



MINISTÉRIO DA  
CIÊNCIA, TECNOLOGIA  
E INOVAÇÕES



sid.inpe.br/mtc-m21c/2020/08.06.14.04-MAN

## MANUAL DE CONFIGURAÇÃO DA VPN SERVER - DIRETOR EMMN

Carolyna Cibelly Fernandes de Almeida

Projeto: Estação Multimissão de  
Natal

URL do documento original:

<<http://urlib.net/8JMKD3MGP3W34R/432H56H>>

INPE  
São José dos Campos  
2020

## **PUBLICADO POR:**

Instituto Nacional de Pesquisas Espaciais - INPE

Gabinete do Diretor (GBDIR)

Serviço de Informação e Documentação (SESID)

CEP 12.227-010

São José dos Campos - SP - Brasil

Tel.:(012) 3208-6923/7348

E-mail: pubtc@inpe.br

## **CONSELHO DE EDITORAÇÃO E PRESERVAÇÃO DA PRODUÇÃO INTELECTUAL DO INPE - CEPPII (PORTARIA Nº 176/2018/SEI-INPE):**

### **Presidente:**

Dra. Marley Cavalcante de Lima Moscati - Centro de Previsão de Tempo e Estudos Climáticos (CGCPT)

### **Membros:**

Dra. Carina Barros Mello - Coordenação de Laboratórios Associados (COCTE)

Dr. Alisson Dal Lago - Coordenação-Geral de Ciências Espaciais e Atmosféricas (CGCEA)

Dr. Evandro Albiach Branco - Centro de Ciência do Sistema Terrestre (COCST)

Dr. Evandro Marconi Rocco - Coordenação-Geral de Engenharia e Tecnologia Espacial (CGETE)

Dr. Hermann Johann Heinrich Kux - Coordenação-Geral de Observação da Terra (CGOBT)

Dra. Ieda Del Arco Sanches - Conselho de Pós-Graduação - (CPG)

Silvia Castro Marcelino - Serviço de Informação e Documentação (SESID)

### **BIBLIOTECA DIGITAL:**

Dr. Gerald Jean Francis Banon

Clayton Martins Pereira - Serviço de Informação e Documentação (SESID)

### **REVISÃO E NORMALIZAÇÃO DOCUMENTÁRIA:**

Simone Angélica Del Ducca Barbedo - Serviço de Informação e Documentação (SESID)

André Luis Dias Fernandes - Serviço de Informação e Documentação (SESID)

### **EDITORAÇÃO ELETRÔNICA:**

Ivone Martins - Serviço de Informação e Documentação (SESID)

Cauê Silva Fróes - Serviço de Informação e Documentação (SESID)



MINISTÉRIO DA  
CIÊNCIA, TECNOLOGIA  
E INOVAÇÕES



sid.inpe.br/mtc-m21c/2020/08.06.14.04-MAN

## MANUAL DE CONFIGURAÇÃO DA VPN SERVER - DIRETOR EMMN

Carolyna Cibelly Fernandes de Almeida

Projeto: Estação Multimissão de  
Natal

URL do documento original:

<<http://urlib.net/8JMKD3MGP3W34R/432H56H>>

INPE  
São José dos Campos  
2020



Esta obra foi licenciada sob uma Licença Creative Commons Atribuição-NãoComercial 3.0 Não Adaptada.

This work is licensed under a Creative Commons Attribution-NonCommercial 3.0 Unported License.



**Manual de configuração da VPN Server - Diretor  
EMMN**

**Junho/2020**



## Resumo

O OpenVPN é um software livre e open-source para criar redes privadas virtuais através de túneis criptografados entre computadores. Ele é capaz de estabelecer conexões diretas entre computadores mesmo que estes estejam atrás de Nat Firewalls sem necessidade de reconfiguração da sua rede. Este documento visa mostrar o passo a passo uso da VPN da EMMN pelo Diretor de operações. A VPN à seguir foi criada com o intuito de permitir o acesso aos serviços internos da estação, portanto só deverá ser utilizada para esta finalidade.



## Sumário

<b>Acesso a página de gerenciamento</b>	<b>4</b>
<b>Cadastrando Usuários</b>	<b>4</b>
<b>Criando uma nova VPN</b>	<b>7</b>
<b>Exportando o certificado do cliente</b>	<b>13</b>

## Acesso a página de gerenciamento

Para acessar a página de gerenciamento da VPN,

1. Abra seu navegador de preferência
2. Digite o IP **192.168.1.1** se estiver conectado a rede local da estação. Caso não esteja, digite o IP **200.137.4.220**
3. Clique em *Avançado* > *Ir para o ip digitado*



Sua conexão não é particular

Invasores podem estar tentando roubar suas informações de **200.137.4.220** (por exemplo, senhas, mensagens ou cartões de crédito). [Saiba mais](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID

Ocultar detalhes

Voltar à segurança

Este servidor não conseguiu provar que é **200.137.4.220**. O certificado de segurança não é confiável para o sistema operacional do seu computador. Isso pode ser causado por uma configuração incorreta ou pela interceptação da sua conexão por um invasor.

