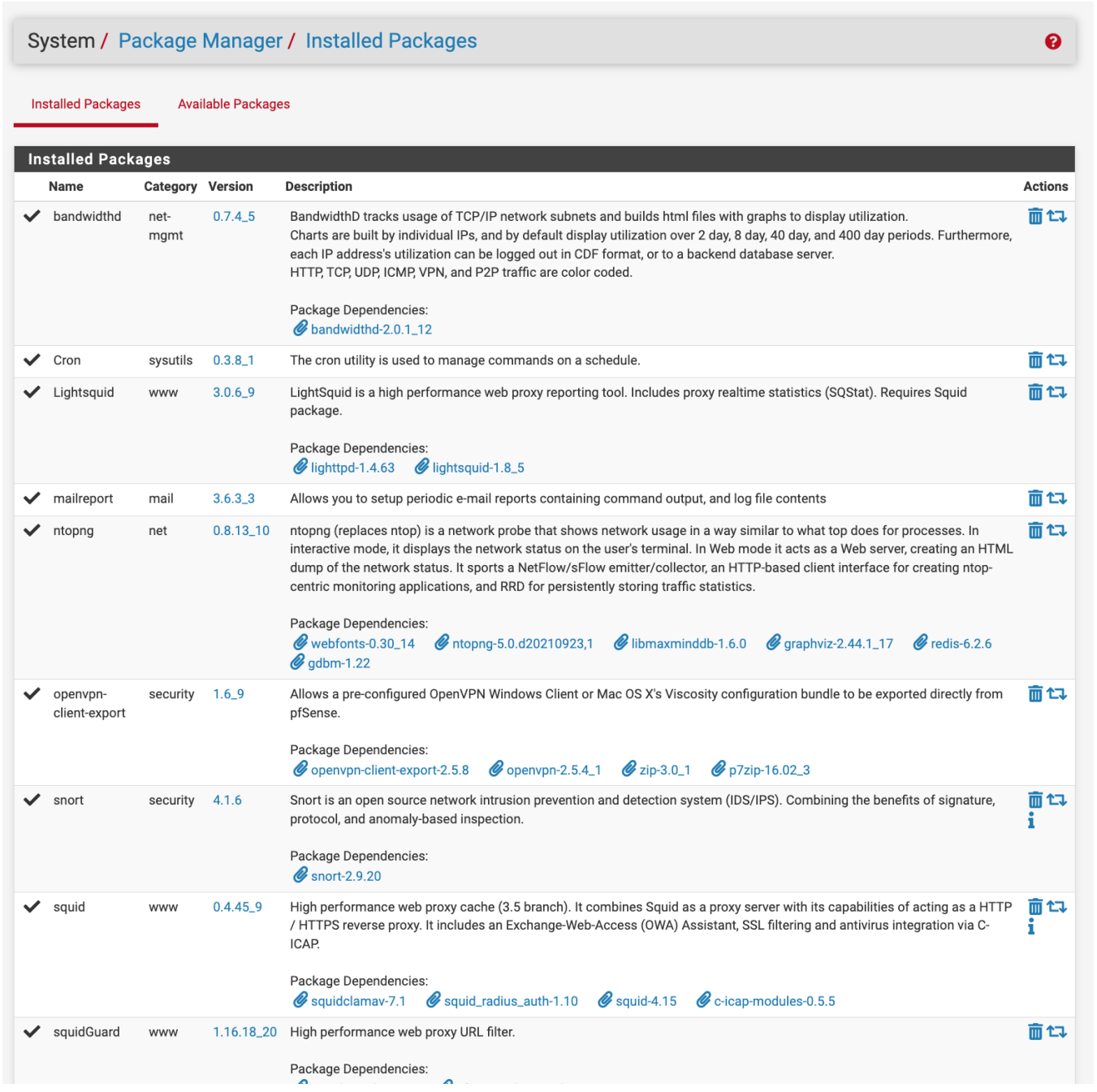
Paste a private key in X.509 PEM format here. This field may remain empty in certain cases, such as when the private key is stored on a PKCS#11 token.

Export Password Export Password

Enter the password to use when using the export buttons below (not stored)

