

***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 ferramenta 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.

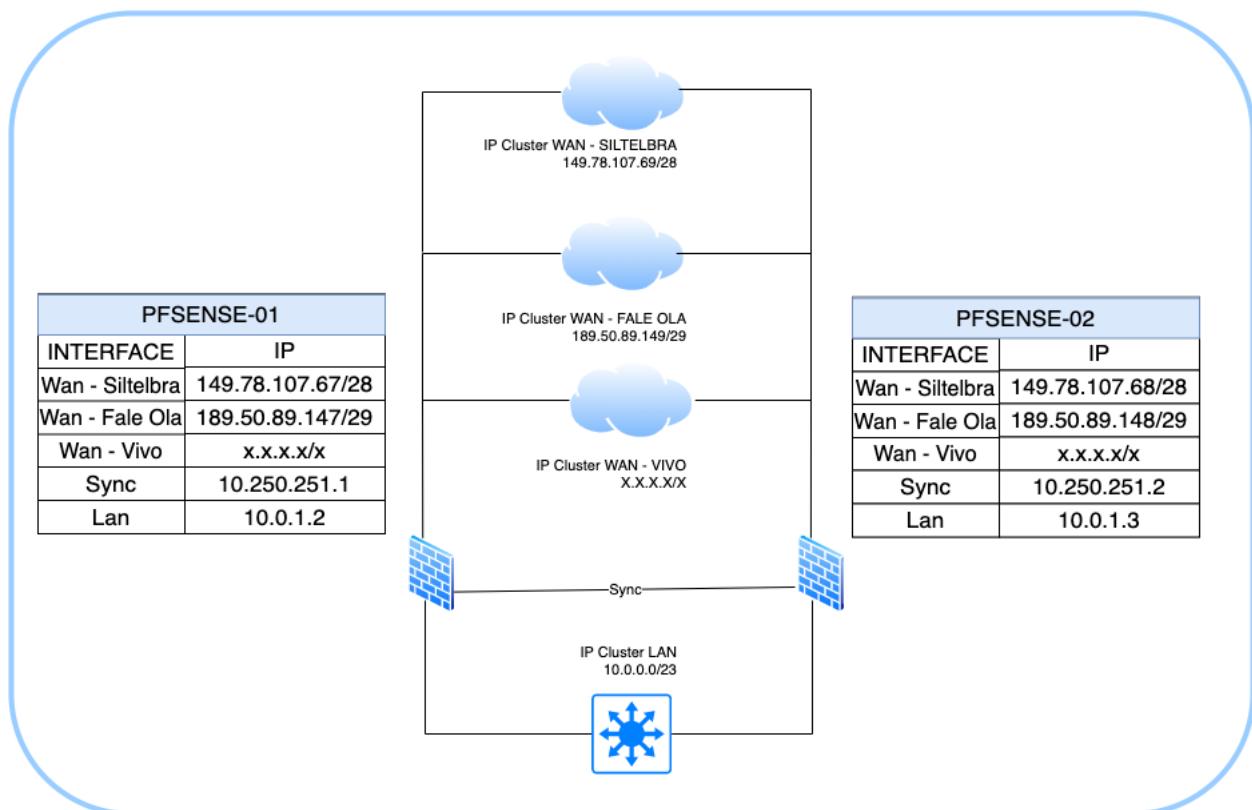
## SOLUÇÃO

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

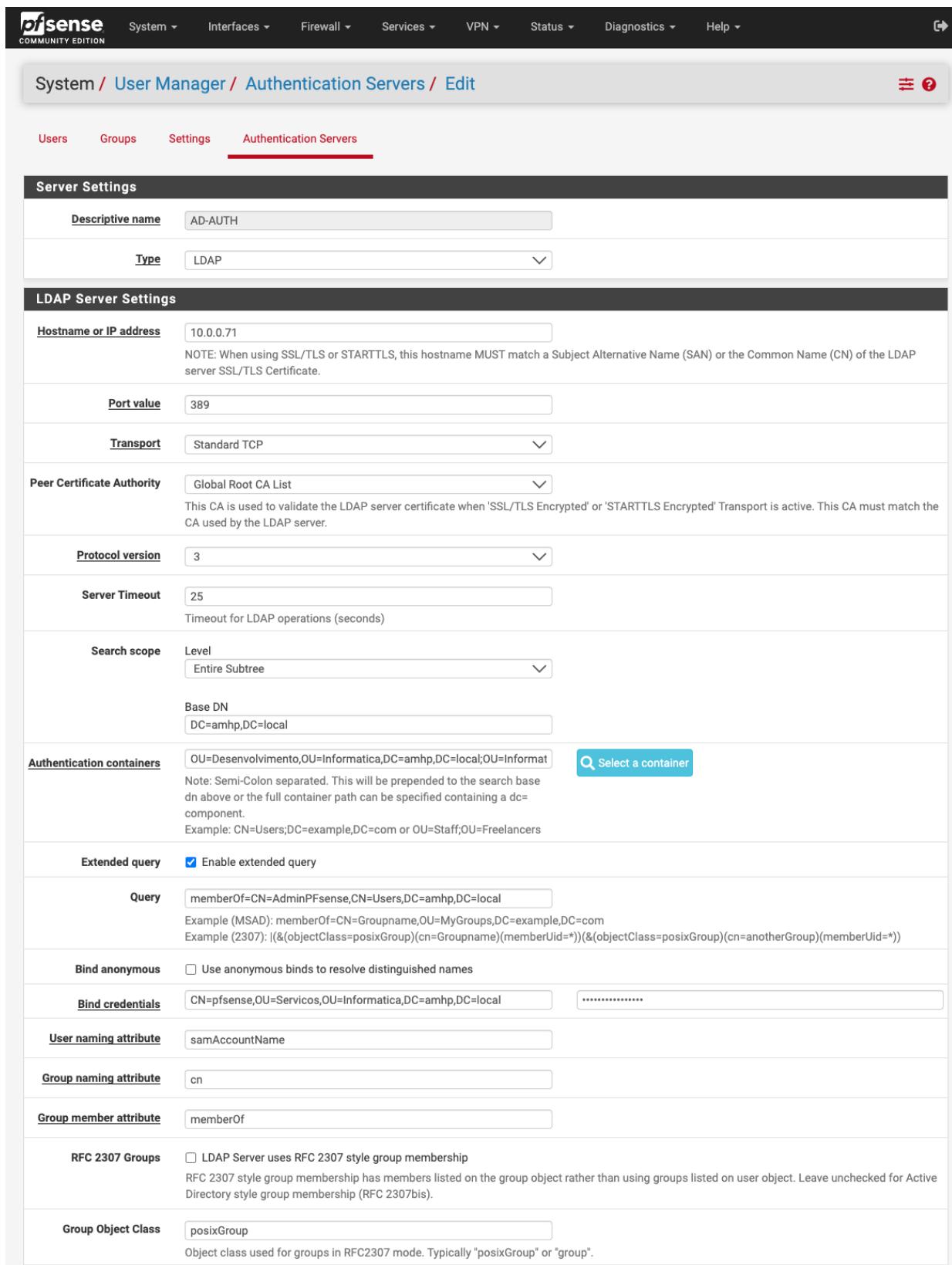


## FIREWALL

<b>Nome</b>	<b>INTERFACE</b>	<b>IP / Mask</b>	<b>VIP</b>	<b>Localização</b>
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"



**System / User Manager / Authentication Servers / Edit**

**Server Settings**

**Descriptive name:** AD-AUTH

**Type:** LDAP

**LDAP Server Settings**

**Hostname or IP address:** 10.0.0.71

NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.

**Port value:** 389

**Transport:** Standard TCP

**Peer Certificate Authority:** Global Root CA List

This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.