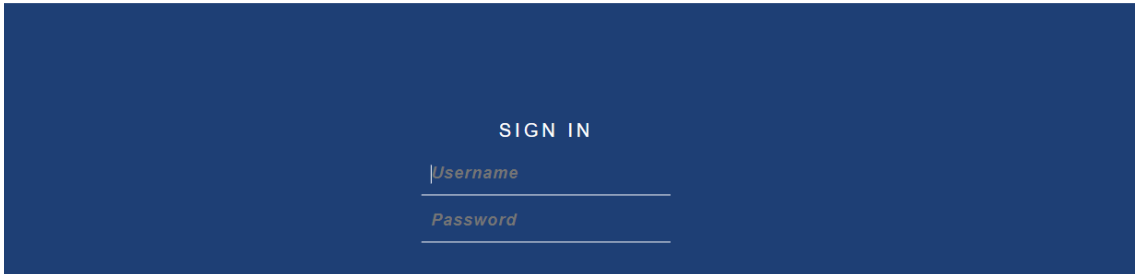
[Ir para 200.137.4.220 \(não seguro\)](#)

4. Entre com o login e senha corrente do PfSense

*Obs: O login e a senha podem ser encontrada no redmine na sessão da Infraestrutura > Serviços disponíveis*



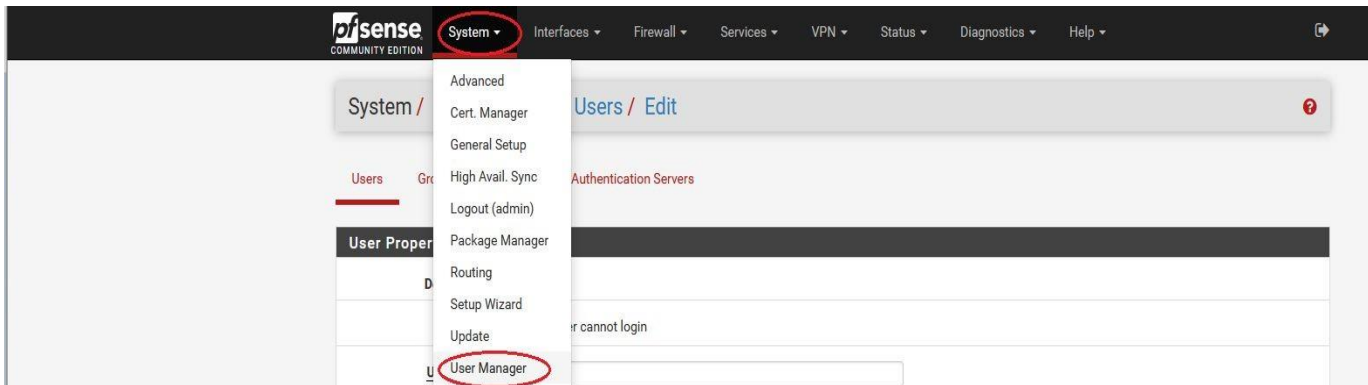
Login to pfSense



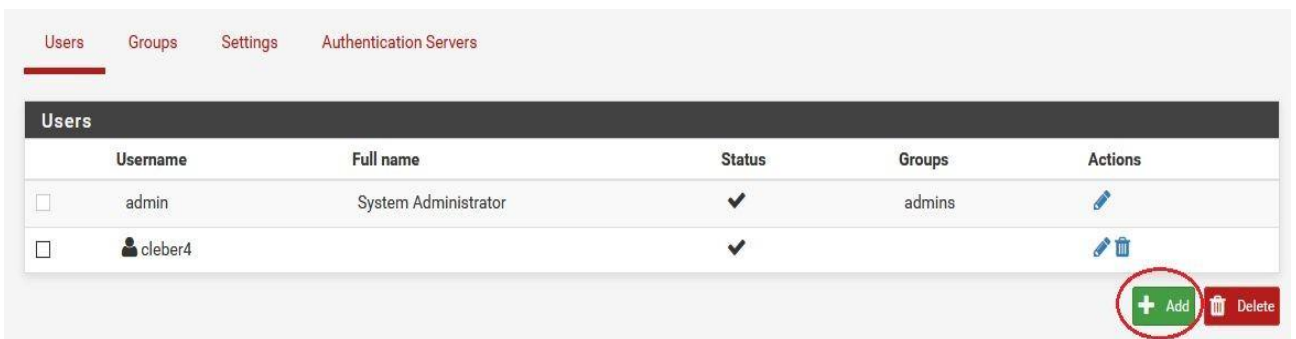
## Cadastrando usuários

1. Vá em *System* -> *User Manager* na barra superior





## 2. Clique no botão *Add*



3. Defina o nome do *usuário* e a *senha* e marque “*Click to create a user certificate*” para gerar o certificado do usuário e salve.

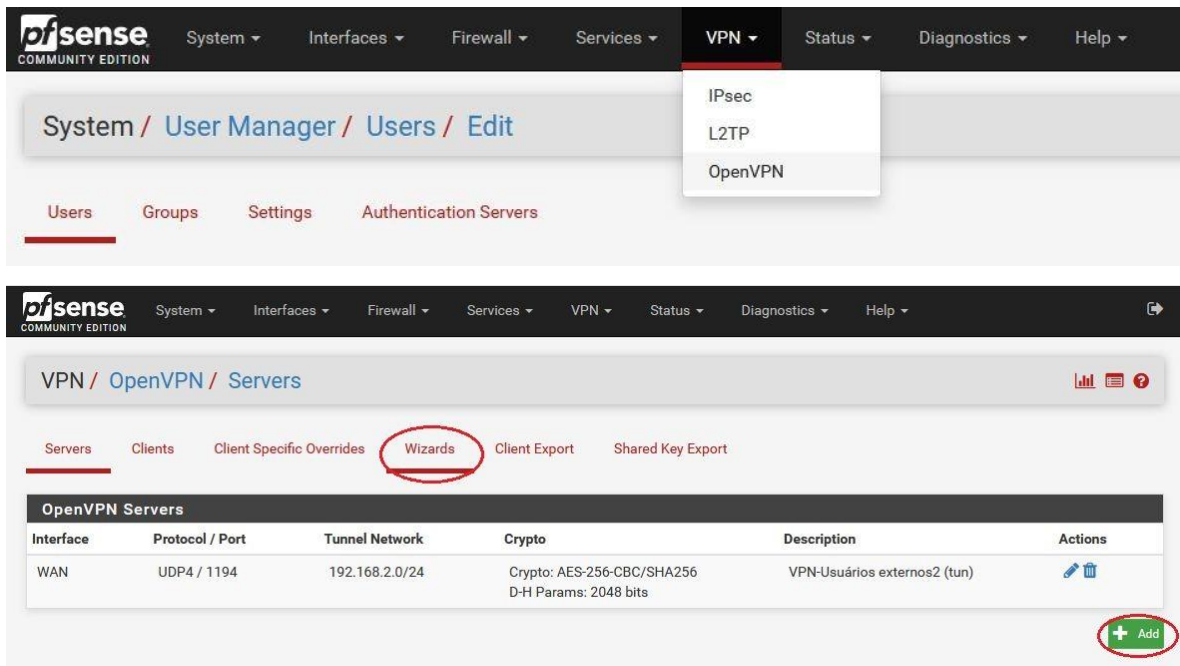
User Properties	
Defined by	USER
Disabled	<input type="checkbox"/> This user cannot login
Username	<input type="text" value="floripa"/>
Password	<input type="password" value="••••"/> <input type="password" value="••••"/>
Full name	<input type="text"/> User's full name, for administrative information only
Expiration date	<input type="text"/> Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.
Group membership	<input type="text" value="admins"/> <input type="text"/> Not member of <span style="margin-left: 200px;">Member of</span>
	<input type="button" value="» Move to 'Member of' list"/> <input type="button" value="« Move to 'Not member of' list"/>
	Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.
Certificate	<input checked="" type="checkbox"/> Click to create a user certificate



Create Certificate for User	
Descriptive name	<input type="text" value="floripa"/>
Certificate authority	<input type="text" value="ca-pfsense"/>
Key length	<input type="text" value="2048 bits"/> The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see <a href="http://keylength.com">keylength.com</a> .
Lifetime	<input type="text" value="3650"/>