Save | Export Private Key | Export PKCS#12

Ativar plugin squid ou squidGuard



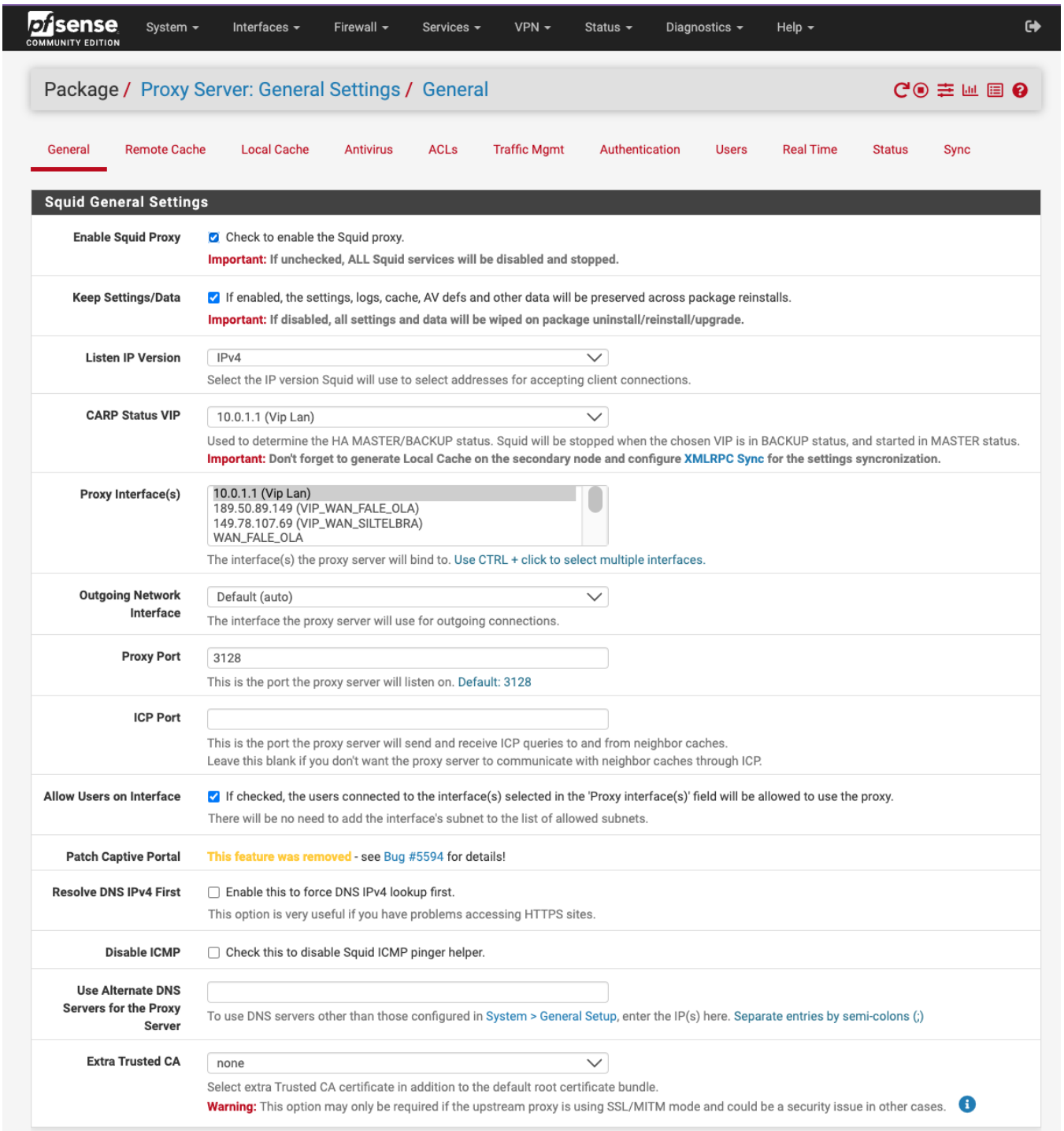
System / Package Manager / Installed Packages

Installed Packages | Available Packages

Installed Packages

	Name	Category	Version	Description	Actions
✔	bandwidthd	net-mgmt	0.7.4_5	BandwidthD tracks usage of TCP/IP network subnets and builds html files with graphs to display utilization. Charts are built by individual IPs, and by default display utilization over 2 day, 8 day, 40 day, and 400 day periods. Furthermore, each IP address's utilization can be logged out in CDF format, or to a backend database server. HTTP, TCP, UDP, ICMP, VPN, and P2P traffic are color coded. Package Dependencies: bandwidthd-2.0.1_12	
✔	Cron	sysutils	0.3.8_1	The cron utility is used to manage commands on a schedule.	
✔	Lightsquid	www	3.0.6_9	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package. Package Dependencies: lighttpd-1.4.63 lightsquid-1.8_5	
✔	mailreport	mail	3.6.3_3	Allows you to setup periodic e-mail reports containing command output, and log file contents	
✔	ntopng	net	0.8.13_10	ntopng (replaces ntop) is a network probe that shows network usage in a way similar to what top does for processes. In interactive mode, it displays the network status on the user's terminal. In Web mode it acts as a Web server, creating an HTML dump of the network status. It sports a NetFlow/sFlow emitter/collector, an HTTP-based client interface for creating ntop-centric monitoring applications, and RRD for persistently storing traffic statistics. Package Dependencies: webfonts-0.30_14 ntopng-5.0.d20210923,1 libmaxminddb-1.6.0 graphviz-2.44.1_17 redis-6.2.6 gdbm-1.22	
✔	openvpn-client-export	security	1.6_9	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense. Package Dependencies: openvpn-client-export-2.5.8 openvpn-2.5.4_1 zip-3.0_1 p7zip-16.02_3	
✔	snort	security	4.1.6	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. Package Dependencies: snort-2.9.20	
✔	squid	www	0.4.45_9	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-7.1 squid_radius_auth-1.10 squid-4.15 c-icap-modules-0.5.5	
✔	squidGuard	www	1.16.18_20	High performance web proxy URL filter. Package Dependencies:	

Fazer integração dos plugins squid ou squidguard com active directory "Windows"



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)

189.50.89.149 (VIP_WAN_FALE_OLA)
149.78.107.69 (VIP_WAN_SILTELBRA)
WAN_FALE_OLA
WAN_X

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 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.**