**Protocol version:** 3

**Server Timeout:** 25

Timeout for LDAP operations (seconds)

**Search scope:** Level

Entire Subtree

**Base DN:** DC=amhp,DC=local

**Authentication containers:** OU=Desenvolvimento,OU=Informatica,DC=amhp,DC=local;OU=Informat

Select a container

Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component.  
Example: CN=Users;DC=example,DC=com or OU=Staff;OU=Freelancers

**Extended query:**  Enable extended query

**Query:** memberOf=CN=AdminPfSense,CN=Users,DC=amhp,DC=local

Example (MSAD): memberOf=CN=Groupname,OU=MyGroups,DC=example,DC=com  
Example (2307): (&(objectClass=posixGroup)(cn=Groupname)(memberUid=\*))&(&(objectClass=posixGroup)(cn=anotherGroup)(memberUid=\*))

**Bind anonymous:**  Use anonymous binds to resolve distinguished names

**Bind credentials:** CN=pfsense,OU=Servicos,OU=Informatica,DC=amhp,DC=local

**User naming attribute:** samAccountName

**Group naming attribute:** cn

**Group member attribute:** memberOf

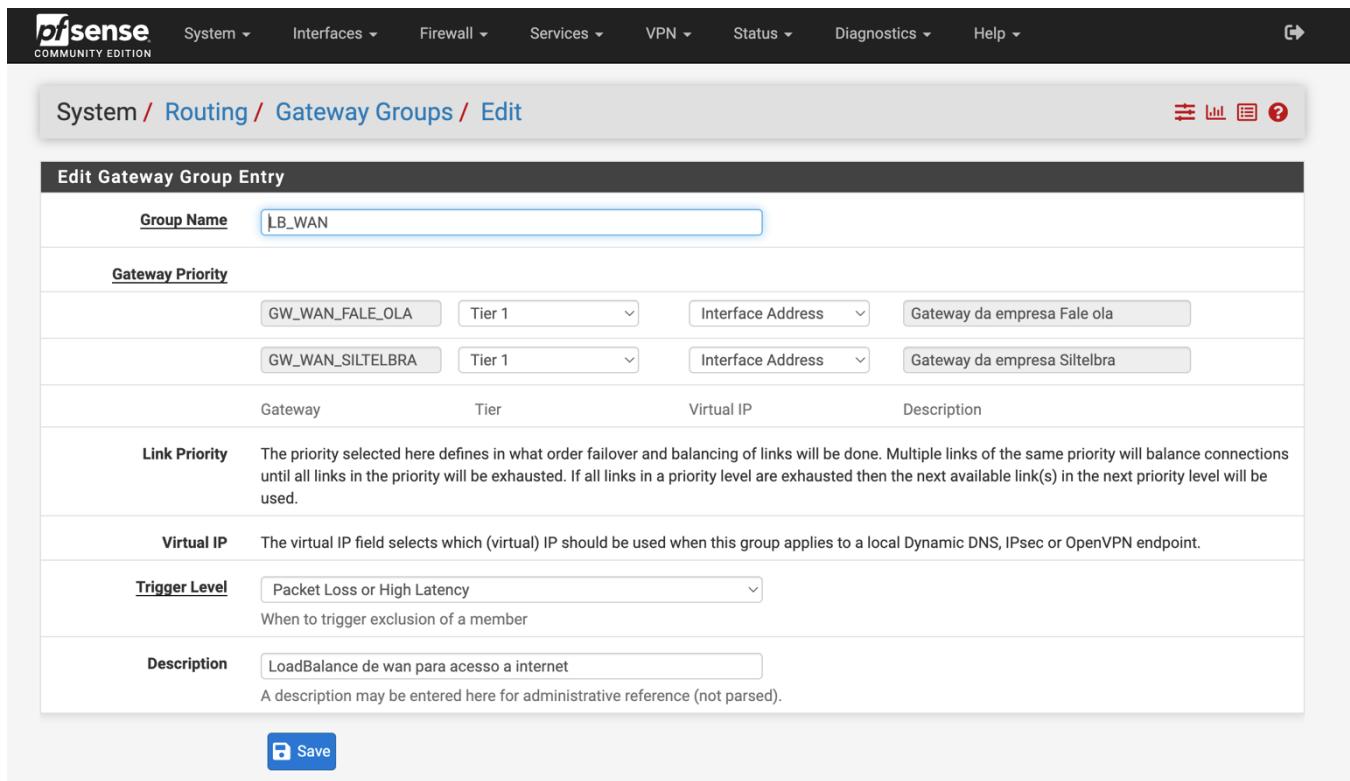
**RFC 2307 Groups:**  LDAP Server uses RFC 2307 style group membership

RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).

**Group Object Class:** posixGroup

Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".

## Criar Loadblancer de 2 interfaces de WAN



The screenshot shows the 'Edit Gateway Group Entry' configuration page in the Pfsense web interface. The 'Group Name' is set to 'LB\_WAN'. Under 'Gateway Priority', two entries are defined: 'GW\_WAN\_FALE\_OLA' (Tier 1, Interface Address: 'Gateway da empresa Fale ola') and 'GW\_WAN\_SILTELBRA' (Tier 1, Interface Address: 'Gateway da empresa Siltelbra'). A table below lists the gateway details: Gateway, Tier, Virtual IP, and Description. The 'Link Priority' section explains that it defines the order for failover and balancing. The 'Virtual IP' section notes that it selects the virtual IP for local Dynamic DNS, IPsec, or OpenVPN endpoints. The 'Trigger Level' is set to 'Packet Loss or High Latency'. The 'Description' field contains the text 'LoadBalance de wan para acesso a internet'. A 'Save' button is at the bottom.

Gateway	Tier	Virtual IP	Description
GW_WAN_FALE_OLA	Tier 1	Interface Address: Gateway da empresa Fale ola	
GW_WAN_SILTELBRA	Tier 1	Interface Address: Gateway da empresa Siltelbra	

## Configurar HA dos servidores de pfsense

**pfSense COMMUNITY EDITION** System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / High Availability Sync

**State Synchronization Settings (pfsync)**

**Synchronize states**  pfsync transfers state insertion, update, and deletion messages between firewalls.  
Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.  
This setting should be enabled on all members of a failover group.  
Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

**Synchronize Interface** SYNC  
If Synchronize States is enabled this interface will be used for communication.  
It is recommended to set this to an interface other than LAN! A dedicated interface works the best.  
An IP must be defined on each machine participating in this failover group.  
An IP must be assigned to the interface on any participating sync nodes.

**pfsync Synchronize Peer**  
**IP** 10.250.251.2  
Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

**Configuration Synchronization Settings (XMLRPC Sync)**

**Synchronize Config to IP** 10.250.251.2  
Enter the IP address of the firewall to which the selected configuration sections should be synchronized.  
XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!  
Do not use the Synchronize Config to IP and password option on backup cluster members!

**Remote System Username** admin  
Enter the webConfigurator username of the system entered above for synchronizing the configuration.  
Do not use the Synchronize Config to IP and username option on backup cluster members!

**Remote System Password** ..... Confirm  
Enter the webConfigurator password of the system entered above for synchronizing the configuration.  
Do not use the Synchronize Config to IP and password option on backup cluster members!

**Synchronize admin**  synchronize admin accounts and autoupdate sync password.  
By default, the admin account does not synchronize, and each node may have a different admin password.  
This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

**Select options to sync**

- User manager users and groups
- Authentication servers (e.g. LDAP, RADIUS)
- Certificate Authorities, Certificates, and Certificate Revocation Lists
- Firewall rules
- Firewall schedules
- Firewall aliases
- NAT configuration
- IPsec configuration
- OpenVPN configuration (Implies CA/Cert/CRL Sync)
- DHCP Server settings
- DHCP Relay settings
- DHCPv6 Relay settings
- WoL Server settings
- Static Route configuration
- Virtual IPs
- Traffic Shaper configuration
- Traffic Shaper Limiters configuration
- DNS Forwarder and DNS Resolver configurations
- Captive Portal

Toggle All

 Save

Pfsense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type	<input checked="" type="radio"/> IP Alias	<input checked="" type="radio"/> CARP	<input type="radio"/> Proxy ARP	<input type="radio"/> 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	0	Base 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).			
<input type="button" value="Save"/>				

**Configurar bond de 2 interfaces LAN, caso necessário**

Interfaces / LAGGs / Edit

**LAGG Configuration**

**Parent Interfaces**

- bge0 (b0:4f:13:fd:a5:d6)
- bge1 (b0:4f:13:fd:a5:d6 | hw: b0:4f:13:fd:a5:d7)
- ovpns2 (ovpns2 | hw: )
- ovpns1 (ovpns1 | hw: )

Choose the members that will be used for the link aggregation.

