FICHA TRABALHO 4
PARTE 2

MODALIDADE:	Aprendizagem +	Não aplicável	
CURSO:	Técnico/a de Cibersegurança		
UC:	Gerir sistemas de deteção de intrusos (IDS)	CÓDIGO UC:	UC01486
FORMADOR/A:	Bruno Silva	DATA:	

OBJETIVOS

- Instalar, configurar e explorar a firewall PfSense

Conexões VPN com Pfsense

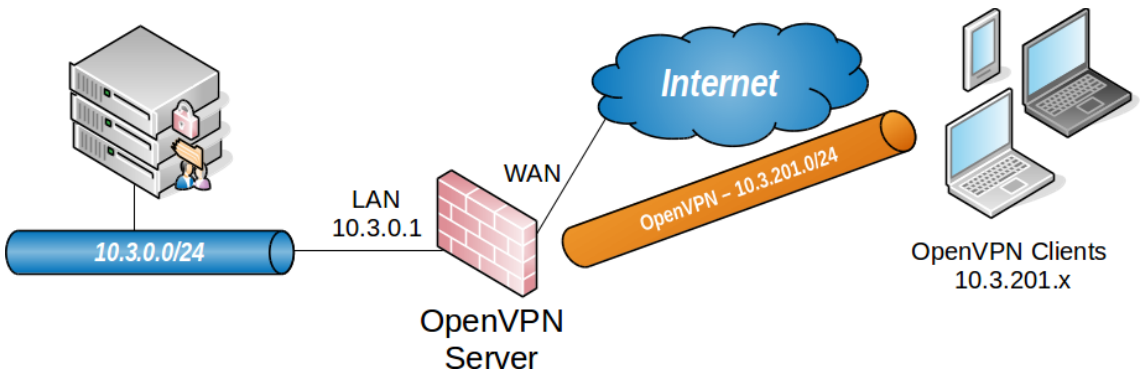
À medida que as empresas/organizações crescem e a tecnologia evolui, a mobilidade e os métodos de trabalho ultrapassam naturalmente a presença dos colaboradores nos escritórios. Ao aumentar a capacidade de conectividade, as organizações precisam de olhar com mais atenção para as ameaças que podem ser geradas como consequência desta realidade.

Quando o assunto é a interligação envolvendo diferentes localizações, a VPN é um tema fortemente abordado e amplamente difundido no mercado.

A VPN (Virtual Private Network), permite o tráfego de dados de forma privada, em redes públicas ou partilhadas (geralmente inseguras), utilizando recursos e encriptação para garantir uma maior segurança.

Para o funcionamento da VPN na firewall do PFsense existem dois requisitos básicos: um gateway VPN e um cliente VPN.

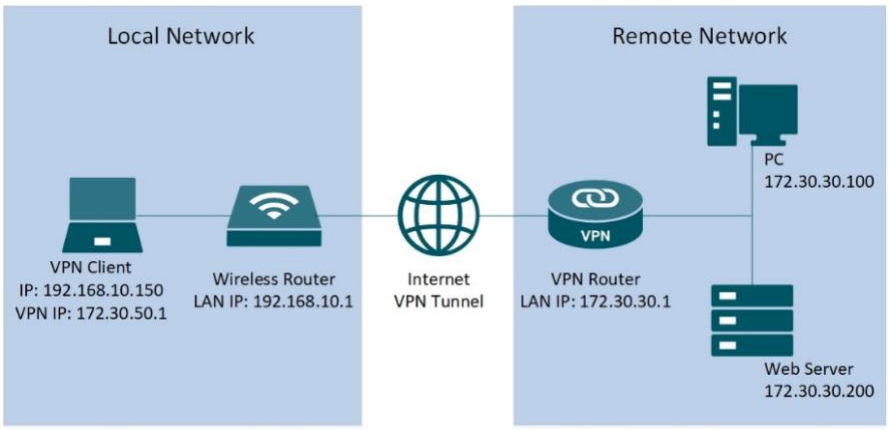
Dentro de um contexto de infraestrutura VPN, o VPN Gateway é um ativo que permite e mantém o acesso ao outro endpoint, tanto no conceito Client-to-Site como no conceito Site-to-Site.



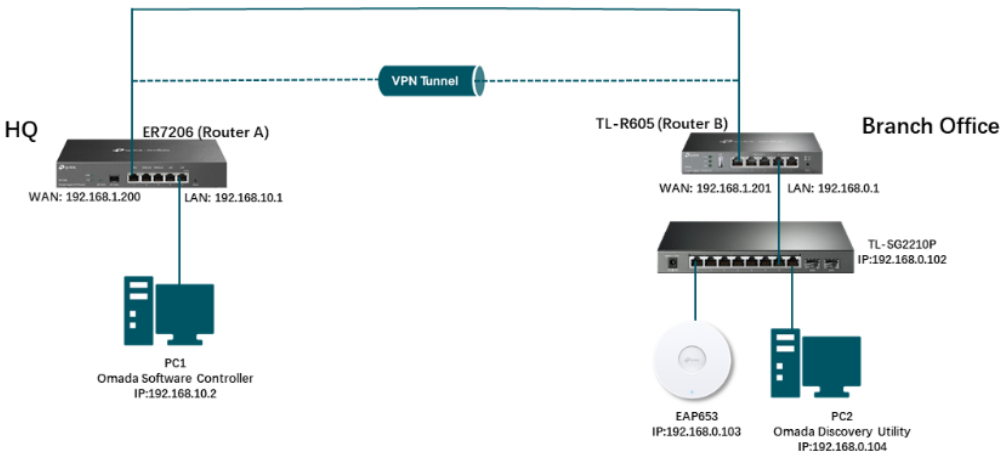
Tipos de conexão VPN

Do ponto de vista da topologia, existem 2 categorias de conexões VPN:

- Client-to-Site (ou Acesso Remoto): é caracterizada por conexões remotas entre utilizadores para a firewall de uma empresa/organização, ou seja, permite estabelecer uma ligação, construindo um túnel seguro para passar os dados de forma mais segura e aceder a recursos dentro da empresa. Numa linguagem simplificada, é uma estrutura "cliente-servidor" (VPN Gateway é o servidor e VPN Client é o cliente);



- Site-to-Site (ou Gateway para Gateway): pode ser aplicado à estrutura de comunicação segura com recurso a VPN que necessitam de interligar unidades de negócio (sedes e filiais), com vários utilizadores em locais diferentes, não existindo um tipo de ligação direta;



Parte 0 – Preparação das máquinas virtuais

Passo 1 – Vamos preparar duas novas máquinas virtuais Pfsense com os seguintes dados:

Máquina Virtual 1 – Máquina Sede

- Nome Máquina: Pfsense_sede
- Memória RAM: 1.5GB
- Espaço disco rígido: 5 GB
- Adaptadores de rede:
  - Adaptador 1: Bridge Adaptor
  - Adaptador 2: Rede Interna (Internal Network)
    - Nome: intnet
    - Modo Promíscuo: Permitir tudo

Na pós-instalação da firewall (no ambiente gráfico), corra a configuração inicial e vamos fazer os seguintes passos:

Passo 2

- **Hostname** colocar o nome : Pfsense_sede
- **Primary DNS Server**: 8.8.8.8
- **Secondary DNS Server**: 4.4.4.4
- **Override DNS**: Desmarcar a opção

Passo 3

- **Timezone**: coloque o fuso horário **Europe/Lisbon**

Passo 4

- **SelectedType**: DHCP
- **Block RFC1918 Private Networks**: Desmarcar a opção
- **Block bogon Networks:** Desmarcar a opção

Passo 5

- **LAN IP Address**: 192.168.20.1
- **Subnet Mask**: 24

Máquina Virtual 2 – Máquina Filial

- Nome Máquina: Pfsense_filial
- Memória RAM: 1.5GB

- Espaço disco rígido: 5 GB
- Adaptadores de rede:
  - Adaptador 1: Bridge Adaptor
  - Adaptador 2: Rede Interna (Internal Network)
    - Nome: intnet2
    - Modo Promíscuo: Permitir tudo

Na pós-instalação da firewall (no ambiente gráfico), corra a configuração inicial e vamos fazer os seguintes passos:

Passo 2

- Hostname colocar o nome : Pfsense_filial
- Primary DNS Server: 8.8.8.8
- Secondary DNS Server: 4.4.4.4
- Override DNS: Desmarcar a opção

Passo 3

- Timezone: coloque o fuso horário Europe/Lisbon

Passo 4

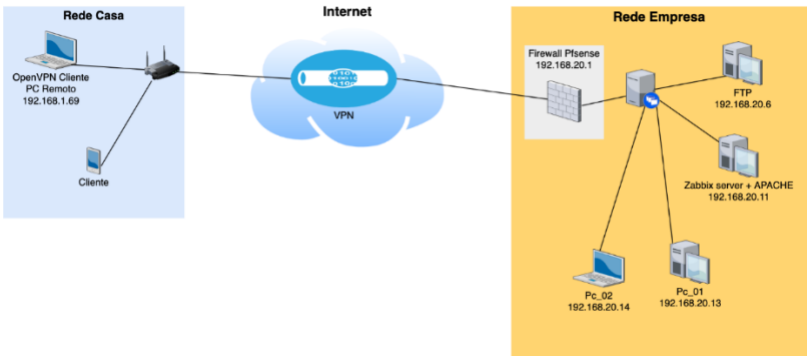
- SelectedType: DHCP
- Block RFC1918 Private Networks: Desmarcar a opção
- Block bogon Networks: Desmarcar a opção

Passo 5

- LAN IP Address: 192.1681.10.1
- Subnet Mask: 24

Parte 1 – Configuração Pfsense Client-to-Site

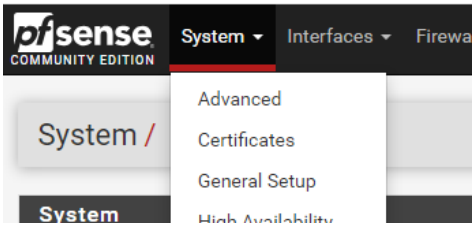
Vamos considerar o seguinte cenário:



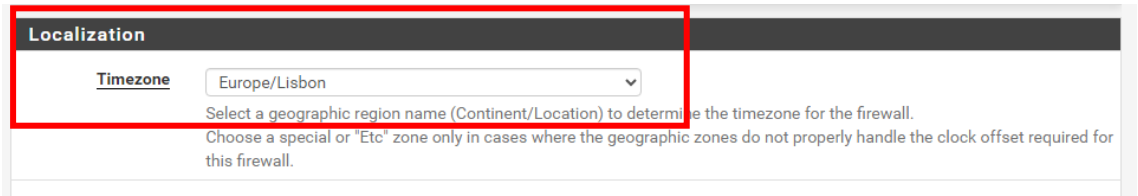
Neste exemplo vamos utilizar a máquina virtual da Pfsense_Sede

Passo 1 – Verificar o fuso horário. Devemos sempre colocar os mesmos fusos horários entre as firewalls, caso contrário, pode haver conflitos na sincronização das informações, erros de protocolos, entre outros problemas.

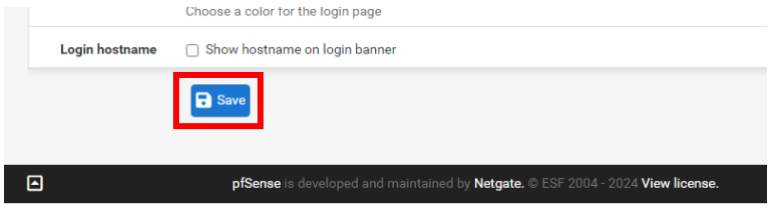
Caso precisa de alterar o fuso horário, deve dirigir até ao menu **System → General Setup**:



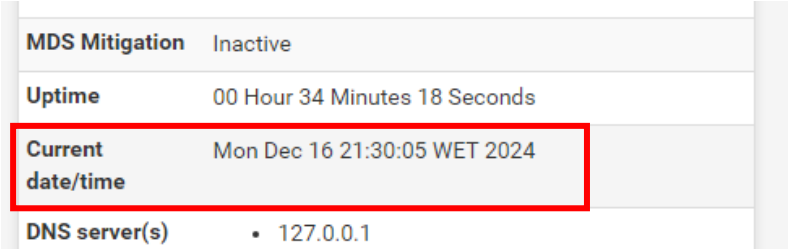
No separador **Localization** temos o campo **Timezone**. Para este caso, coloque o fuso horário **Europe/Lisbon**:



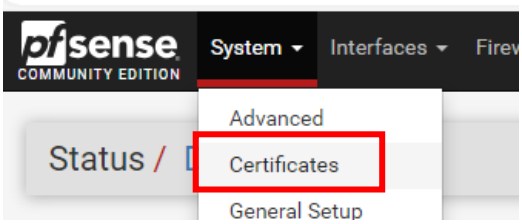
No final, deve gravar as novas alterações:



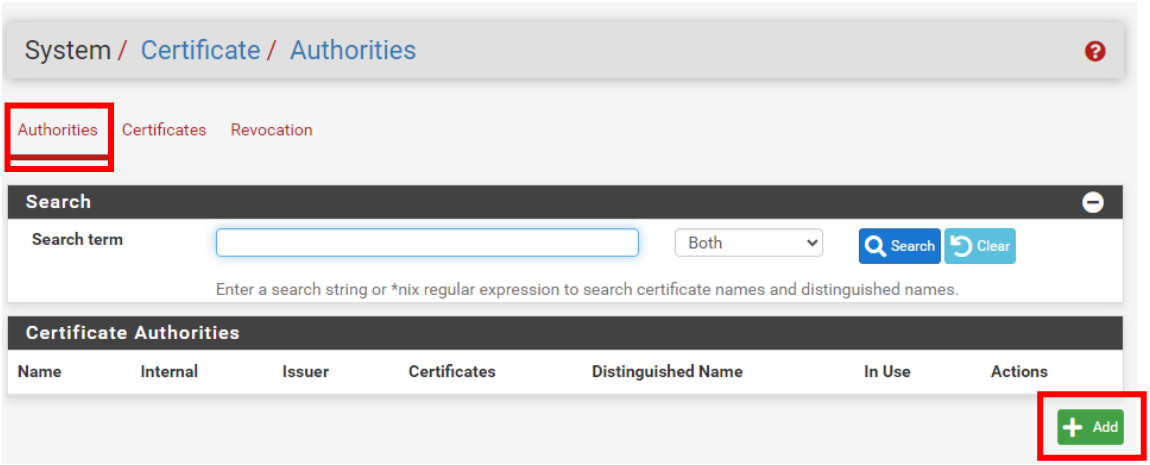
Passo 2 - Retorne a página principal da firewall e verifique se o fuso horário condiz com o relógio da máquina física:



Passo 3 – Em seguida, crie uma nova **Autoridade de Certificação** (menu **System → Certificates**):

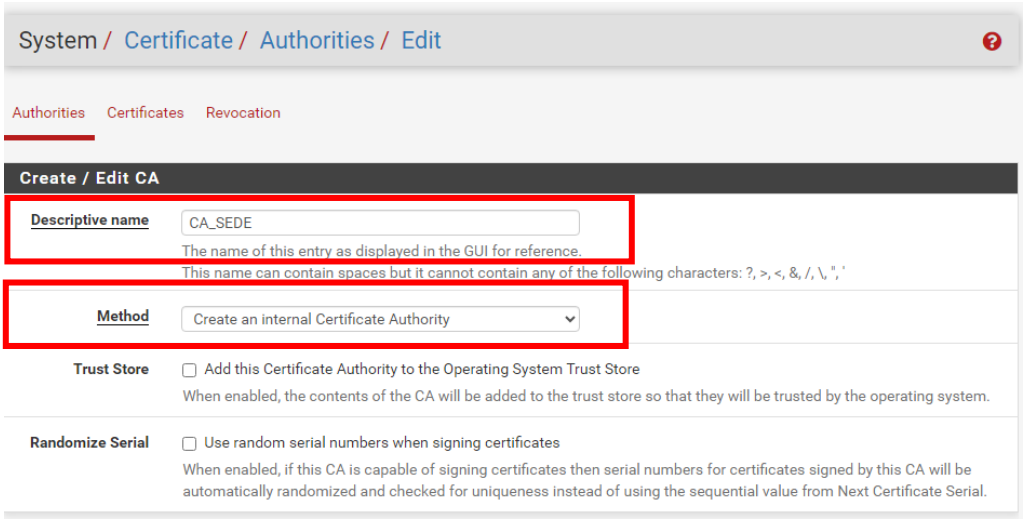


Dentro da página dos certificados (separador **Authorities**), clique no botão **New**:

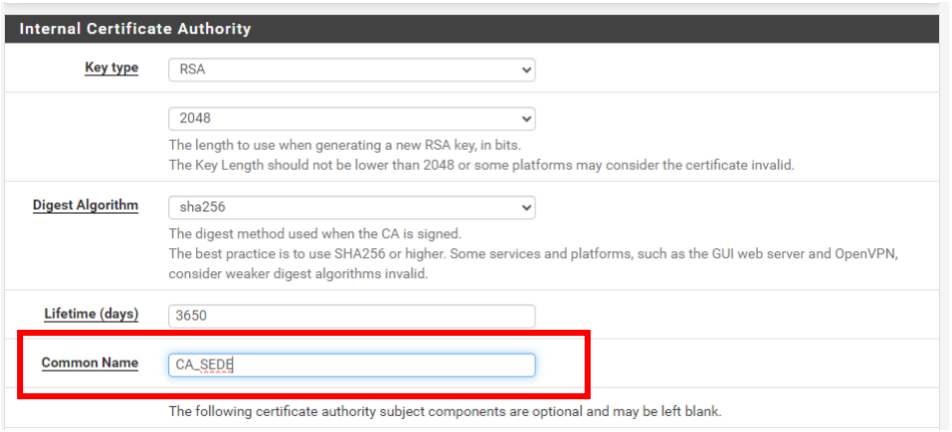


Passo 3.1 – O certificado que vamos gerar **é responsável por autenticar a identidade do servidor da VPN** e autenticar o certificado do utilizador. Como tal, vamos dar uma descrição e um nome comum para criar uma nova autoridade de certificação. Para este exemplo vamos considerar os seguintes campos:

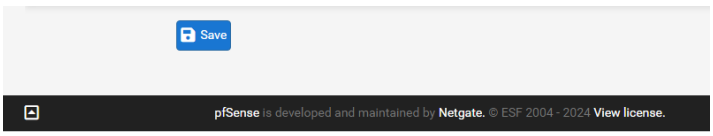
- **Descriptive Name:** CA_SEDE
- **Method:** Create an internal Certificate Authority



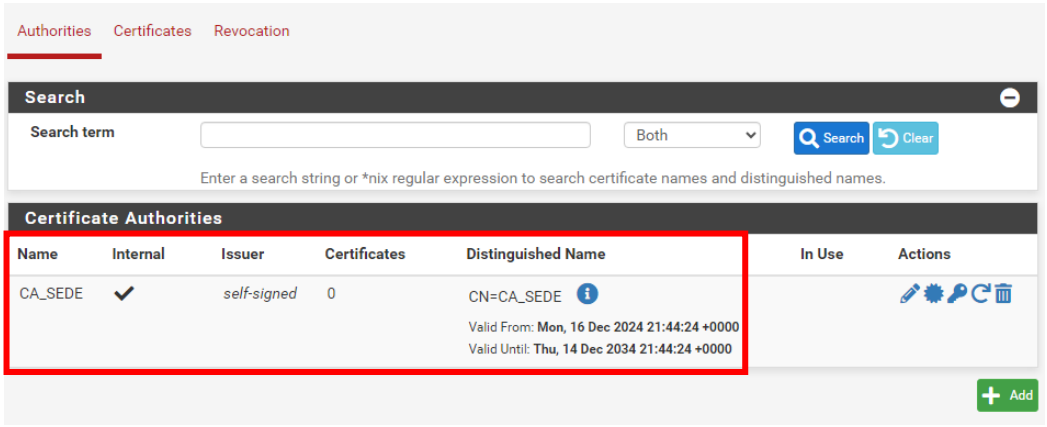
Passo 3.2 – Deixamos estar os valores por defeito e no campo Common Name, vamos dar o mesmo nome que na descrição "CA_SEDE":



Passo 3.3 – No final não esqueça de gravar as novas informações.

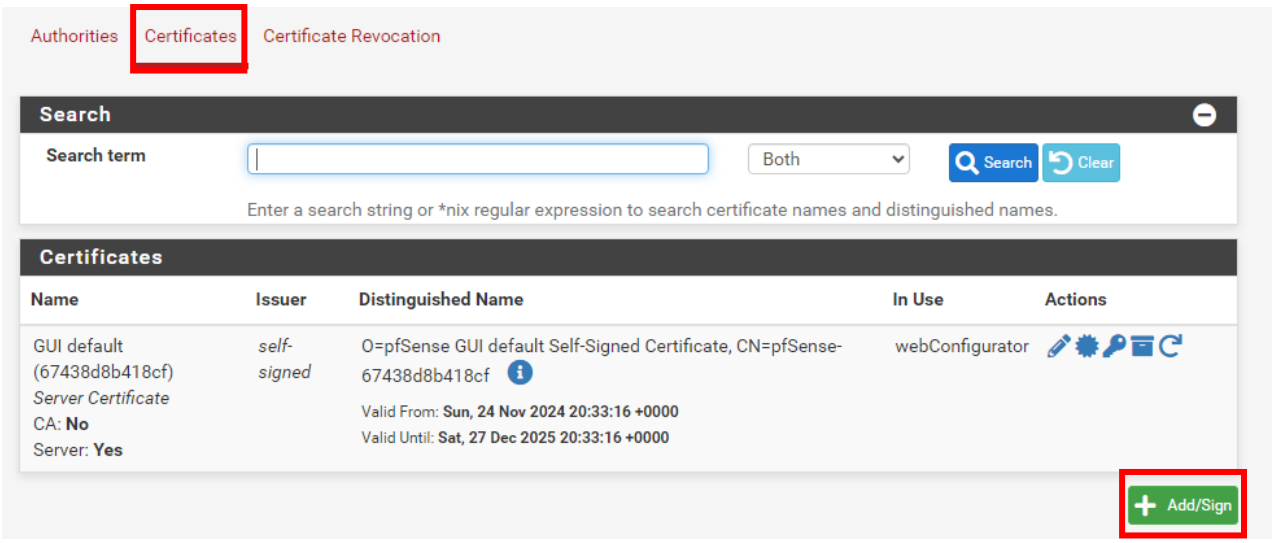


Resultado:



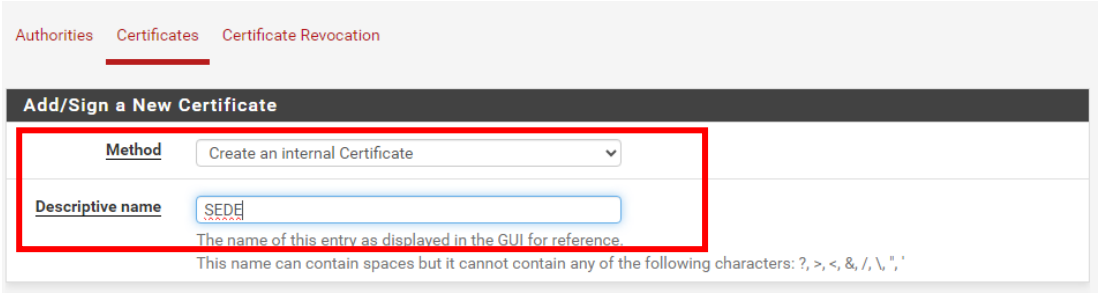
Parte 2 – Criação do certificado com base na Autoridade de certificadora

Passo 1 – Vamos criar um **certificado para a rede virtual privada** (VPN). Ainda no menu **System** → **Certificates** tem 3 separadores. Clique no separador do meio com o nome "**Certificates**" e de seguida no botão **Add/Sign**:



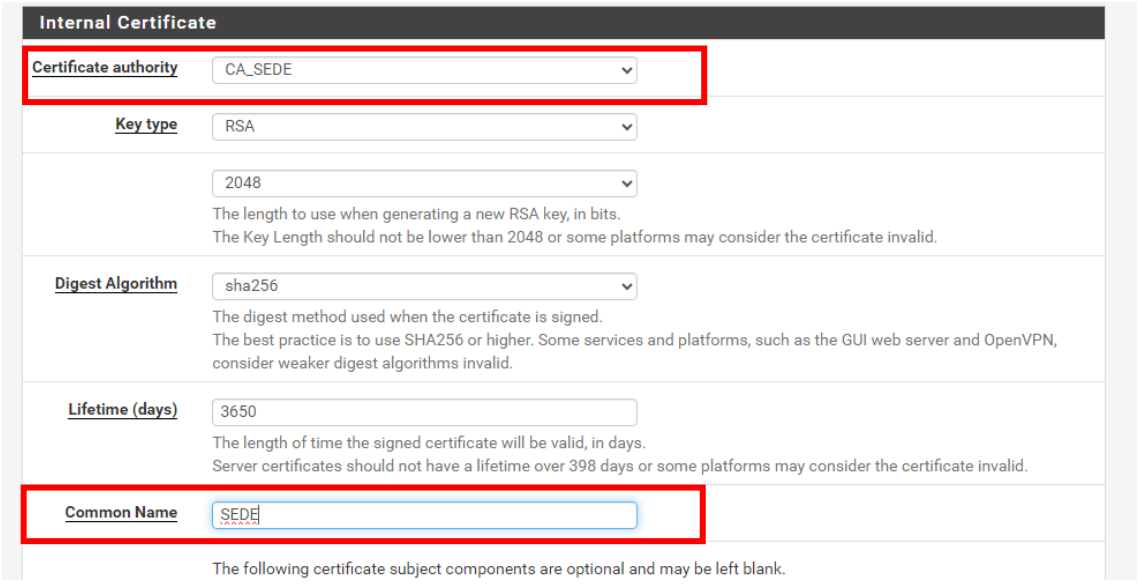
Passo 1.1 – Adicione uma descrição e um nome comum para criar um novo certificado para o servidor com os dados:

- **Method:** Create an internal Certificate Authority
- **Descriptive Name:** SEDE

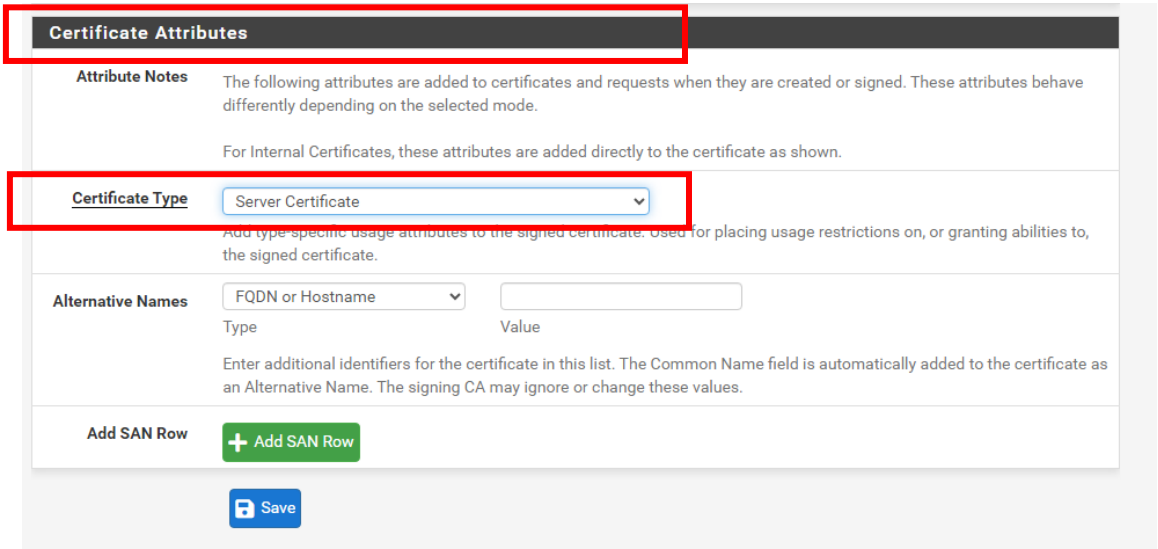


Passo 1.2 – Mais abaixo, no separador Internal Certificates, coloque os seguintes dados:

- **Certificate Authority:** CA_SEDE (a entidade certificadora que criou no passo 3);
- **Common Name:** SEDE (o mesmo nome do certificado);

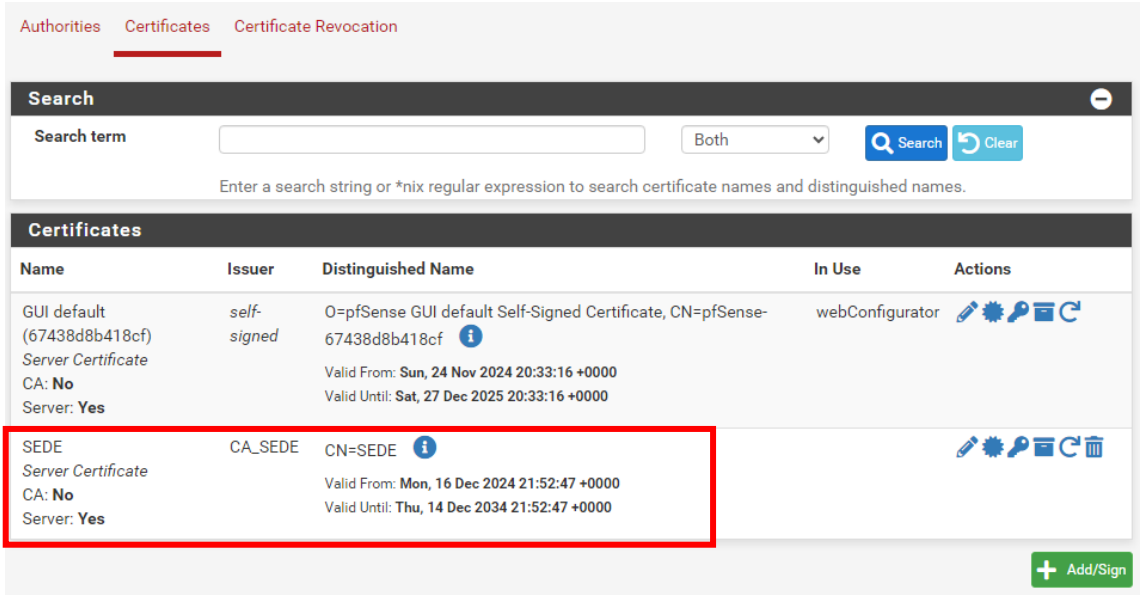


Passo 1.3 – Mais abaixo, mais especificamente, no separador "Certificate Attributes", vamos indicar que o **tipo de certificado** é para o **servidor** (que é diferente para os utilizadores da VPN). No campo **Certification Type** selecione o valor **Server Certificate** e grave as novas alterações:



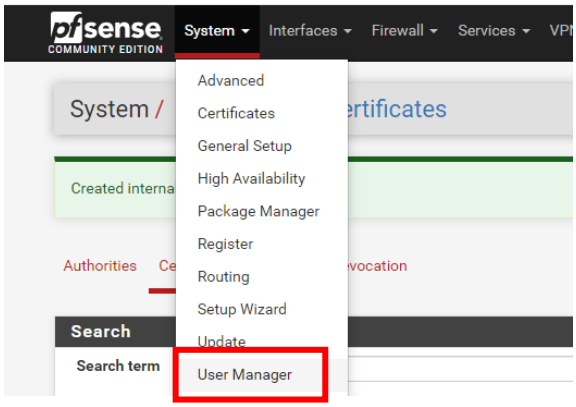
Passo 1.4 – No final não esqueça de gravar as novas alterações!

Resultado da geração:

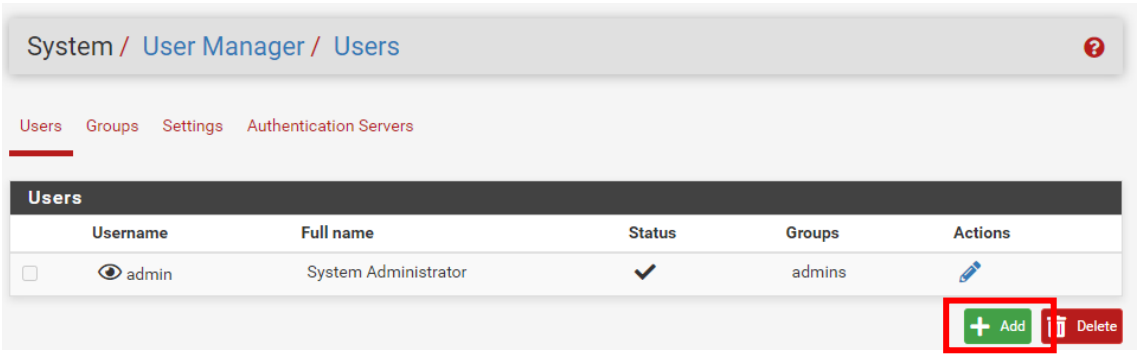


Parte 3 – Criar utilizador para usar na VPN + Certificado

Passo 1 – Vamos criar novo utilizador para a ligação da rede privada virtual e um certificado de acesso. Vamos ao menu **System → User Manager** e crie um novo utilizador:

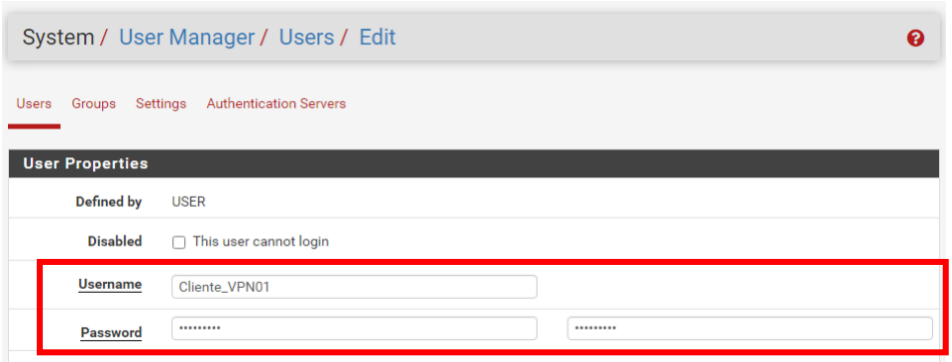


Passo 1.1 – Clique no botão para adicionar novo utilizador:



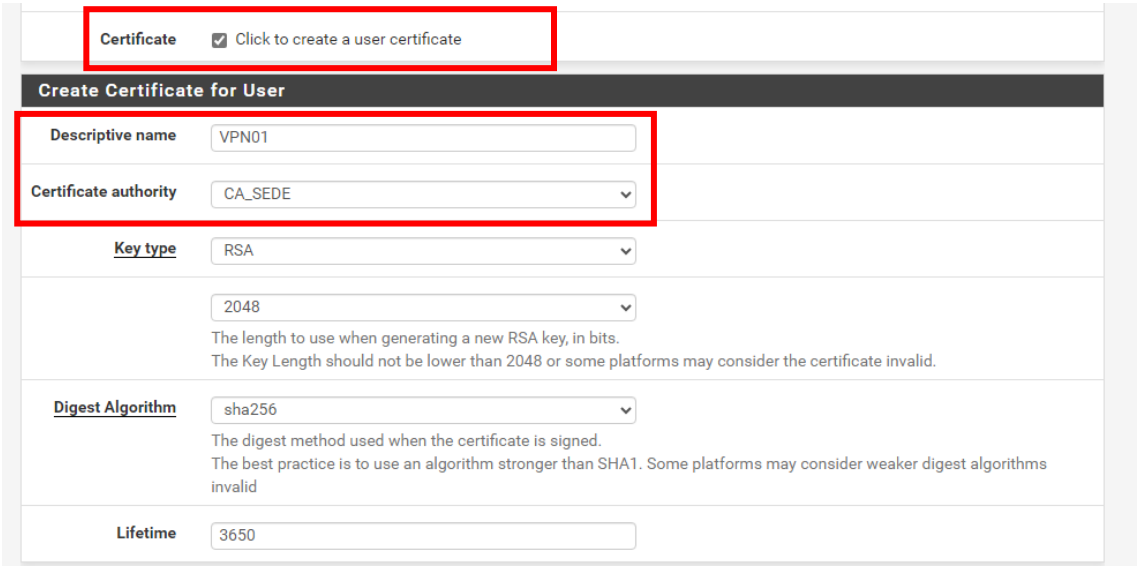
Passo 1.2 – Coloque as informações:

- **Username**: Cliente_VPN01
- **Password:** Teste123!

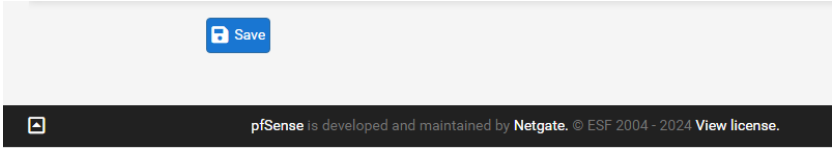


Passo 1.3 – Mais abaixo, deve selecionar a opção de gerar certificado para o novo utilizador (campo **Certificate**). Ao selecionar a nova opção, será exibida a nova seção com as informações do certificado que vai gerar. Dentro da nova seção, coloque as informações:

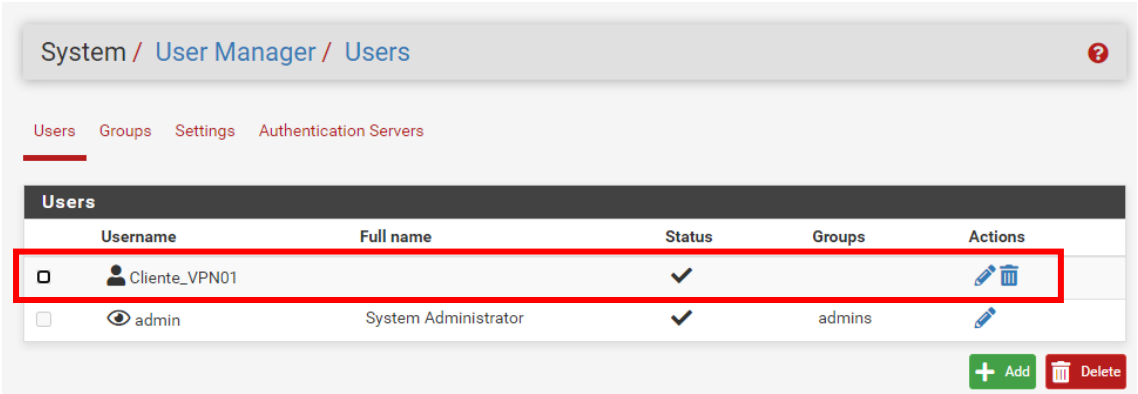
- **Certificate**: gerar novo certificado para o utilizador que está a criar;
- **Descriptive Name:** VPN01
- **Certificate Authority**: apenas terá disponível CA_SEDE (que foi o certificado de autoridade que criou anteriormente. Se tiver mais criados, serão exibidos mais abaixo):



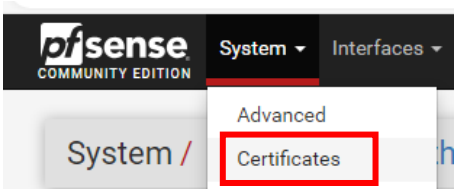
Passo 1.4 – No final não esqueça de gravar as novas alterações:



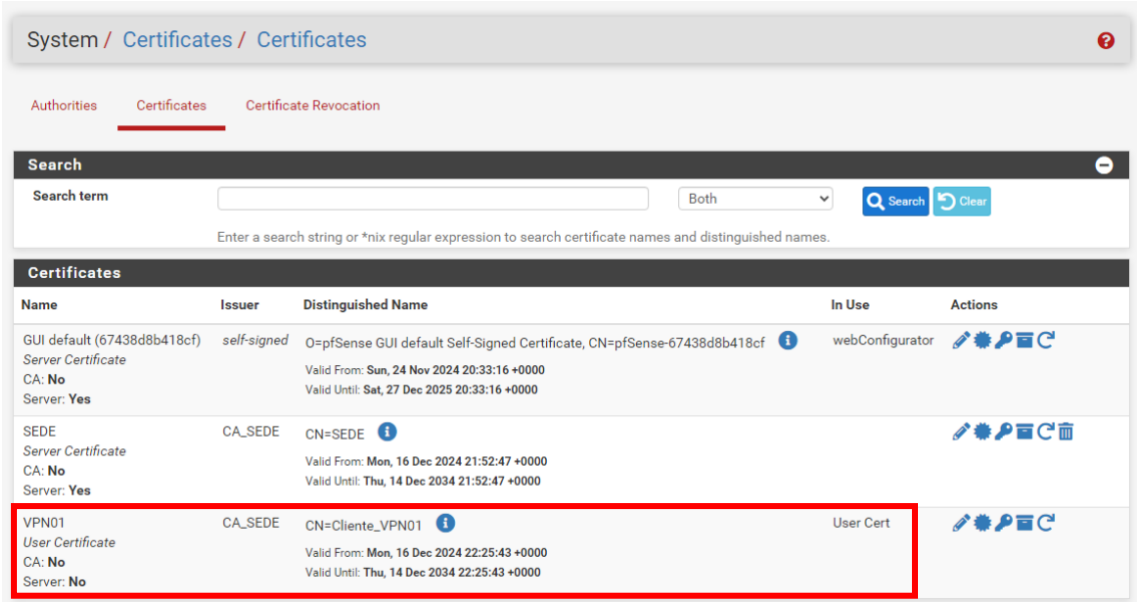
Resultado: (neste caso apenas criou um único utilizador, mas pode criar mais)



Passo 1.5 – No final, retorne ao menu **System → Certificates**, e no separador "**Certificates**" e verifique se o novo certificado para o utilizador foi anexado (para além daquele que criou para o servidor):



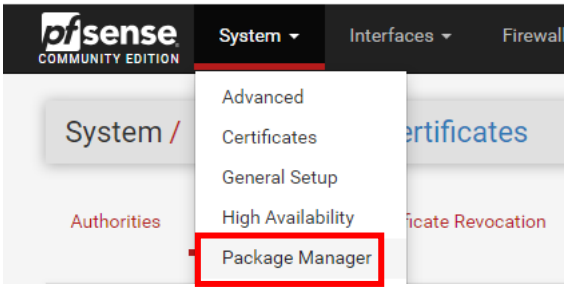
Verificar a criação do novo certificado (quando clicou na opção Certificate):

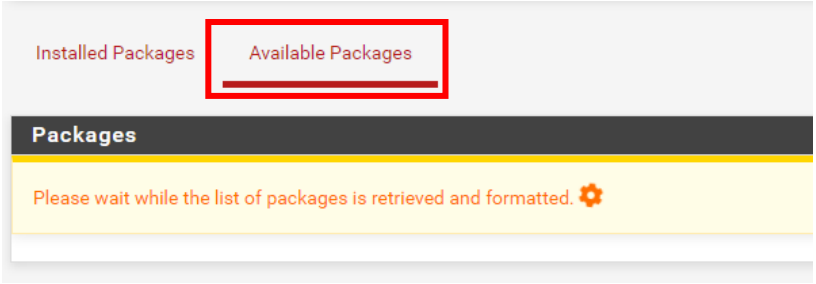


Parte 4 – Instalação do pacote OpenVPN-Client-Export (para exportar o ficheiro de configuração com a ligação VPN)

Neste momento já temos os certificados gerados, mas ainda falta ter a ferramenta para exportar os ficheiros de configuração para passar aos utilizadores. Na firewall do Pfsense, temos um pacote que permite fazer configuração passo-a-passo dessa configuração e exportar os dados mais rapidamente.

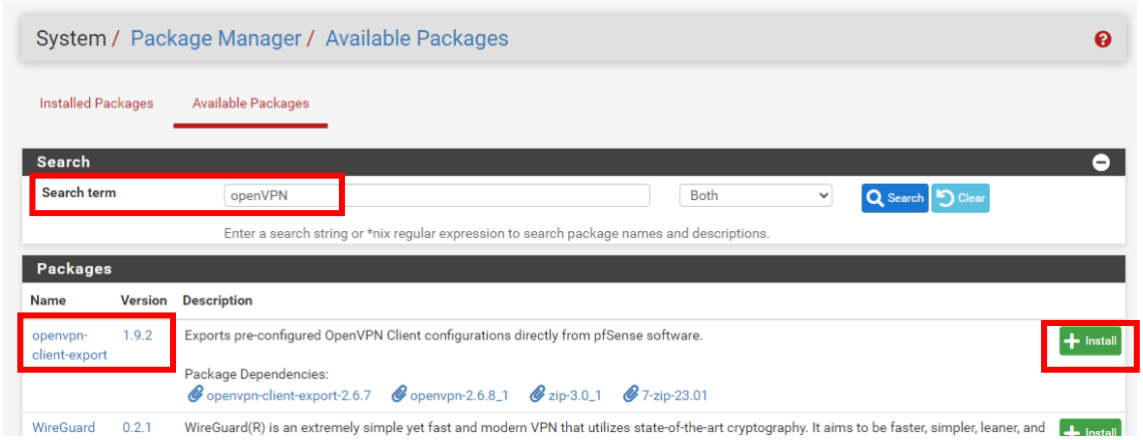
Passo 1 - Vamos ao menu **System → Packet Manager** e selecione o separador **Available Packages** (este processo pode demorar um pouco a fazer a sincronização dos pacotes na Internet):



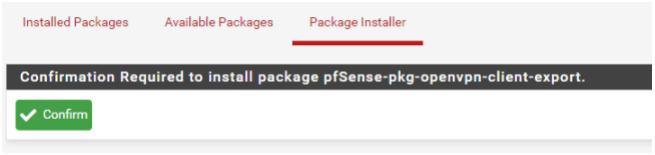


Passo 2 - Depois de sincronizar, aparece várias informações. Como tal, queremos instalar o pacote OpenVPN que já traz os processos de configuração e exportação de dados (para importar no cliente, em vez de configurar tudo manualmente).

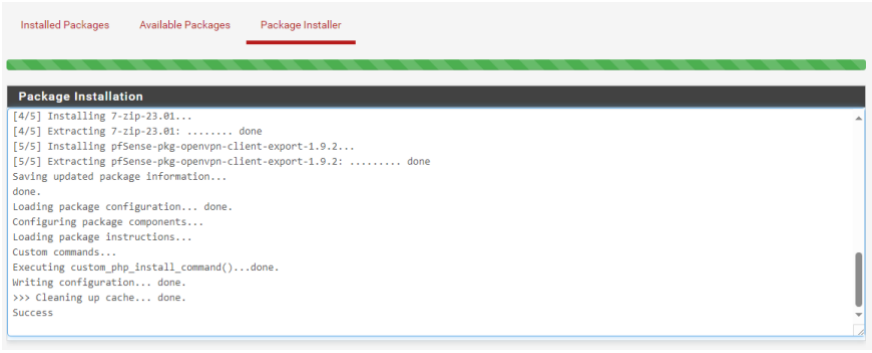
Procure pela expressão "OpenVPN" e de seguida instale a opção "openvpn-client-export":



Passo 3 - Faça a instalação do pacote, clicando no botão verde Install/Confirm e confirme a operação:

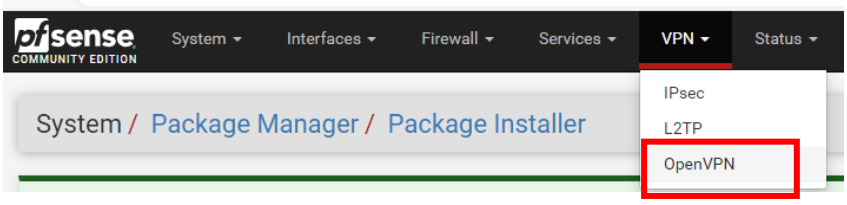


Este por sua vez, aparece uma consola a mostrar o progresso da obtenção e instalação do software (espere até que apareça a informação de sucesso):

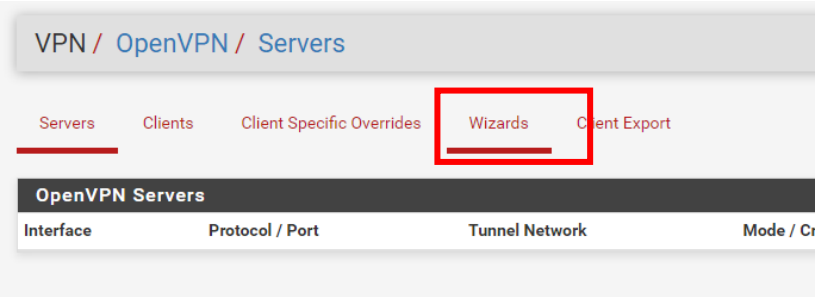


NOTA IMPORTANTE: cada cliente possui um ficheiro de configuração separado para importar. Deve personalizar a exportação da informação por cada utilizador!!!!