## Criando uma nova VPN

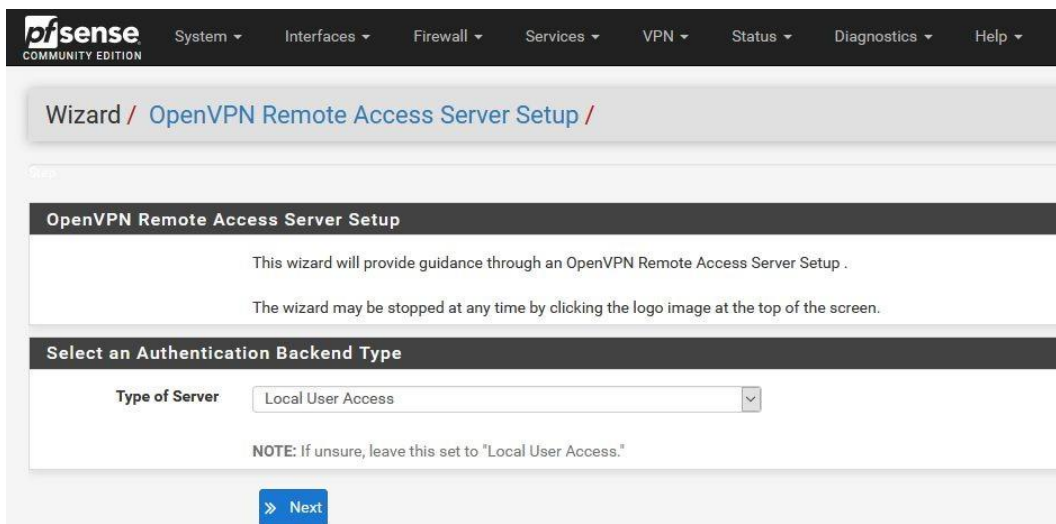
1. Vá em VPN, OpenVPN , na aba Wizards clique em **ADD**



The screenshot shows the pfSense web interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. The 'VPN' menu is open, showing options for 'IPsec', 'L2TP', and 'OpenVPN'. Below this, the breadcrumb trail is 'System / User Manager / Users / Edit'. The main content area shows the 'Users' tab selected, with sub-tabs for 'Groups', 'Settings', and 'Authentication Servers'. A second screenshot below shows the 'VPN / OpenVPN / Servers' page. The 'Wizards' tab is circled in red. Below the tabs is a table of OpenVPN Servers with columns for Interface, Protocol / Port, Tunnel Network, Crypto, Description, and Actions. A green '+ Add' button is circled in red at the bottom right of the table.

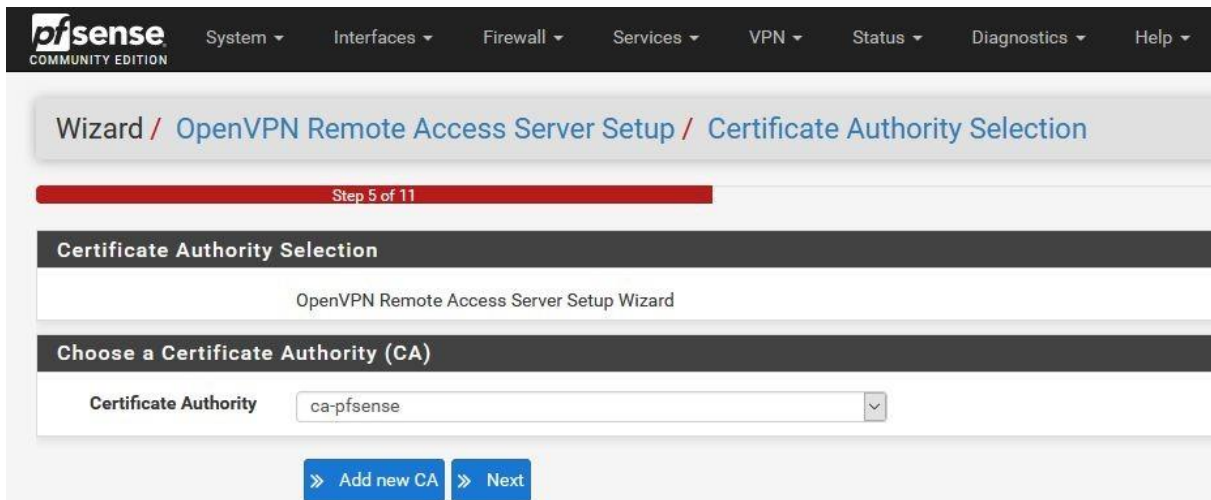
Interface	Protocol / Port	Tunnel Network	Crypto	Description	Actions
WAN	UDP4 / 1194	192.168.2.0/24	Crypto: AES-256-CBC/SHA256 D-H Params: 2048 bits	VPN-Usuários externos2 (tun)	 