**LAGG Protocol**

FAILOVER

- **NONE**  
This protocol is intended to do nothing: it disables any traffic without disabling the lagg interface itself.
- **LACP**  
Supports the IEEE 802.3ad Link Aggregation Control Protocol (LACP) and the Marker Protocol. LACP will negotiate a set of aggregable links with the peer in to one or more Link Aggregated Groups. Each LAG is composed of ports of the same speed, set to full-duplex operation. The traffic will be balanced across the ports in the LAG with the greatest total speed, in most cases there will only be one LAG which contains all ports. In the event of changes in physical connectivity, Link Aggregation will quickly converge to a new configuration.
- **FAILOVER**  
Sends and receives traffic only through the master port. If the master port becomes unavailable, the next active port is used.
- **LOADBALANCE**  
Balances outgoing traffic across the active ports based on hashed protocol header information and accepts incoming traffic from any active port. This is a static setup and does not negotiate aggregation with the peer or exchange frames to monitor the link. The hash includes the Ethernet source and destination address, and, if available, the VLAN tag, and the IP source and destination address.
- **ROUNDROBIN**  
Distributes outgoing traffic using a round-robin scheduler through all active ports and accepts incoming traffic from any active port.

**Failover Master Interface**

bge0 (b0:4f:13:fd:a5:d6)

Master interface for the FAILOVER mode. If auto is selected, then the first interface added is the master port; any interfaces added after that are used as failover devices.

**Description**

Lan Failover Local

Enter a description here for reference only (Not parsed).

**Save**

## *Configurar VPN “OPENVPN” Client to server*

**pfSense** COMMUNITY EDITION    System ▾    Interfaces ▾    Firewall ▾    Services ▾    VPN ▾    Status ▾    Diagnostics ▾    Help ▾    [Logout](#)

VPN / OpenVPN / Servers / Edit

[Servers](#)    [Clients](#)    [Client Specific Overrides](#)    [Wizards](#)    [Client Export](#)    [Shared Key Export](#)

**General Information**

Description	<input type="text" value="VPN-SUPER-USER"/>
A description of this VPN for administrative reference.	
Disabled	<input type="checkbox"/> Disable this server Set this option to disable this server without removing it from the list.
Unique VPN ID	Server 3 (ovpn3)

**Mode Configuration**

Server mode	Remote Access ( SSL/TLS + User Auth )
Backend for authentication	<input type="checkbox"/> AD-AUTH <input type="checkbox"/> AD-VPN-USER <input checked="" type="checkbox"/> AD-AUTH-VPN-SUPER <input type="checkbox"/> AUTH-TESTE
Device mode	tun - Layer 3 Tunnel Mode  "tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms. "tap" mode is capable of carrying 802.3 (OSI Layer 2.)

**Endpoint Configuration**

Protocol	UDP on IPv4 only
Interface	any
The interface or Virtual IP address where OpenVPN will receive client connections.	
Local port	1195
The port used by OpenVPN to receive client connections.	

**Cryptographic Settings**

TLS Configuration	<input checked="" type="checkbox"/> Use a TLS Key  A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.
TLS Key	<pre># # 2048 bit OpenVPN static key # -----BEGIN OpenVPN Static key V1----- 52a4f4dfb55cc6c266309ff9c69b3378</pre>
Paste the TLS key here. This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.	
TLS Key Usage Mode	TLS Authentication
In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.	
TLS keydir direction	Use default direction
The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.	
Peer Certificate Authority	CA-FIREWALL
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: <a href="#">System &gt; Cert. Manager</a>
OCSP Check	<input type="checkbox"/> Check client certificates with OCSP

<small>This may be set to either the address in which case the test key will be used automatically.</small>																							
<u>Peer Certificate Authority</u>	CA-FIREWALL <input type="button" value="▼"/>																						
<u>Peer Certificate Revocation list</u>	No Certificate Revocation Lists defined. One may be created here: <a href="#">System &gt; Cert. Manager</a>																						
<u>OCSP Check</u>	<input type="checkbox"/> Check client certificates with OCSP																						
<u>Server certificate</u>	CERT-VPN (Server: Yes, CA: CA-FIREWALL, In Use) <input type="button" value="▼"/>																						
<u>DH Parameter Length</u>	4096 bit <input type="button" value="▼"/> Diffie-Hellman (DH) parameter set used for key exchange. 																						
<u>ECDH Curve</u>	Use Default <input type="button" value="▼"/> 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.																						
<u>Data Encryption Negotiation</u>	<input checked="" type="checkbox"/> 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.																						
<u>Data Encryption Algorithms</u>	<table border="1"> <tr><td>AES-128-CBC (128 bit key, 128 bit block)</td><td><input checked="" type="radio"/></td></tr> <tr><td>AES-128-CFB (128 bit key, 128 bit block)</td><td><input type="radio"/></td></tr> <tr><td>AES-128-CFB1 (128 bit key, 128 bit block)</td><td><input type="radio"/></td></tr> <tr><td>AES-128-CFB8 (128 bit key, 128 bit block)</td><td><input type="radio"/></td></tr> <tr><td>AES-128-GCM (128 bit key, 128 bit block)</td><td><input type="radio"/></td></tr> <tr><td>AES-128-OFB (128 bit key, 128 bit block)</td><td><input type="radio"/></td></tr> <tr><td>AES-192-CBC (192 bit key, 128 bit block)</td><td><input type="radio"/></td></tr> <tr><td>AES-192-CFB (192 bit key, 128 bit block)</td><td><input type="radio"/></td></tr> <tr><td>AES-192-CFB1 (192 bit key, 128 bit block)</td><td><input type="radio"/></td></tr> <tr><td>AES-192-CFB8 (192 bit key, 128 bit block)</td><td><input type="radio"/></td></tr> </table> <p>Available Data Encryption Algorithms Click to add or remove an algorithm from the list</p>	AES-128-CBC (128 bit key, 128 bit block)	<input checked="" type="radio"/>	AES-128-CFB (128 bit key, 128 bit block)	<input type="radio"/>	AES-128-CFB1 (128 bit key, 128 bit block)	<input type="radio"/>	AES-128-CFB8 (128 bit key, 128 bit block)	<input type="radio"/>	AES-128-GCM (128 bit key, 128 bit block)	<input type="radio"/>	AES-128-OFB (128 bit key, 128 bit block)	<input type="radio"/>	AES-192-CBC (192 bit key, 128 bit block)	<input type="radio"/>	AES-192-CFB (192 bit key, 128 bit block)	<input type="radio"/>	AES-192-CFB1 (192 bit key, 128 bit block)	<input type="radio"/>	AES-192-CFB8 (192 bit key, 128 bit block)	<input type="radio"/>	<table border="1"> <tr><td>AES-256-GCM</td></tr> </table> <p>Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list</p>	AES-256-GCM
AES-128-CBC (128 bit key, 128 bit block)	<input checked="" type="radio"/>																						
AES-128-CFB (128 bit key, 128 bit block)	<input type="radio"/>																						
AES-128-CFB1 (128 bit key, 128 bit block)	<input type="radio"/>																						
AES-128-CFB8 (128 bit key, 128 bit block)	<input type="radio"/>																						
AES-128-GCM (128 bit key, 128 bit block)	<input type="radio"/>																						
AES-128-OFB (128 bit key, 128 bit block)	<input type="radio"/>																						
AES-192-CBC (192 bit key, 128 bit block)	<input type="radio"/>																						
AES-192-CFB (192 bit key, 128 bit block)	<input type="radio"/>																						
AES-192-CFB1 (192 bit key, 128 bit block)	<input type="radio"/>																						
AES-192-CFB8 (192 bit key, 128 bit block)	<input type="radio"/>																						
AES-256-GCM																							
	The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode. 																						
<u>Fallback Data Encryption Algorithm</u>	AES-256-CBC (256 bit key, 128 bit block) <input type="button" value="▼"/>	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.																					
<u>Auth digest algorithm</u>	SHA256 (256-bit) <input type="button" value="▼"/>	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.																					
<u>Hardware Crypto</u>	Intel RDRAND engine - RAND <input type="button" value="▼"/>																						
<u>Certificate Depth</u>	One (Client+Server) <input type="button" value="▼"/>	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.																					
<u>Strict User-CN Matching</u>	<input type="checkbox"/> Enforce match When authenticating users, enforce a match between the common name of the client certificate and the username given at login.																						
<u>Client Certificate Key Usage Validation</u>	<input type="checkbox"/> Enforce key usage Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").																						