SSL Intercept Interface(s)

10.0.1.1 (Vip Lan)
189.50.89.149 (VIP_WAN_FALE_OLA)
149.78.107.69 (VIP_WAN_SILTELBRA)
WAN_FALE_OLA

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

Intermediate

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

CA-FIREWALL

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

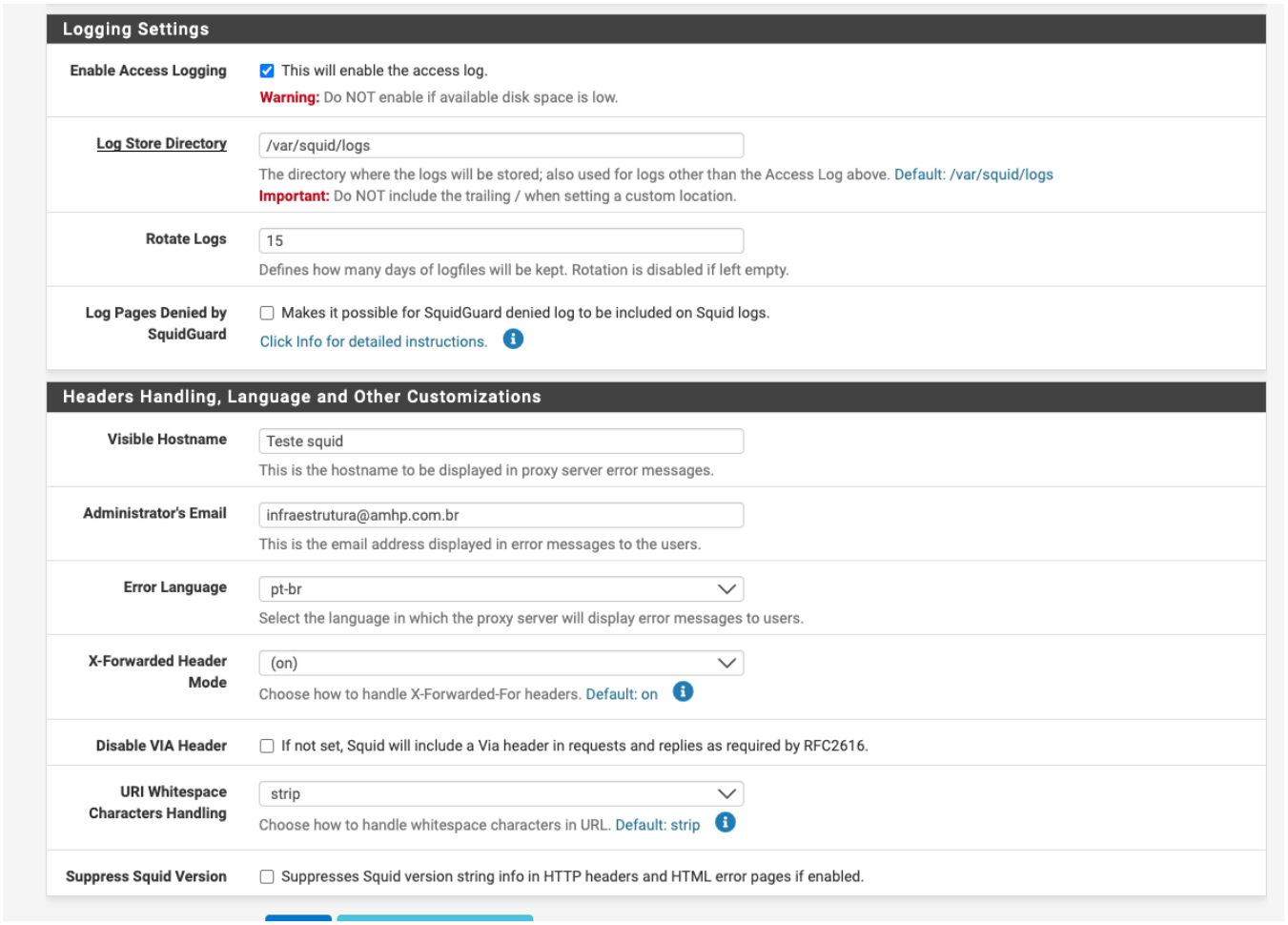
Accept remote server certificate with errors
Do not verify remote certificate

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.



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
15
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.

Headers Handling, Language and Other Customizations

Visible Hostname
Teste squid
This is the hostname to be displayed in proxy server error messages.

Administrator's Email
infraestrutura@amhp.com.br
This is the email address displayed in error messages to the users.

Error Language
pt-br
Select the language in which the proxy server will display error messages to users.

X-Forwarded Header Mode
(on)
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
strip
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.

Advanced Features

Integrations

```
url_rewrite_program /usr/local/bin/squidGuard -c
/usr/local/etc/squidGuard/squidGuard.conf;url_rewrite_bypass
off;url_rewrite_children 16 startup=8 idle=4 concurrency=0
```

Squid options added from packages like SquidGuard for Squid integration.