2. Na primeira tela, *Select an Authentication Backend Type*, escolha **Local User Access**, e clique em **Next**



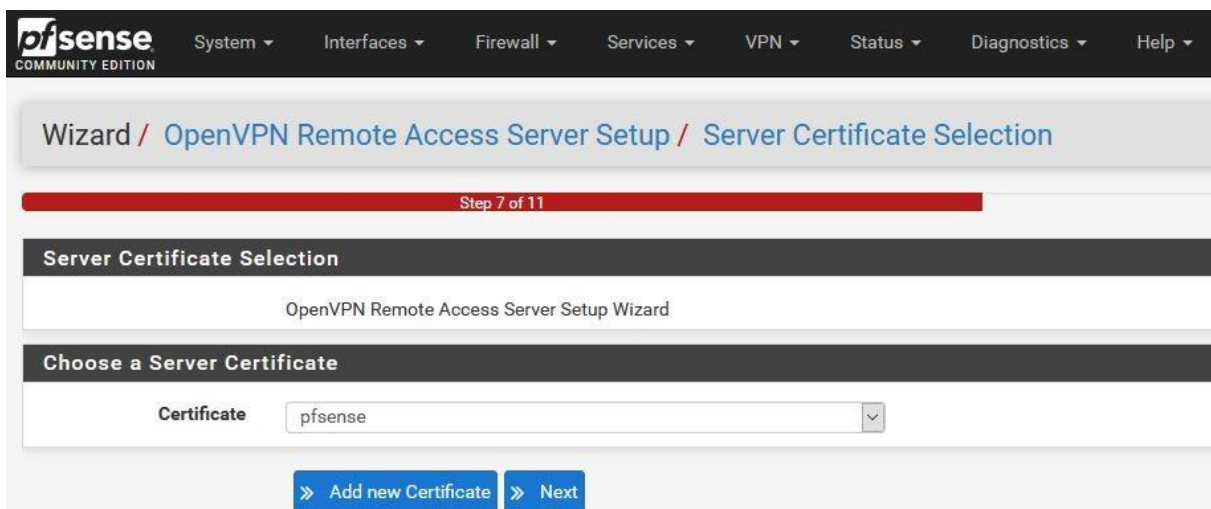
The screenshot shows the 'Wizard / OpenVPN Remote Access Server Setup /' page. The main heading is 'OpenVPN Remote Access Server Setup'. Below this, there is a text block: 'This wizard will provide guidance through an OpenVPN Remote Access Server Setup . The wizard may be stopped at any time by clicking the logo image at the top of the screen.' The next section is 'Select an Authentication Backend Type'. It contains a dropdown menu labeled 'Type of Server' with 'Local User Access' selected. Below the dropdown is a note: 'NOTE: If unsure, leave this set to "Local User Access."' At the bottom, there is a blue button labeled 'Next'.

3. Na segunda tela, *Choose a Certificate Authority (CA)*, selecione a autoridade certificadora que já foi criada previamente “ca-pfsense”, e clique em next



The screenshot shows the pfSense web interface for the OpenVPN Remote Access Server Setup Wizard. The breadcrumb trail is "Wizard / OpenVPN Remote Access Server Setup / Certificate Authority Selection". A progress bar indicates "Step 5 of 11". The main heading is "Certificate Authority Selection". Below it, the text "OpenVPN Remote Access Server Setup Wizard" is displayed. The section "Choose a Certificate Authority (CA)" contains a dropdown menu labeled "Certificate Authority" with "ca-pfsense" selected. At the bottom, there are two buttons: "Add new CA" and "Next".

4. Na terceira tela, *Choose a Server Certificate*, selecione o certificado de servidor que já está criado “pfsense” e clique em Next



The screenshot shows the pfSense web interface for the OpenVPN Remote Access Server Setup Wizard. The breadcrumb trail is "Wizard / OpenVPN Remote Access Server Setup / Server Certificate Selection". A progress bar indicates "Step 7 of 11". The main heading is "Server Certificate Selection". Below it, the text "OpenVPN Remote Access Server Setup Wizard" is displayed. The section "Choose a Server Certificate" contains a dropdown menu labeled "Certificate" with "pfsense" selected. At the bottom, there are two buttons: "Add new Certificate" and "Next".

5. Na tela seguinte, *Server Setup*, vamos configurar o servidor da VPN.

Aqui, você deve preencher de acordo com as configurações da rede.