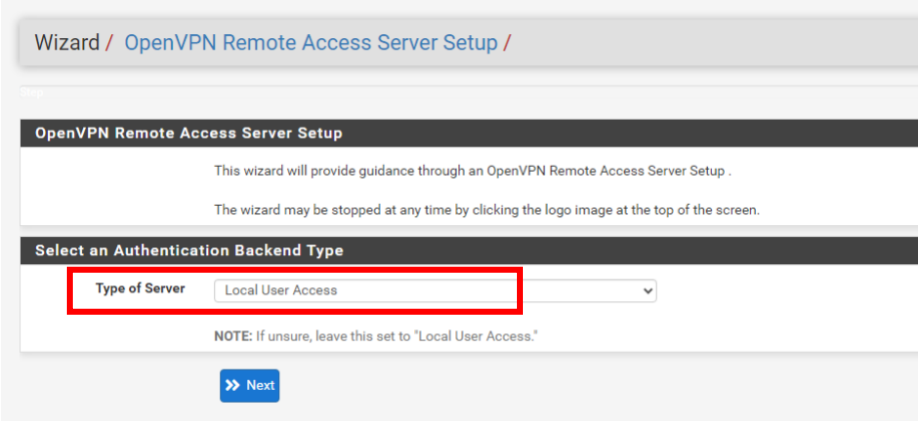
Passo 4 - De seguida, vamos ao menu **VPN → OpenVPN**:



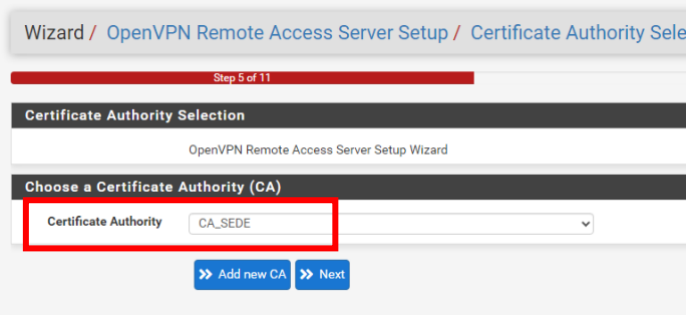
Passo 5 - Clique no separador **Wizard** (assistente de configuração/exportação de informação) e vamos configurar a rede virtual para acesso remoto a um utilizador:



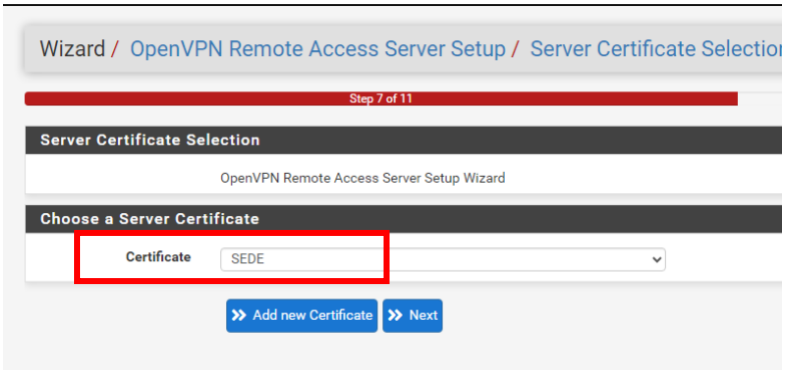
Passo 6 - Este vai abrir a página do assistente de configuração e na seção "Select an Authentication Backend Type", selecione a opção "Local User Access":



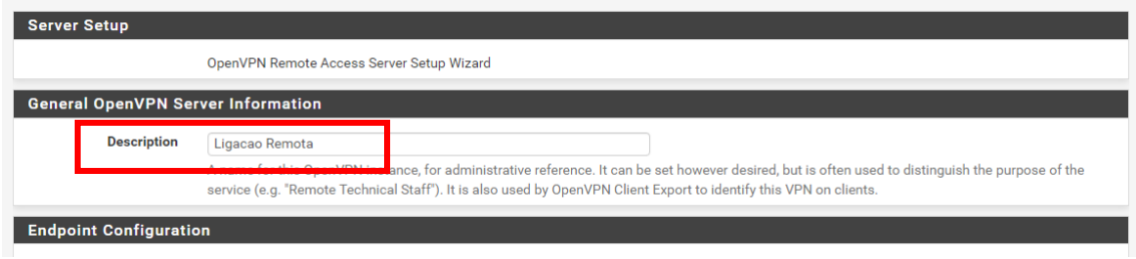
Passo 7 - Selecione o certificado de autoridade (que criou anteriormente, neste caso CA_SEDE):



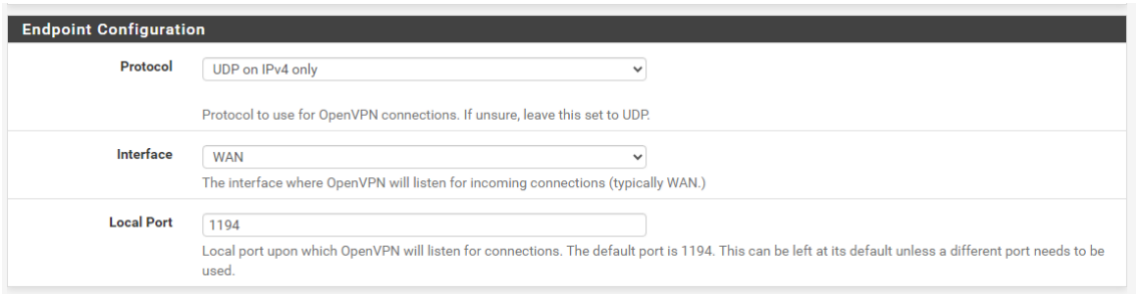
Passo 8 - Selecione o certificado que criou para o servidor (como criado anteriormente com o nome SEDE) e clique em NEXT (seguinte):



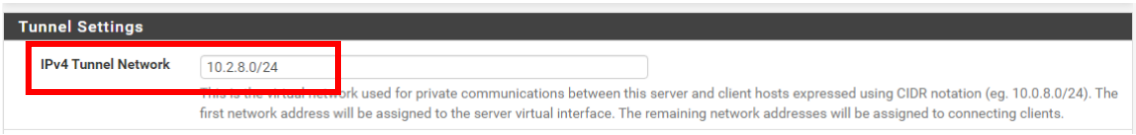
Passo 9 - Adicione uma descrição para o túnel da ligação VPN (como por exemplo "Ligacao remota", sem acentos):



Passo 10 - Na seção "Endpoint Configuration", devemos deixar as opções predefinidas:

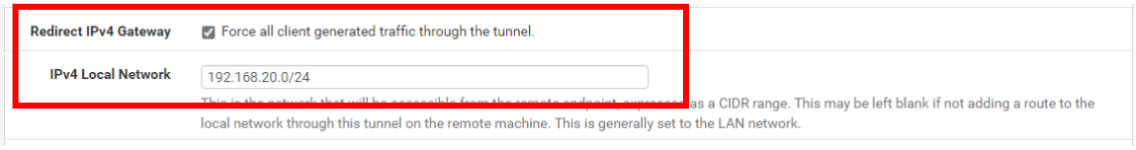


Passo 11 - Em seguida, vamos até a seção "Tunnel Settings", para configurar o endereço IP para a ligação do túnel VPN. Configure uma nova sub-rede para alocar aos dispositivos no túnel. Note que vamos utilizar uma sub-rede não utilizada somente para o túnel VPN entre as duas entidades (neste caso, vamos considerar o domínio 10.2.8.0/24)

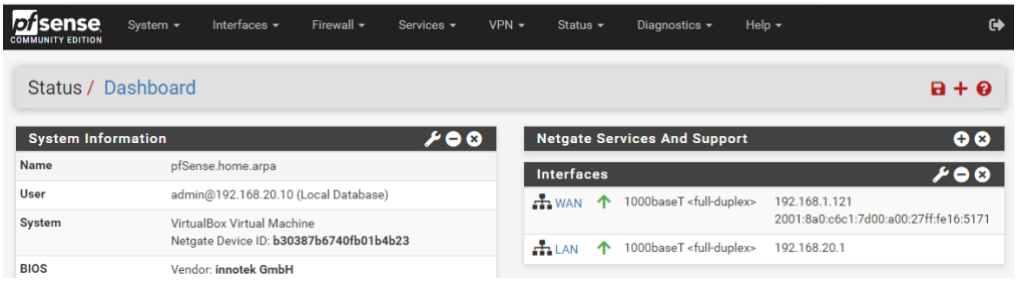


Passo 12 – Vamos permitir que os dispositivos acedam a rede local remotamente, por isso, vamos ter de adicionar uma nova rota:

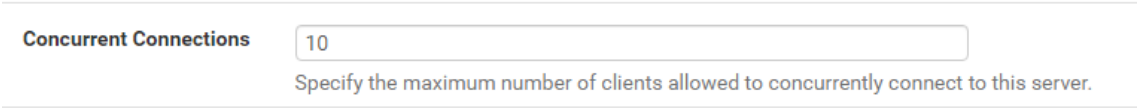
MUITA ATENÇÃO: Neste caso, a rede LAN foi configurada com o domínio 192.168.20.0/24. Como tal, vamos ter de meter o mesmo domínio na caixa do IPv4 Local Network, caso contrário, não vai saber como interligar as redes!!!!



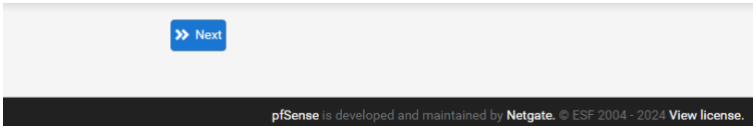
Nota Importante: se não sabe o domínio da LAN, abra a página inicial da firewall Pfsense e verifique o domínio da LAN.



Passo 13 - Especifique o número máximo de clientes com permissão para conectar simultaneamente a este servidor (neste caso vamos considerar que podem ser 10):

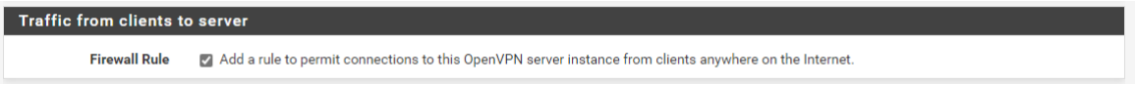


Passo 14 - No fundo da página clique na opção Next (seguinte)

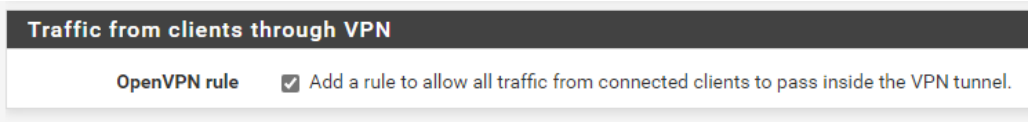


Passo 15 – Vamos pedir para adicionar as regras na firewall de forma automática:

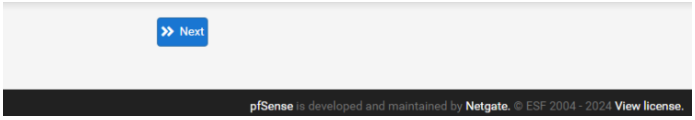
- Adicione uma regra para permitir conexões a esta instância do servidor OpenVPN de clientes em qualquer lugar da Internet:



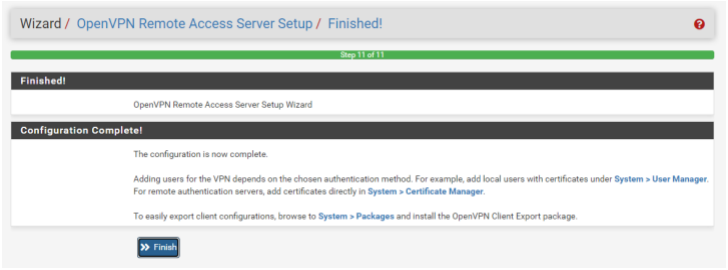
- Adicione uma regra para permitir que todo o tráfego dos clientes conectados passe dentro do túnel VPN:



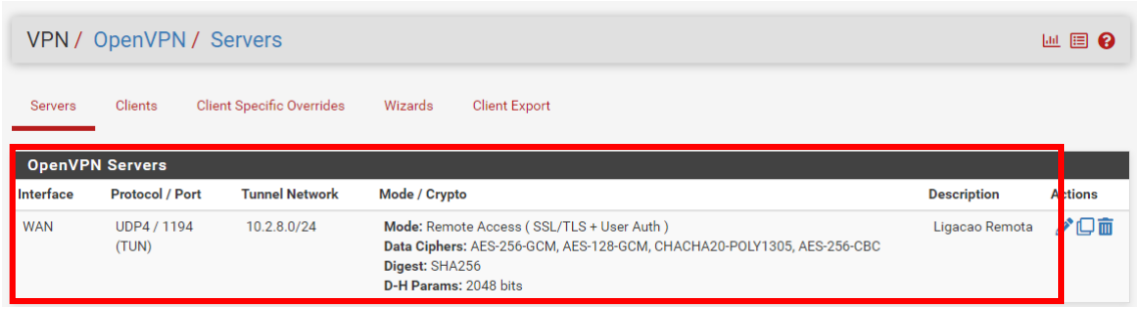
- No fundo da página clique na opção Next (seguinte):



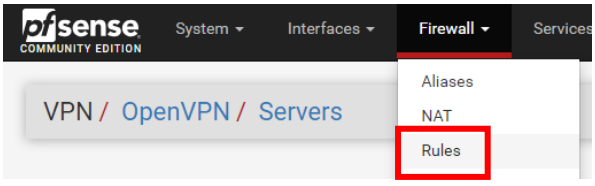
Passo 16 – Finalize o assistente:



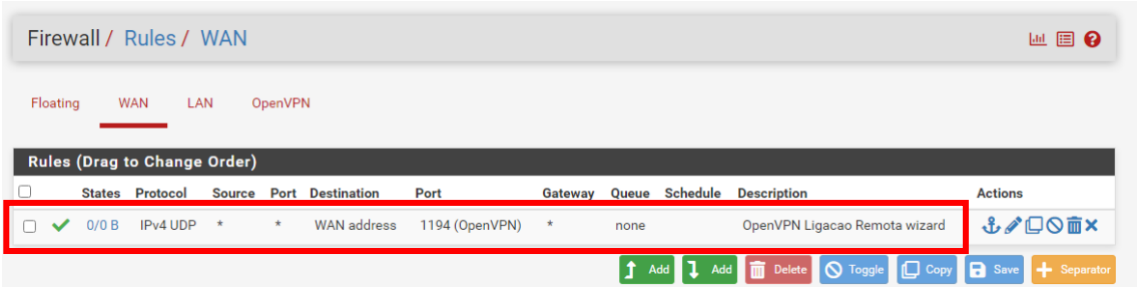
Resultado:



Passo 16 – Após esta personalização, vamos confirmar se o assistente de configuração colocou as regras na firewall. Como tal, deve aceder ao menu **Firewall → Rules** e ver se foi adicionada a regras IPv4 UDP na porta 1194 (openVPN):

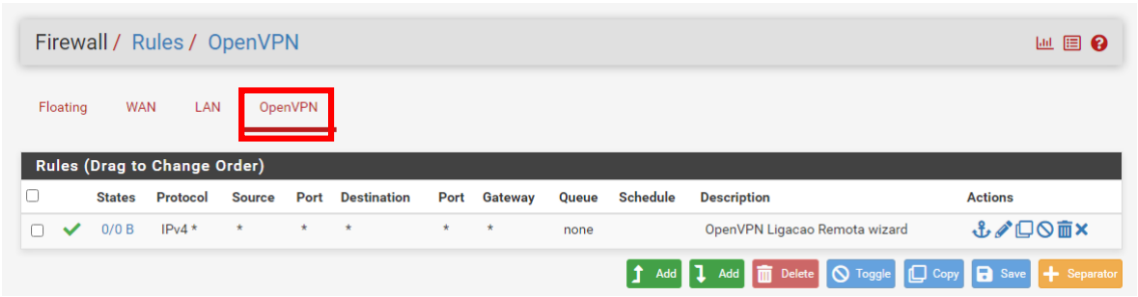


Passo 16.1 – Clique no separador WAN (se é que já não abra por defeito no mesmo) e verifique a inclusão da nova regra:



Repare que as regras foram adicionadas a firewall para permitir que os clientes estabeleçam ligações com o servidor!

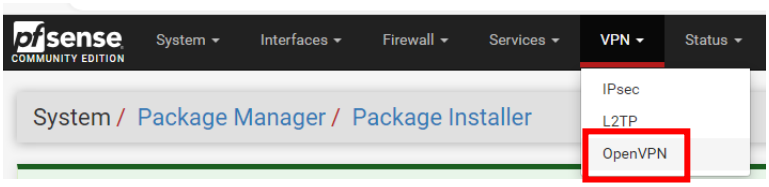
Passo 16.2 – Clique no separador OpenVPN e verifique se aparece a configuração do processo do assistente:



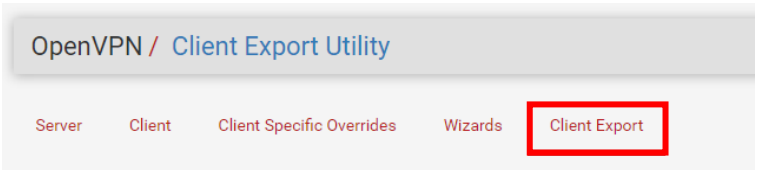
Parte 5 – Exportação da configuração para clientes

O cliente que precise de ligar ao servidor, necessita de um ficheiro de configuração com todos os dados que foram feitos até ao momento, ou seja, os certificados e a ligação do utilizador.

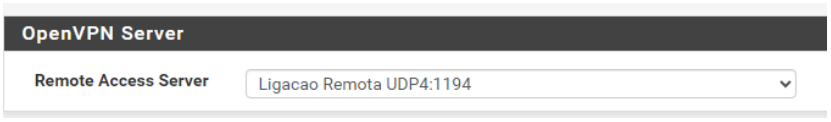
Passo 1 - vamos ao menu **VPN → OpenVPN**:



Passo 2 - Clique no separador "**Client Export**" e fazer os seguintes passos:



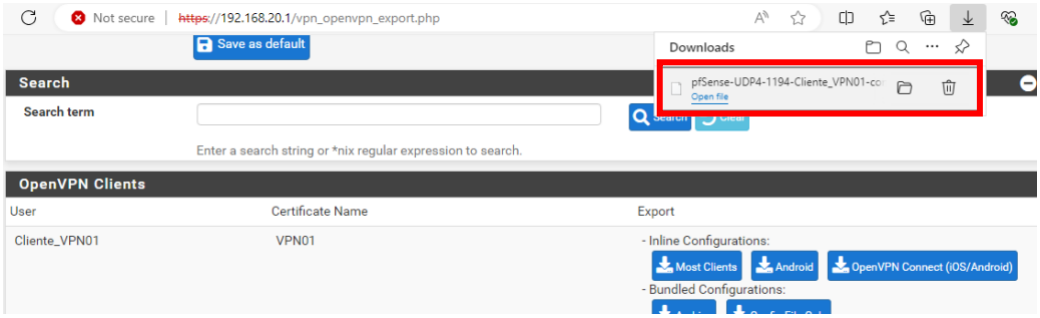
- **Passo 2.1 - Separador OpenVPN Server**: selecione a opção Ligacao Remota (ligação do túnel que foi criada anteriormente):



- **Passo 2.2 -** Vamos mais para o fundo da página e vai ter a seção para descarregar os ficheiros de configuração para as mais diferentes plataformas. Selecione o botão **Most Clientes** na zona "**Inline Configurations**:



Este por sua vez descarregou o ficheiro com as informações:

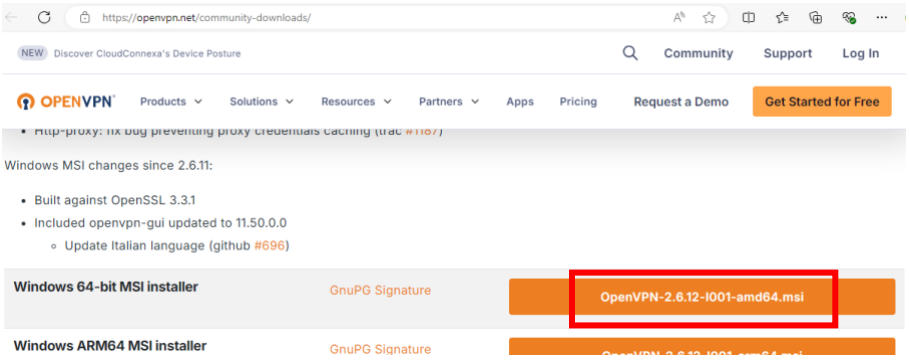


Parte 6 – Instalar software e configurações no Cliente

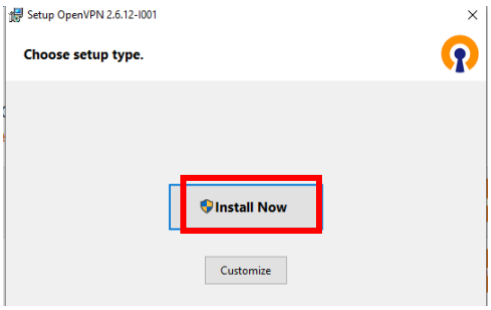
No fundo da página do menu **VPN → OpenVPN**, mais especificamente, no separador **Client Export**, temos as hiperligações para descarregar o software cliente para ligar a nossa VPN na firewall.