<b>Tunnel Settings</b>	
<b>IPv4 Tunnel Network</b>	<input type="text" value="10.200.220.0/26"/>
<p>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.</p>	
<b>IPv6 Tunnel Network</b>	<input type="text"/>
<p>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.</p>	
<b>Redirect IPv4 Gateway</b>	<input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
<b>Redirect IPv6 Gateway</b>	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
<b>IPv4 Local network(s)</b>	<input type="text" value="10.0.0.0/23"/>
<p>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.</p>	
<b>IPv6 Local network(s)</b>	<input type="text"/>
<p>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.</p>	
<b>Concurrent connections</b>	<input type="text"/>
<p>Specify the maximum number of clients allowed to concurrently connect to this server.</p>	
<b>Allow Compression</b>	<input type="button" value="Refuse any non-stub compression (Most secure)"/>
<p>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.</p>	
<p>Asymmetric compression allows an easier transition when connecting with older peers.</p>	
<b>Type-of-Service</b>	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
<b>Inter-client communication</b>	<input type="checkbox"/> Allow communication between clients connected to this server
<b>Duplicate Connection</b>	<input type="checkbox"/> Allow multiple concurrent connections from the same user
<p>When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session.</p>	
<p>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.</p>	
<b>Client Settings</b>	
<b>Dynamic IP</b>	<input checked="" type="checkbox"/> Allow connected clients to retain their connections if their IP address changes.
<b>Topology</b>	<input type="button" value="Subnet – One IP address per client in a common subnet"/>
<p>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".</p>	

<b>Ping settings</b>	
<b>Inactive</b>	<input type="text" value="300"/>
<p>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.</p>	
<b>Ping method</b>	<input type="text" value="keepalive – Use keepalive helper to define ping configuration"/> <input type="button" value="▼"/>
<p>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</p>	
<b>Interval</b>	<input type="text" value="10"/>
<b>Timeout</b>	<input type="text" value="60"/>
<b>Advanced Client Settings</b>	
<b>DNS Default Domain</b>	<input checked="" type="checkbox"/> Provide a default domain name to clients
<b>DNS Default Domain</b>	<input type="text" value="amhp.local"/>
<b>DNS Server enable</b>	<input checked="" type="checkbox"/> Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
<b>DNS Server 1</b>	<input type="text" value="10.0.0.71"/>
<b>DNS Server 2</b>	<input type="text"/>
<b>DNS Server 3</b>	<input type="text"/>
<b>DNS Server 4</b>	<input type="text"/>
<b>Block Outside DNS</b>	<input type="checkbox"/> Make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. <small>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.</small>
<b>Force DNS cache update</b>	<input type="checkbox"/> Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation. <small>This is known to kick Windows into recognizing pushed DNS servers.</small>
<b>NTP Server enable</b>	<input checked="" type="checkbox"/> Provide an NTP server list to clients
<b>NTP Server 1</b>	<input type="text" value="10.0.0.71"/>
<b>NTP Server 2</b>	<input type="text"/>
<b>NetBIOS enable</b>	<input checked="" type="checkbox"/> Enable NetBIOS over TCP/IP <small>If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.</small>
<b>Node Type</b>	<input type="text" value="m-node"/> <input type="button" value="▼"/>
<small>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)</small>	
<b>Scope ID</b>	<input type="text"/>
<small>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</small>	
<b>WINS server enable</b>	<input type="checkbox"/> 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

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

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

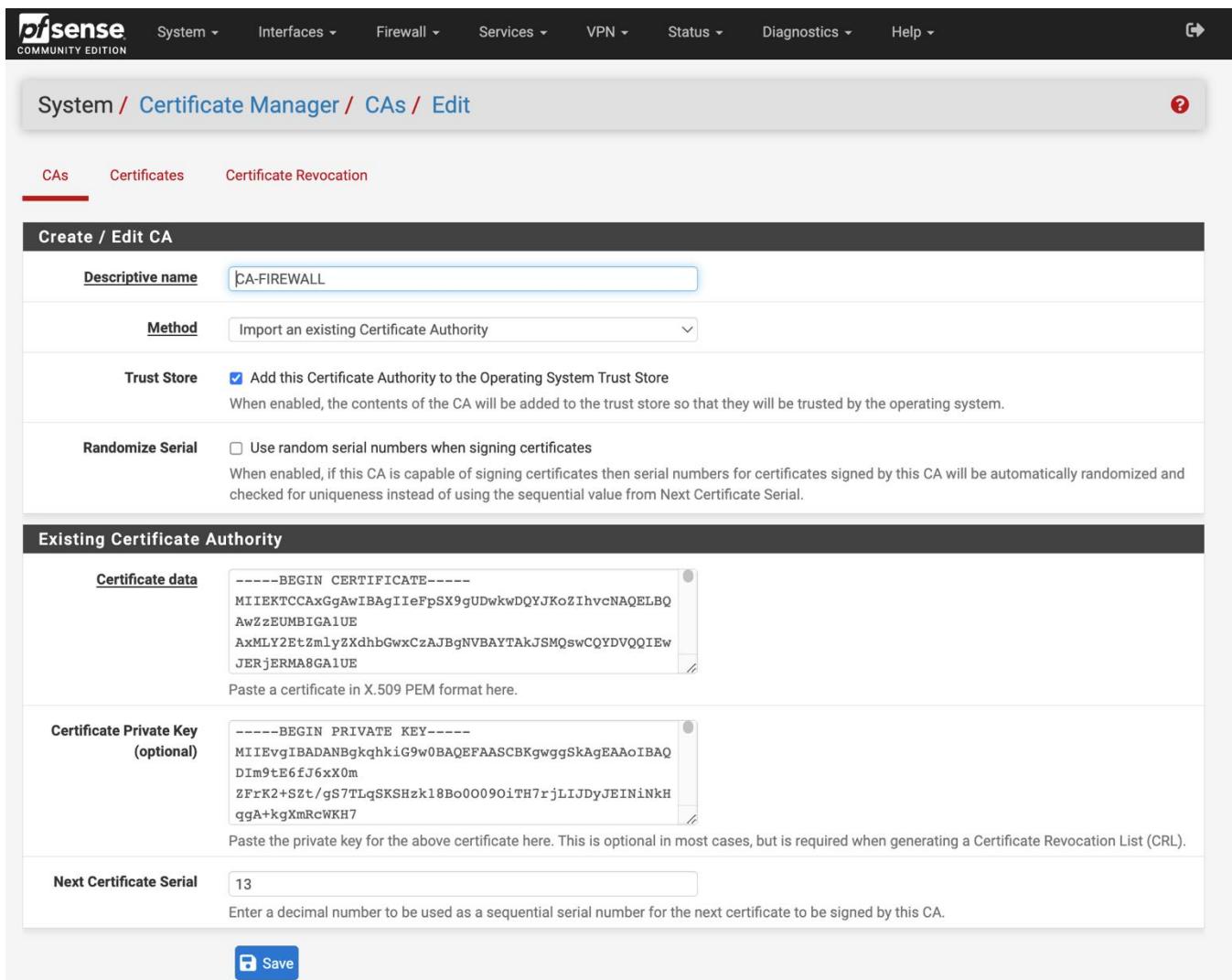
Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output.

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

**Criar certificado local open source para acesso VPN**

The screenshot shows the pfSense Certificate Manager interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main title is "System / Certificate Manager / CAs / Edit". Below the title, there are tabs for CAs (selected), Certificates, and Certificate Revocation.

**Create / Edit CA**

**Descriptive name:** CA-FIREWALL

**Method:** Import an existing Certificate Authority

**Trust Store:**  Add this Certificate Authority to the Operating System Trust Store  
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

**Randomize Serial:**  Use random serial numbers when signing certificates  
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

**Existing Certificate Authority**

**Certificate data:**

```
-----BEGIN CERTIFICATE-----
MIIEKTC...  
-----END CERTIFICATE-----
```

Paste a certificate in X.509 PEM format here.