Custom Options (Before Auth)

```
acl whatsapp ssl::server_name web.whatsapp.com whatsapp.com whatsapp.net
acl DiscoverSNIHost at_step SslBump1
ssl_bump peek DiscoverSNIHost
ssl_bump splice whatsapp


# Certificado ssl
acl CertificadoConfiavel dstdomain 10.0.1.2
sslproxy_cert_error allow CertificadoConfiavel
```

Put your own custom options here, one per line. They'll be added to the configuration before authetication ACLS (if any).
Warning: These need to be squid.conf native options, otherwise Squid will NOT work.

Custom Options (After Auth)

Put your own custom options here, one per line. They'll be added to the configuration after authentication definition (if any).
Warning: These need to be squid.conf native options, otherwise Squid will NOT work.

Custom Options (SSL/MITM)

Put your own custom options here, one per line. They'll be added to the configuration in place of the default SSL/MITM configuration.
Ignored unless 'SSL/MITM Mode' is set to 'Custom'. Click Info for details.

Warning: These need to be squid.conf native options, otherwise Squid will NOT work.

Save | Hide Advanced Options

pfsense COMMUNITY EDITION | 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 CN=fw-01,OU=Servicos,OU=Informatica,DC=amhp,DC=local
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 300
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 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

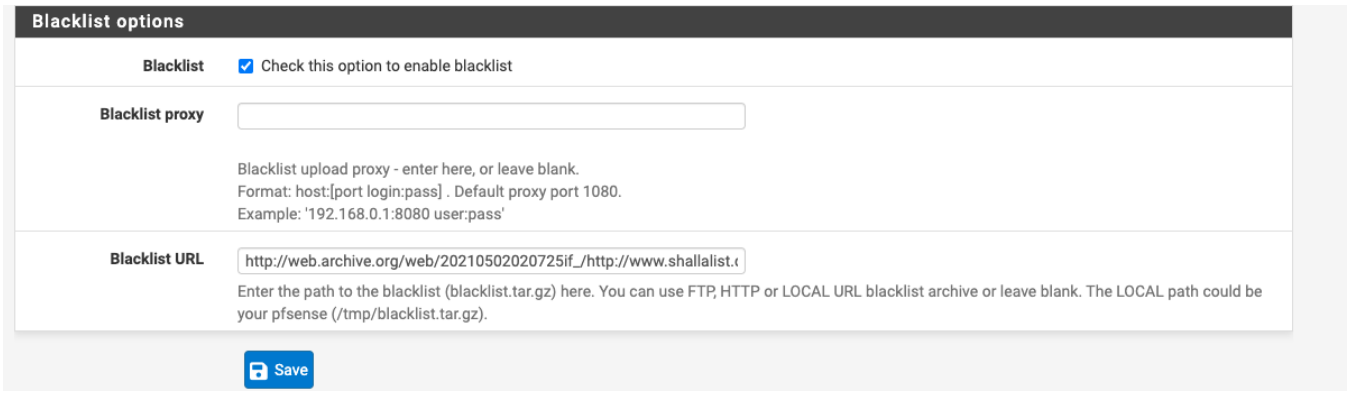
Enable GUI log ☑ Check this option to log the access to the Proxy Filter GUI.

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.

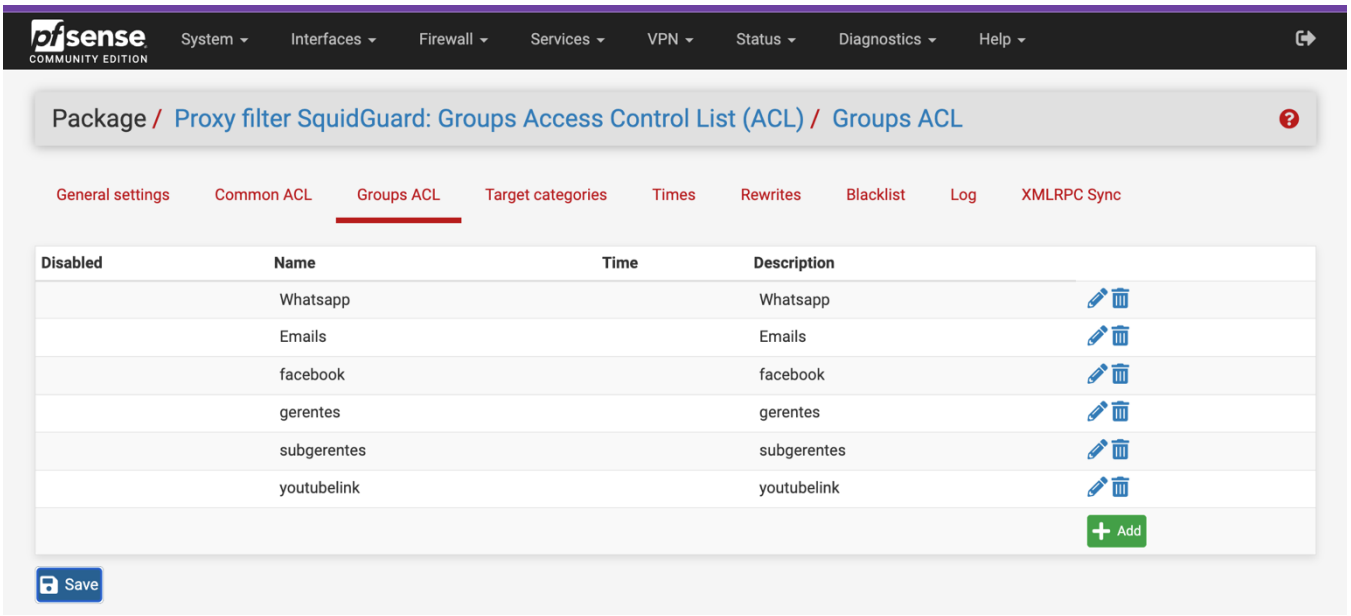
Enable log rotation ☑ Check this option to rotate the logs every day. This is recommended if you enable any kind of logging to limit file size and do not run out of disk space.