**Interface:** WAN (interface de rede na qual o servidor aguardará pela conexão do cliente, deve apresentar conexão com a Internet)

**Protocol:** UDP

**Local Port:** 1194 (porta na qual o servidor aguardará pela conexão do cliente, 1194 é a porta convencional para o protocolo OpenVPN, você pode utilizar essa porta para a primeira VPN, mas se for criar outras, deverá reservar portas diferentes para cada VPN, por exemplo 1195, 1196...)

**Description:** Descrição da VPN, deve ser um nome informativo, até porque aparecerá na tela do cliente identificando a conexão.

**Tunnel Network:** É a rede definida para o túnel VPN, que será distribuída para os clientes. Esta rede escolhida não pode ser a mesma que a rede local. O pfSense tomará o primeiro endereço IP para ele, nesse exemplo 192.168.2.1, e os demais endereços IPs serão atribuídos aos clientes

**Local Network:** São as redes locais que os clientes conectados poderão ter acesso.

### Server Setup

OpenVPN Remote Access Server Setup Wizard

#### General OpenVPN Server Information

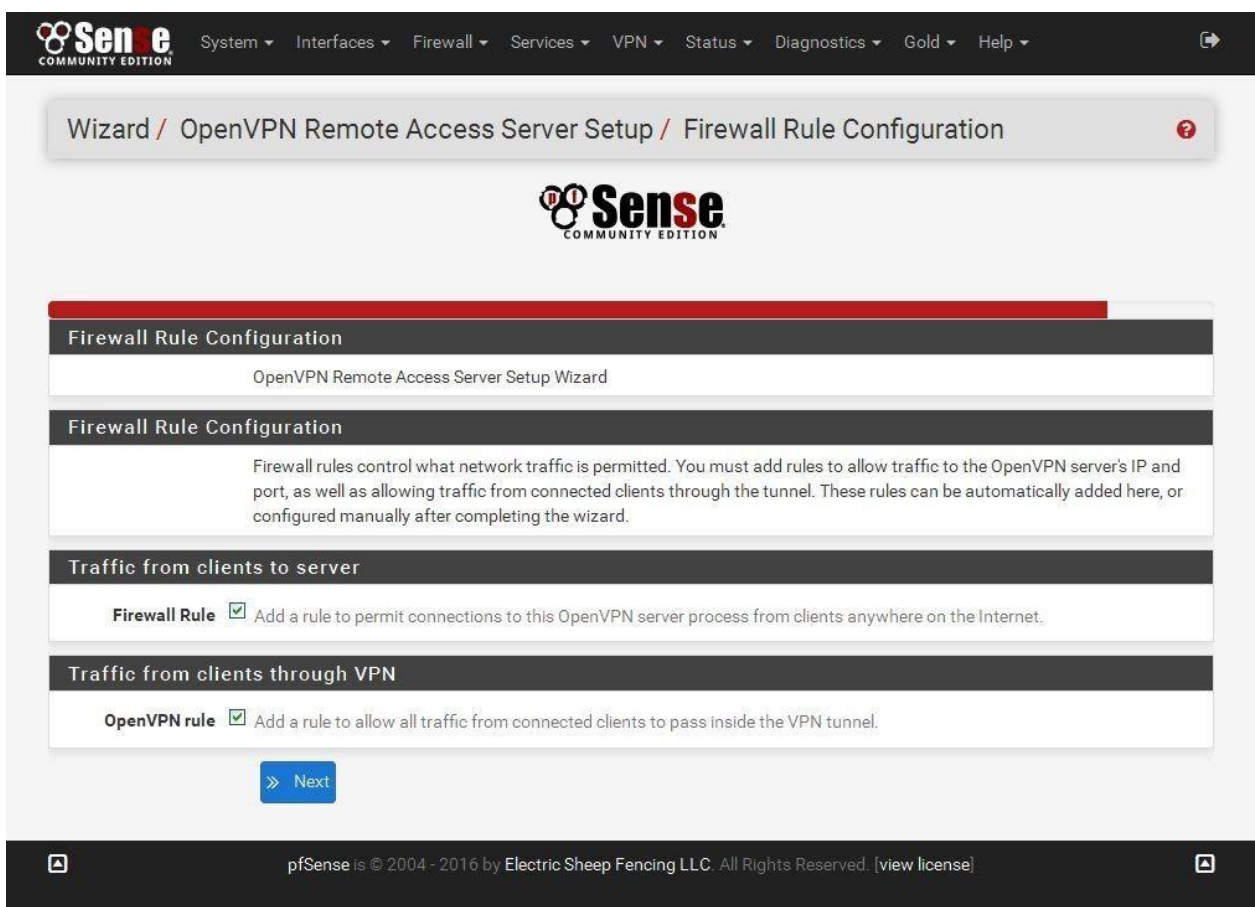
<b>Interface</b>	<input type="text" value="WAN"/>
The interface where OpenVPN will listen for incoming connections (typically WAN.)	
<b>Protocol</b>	<input type="text" value="UDP on IPv4 only"/>
Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.	
<b>Local Port</b>	<input type="text" value="1194"/>
Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.	
<b>Description</b>	<input type="text" value="VPN-Usuários externos"/>
A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.	