**Certificate Private Key (optional)**

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwg...  
-----END PRIVATE KEY-----
```

Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).

**Next Certificate Serial:** 13

Enter a decimal number to be used as a sequential serial number for the next certificate to be signed by this CA.

**Save**

System / Certificate Manager / Certificates ?

CAs Certificates Certificate Revocation

**Edit an Existing Certificate**

**Method**

**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
DIE19TWsau175j
7RqQPUSwI2zucqoM0mTydNQMhZvfQuhky9Z6tNJ4DItgbYJ6Z7D
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**   
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	
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 		
✓ 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: 		
✓ 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"**

**pfSense COMMUNITY EDITION** System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Package / Proxy Server: General Settings / General

General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authentication Users Real Time Status Sync

### Squid General Settings

Enable Squid Proxy	<input checked="" type="checkbox"/> Check to enable the Squid proxy. <b>Important:</b> If unchecked, ALL Squid services will be disabled and stopped.
Keep Settings/Data	<input checked="" type="checkbox"/> If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls. <b>Important:</b> If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.
Listen IP Version	IPv4 Select the IP version Squid will use to select addresses for accepting client connections.
CARP Status VIP	10.0.1.1 (Vip Lan) Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status. <b>Important:</b> Don't forget to generate Local Cache on the secondary node and configure <a href="#">XMLRPC Sync</a> for the settings synchronization.
Proxy Interface(s)	10.0.1.1 (Vip Lan) 189.50.89.149 (VIP_WAN_FALEOLA) 149.78.107.69 (VIP_WAN_SILTELBRA) WAN_FALEOLA The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.
Outgoing Network Interface	Default (auto) The interface the proxy server will use for outgoing connections.
Proxy Port	3128 This is the port the proxy server will listen on. Default: 3128
ICP Port	 This is the port the proxy server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.
Allow Users on Interface	<input checked="" type="checkbox"/> If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy. There will be no need to add the interface's subnet to the list of allowed subnets.
Patch Captive Portal	This feature was removed - see <a href="#">Bug #5594</a> for details!
Resolve DNS IPv4 First	<input type="checkbox"/> Enable this to force DNS IPv4 lookup first. This option is very useful if you have problems accessing HTTPS sites.
Disable ICMP	<input type="checkbox"/> Check this to disable Squid ICMP pinger helper.
Use Alternate DNS Servers for the Proxy Server	 To use DNS servers other than those configured in <a href="#">System &gt; General Setup</a> , enter the IP(s) here. Separate entries by semi-colons ( ; )
Extra Trusted CA	none Select extra Trusted CA certificate in addition to the default root certificate bundle. <b>Warning:</b> This option may only be required if the upstream proxy is using SSL/MITM mode and could be a security issue in other cases. 