Miscellaneous

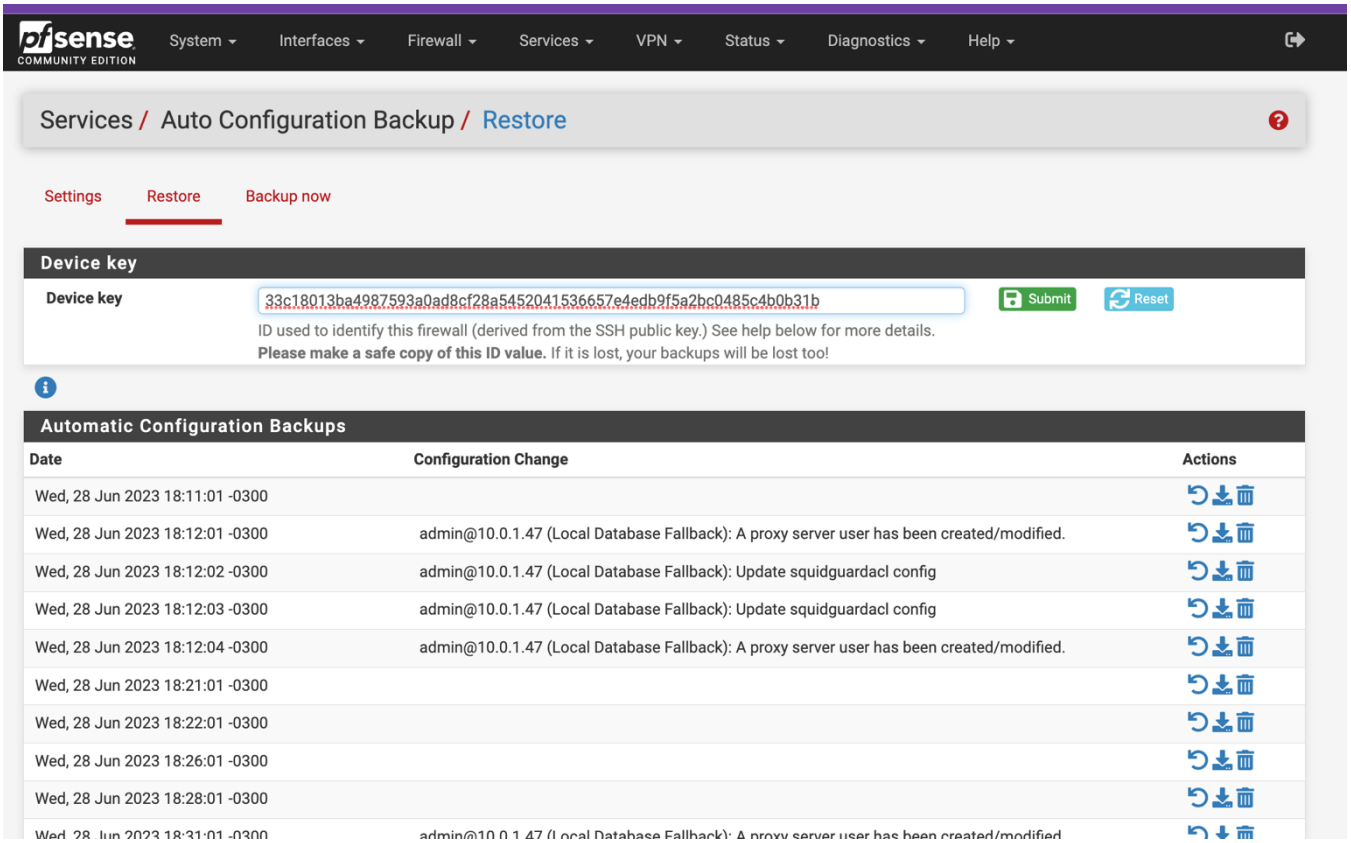
Clean Advertising ☐ Check this option to display a blank gif image instead of the default block page. With this option the user gets a cleaner webpage.