Também pode clicar na seguinte hiperligação para ir diretamente para a página do software: [Community Downloads - Open Source VPN | OpenVPN]

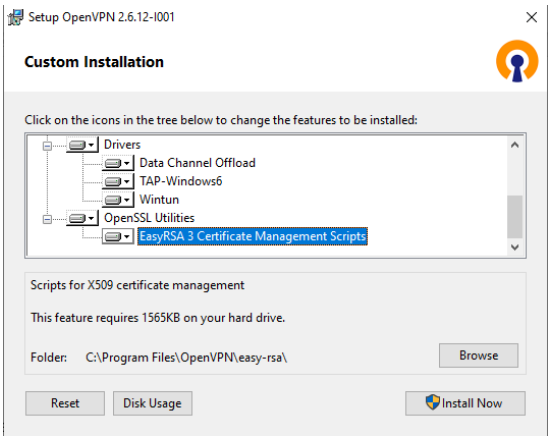
Passo 1 – Descarregue o ficheiro "**Windows 64-bit MSI installer**" (repare que tem mais opções de downloads) e faça a instalação no seu computador:



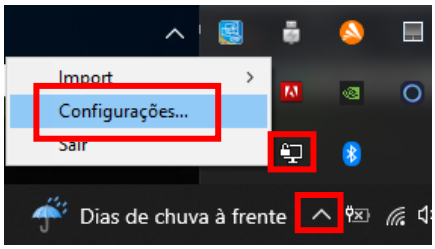
Passo 2 – Selecione instalação "Customize" para verificar se os pacotes estão todos selecionados:



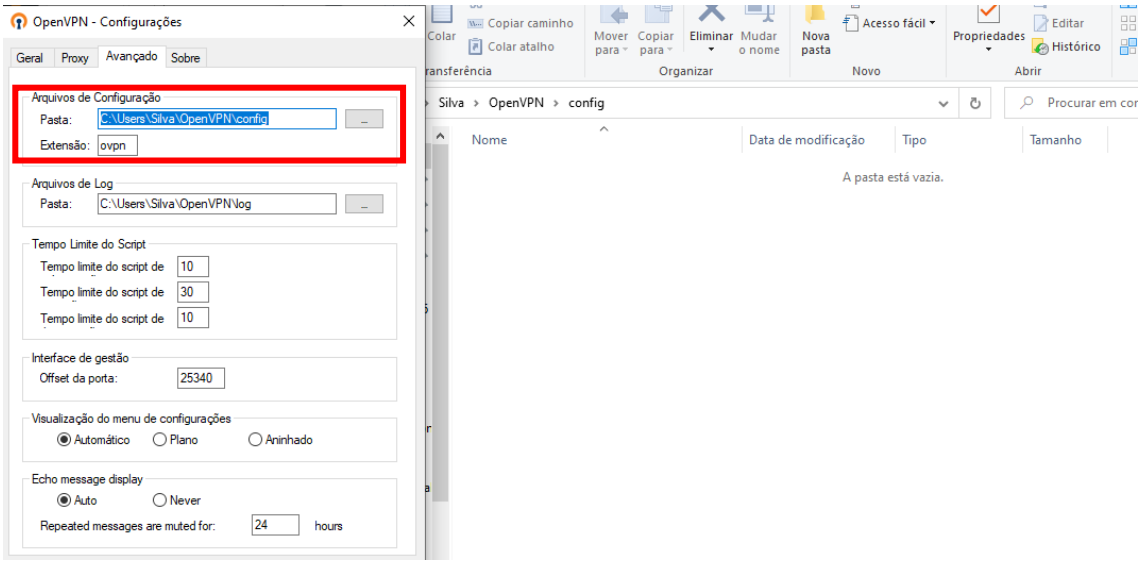
Passo 3 – Ative todas as funcionalidades e depois clique em instalar:



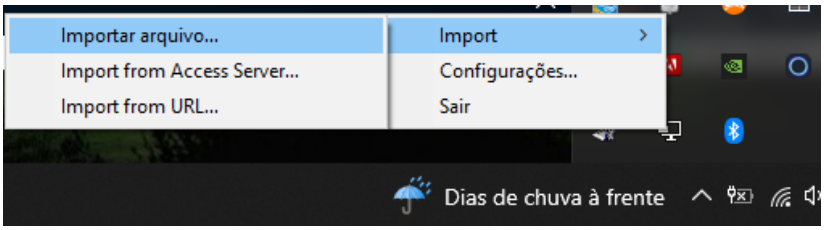
Passo 4 – Após a instalação, este fica a correr em segundo plano na barra do sistema. Clique no ícone da barra do sistema com o lado direito do rato e selecione a opção "Configurações". Verifique onde é que este vai importar os certificados:



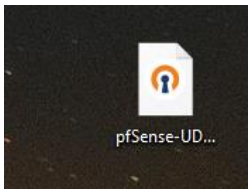
Passo 5 – Clique no ícone da barra do sistema com o lado direito do rato e selecione a opção "Configurações". Verifique onde é que este vai importar os certificados:



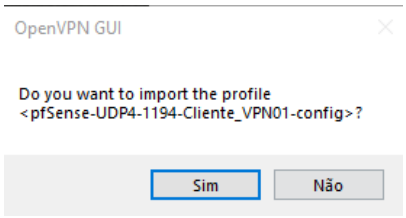
Passo 6 – Para a aplicação funcionar precisamos de importar o ficheiro de configuração que foi descarregado da Firewall Pfsense. Como tal, vamos clicar com o lado direito do rato em cima do ícone da barra de sistema e selecionar a opção "**Import → Importar arquivo**..." e indicar a localização do ficheiro

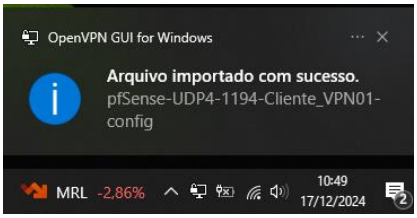


Ou numa forma mais rápida, clicar duas vezes em cima do ficheiro da configuração que descarregou (do qual vai fazer a importação automática):

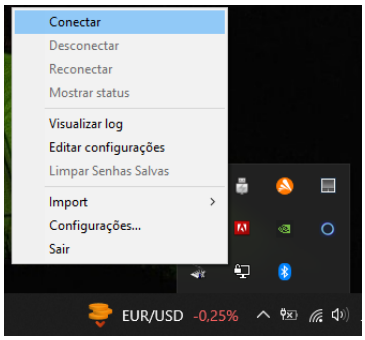


Passo 7 – Este vai perguntar se deseja mesmo importar o ficheiro de configuração. Aceite a confirmação e se tudo correr bem será exibida a mensagem da importação com sucesso:



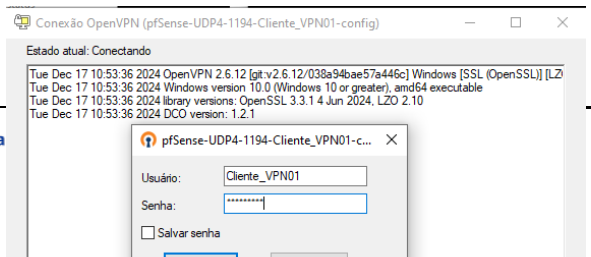


Passo 8 – Clique de novo no ícone da barra do sistema e clique na opção "**conectar**", pois neste momento só temos apenas um ficheiro importado (Se tiver mais, vai ter a possibilidade de clicar em qual ligação deseja ligar):



Passo 9 – Coloque as credenciais no programa (de acordo com o utilizador que criou anteriormente para a ligação VPN).

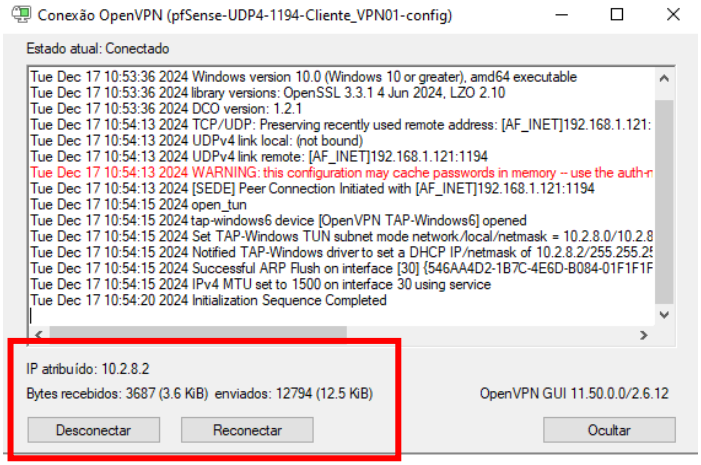
Neste caso foram os seguintes dados:



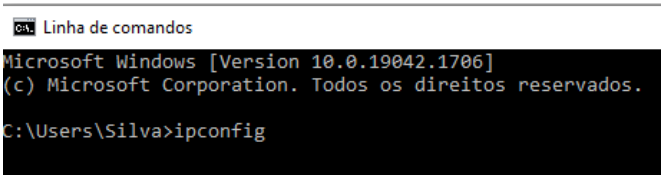
Utilizador: Cliente_VPN01

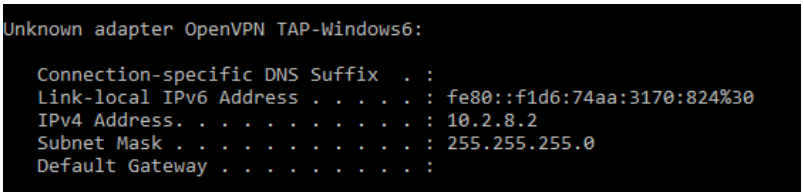
Password: Teste123!

Se tudo correr bem a consola irá mostrar o sucesso na ligação e passado 3 segundos a janela será ocultada (repare no endereço IP que foi atribuído e na circulação da informação de pacotes recebidos e enviados):



Passo 10 – Abra o terminal do sistema operativo e vamos ver qual o endereço IP atribuído:



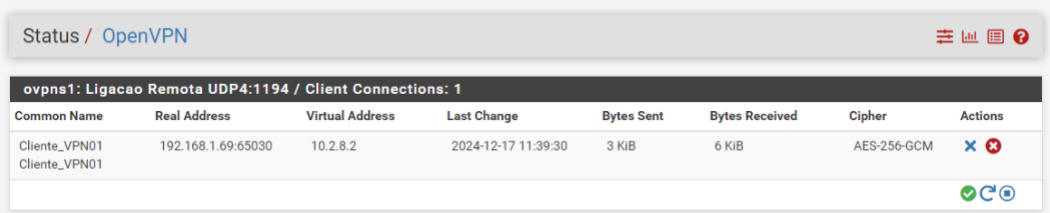


E verifiquem que a ligação wireless continua intacta:

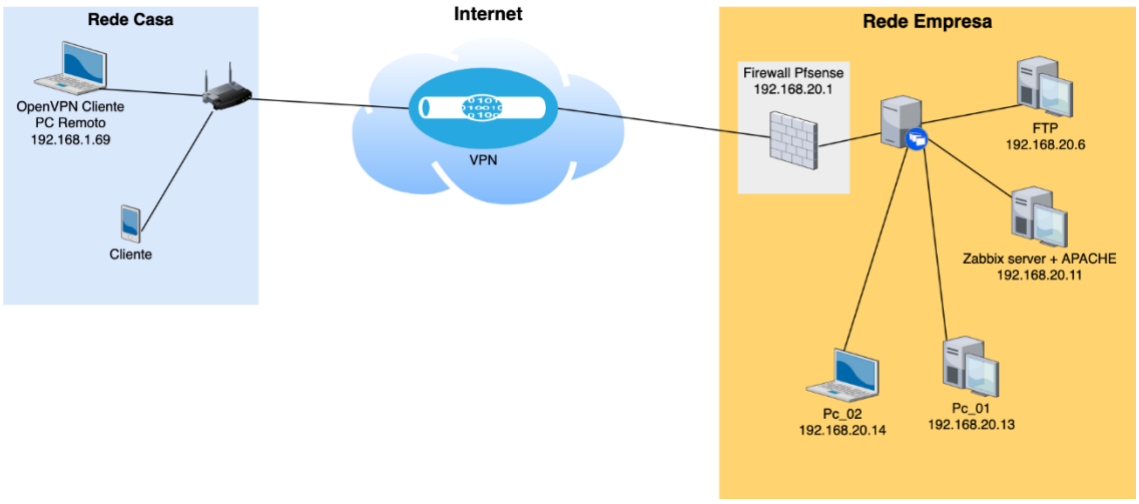
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : Home
   IPv6 Address. . . . . . . . . . . : 2001:8a0:c6c1:7d00:199b:b30b:dc65:5668
   Temporary IPv6 Address. . . . . . : 2001:8a0:c6c1:7d00:91c7:98bb:4cc5:7a7c
   Link-local IPv6 Address . . . . . : fe80::199b:b30b:dc65:5668%9
   IPv4 Address. . . . . . . . . . . : 192.168.1.69
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::206:91ff:fe57:bdef%9
                                       192.168.1.254
```

Na firewall do PFsense, veja a conexão realizada no menu Status → OpenVPN:

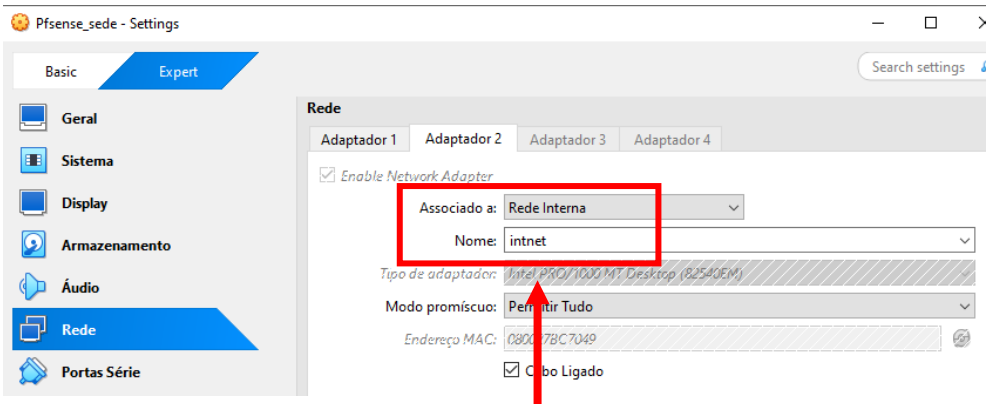


Passo 11 - Vamos a um teste final de ligação. Neste momento temos o seguinte diagrama de rede (para este exemplo):

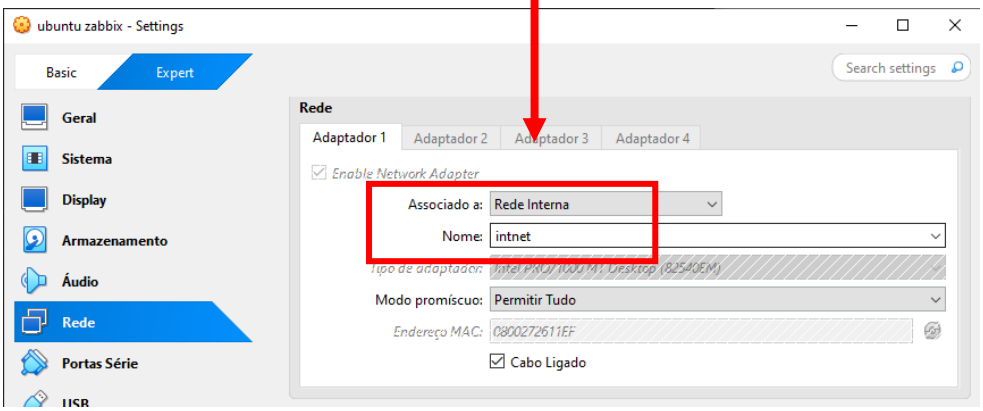


Foram alteradas as ligações de rede da máquina do Ubuntu (onde está instalado o software de monitorização de redes - Zabbix) de **Bridge Adaptor** para **Rede Interna** (com o mesmo **nome da placa de rede interna** da firewall):

Máquina Pfsense (adaptador 2 – rede interna)

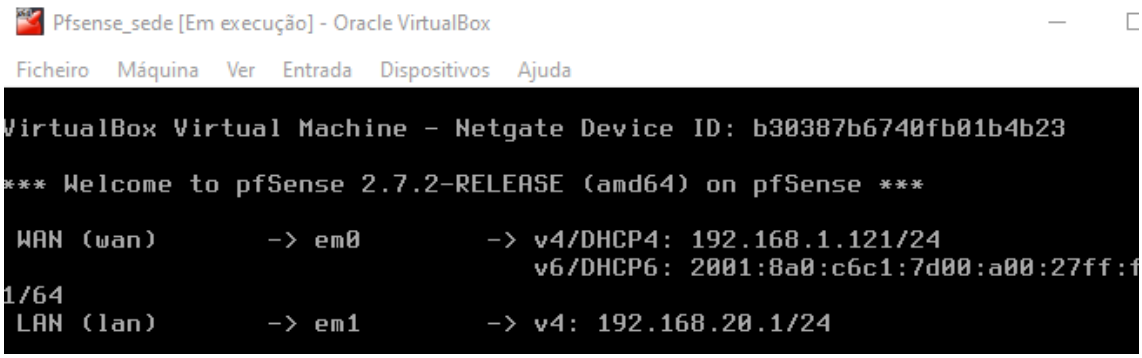


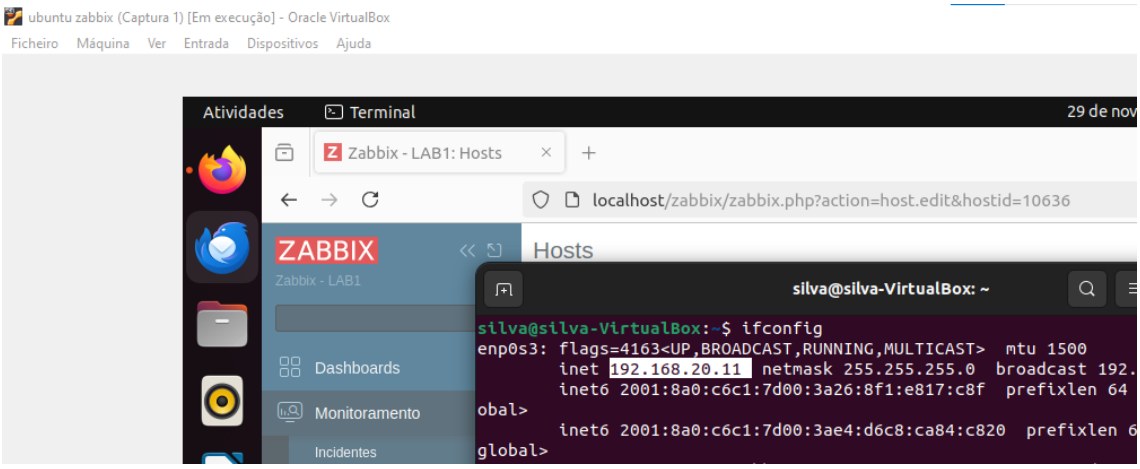
Máquina Ubuntu Zabbix (adaptador 1 – rede interna)



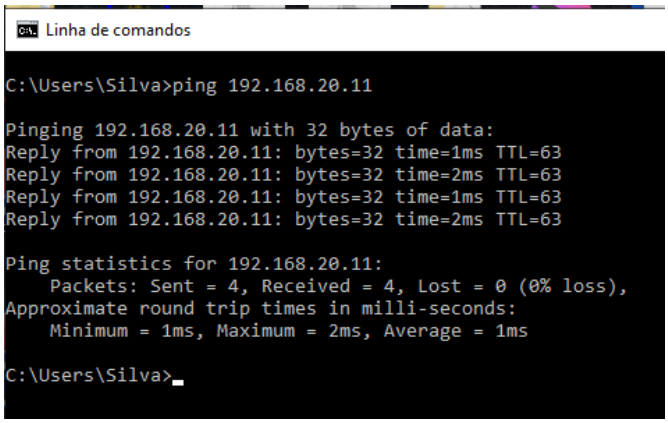
Passo 12 - Quando a nova rede for atribuída na máquina do Ubuntu, abra um terminal e digite o comando ifconfig para ver a diferença no endereço IP (placa enp0s3) e verificar se está dentro do domínio da LAN do servidor da firewall PFsense:

Nota Importante: para um efeito mais rápido, desative e volte a ativar a placa de rede na máquina virtual)

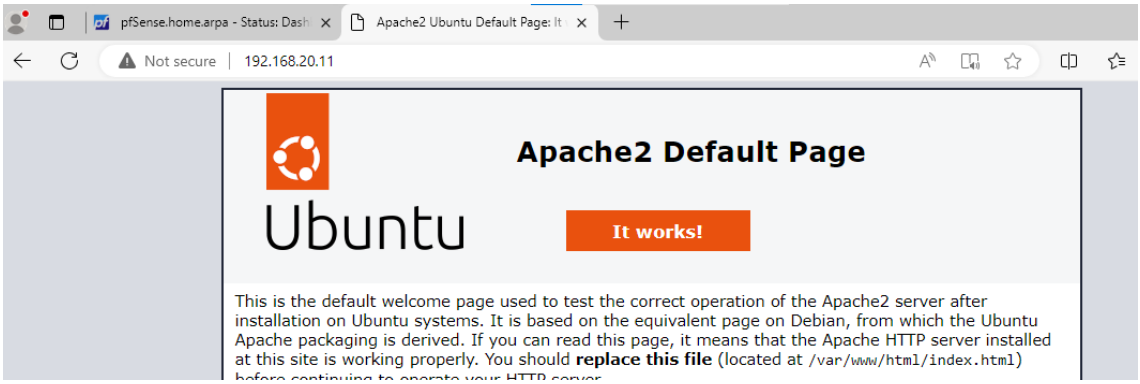




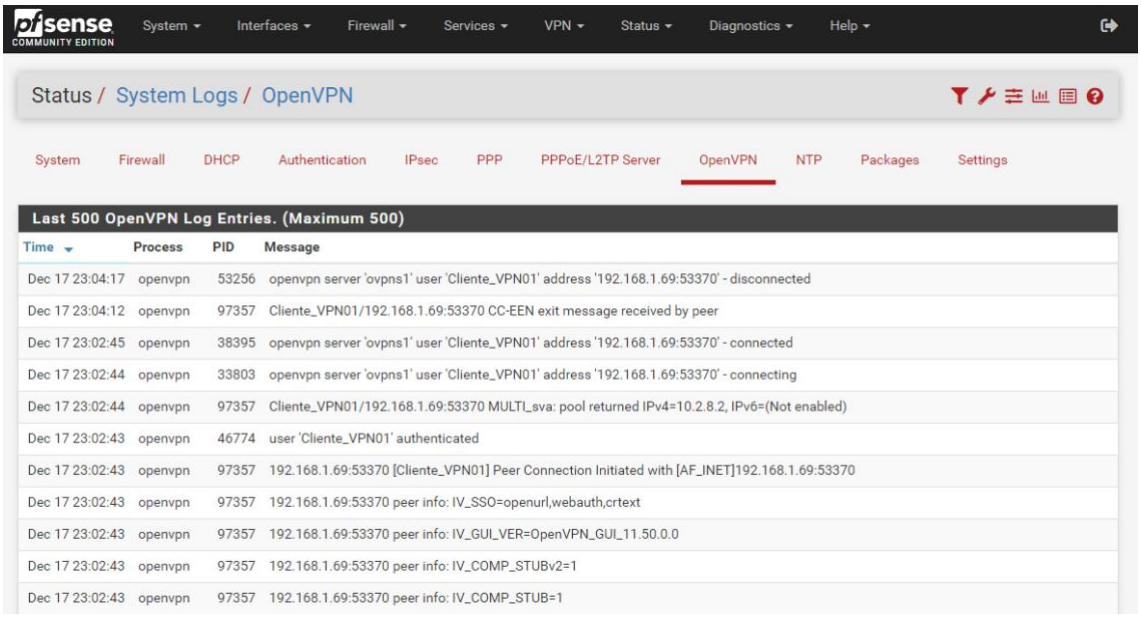
Se pingar da máquina virtual (Windows onde ligou o cliente VPN), para dentro da LAN da firewall, mais especificamente, a máquina do Ubuntu com o IP 192.168.20.11 e veja o resultado:



Se tiver o servidor Apache instalado e a funcionar corretamente, desde que tenha a ligação VPN ativa, pode aceder aos portais WEB da rede da empresa:



Também pode analisar os logs (monitorização do histórico) e ver quando a ligação foi feita, quando terminou, entre outras opções:


pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Status / System Logs / OpenVPN
System
Firewall
DHCP
Authentication
IPsec
PPP
PPPoE/L2TP Server
OpenVPN
NTP
Packages
Settings
Last 500 OpenVPN Log Entries. (Maximum 500)
Time
Process
PID
Message
Dec 17 23:04:17 openvpn 53256 openvpn server 'ovpns1' user 'Cliente_VPN01' address '192.168.1.69:53370' - disconnected
Dec 17 23:04:12 openvpn 97357 Cliente_VPN01/192.168.1.69:53370 CC-EEN exit message received by peer
Dec 17 23:02:45 openvpn 38395 openvpn server 'ovpns1' user 'Cliente_VPN01' address '192.168.1.69:53370' - connected
Dec 17 23:02:44 openvpn 33803 openvpn server 'ovpns1' user 'Cliente_VPN01' address '192.168.1.69:53370' - connecting
Dec 17 23:02:44 openvpn 97357 Cliente_VPN01/192.168.1.69:53370 MULTI_sva: pool returned IPv4=10.2.8.2, IPv6=(Not enabled)
Dec 17 23:02:43 openvpn 46774 user 'Cliente_VPN01' authenticated
Dec 17 23:02:43 openvpn 97357 192.168.1.69:53370 [Cliente_VPN01] Peer Connection Initiated with [AF_INET]192.168.1.69:53370
Dec 17 23:02:43 openvpn 97357 192.168.1.69:53370 peer info: IV_SSO=openurl,webauth,crtext
Dec 17 23:02:43 openvpn 97357 192.168.1.69:53370 peer info: IV_GUI_VER=OpenVPN_GUI_11.50.0.0
Dec 17 23:02:43 openvpn 97357 192.168.1.69:53370 peer info: IV_COMP_STUBv2=1
Dec 17 23:02:43 openvpn 97357 192.168.1.69:53370 peer info: IV_COMP_STUB=1

Parte 7 – Problema do endereço IP público dinâmico

Algumas operadoras mudam o endereço IP público com alguma frequência (devido a ser um endereço **IP dinâmico** que muda com o tempo), como por exemplo, quando reinicia o dispositivo do ISP (router) ou altera as configurações internas.

Quer aceder ao computador/equipamento da rede interna da empresa, a partir da Internet, mas este não tem um endereço público?

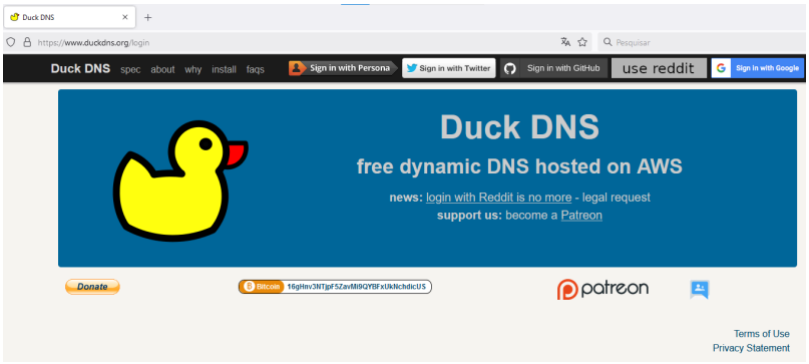
Mesmo existindo um endereço público associado ao router, sabia que este mudo de X em X tempo?

Como solução para este problema, devemos usar um serviço dedicado de conversão de endereços para um nome (endereço), em vez do indicar o endereço IP na configuração da ligação (números IPv4 ou IPv6). Como tal, existe o popular serviço no-ip como o Duck DNS (embora que exista outros como o dynIP da SAPO).

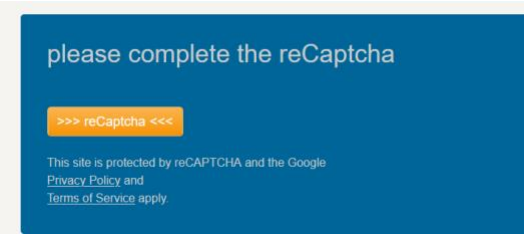
O DuckDNS é um serviço que permite traduzir o endereço IP dinâmico do router, computador ou outro equipamento (por exemplo: 81.112.159.76) por um "nome". Este serviço está alojado na plataforma de cloud da Amazon e o código do serviço está disponível sob a licença GNU GPLv3 desde Maio de 2016.