## Transparent Proxy Settings

<b>Transparent HTTP Proxy</b>	<input type="checkbox"/> Enable transparent mode to forward all requests for destination port 80 to the proxy server.
<p><b>Transparent Proxy Interface(s)</b></p> <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;">           189.50.89.149 (VIP_WAN_FALE_OLA)            149.78.107.69 (VIP_WAN_SILTELBRA)            WAN_FALE_OLA            WAN_X         </div> <p>The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.</p>	
<b>Bypass Proxy for Private Address Destination</b>	<input type="checkbox"/> Do not forward traffic to Private Address Space (RFC 1918 and IPv6 ULA) destinations. Destinations in Private Address Space ( <a href="#">RFC 1918</a> and <a href="#">IPv6 ULA</a> ) are passed directly through the firewall, not through the proxy server.
<b>Bypass Proxy for These Source IPs</b>	<input type="text"/> Do not forward traffic from these source IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall. <b>Applies only to transparent mode.</b> Separate entries by semi-colons ( ; )
<b>Bypass Proxy for These Destination IPs</b>	<input type="text"/> Do not proxy traffic going to these destination IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall. <b>Applies only to transparent mode.</b> Separate entries by semi-colons ( ; )

## SSL Man In the Middle Filtering

<b>HTTPS/SSL Interception</b>	<input checked="" type="checkbox"/> Enable SSL filtering.
<b>SSL/MITM Mode</b>	<input type="text" value="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. <a href="#">Click Info for details.</a>
<b>SSL Intercept Interface(s)</b>	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;">           10.0.1.1 (Vip Lan)            189.50.89.149 (VIP_WAN_FALE_OLA)            149.78.107.69 (VIP_WAN_SILTELBRA)            WAN_FALE_OLA         </div> <p>The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.</p>
<b>SSL Proxy Port</b>	<input type="text"/> This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129
<b>SSL Proxy Compatibility Mode</b>	<input type="text" value="Intermediate"/> The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. <a href="#">Click Info for details.</a>
<b>DHParams Key Size</b>	<input type="text" value="2048 (default)"/> DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.
<b>CA</b>	<input type="text" value="CA-FIREWALL"/> Select Certificate Authority to use when SSL interception is enabled. <a href="#">Click Info for details.</a>
<b>SSL Certificate Deamon Children</b>	<input type="text"/> This is the number of SSL certificate deamon children to start. May need to be increased in busy environments. Default: 5
<b>Remote Cert Checks</b>	<input type="text" value="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.
<b>Certificate Adapt</b>	<input type="text"/> 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	<input checked="" type="checkbox"/> This will enable the access log. <b>Warning:</b> 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 <b>Important:</b> 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	<input type="checkbox"/> 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	<input type="checkbox"/> 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	<input type="checkbox"/> 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 authentication 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.