### Tunnel Settings

<b>Tunnel Network</b>	<input type="text" value="192.168.2.0/24"/>
This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.	
<b>Redirect Gateway</b>	<input type="checkbox"/>
Force all client generated traffic through the tunnel.	
<b>Local Network</b>	<input type="text" value="192.168.1.0/24"/>
This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. 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.	

6. Quando terminar, clique em *next*

7. Na penúltima tela do assistente, *Firewall Rule Configuration*, certifique-se de que as duas opções *Firewall Rule* e *OpenVPN rule* estejam marcadas. Com isso, o pfSense criará automaticamente as regras de *firewall* necessárias para que a VPN funcione. Clique em Next



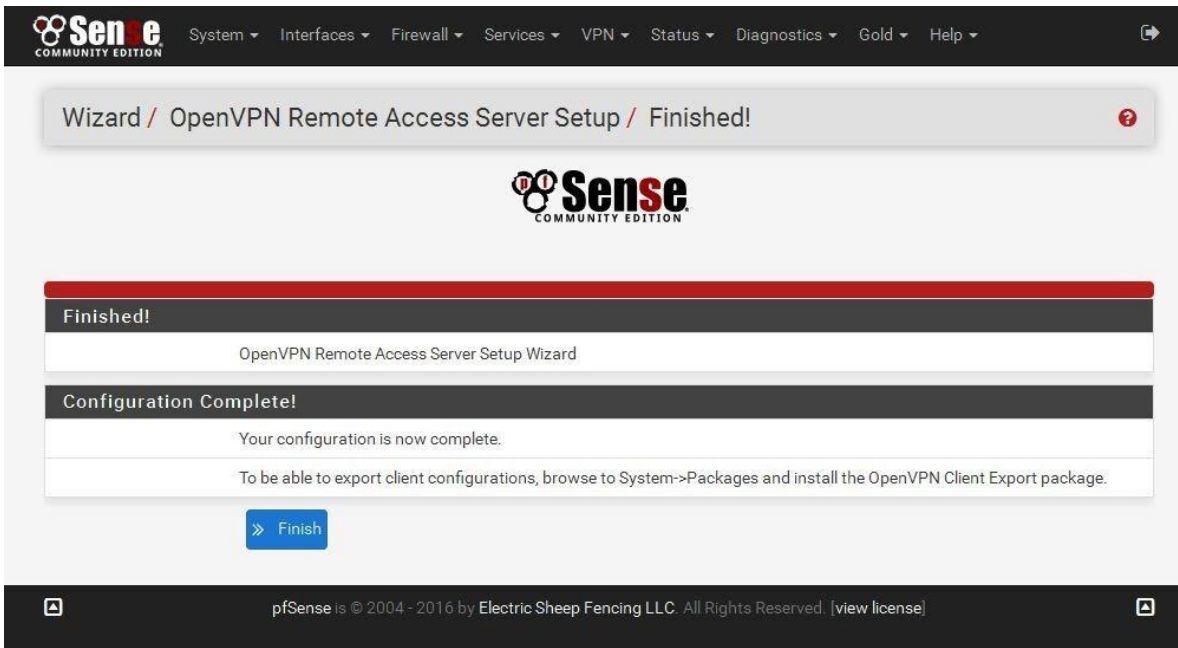
The screenshot shows the pfSense web interface during the 'Firewall Rule Configuration' step of the 'OpenVPN Remote Access Server Setup Wizard'. The breadcrumb trail at the top reads 'Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration'. The main content area is titled 'Firewall Rule Configuration' and contains the following sections:

- OpenVPN Remote Access Server Setup Wizard**
- Firewall Rule Configuration**: A text box explaining that firewall rules control network traffic and that rules for the OpenVPN server and tunnel should be added here.
- Traffic from clients to server**: A checkbox labeled 'Firewall Rule' is checked, with the text 'Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.'
- Traffic from clients through VPN**: A checkbox labeled 'OpenVPN rule' is checked, with the text 'Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.'

A blue 'Next' button is located at the bottom of the configuration area. The footer of the page contains the copyright information: 'pfSense is © 2004 - 2016 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]'.