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
http://web.archive.org/web/20210502020725if_/http://www.shallalist.
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

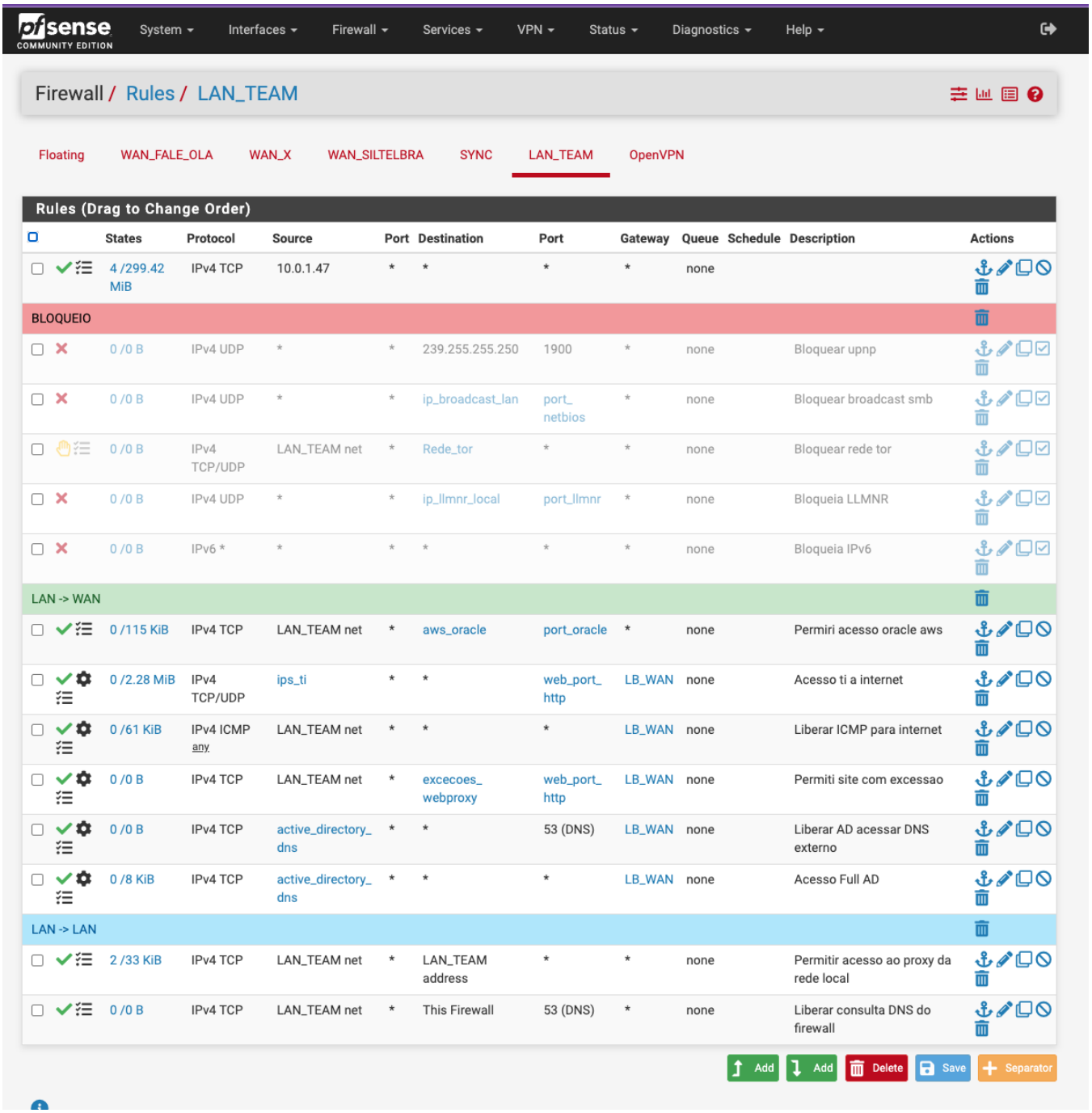
Definir grupos de acesso a internet via AD