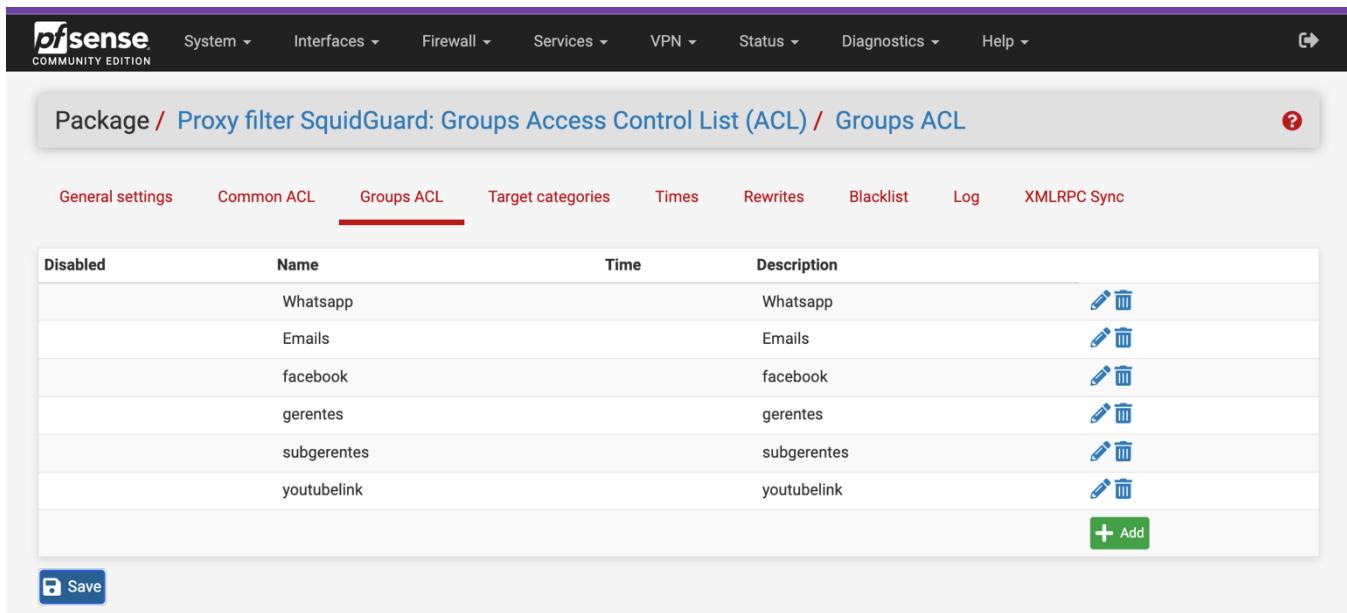
### Miscellaneous

**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**

<b>Blacklist</b>	<input checked="" type="checkbox"/> Check this option to enable blacklist
<b>Blacklist proxy</b>	<input type="text"/>
<p>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'</p>	
<b>Blacklist URL</b>	<input type="text" value="http://web.archive.org/web/20210502020725if_/http://www.shallalist.c..."/>
<p>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).</p>	
<b>Save</b>	

## Definir grupos de acesso a internet via AD

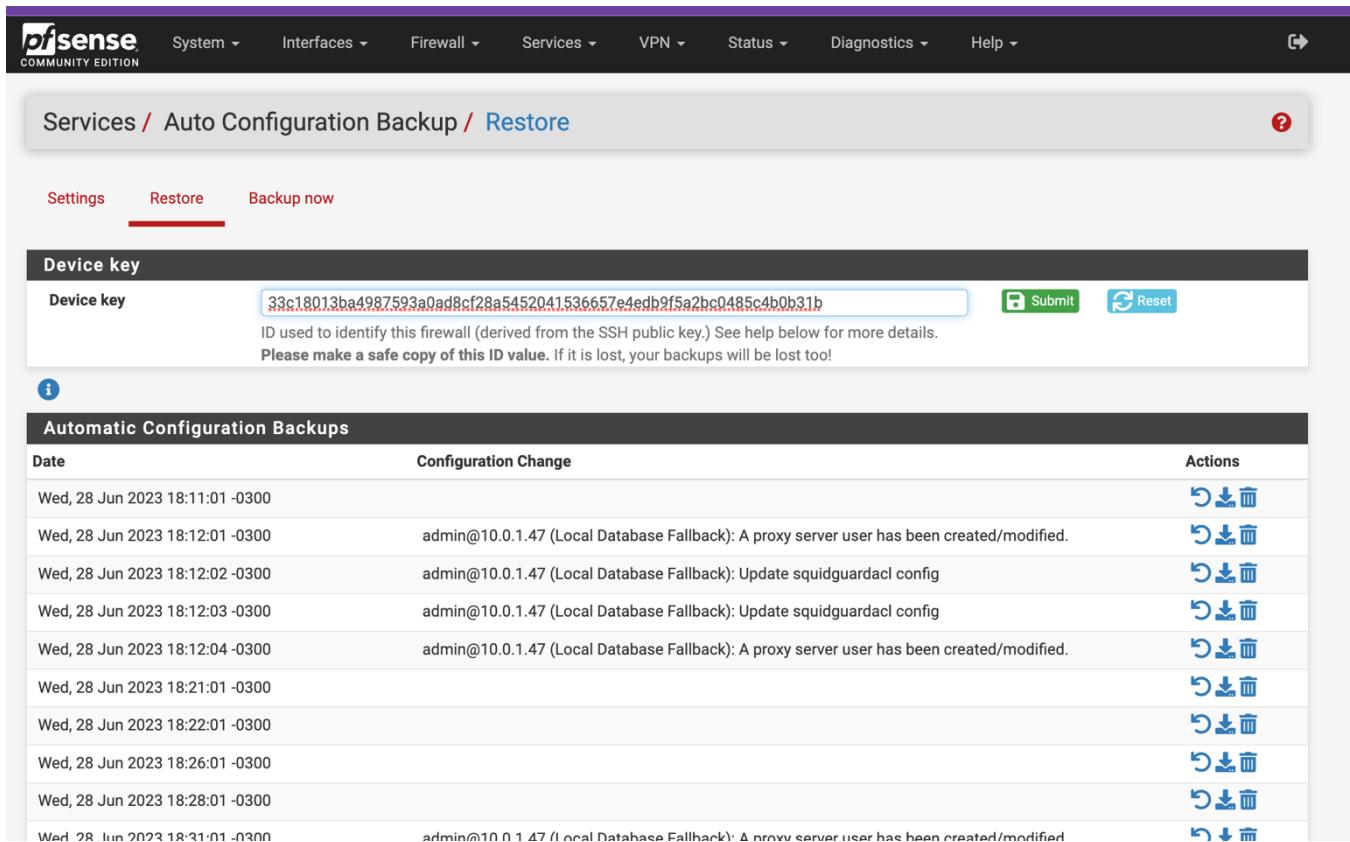


The screenshot shows the 'Groups ACL' tab selected in the Pfsense interface. The table lists the following groups:

Disabled	Name	Time	Description	Action
	Whatsapp		Whatsapp	 
	Emails		Emails	 
	facebook		facebook	 
	gerentes		gerentes	 
	subgerentes		subgerentes	 
	youtubelink		youtubelink	 

**Buttons:**

- + Add
- Save

**Criar backup da configuração do pfsense**

Services / Auto Configuration Backup / Restore

Settings    **Restore**    Backup now

**Device key**

Device key  Submit Reset

ID used to identify this firewall (derived from the SSH public key.) See help below for more details.  
Please make a safe copy of this ID value. If it is lost, your backups will be lost too!

**Automatic Configuration Backups**

Date	Configuration Change	Actions
Wed, 28 Jun 2023 18:11:01 -0300		
Wed, 28 Jun 2023 18:12:01 -0300	admin@10.0.1.47 (Local Database Fallback): A proxy server user has been created/modified.	
Wed, 28 Jun 2023 18:12:02 -0300	admin@10.0.1.47 (Local Database Fallback): Update squidguardacl config	
Wed, 28 Jun 2023 18:12:03 -0300	admin@10.0.1.47 (Local Database Fallback): Update squidguardacl config	
Wed, 28 Jun 2023 18:12:04 -0300	admin@10.0.1.47 (Local Database Fallback): A proxy server user has been created/modified.	
Wed, 28 Jun 2023 18:21:01 -0300		
Wed, 28 Jun 2023 18:22:01 -0300		
Wed, 28 Jun 2023 18:26:01 -0300		
Wed, 28 Jun 2023 18:28:01 -0300		
Wed, 28 Jun 2023 18:31:01 -0300	admin@10.0.1.47 (Local Database Fallback): A proxy server user has been created/modified.	

## Criação das regras de firewall de acesso a internet

**pfSense COMMUNITY EDITION**

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

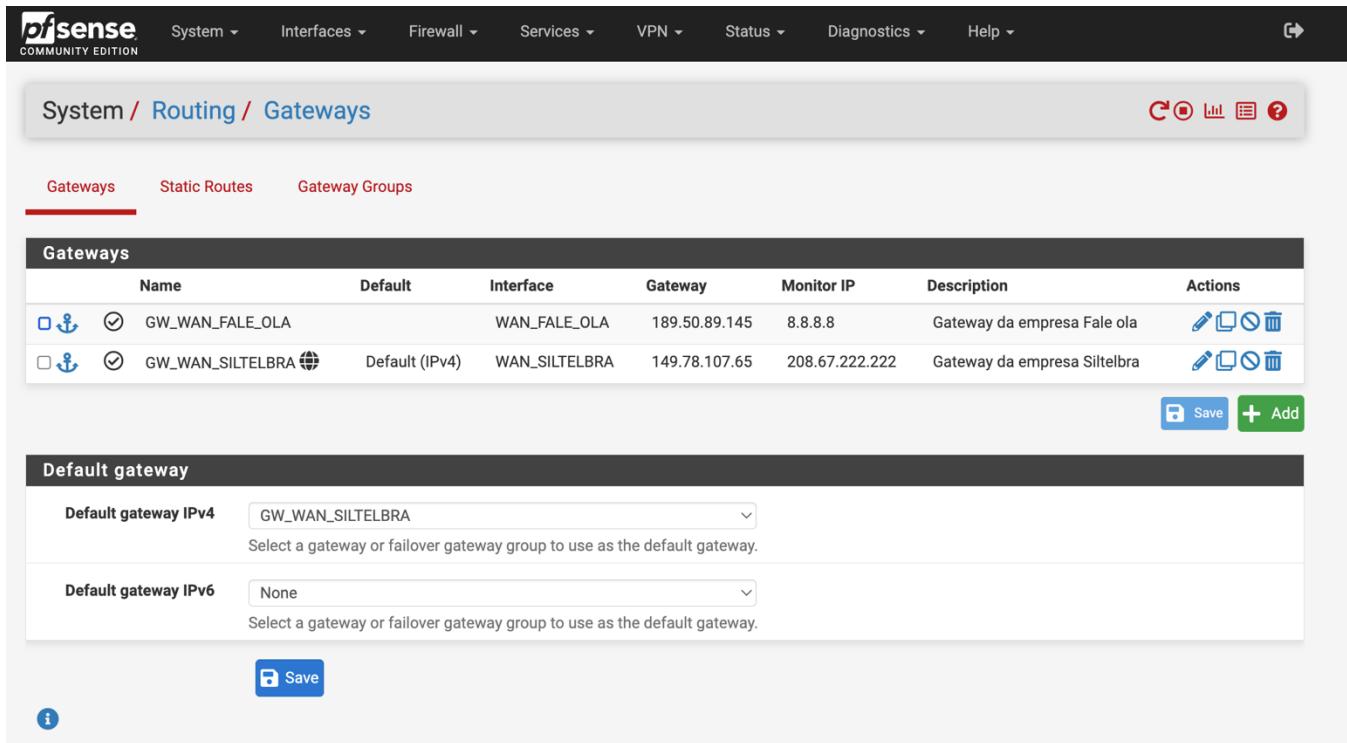
Firewall / Rules / LAN\_TEAM

Floating WAN\_FALE\_OLA WAN\_X WAN\_SILTELBRA SYNC **LAN\_TEAM** OpenVPN

**Rules (Drag to Change Order)**

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>   4 / 299.42 MiB	IPv4 TCP	10.0.1.47	*	*	*	*	none			   
<b>BLOQUEIO</b>										
<input type="checkbox"/>  0 / 0 B	IPv4 UDP	*	*	239.255.255.250	1900	*	none		Bloquear upnp	   
<input type="checkbox"/>  0 / 0 B	IPv4 UDP	*	*	ip_broadcast_lan	port_netbios	*	none		Bloquear broadcast smb	   
<input type="checkbox"/>   0 / 0 B	IPv4 TCP/UDP	LAN_TEAM net	*	Rede_tor	*	*	none		Bloquear rede tor	   
<input type="checkbox"/>  0 / 0 B	IPv4 UDP	*	*	ip_llmnr_local	port_llmnr	*	none		Bloqueia LLMNR	   
<input type="checkbox"/>  0 / 0 B	IPv6 *	*	*	*	*	*	none		Bloqueia IPv6	   
<b>LAN &gt; WAN</b>										
<input type="checkbox"/>   0 / 115 KIB	IPv4 TCP	LAN_TEAM net	*	aws_oracle	port_oracle	*	none		Permitir acesso oracle aws	   
<input type="checkbox"/>   0 / 2.28 MiB	IPv4 TCP/UDP	ips_ti	*	*	web_port_http	LB_WAN	none		Acesso ti a internet	   