Para tal basta que acedam ao endereço www.duckdns.org e autentiquem-se usando um dos serviços apresentados na zona superior (Ex. Facebook, Twitter, Google, etc).

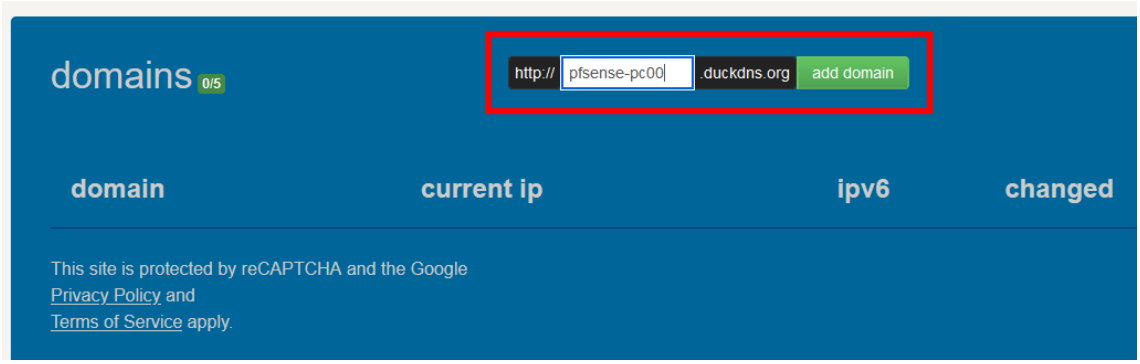
Passo 1 – Aceda ao portal: www.duckdns.org e faça o login.



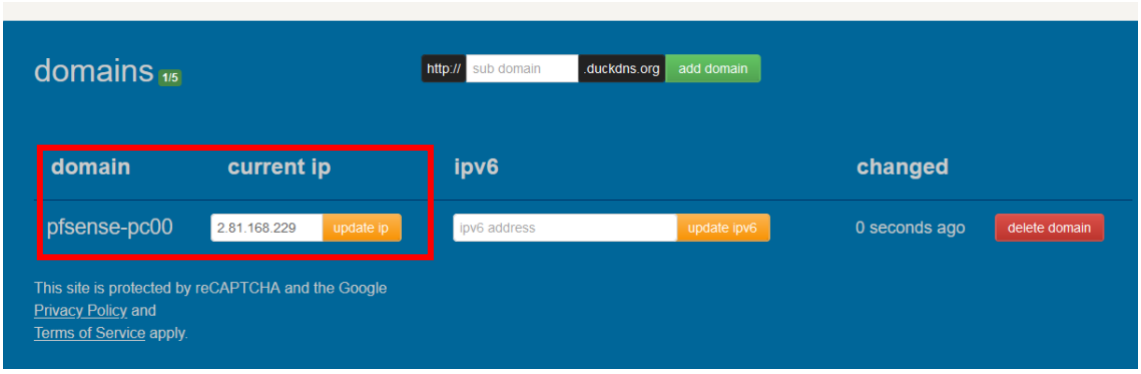
Passo 2 – Confirme a verificação Captcha:



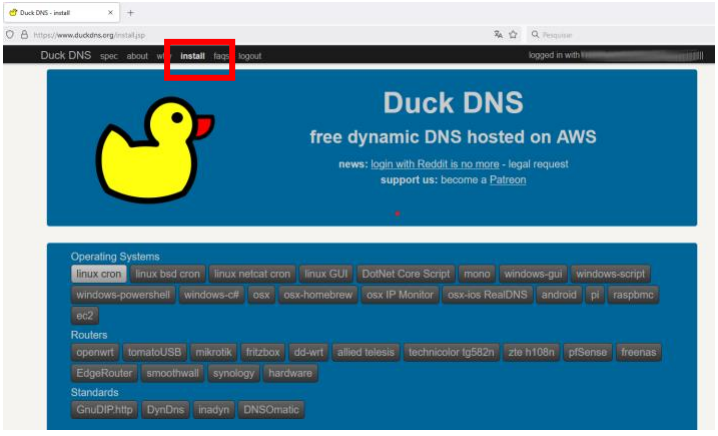
Passo 3 – Crie um endereço/domínio (atenção que o nome do endereço será algo como xxxxx@duckdns.org). Não esqueça de que só pode utilizar letras, números e traços (-):



Resultado:



Passo 4 – Depois de concluir a conta de criação do domínio, devemos seguir as instruções da instalação/associação do domínio DuckDns que estão disponíveis na página oficial do DuckDns, mais especificamente no menu **Install**:

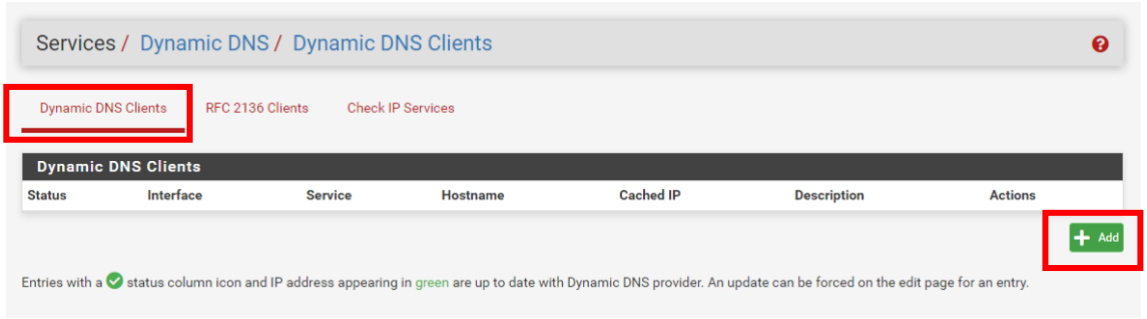


Mais abaixo, selecione a opção Pfsense e depois escolha qual o domínio a trabalhar:

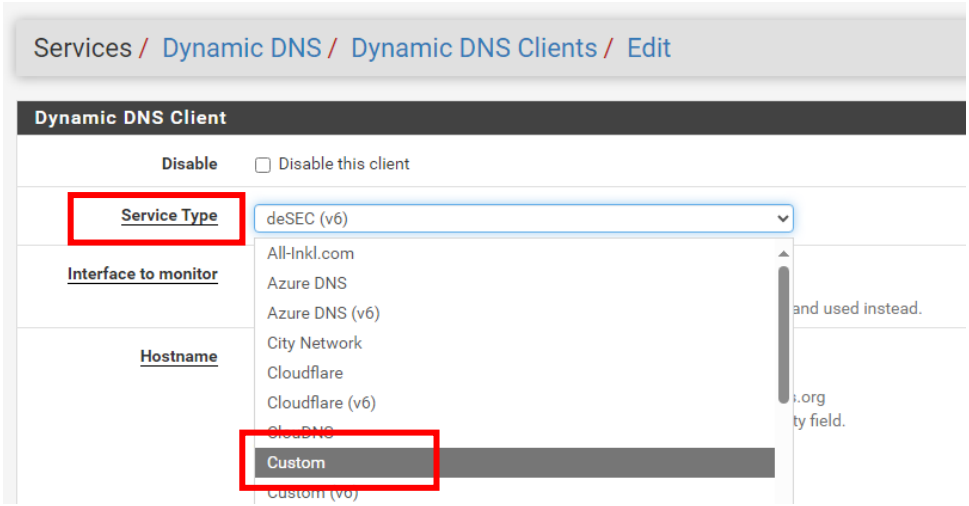


Nota Importante: mais abaixo estão as instruções para associar os dados na firewall

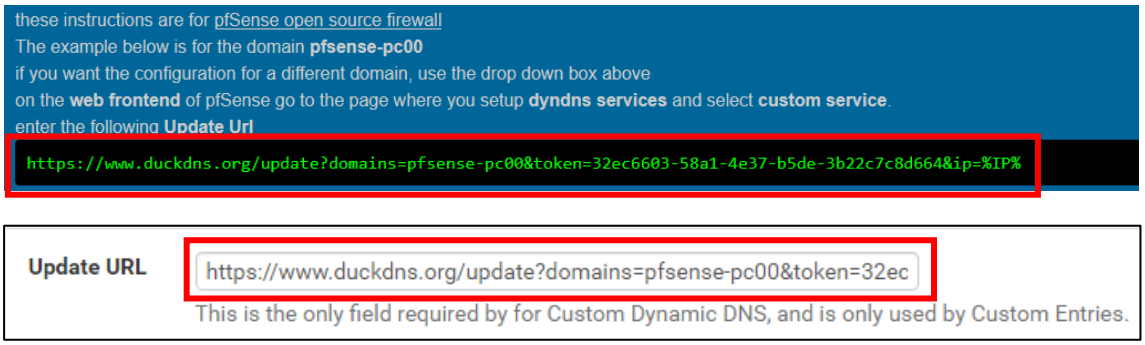
Passo 5 – Dentro da firewall PFsense deve ir ao menu **Services → Dynamic** DNS para configurar o domínio com base no DuckDNS. Por defeito, este vai selecionar o separador "**Dynamic DNS Clients**" (se não tiver selecione o mesmo) e clique no botão **Add**:



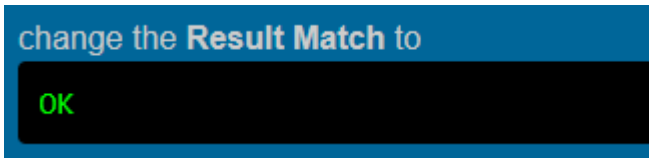
Passo 6 – No campo **Service Type**, selecione a opção **Custom**:

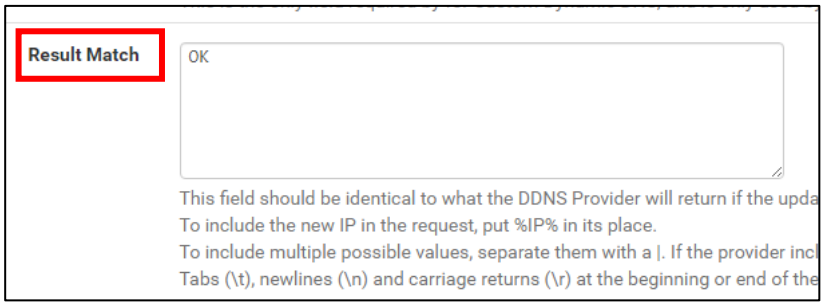


Passo 7 – No campo **Update URL**, coloque a **hiperligação** que foi dada na página DuckDNS:

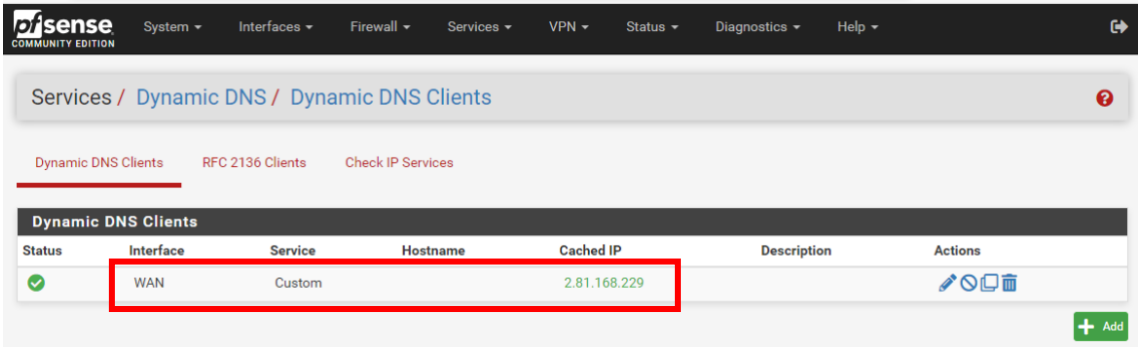


Passo 8 – No campo **Result Match**, coloque a mensagem **OK** da página DuckDNS:

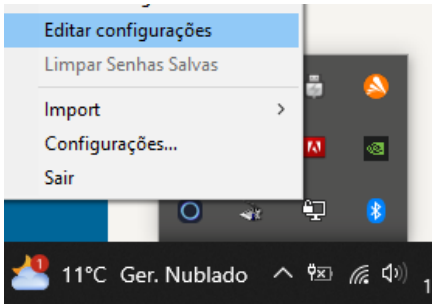


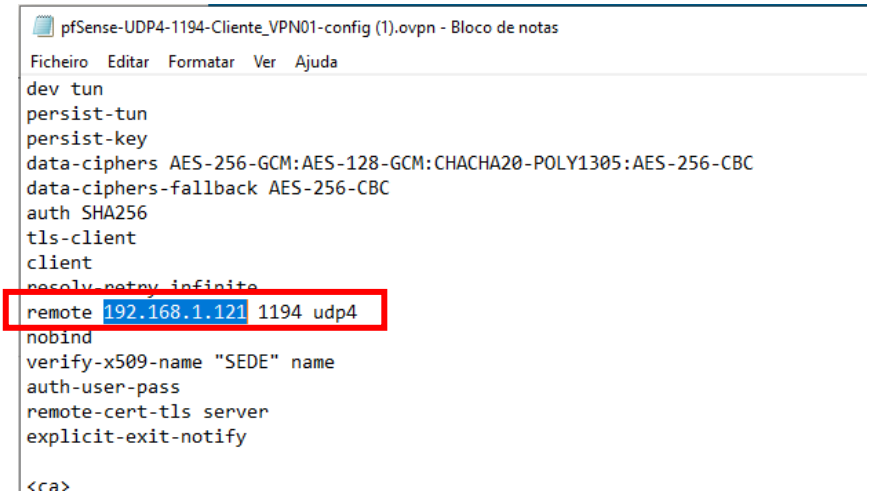


Feito os passos anteriores, o domínio com o nome dinâmico foi configurado com sucesso:



Passo 9 – Agora devemos fazer uma alteração muito importante. No ficheiro de configuração do OpenVPN que exportou para o computador do cliente, deve editar o ficheiro e devemos colocar o código identificador do domínio do DuckDNS (seguido de duckdns.org) em vez do endereço IP:





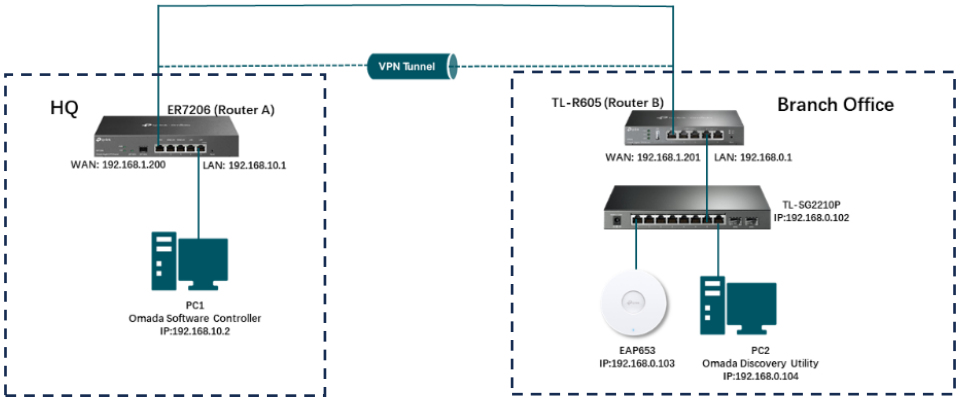
Colocar o código identificador do domínio do DuckDNS (seguido de duckdns.org) em vez do endereço IP:



Parte 8 – Configuração Pfsense Site-to-Site

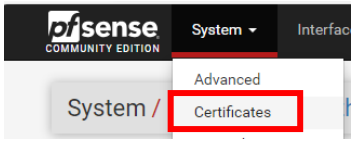
Parte 8.1 – Configuração Pfsense Site-to-Site (Lado Servidor)

Site-to-Site (ou Gateway para Gateway): esta forma de ligação pode ser aplicada à estrutura de comunicação segura com recurso a VPN que necessitam de interligar **unidades de negócio (sedes e filiais)**, com vários utilizadores em locais diferentes, não existindo um tipo de ligação direta

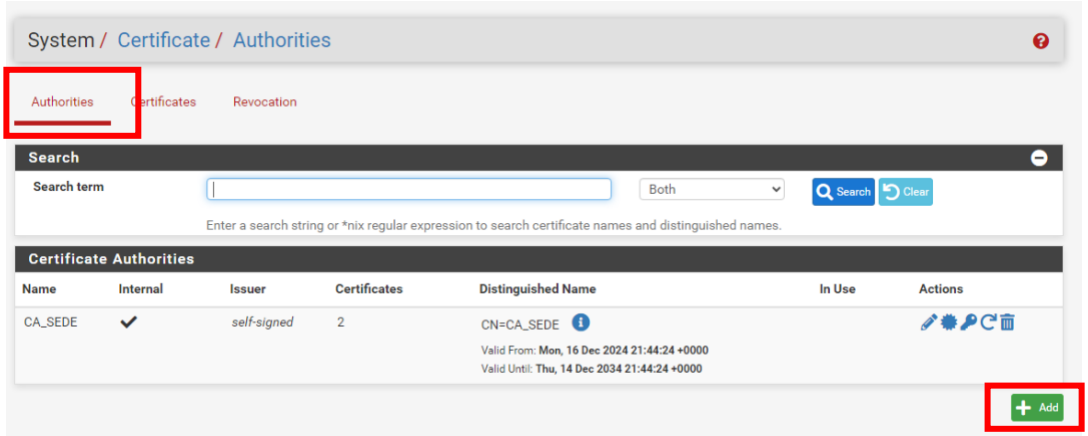


Vamos assumir que a rede para SEDE será a máquina já trabalhamos nos exercícios anteriores e agora vamos utilizar a máquina virtual da FILIAL (com o endereço 192.168.10.1)

Passo 1 – Na máquina virtual da SEDE, vamos gerar nova autoridade (dedicada para as ligações site-to-site ao contrário do que fez anteriormente). Vamos ao menu System → Certificates:

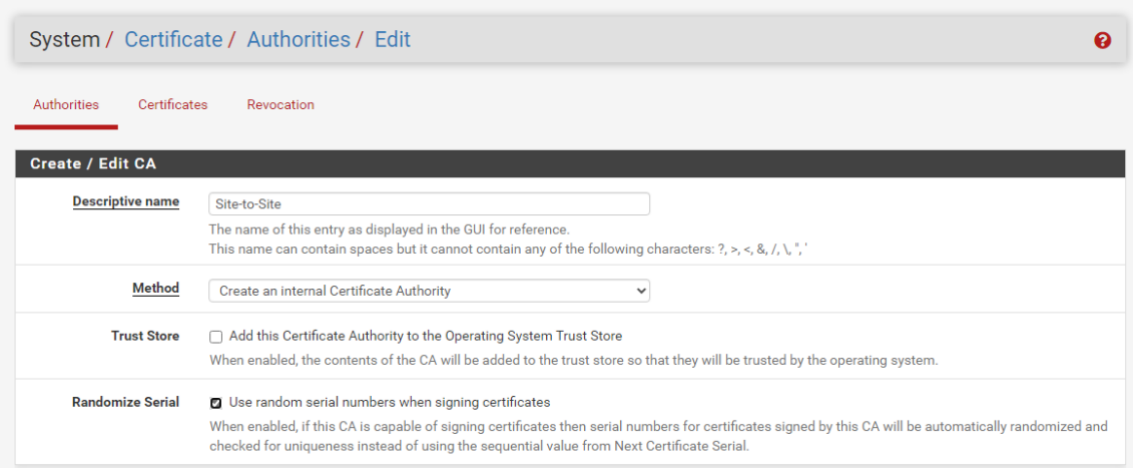


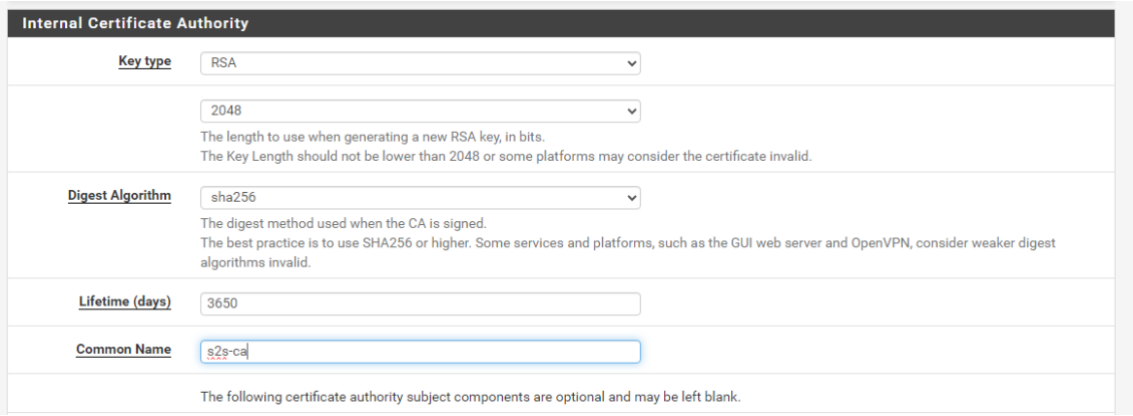
Passo 2 – Na página dos certificados, vamos criar um novo autoridade:



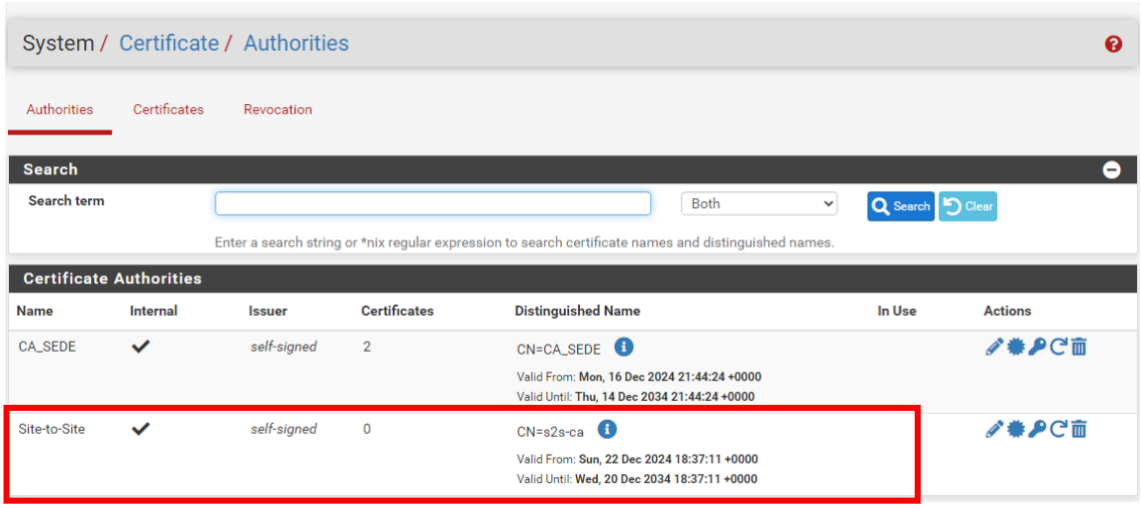
Passo 3 – Coloque as seguintes informações:

- **Descriptive Name**: Site-to-Site
- **Method**: Create an internal Certificate Authority
- **Randomize Serial**: ativar esta opção
- **Common Name**: s2s-ca

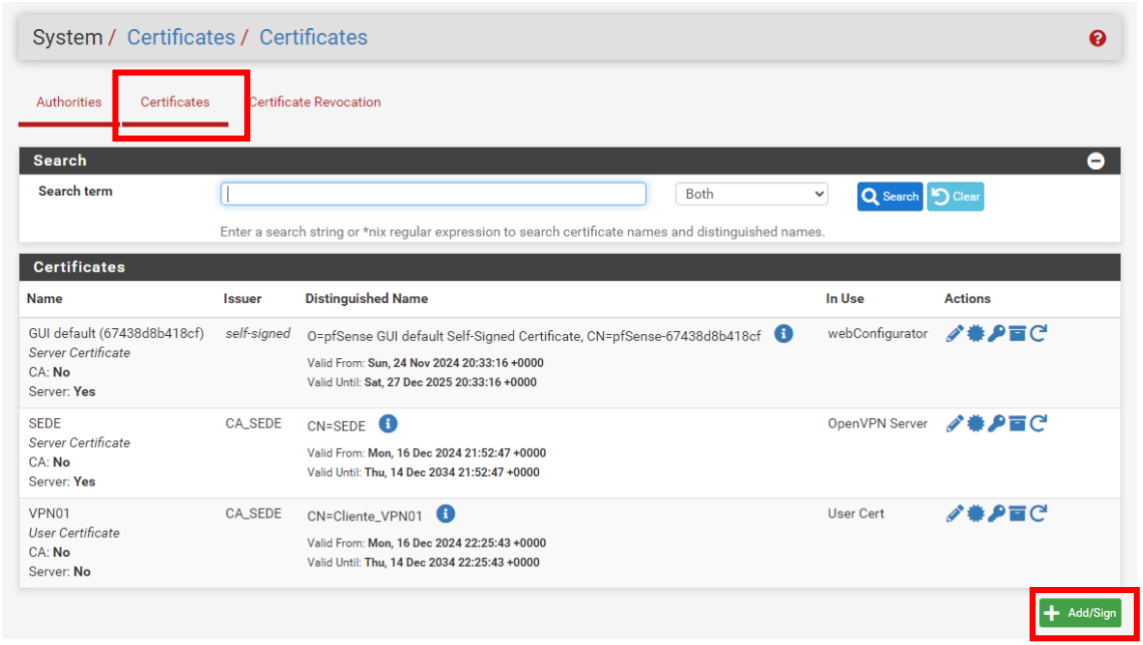




Resultado:



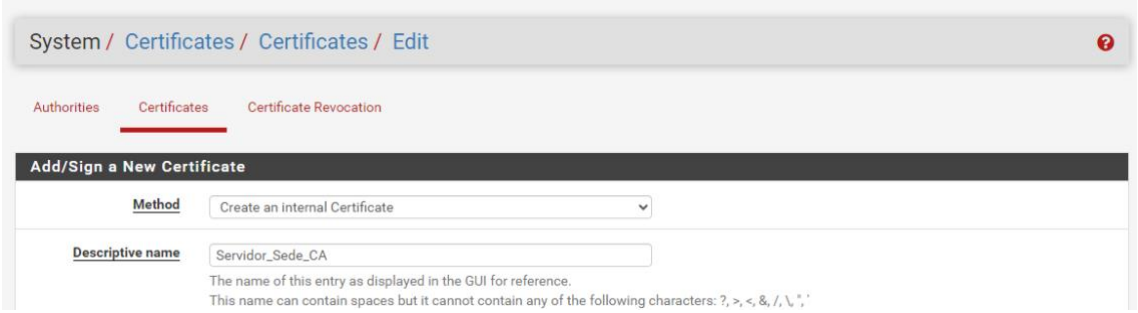
Passo 4 – Após criar a entidade, vamos gerar certificado na firewall da sede. Como tal, vamos ao separador Certificates e carregue no botão Add:

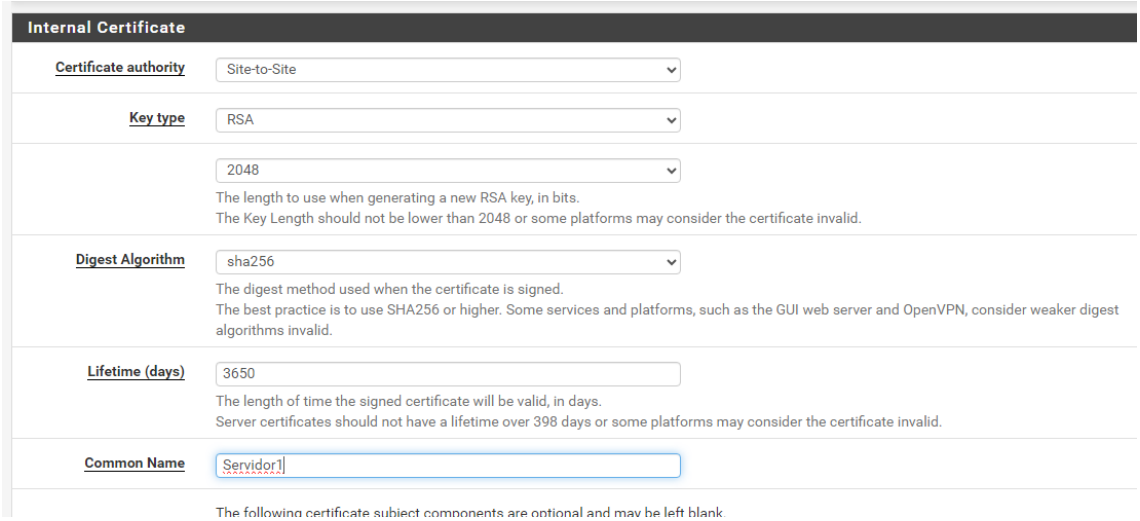


Passo 5 – Vamos colocar os seguintes dados:

- **Method**: Create na internal Certificate
- **Descriptive Name**: Servidor_Sede_CA

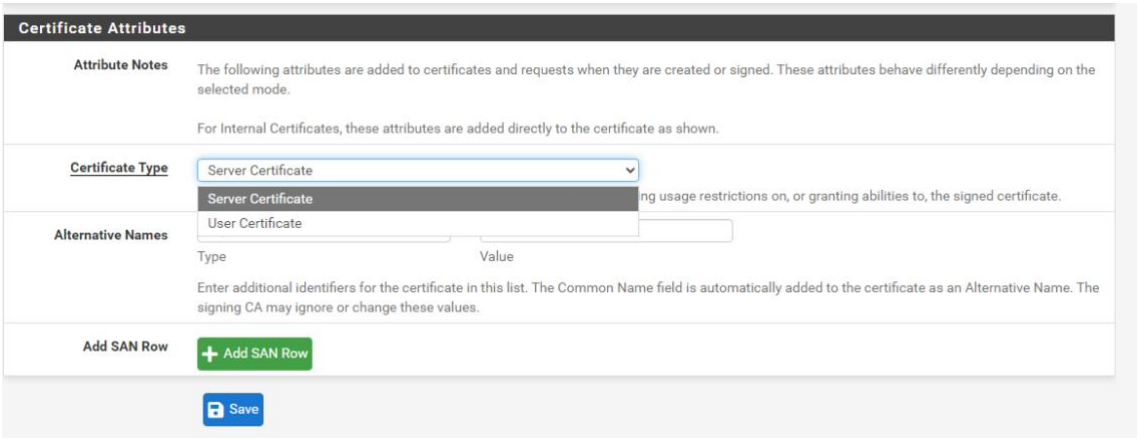
- **Certificate Authority**: Site-to-Site (entidade certificadora que criou no passo anterior)
- **Common Name**: Servidor1



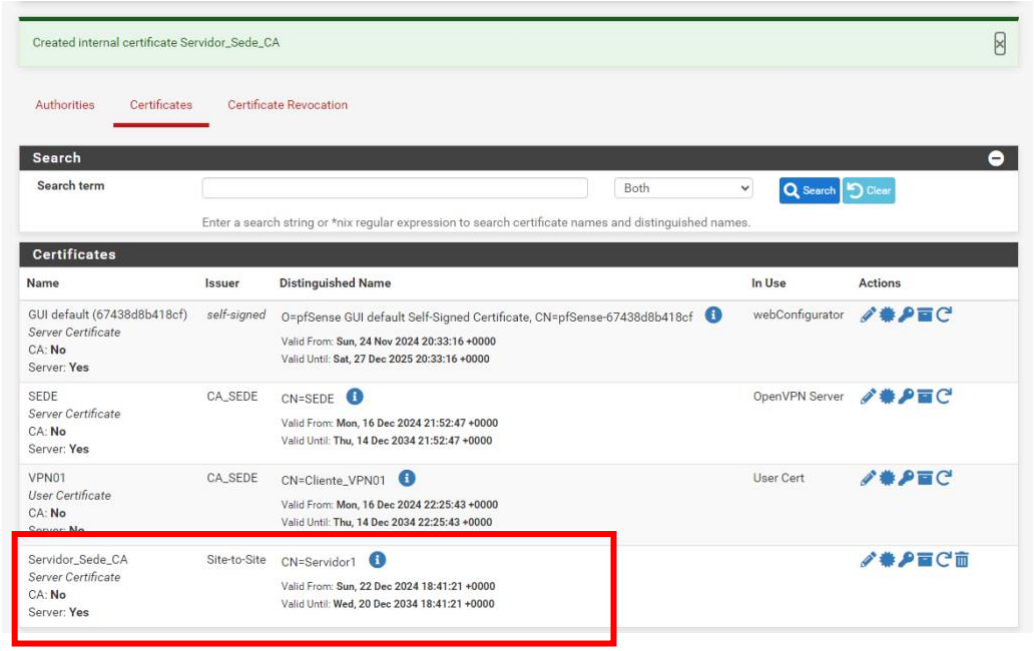


Por último, no separador “Certificate Atrributes”, vamos indicar as seguintes opções:

- Ceritificate Type: Server Certificate

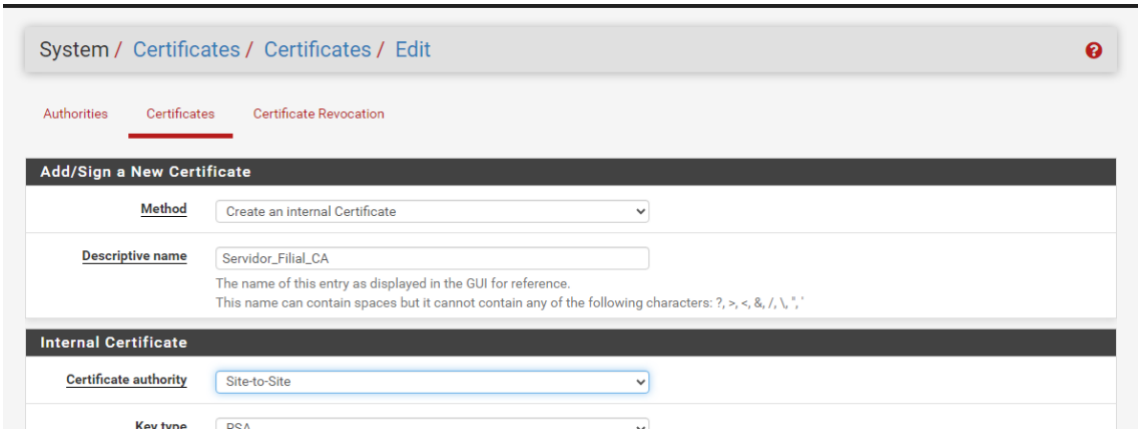


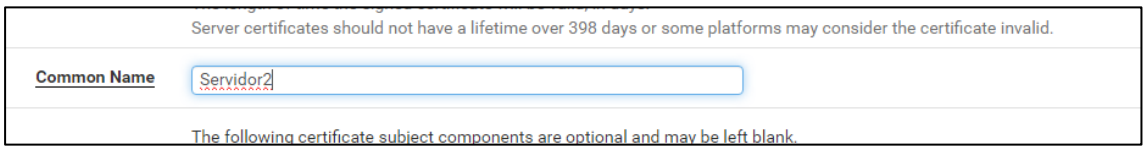
Resultado:



Passo 6 – Após criar a entidade e o certificado na firewall da sede, também vamos precisar de criar o certificado cliente (filial) para depois exportar e associar no servidor remoto VPN da firewall filial. Ainda no separador da criação os certificados, coloque os seguintes dados:

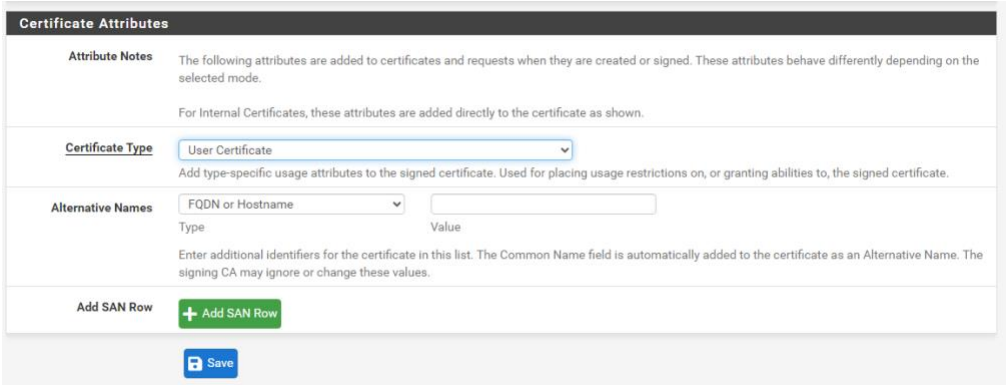
- **Method**: Create na internal Certificate
- **Descriptive Name**: Servidor_Filial_CA
- **Certificate Authority**: Site-to-Site (entidade certificadora que criou no passo anterior)
- **Common Name**: Servidor2



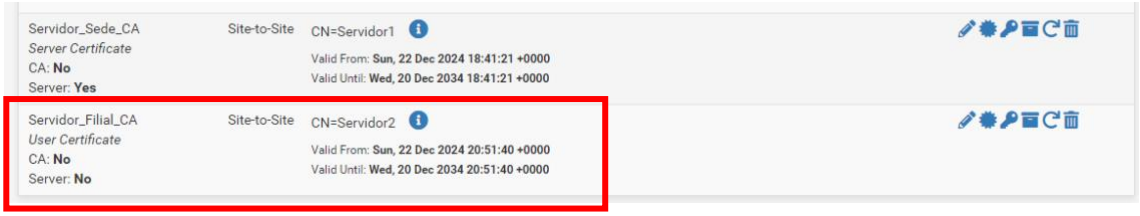


Por último, no separador "Certificate Atrributes", vamos indicar as seguintes opções:

- Ceritificate Type: User Certificate



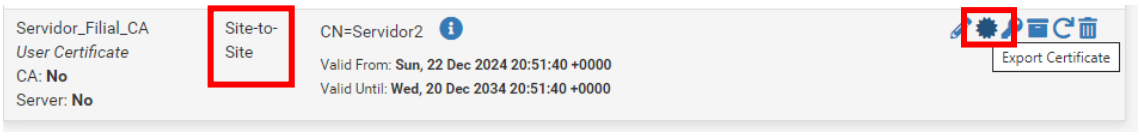
Resultado:

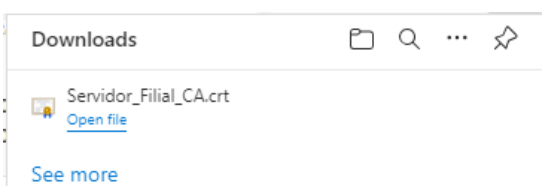


Passo 7 – Com a entidade e certificados para as duas firewalls criados, o próximo passo será exportar os certificados e as chaves que o cliente (filial) necessita quando precisar de realizar a conexão com o servidor OpenVPN (na sede).

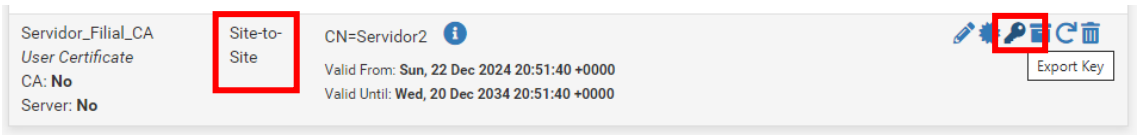
Como tal, vamos fazer as seguintes operações:

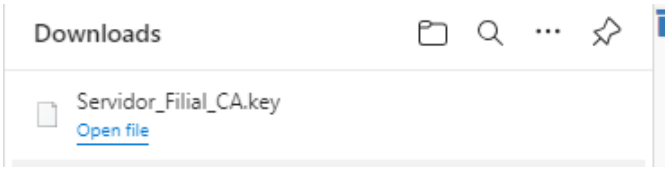
- Tarefa 1 – Ainda no separador dos certificados e vamos clicar no 2 botão (ícone da roda dentada) para fazer download do ficheiro com os dados do certificado:





- **Tarefa 2 –** Faça a mesma ação para o ícone ao lado (3º ícone da chave) para descarregar a chave pública de acesso:

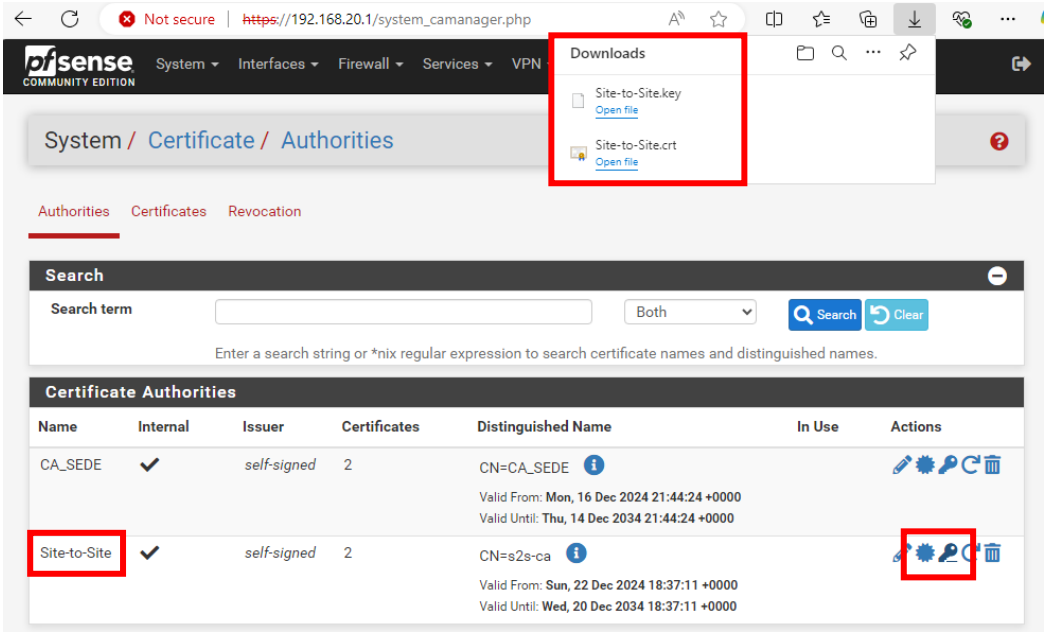




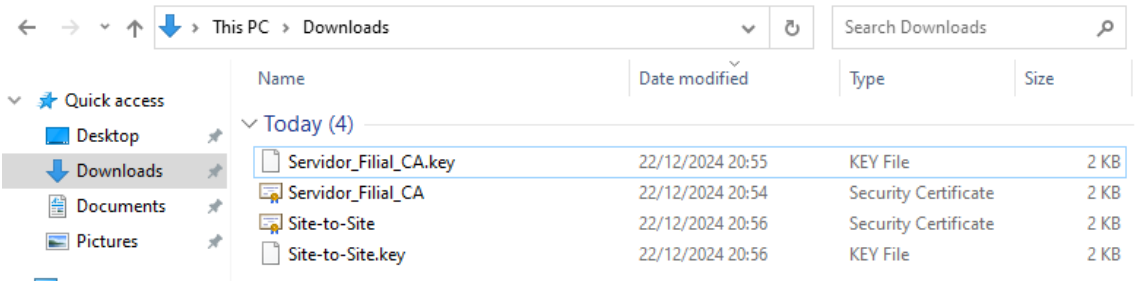
Passo 8 – Faça a mesma operação do passo anterior, mas desta vez, deve fazer a operação no separador da entidade certificadora (Site-to-Site) que criou anteriormente.

- **Tarefa 1 –** Ainda no separador dos certificados e vamos clicar no 2 botão (ícone da roda dentada) para fazer download do ficheiro com os dados do certificado;

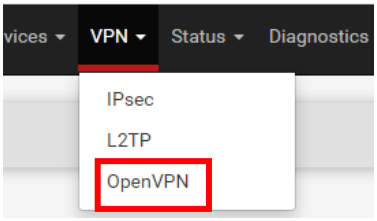
- **Tarefa 2 –** Faça a mesma ação para o ícone ao lado (3º ícone da chave) para descarregar a chave pública de acesso:



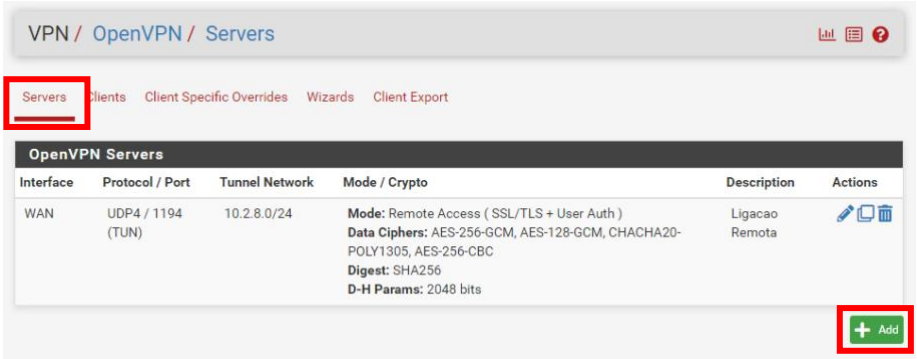
Confirmação das transferências dos ficheiros (Passo 6 e Passo 7):



Passo 9 – Próximo passo será configurar conexão da instância do servidor OpenVPN. Vamos ao menu VPN → OpenVPN:

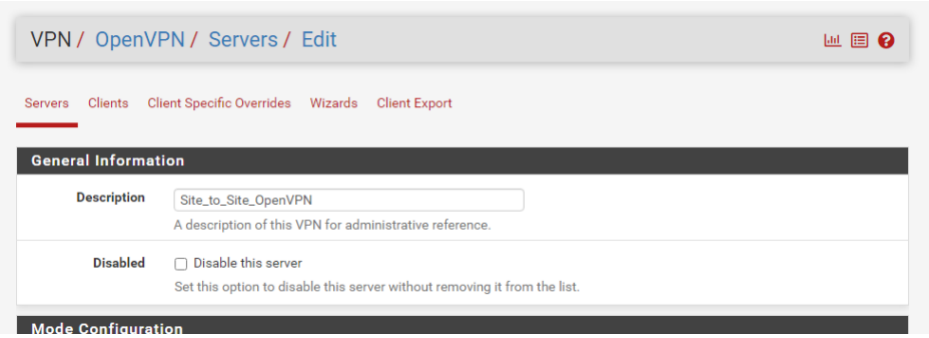


Passo 10 – Verifique se tem o separador Servers selecionado e de seguida, vamos criar uma nova ligação:

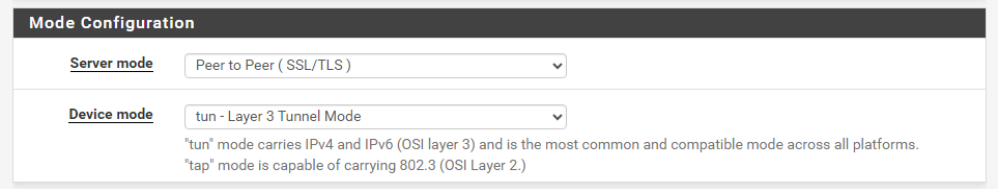


Passo 11 – Na nova ligação, vamos colocar os seguintes dados:

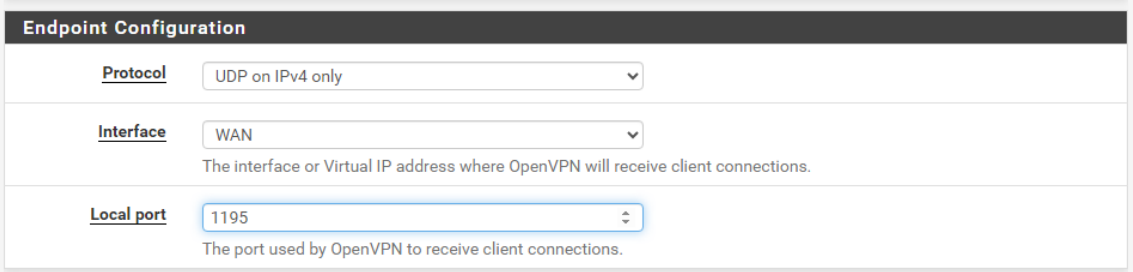
- **Description**: Site_to_Site_OpenVPN



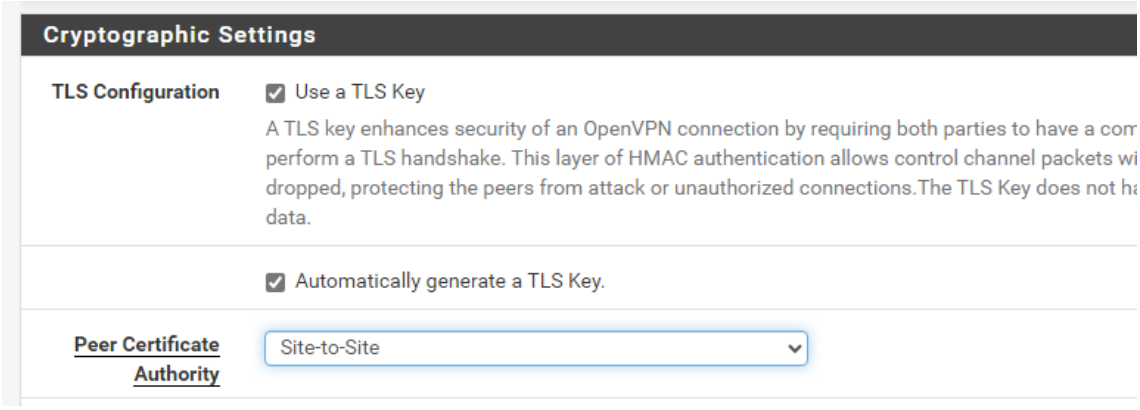
- **Server Mode**: Peer to Peer (SSL/TLS)
- **Device Mode**: tun – Layer 3 Tunnel Mode



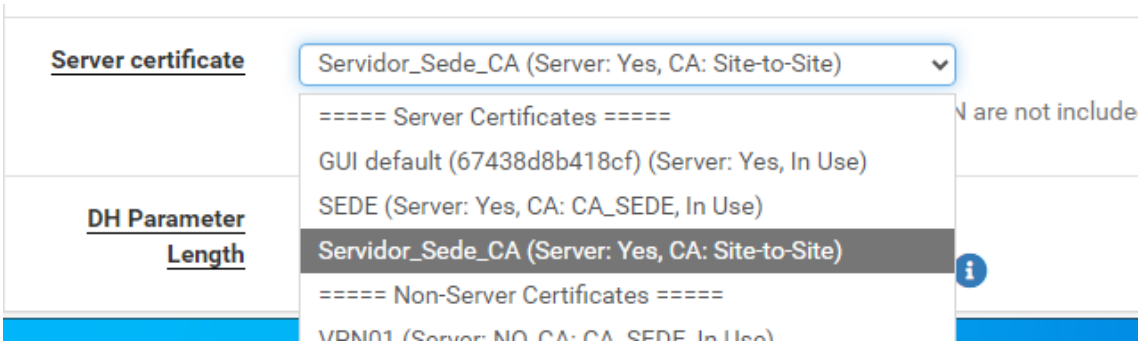
- **Protocolo**: UDP on IPv4 Only
- **Interface**: WAN
- **Local Port**: 1195 (porta 1194 já está a ser utilizada no exercício anterior)



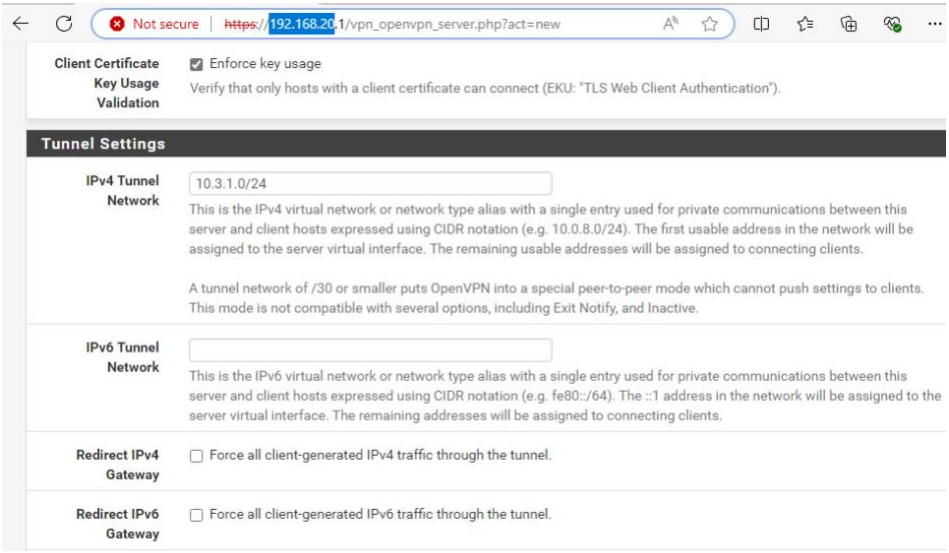
- **TLS Configuration + Automatically generate a TLS Key**: ativar estas opções
- **Peer Certificate Authority**: Site-to-Site (Entidade certificadora que criou anteriomente)



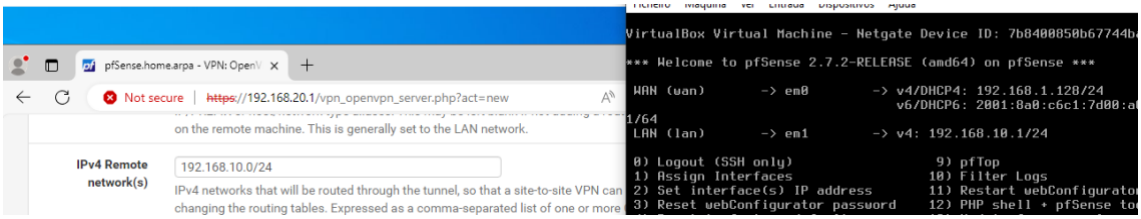
- Server Certificate: vão aparecer todos os certificados para servidores e nãoservidores que criou até agora. Vamos selecionar a opção Servidor_Sede_CA (certificado que criou anteriormente)



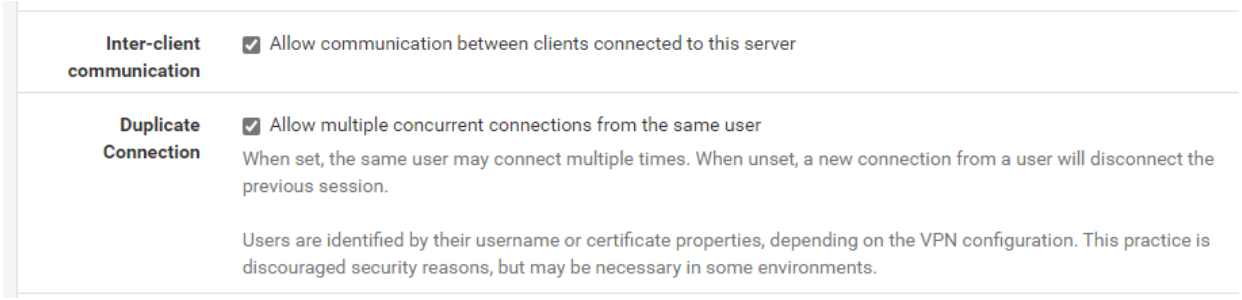
- Client Certificate Key Usage Validation: ativar esta opção
- IPv4 Tunnel Network: canal por onde vao navegar a ligação VPN até chegar a ambas as extremidades da LAN. Vamos assumir o endereço 10.3.1.0/24



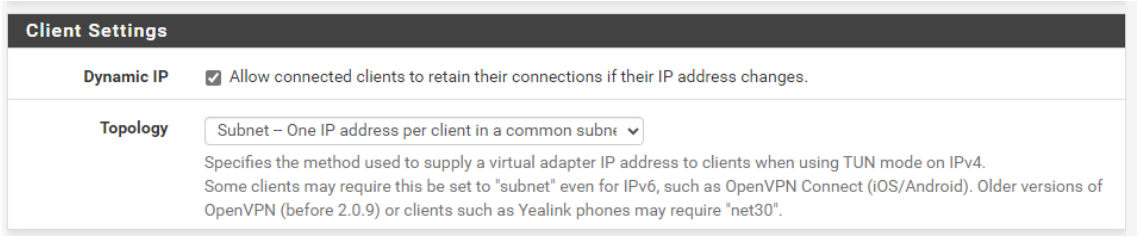
- IPV4 Local Network(s): colocar o endereço IP do domínio da LAN e respetiva mascara de rede (neste caso é o 192.168.10.0/24). Caso não saiba o domínio, deve consultar a página principal da firewall (neste caso a da Sede) ou na máquina onde está a funcionar a firewall



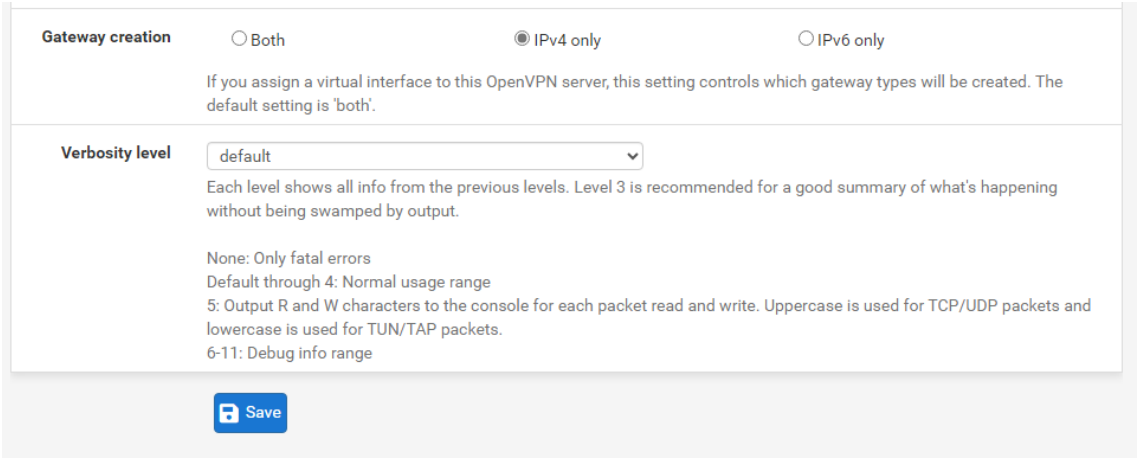
- Inter-client communication: ativar esta opção
- Duplicate Connection: ativar esta opção



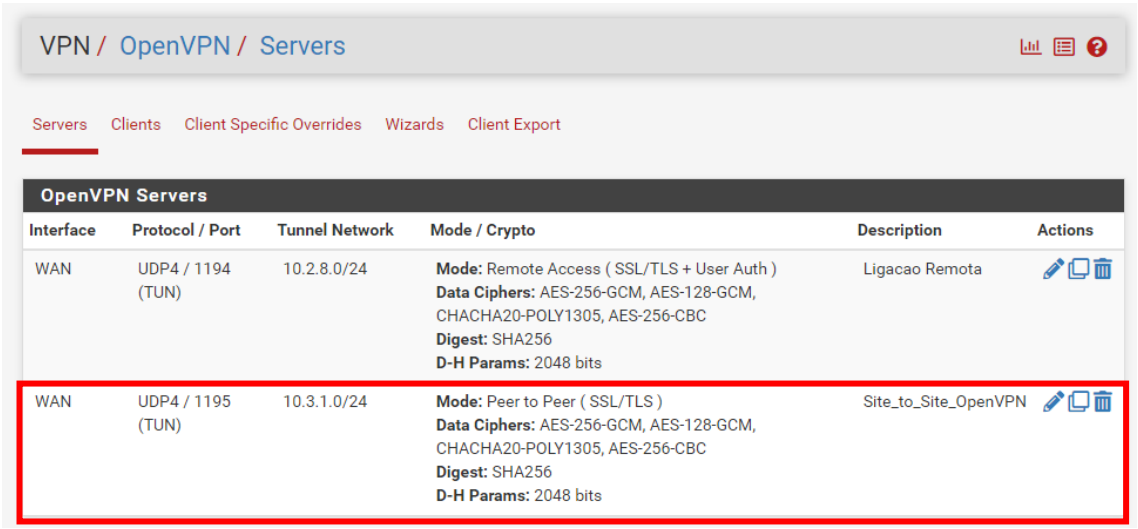
- Dynamic IP: ativar esta opção



- Gateway creation: IPv4 Only

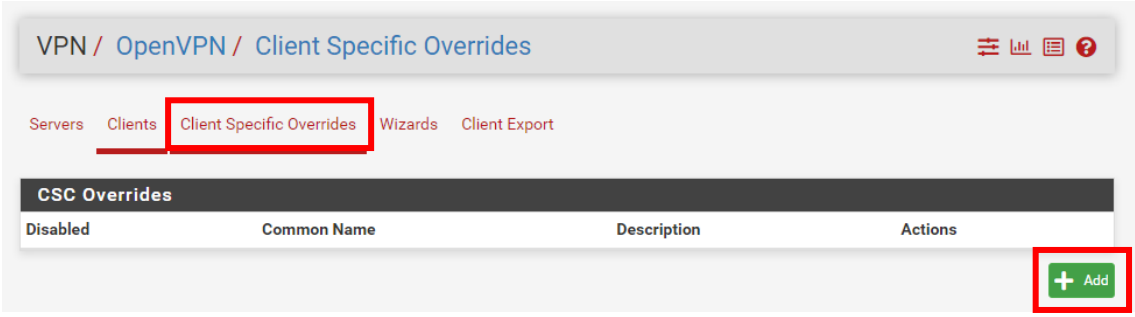


Resultado:



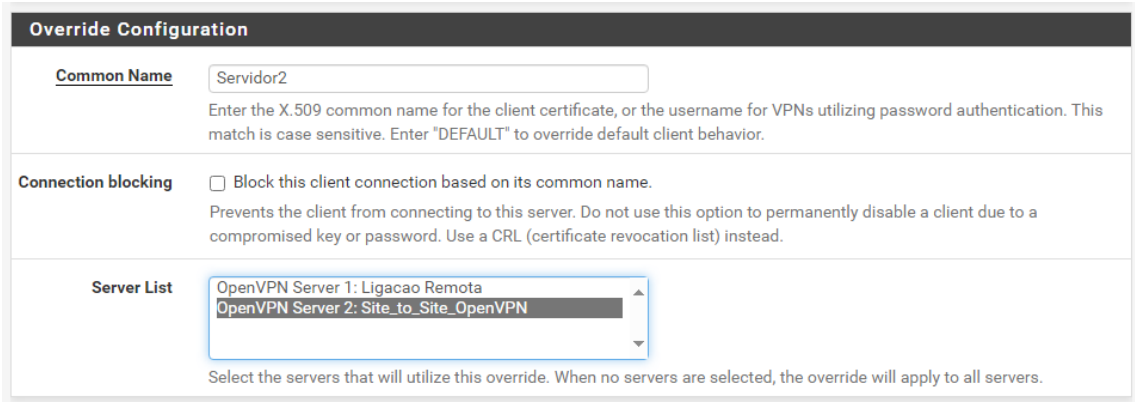
Passo 12 – Agora vamos adicionar a conexão do cliente de forma especifica. Esta ligação vai ligar uma sub-rede do cliente a um certificado específico para que o OpenVPN possa ligar adequadamente uma sub-rede para o sistema correto.

Como tal, vamos selecionar o navegador Client Specific Overrides e clicar no botão ADD:

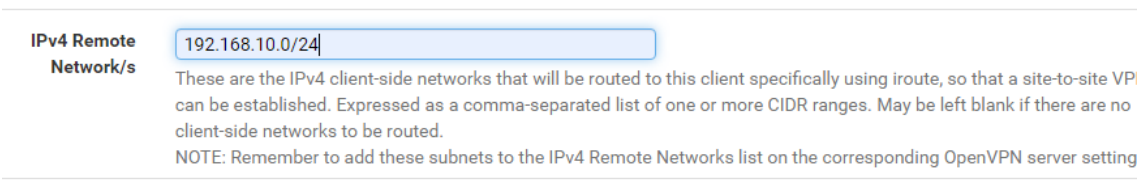


Passo 13 – Na nova configuração, vamos colocar os seguintes dados:

- **Common Name**: Servidor2