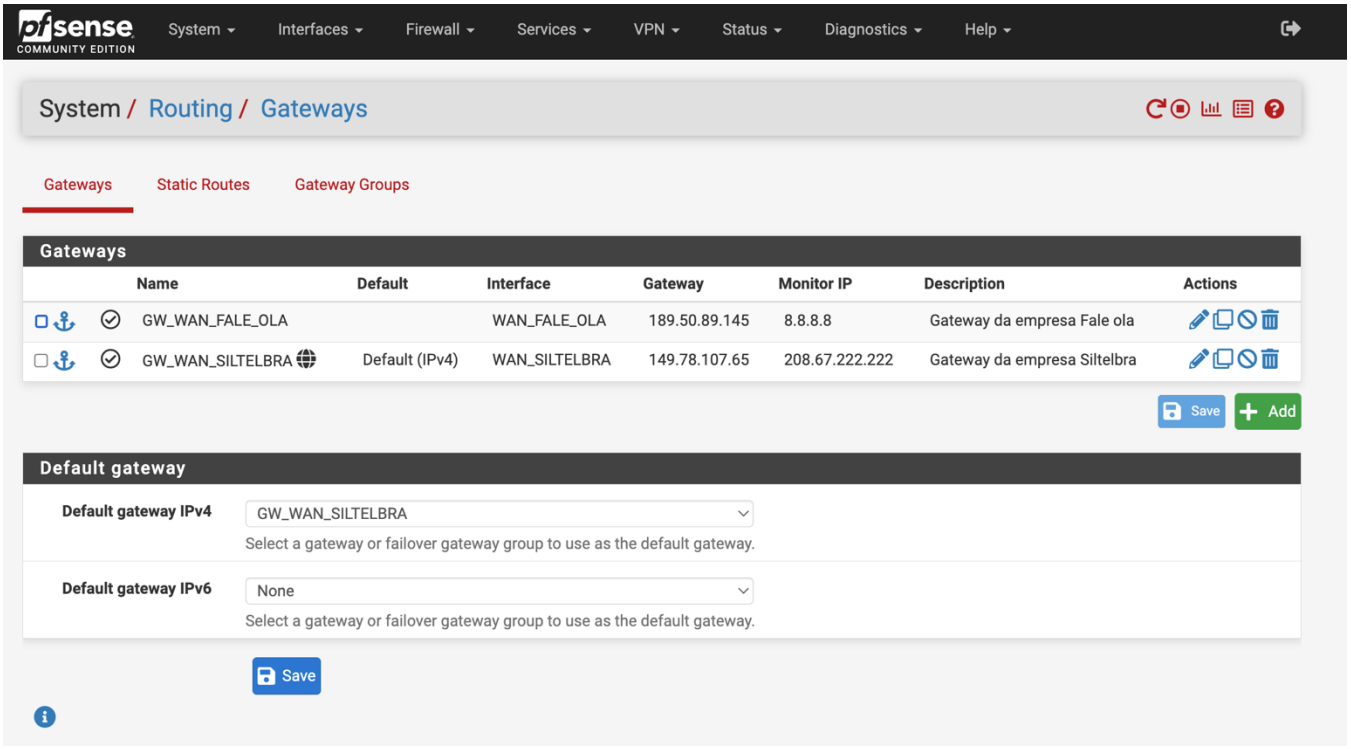
Criar backup da configuração do pfsense



Criação das regras de firewall de acesso a internet



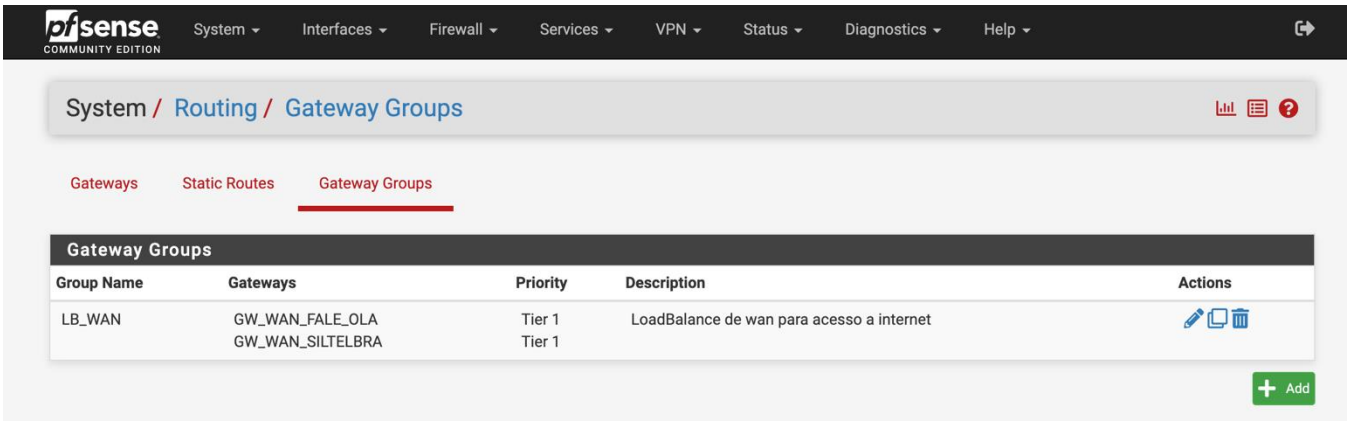
Definir rotas para o Pfsense



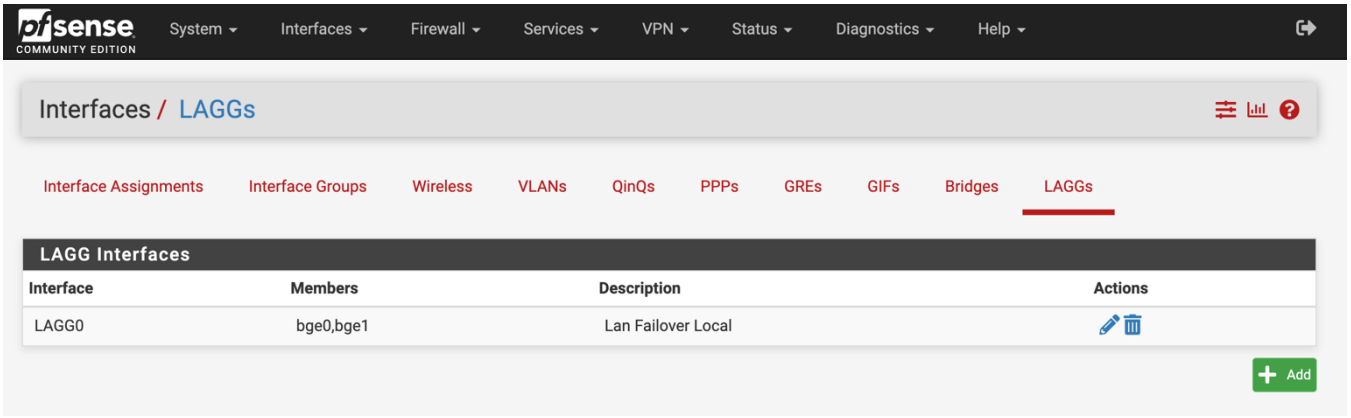
Validação dos acessos