<input type="checkbox"/>   0 / 61 KIB	IPv4 ICMP any	LAN_TEAM net	*	*	*	LB_WAN	none		Liberar ICMP para internet	   
<input type="checkbox"/>   0 / 0 B	IPv4 TCP	LAN_TEAM net	*	excecoes_webproxy	web_port_http	LB_WAN	none		Permiti site com excessao	   
<input type="checkbox"/>   0 / 0 B	IPv4 TCP	active_directory_dns	*	*	53 (DNS)	LB_WAN	none		Liberar AD acessar DNS externo	   
<input type="checkbox"/>   0 / 8 KIB	IPv4 TCP	active_directory_dns	*	*	*	LB_WAN	none		Acesso Full AD	   
<b>LAN &gt; LAN</b>										
<input type="checkbox"/>   2 / 33 KIB	IPv4 TCP	LAN_TEAM net	*	LAN_TEAM address	*	*	none		Permitir acesso ao proxy da rede local	   
<input type="checkbox"/>   0 / 0 B	IPv4 TCP	LAN_TEAM net	*	This Firewall	53 (DNS)	*	none		Liberar consulta DNS do firewall	   
<input type="button" value="↑ Add"/> <input type="button" value="↓ Add"/> <input type="button" value="Delete"/> <input type="button" value="Save"/> <input type="button" value="Separador"/>										

## Definir rotas para o Pfsense



The screenshot shows the Pfsense web interface with the following details:

**Header:** pfSense COMMUNITY EDITION, System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help.

**Breadcrumbs:** System / Routing / Gateways

**Buttons:** CO, LL, G, ?

**Navigation:** Gateways (selected), Static Routes, Gateway Groups.

**Table: Gateways**

Name	Default	Interface	Gateway	Monitor IP	Description	Actions
GW_WAN_FALE_OLA	<input checked="" type="checkbox"/>	WAN_FALE_OLA	189.50.89.145	8.8.8.8	Gateway da empresa Fale ola	  
GW_WAN_SILTELBRA	<input checked="" type="checkbox"/>	WAN_SILTELBRA	149.78.107.65	208.67.222.222	Gateway da empresa Sitelbra	  

**Buttons:** Save, Add.

**Section: Default gateway**

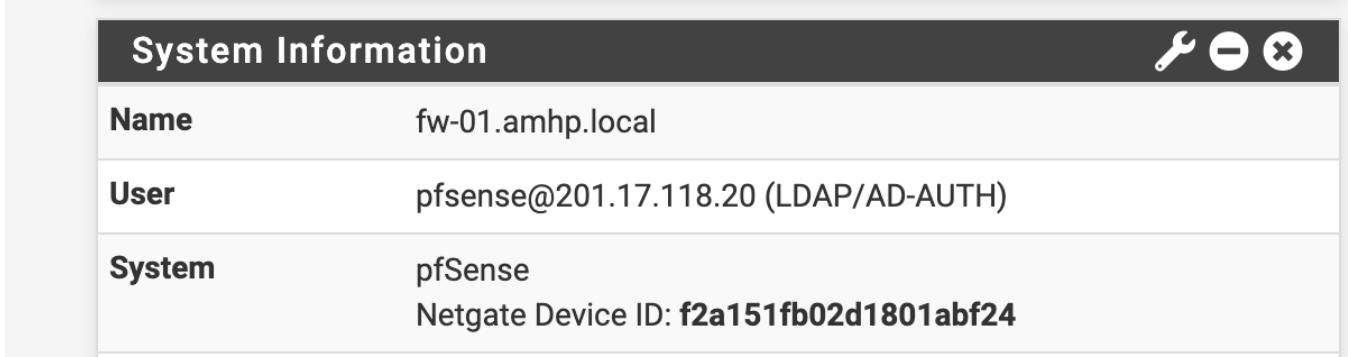
**Default gateway IPv4:** GW\_WAN\_SILTELBRA (dropdown menu)  
Select a gateway or failover gateway group to use as the default gateway.

**Default gateway IPv6:** None (dropdown menu)  
Select a gateway or failover gateway group to use as the default gateway.

**Buttons:** Save.

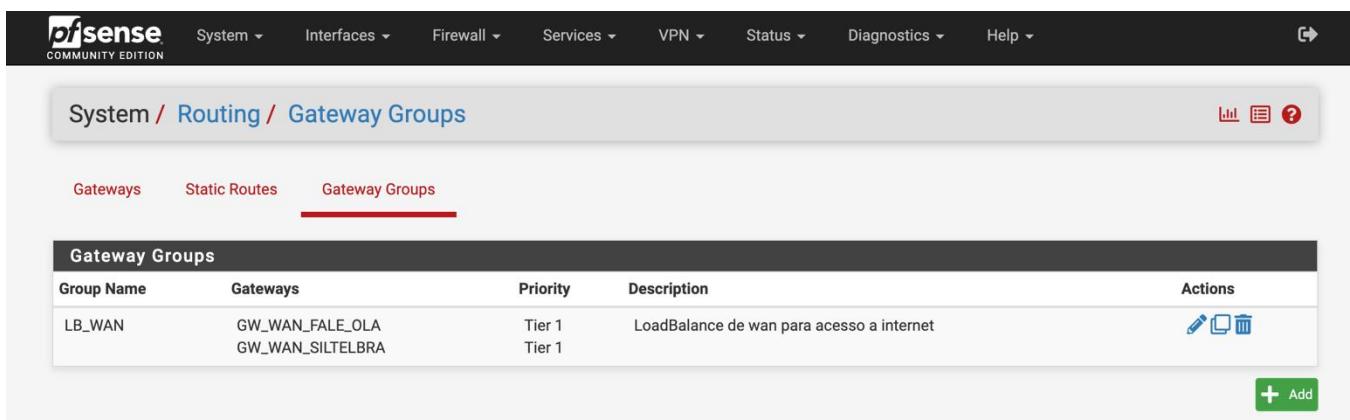
## Validação dos acessos

- Acesso vi active directory**



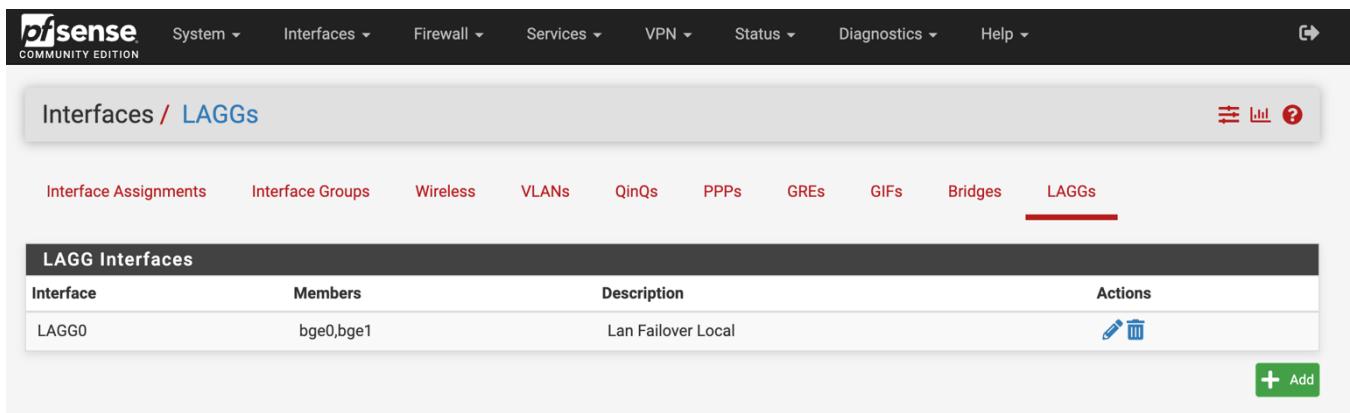
System Information	
Name	fw-01.amhp.local
User	pfsense@201.17.118.20 (LDAP/AD-AUTH)
System	pfSense Netgate Device ID: <b>f2a151fb02d1801abf24</b>

- HA das Interfaces WAN**



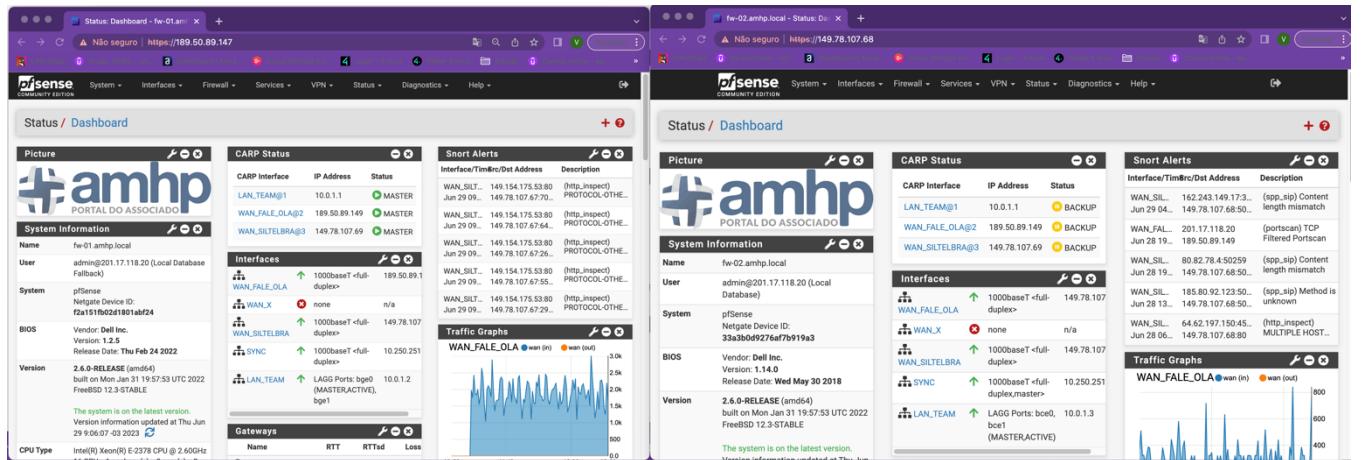
Gateway Groups				
Group Name	Gateways	Priority	Description	Actions
LB_WAN	GW_WAN_FALE_OLA GW_WAN_SILTELBRA	Tier 1 Tier 1	LoadBalance de wan para acesso a internet	

- HA das Interfaces LAN**

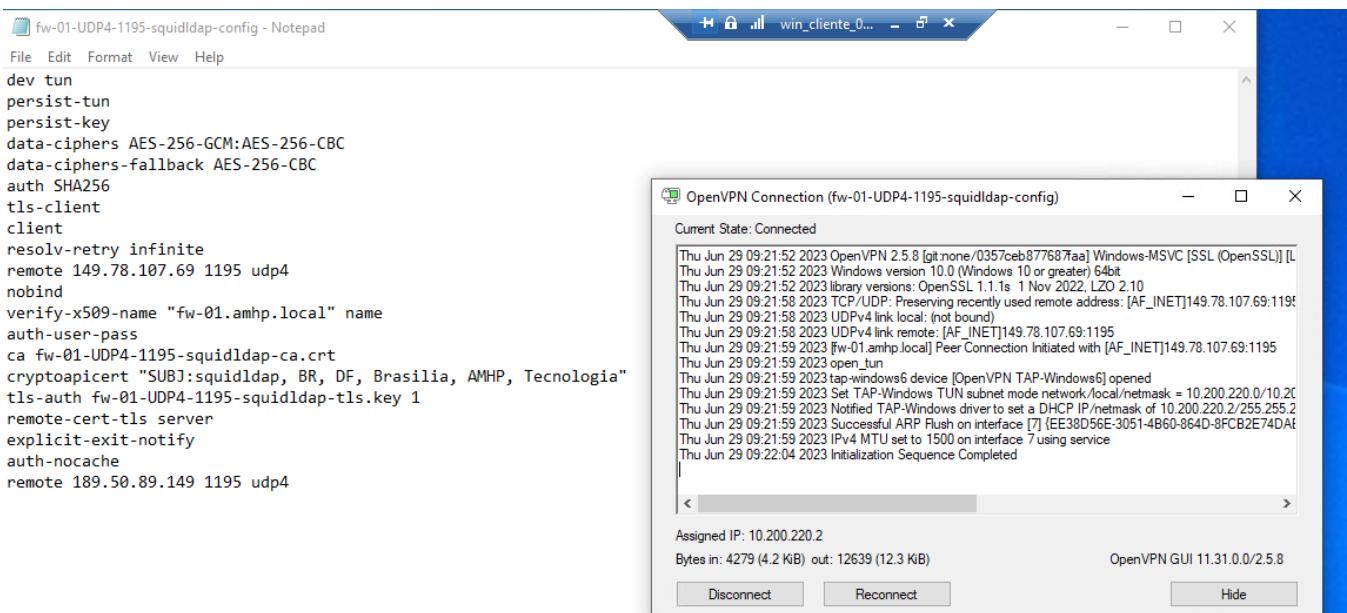


LAGG Interfaces			
Interface	Members	Description	Actions
LAGG0	bge0,bge1	Lan Failover Local	

- HA do firewall



- Acesso da VPN



```

fw-01-UDP4-1195-squidldap-config - Notepad
File Edit Format View Help
dev tun
persist-tun
persist-key
data-ciphers AES-256-GCM:AES-256-CBC
data-ciphers-fallback AES-256-CBC
auth SHA256
tls-client
client
resolv-retry infinite
remote 149.78.107.69 1195 udp4
nobind
verify-x509-name "fw-01.amhp.local" name
auth-user-pass
ca fw-01-UDP4-1195-squidldap-ca.crt
cryptoapicert "SUBJ:squidldap, BR, DF, Brasilia, AMHP, Tecnologia"
tls-auth fw-01-UDP4-1195-squidldap-tls.key 1
remote-cert-tls server
explicit-exit-notify
auth-nocache
remote 189.50.89.149 1195 udp4

```

- *Liberação internet via squid*