8. A última tela apenas informa que a VPN foi criada. Clique em *Finish*

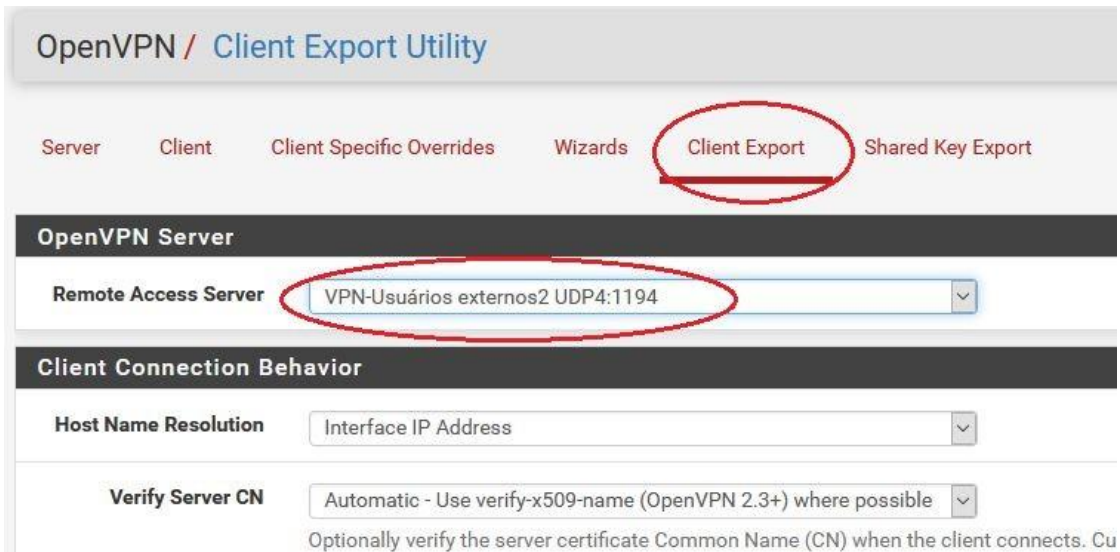


The screenshot shows the pfSense web interface. At the top, there is a navigation menu with items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. Below the menu, a breadcrumb trail reads "Wizard / OpenVPN Remote Access Server Setup / Finished!". The main content area features the pfSense logo and a large red progress bar. Below the bar, the text "Finished!" is displayed in a dark box, followed by "OpenVPN Remote Access Server Setup Wizard". Underneath, a dark box contains the text "Configuration Complete!". Below this, two lines of text provide instructions: "Your configuration is now complete." and "To be able to export client configurations, browse to System->Packages and install the OpenVPN Client Export package." At the bottom of the main content area, there is a blue button with a right-pointing arrow and the text "Finish". The footer of the page contains the copyright information: "pfSense is © 2004 - 2016 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]"



## Exportando o certificado do cliente

1. Vá em VPN, OpenVPN, aba Client Export e selecione a vpn desejada



OpenVPN / Client Export Utility

Server Client Client Specific Overrides Wizards **Client Export** Shared Key Export

**OpenVPN Server**

Remote Access Server VPN-Usuários externos2 UDP4:1194

**Client Connection Behavior**

Host Name Resolution Interface IP Address

Verify Server CN Automatic - Use verify-x509-name (OpenVPN 2.3+) where possible

Optionally verify the server certificate Common Name (CN) when the client connects. Cu

2. No final da página, estarão os clientes que já foram cadastrados e seus respectivos arquivos .ovpn contendo seus certificados. Basta clicar sobre o que corresponde ao sistema operacional desejado e realizar a exportação

OpenVPN Clients		
User	Certificate Name	Export
cleber4	cleber4	<p>- Inline Configurations:</p> <p><a href="#">Most Clients</a> <a href="#">Android</a> <a href="#">OpenVPN Connect (iOS/Android)</a></p> <p>- Bundled Configurations:</p> <p><a href="#">Archive</a> <a href="#">Config File Only</a></p> <p>- Current Windows Installer (2.4.8-lx02):</p> <p><a href="#">7/8/8.1/2012r2</a> <a href="#">10/2016/2019</a></p> <p>- Old Windows Installers (2.3.18-lx02):</p> <p><a href="#">x86-xp</a> <a href="#">x64-xp</a> <a href="#">x86-win6</a> <a href="#">x64-win6</a></p> <p>- Viscosity (Mac OS X and Windows):</p> <p><a href="#">Viscosity Bundle</a> <a href="#">Viscosity Inline Config</a></p>