- ***Acesso vi active directory***

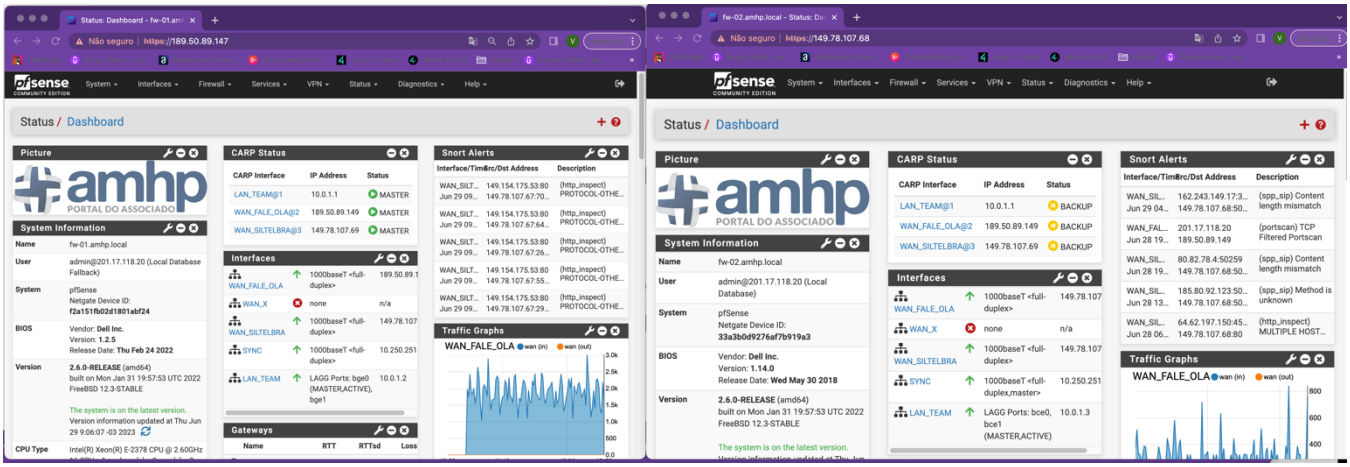
- ***HA das Interfaces WAN***



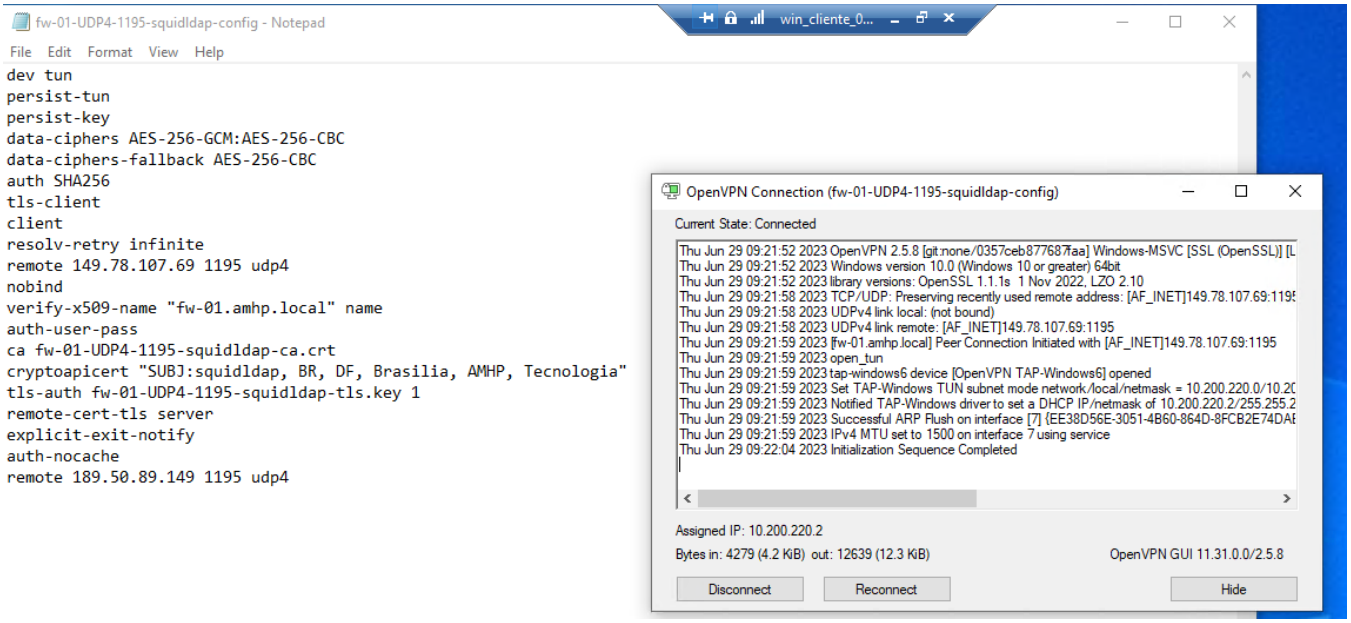
- ***HA das Interfaces LAN***



- ***HA do firewall***



- ***Acesso da VPN***



- ***Liberação internet via squid***