- **Server List**: OpenVPN Server 2: Site_to_Site_OpenVPN

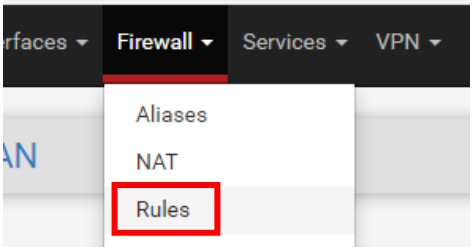


- **IPv4 Remote Address**: 192.168.10.0/24 (domínio da rede LAN do servidor)

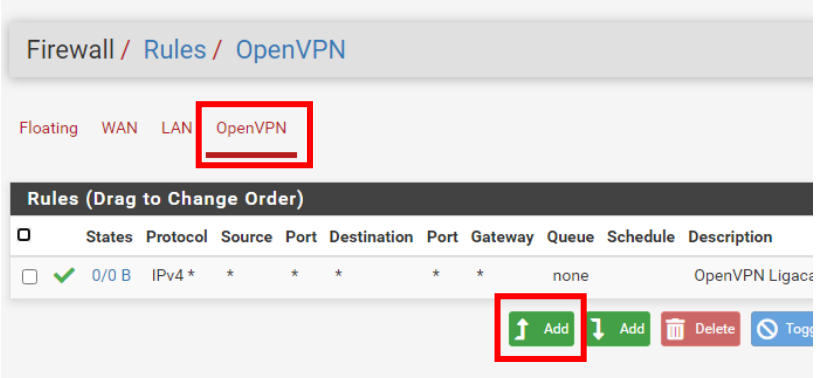


No final não esqueça de gravar as novas informações.

Passo 14 – Adicionadas as configurações de ligação no servidor, vamos adicionar a regra para que o OpenVPN deixe passar o tráfico pela VPN do lado do cliente (mais especificamente na rede da LAN). Vamos ao menu Firewall → Rules:

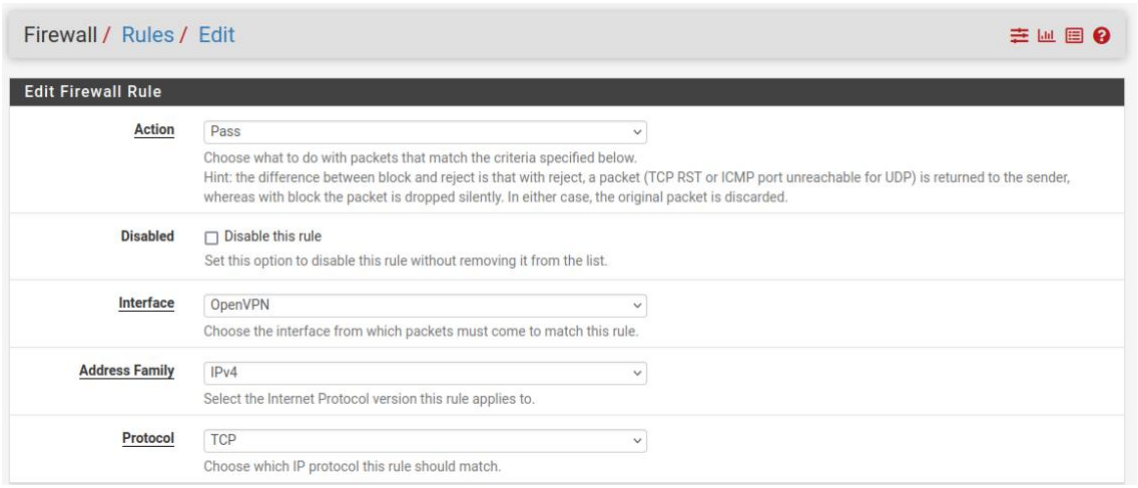


Passo 15 – Selecione o separador OpenVPN e clique no botão ADD:

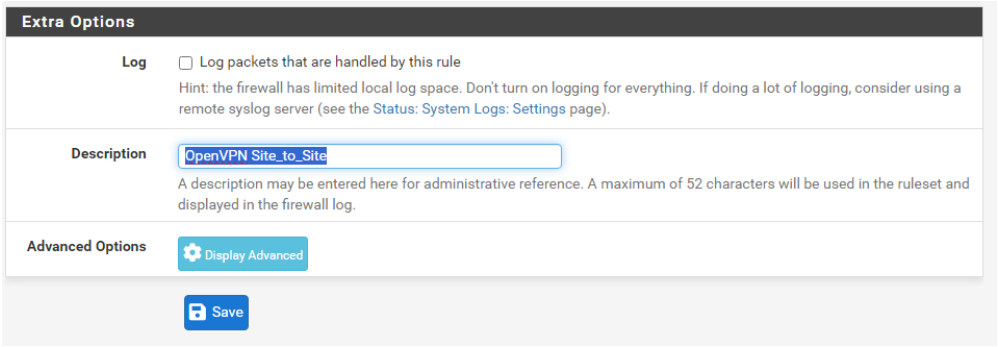


Passo 16 – Na configuração da regra, vamos colocar os seguintes dados:

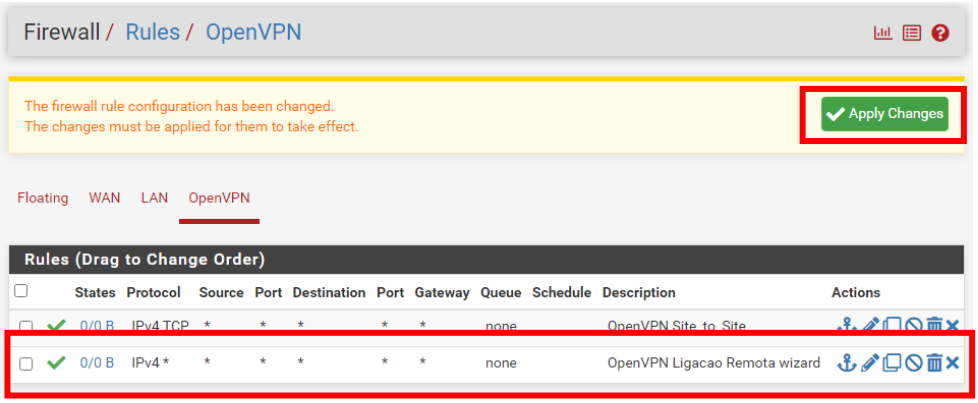
- **Action**: Pass
- **Interface**: OpenVPN
- **Address Family**: Ipv4
- **Protocol**: TCP



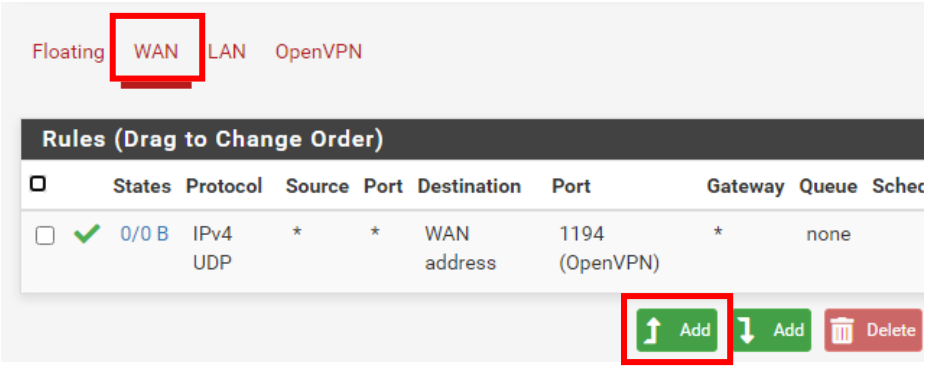
- **Description**: OpenVPN Site_to_Site



Passo 17 – Aplique as novas regras:



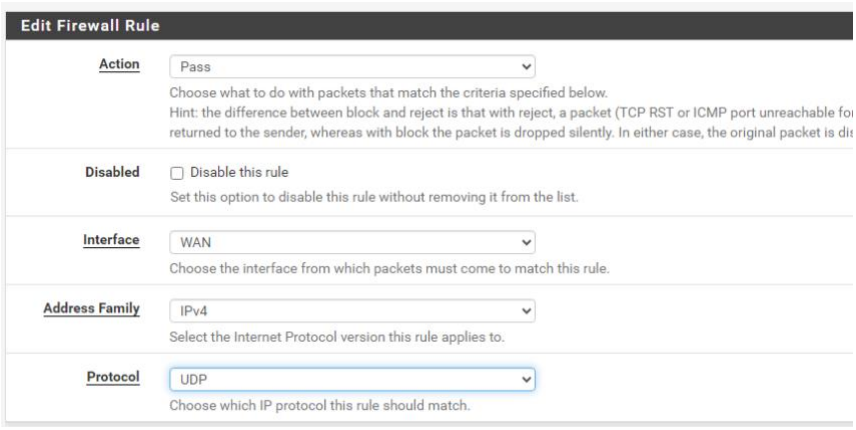
Passo 18 – Selecione o separador WAN e vamos adicionar a regra que vai permitir acesso ao servidor OpenVPN. Clique no botão ADD:



Passo 19 – Na configuração da regra, vamos colocar os seguintes dados:

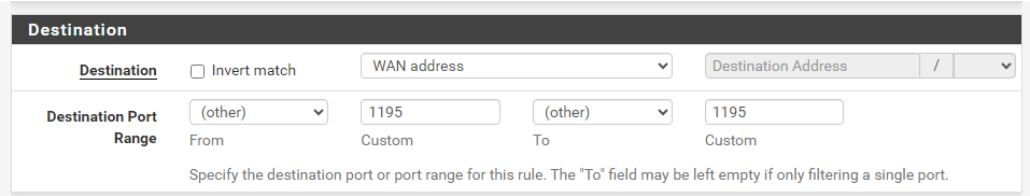
- **Action**: Pass
- **Interface**: WAN

- Address Family: Ipv4
- Protocol: UDP

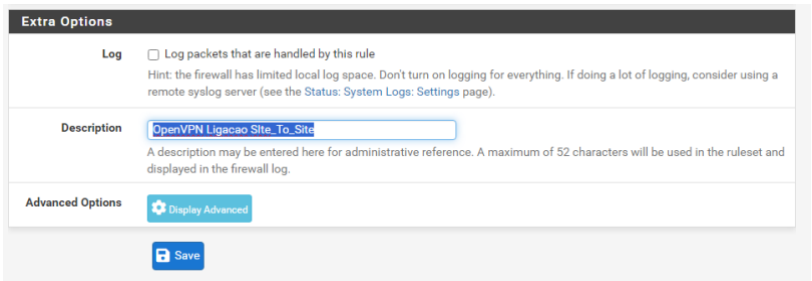


- Destination: WAN Address
- Destination Port Range:
  - From: other
  - Custom: 1195
  - To: other
  - Custom: 1195

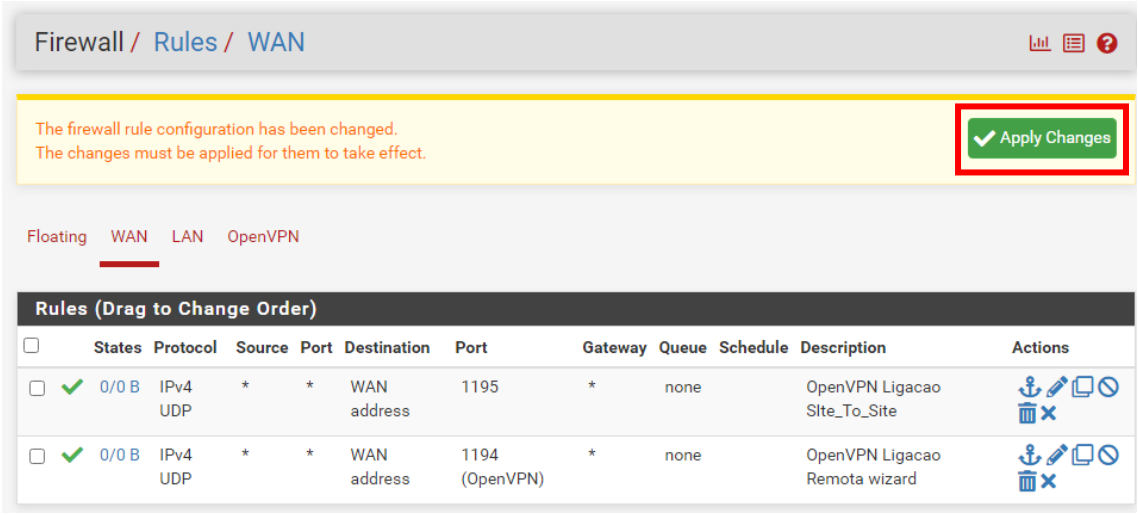
Não esquecer da porta 1195 (como feito no configurador anterior) em vez da tradicional 1194



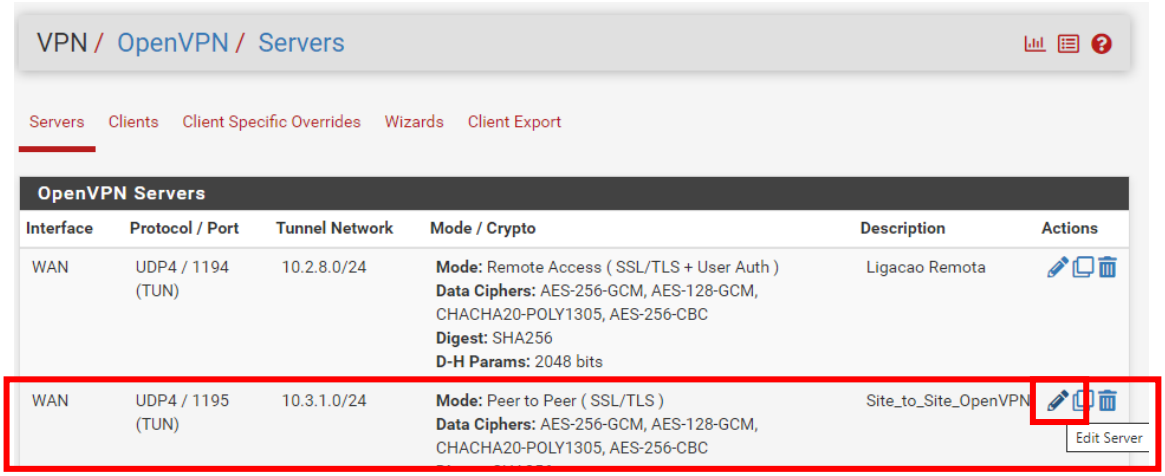
- Description: OpenVPN Ligacao Site_to_Site



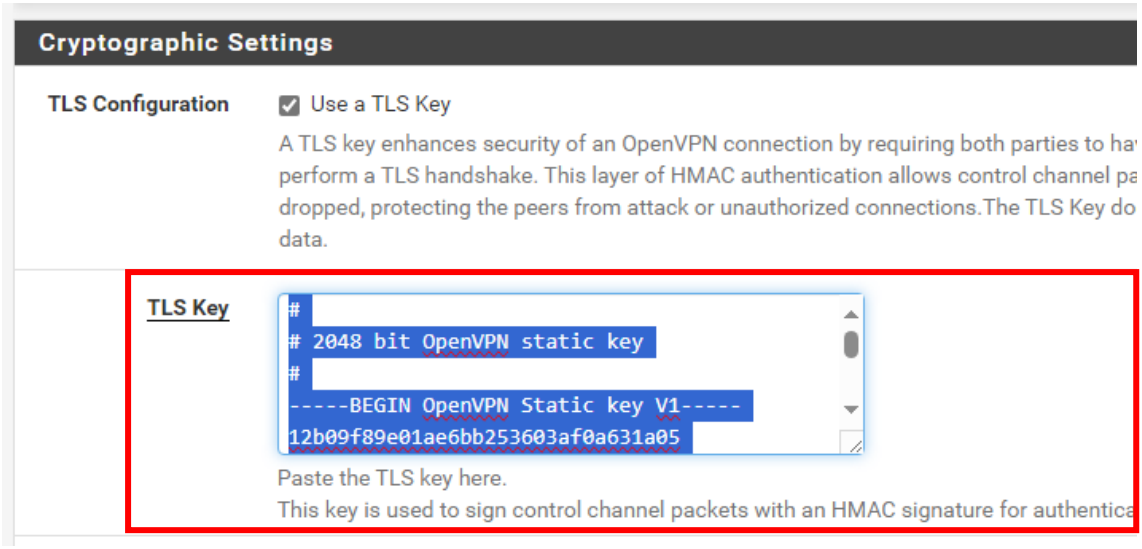
Passo 20 – Aplique as novas regras:



Passo 21 – Como último passo, vamos copiar a chave TLS (encriptação da ligação) da instância do servidor para depois usar no cliente. Vamos ao menu VPN → OpenVPN, selecionar o separador Servers e clique no ícone do lápis da ligação WAN que criou por último (a que tem a porta 1195) com a descrição Site_to_Site_OpenVPN:



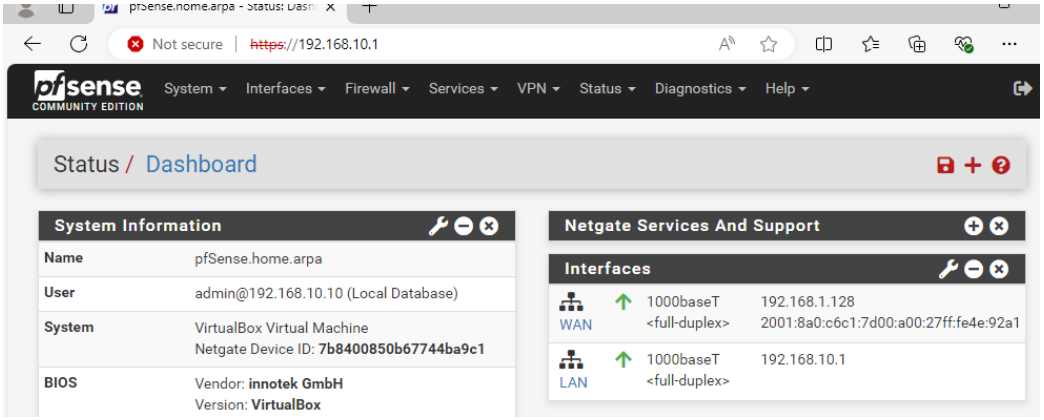
Copie o conteúdo dentro do campo TLS Key para um bloco de notas (vamos necessitar disto mais a frente, mais especificamente, quando configurar a ligação OpenVPN no lado do cliente):


Cryptographic Settings
TLS Configuration
Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to ha
perform a TLS handshake. This layer of HMAC authentication allows control channel pa
dropped, protecting the peers from attack or unauthorized connections.The TLS Key do
data.
TLS Key
#
2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
12b09f89e01ae6bb253603af0a631a05
Paste the TLS key here.
This key is used to sign control channel packets with an HMAC signature for authentica

Parte 8.2 – Configuração Pfsense Site-to-Site (Lado Cliente)

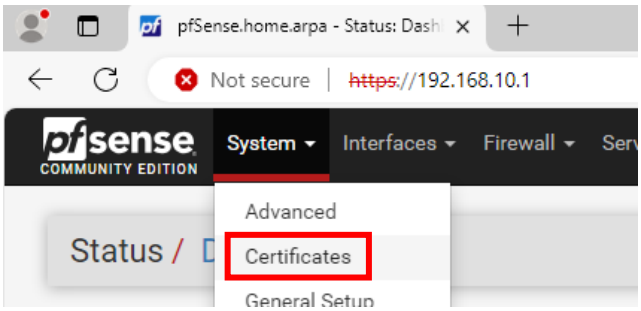
Neste momento já temos o lado do servidor configurado. Mas, agora vamos ter de configurar a ligação do lado do cliente e importar os ficheiros que fez download no lado do servidor (autoridade e certificados).

Passo 1 – Aceda a firewall do lado da filial (Pfsense_Filial):

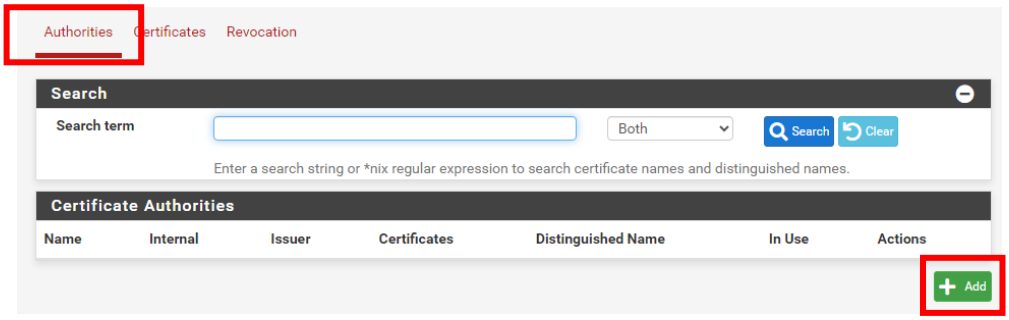


Passo 2 – Vamos começar por criar e importar a entidade certificadora que foi extraída do servidor ficheiro com o nome Site-to-Site.crt (que descarregou anteriormente).

Vamos ao menu System → Certificates:



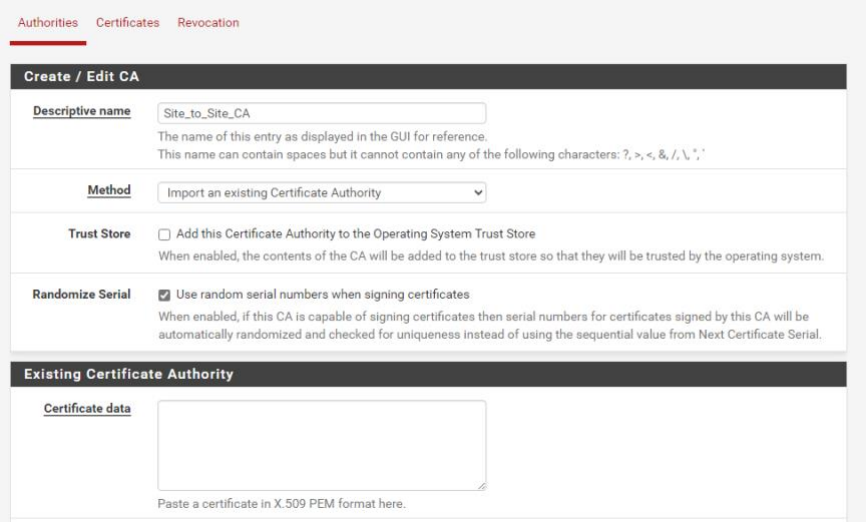
Selecione o separador Authorities e depois clique no botão ADD:



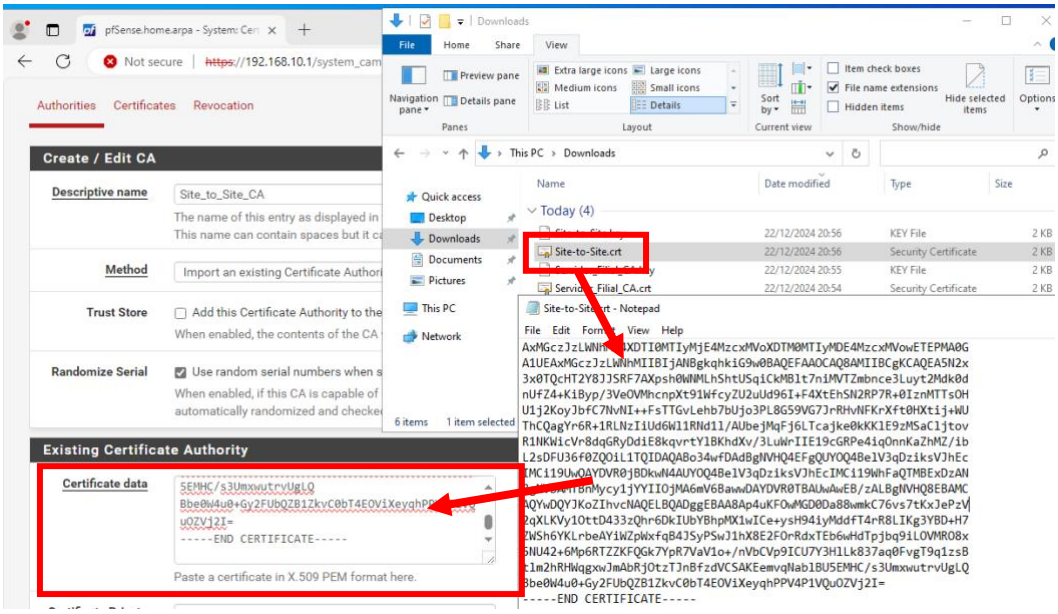
Passo 3 – Mesmo indicando que quero criar um certificado, nas propriedades internas é possível modificar a operação de criar para importar (que é o nosso objetivo, pois já exportamos essas configurações do lado do servidor).

Coloque as seguintes opções:

- **Descriptive Name**: Site_to_Site_CA
- **Method**: Import an existing Certificate Authority (ao selecionar esta opção, mais abaixo vai aparecer um nova seção/caixa para colocar a informação do certificado da entidade certificadora)
- **Randomize Serial**: ative esta opção

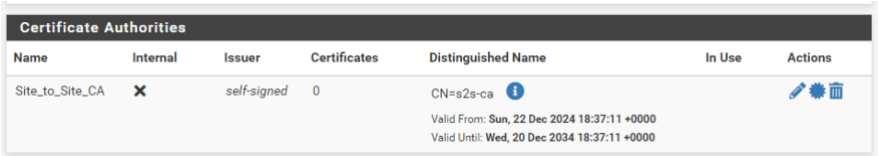


Passo 4 – Abra o ficheiro Site-to-Site.crt e copie toda a informação dentro do ficheiro para a caixa de texto do campo Certificate data:

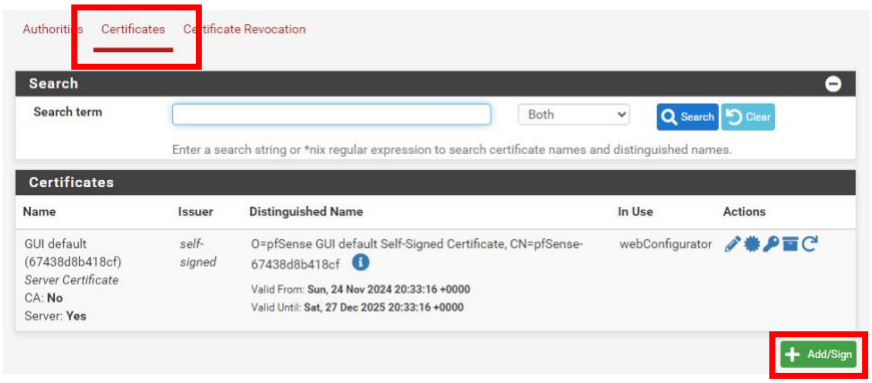


No final não esquecer de gravar as novas informações.

Resultado:

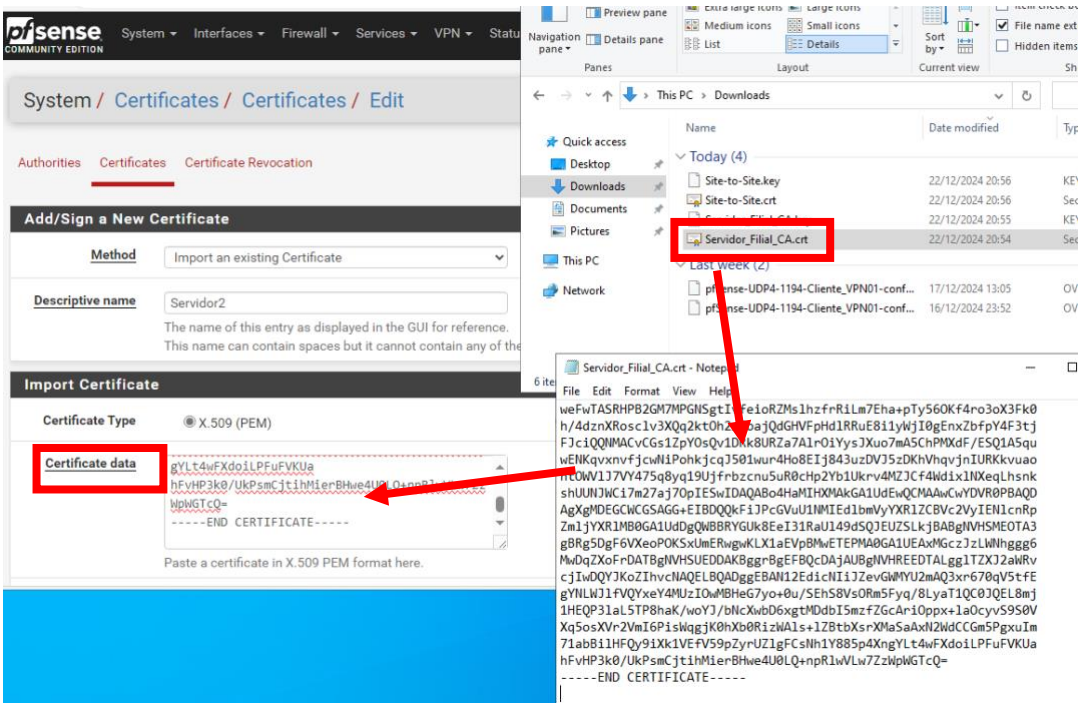


Passo 5 – Vamos importar os certificados que retirou do servidor. Vamos ao separador Certificates e carregar no botão Add/Sign:

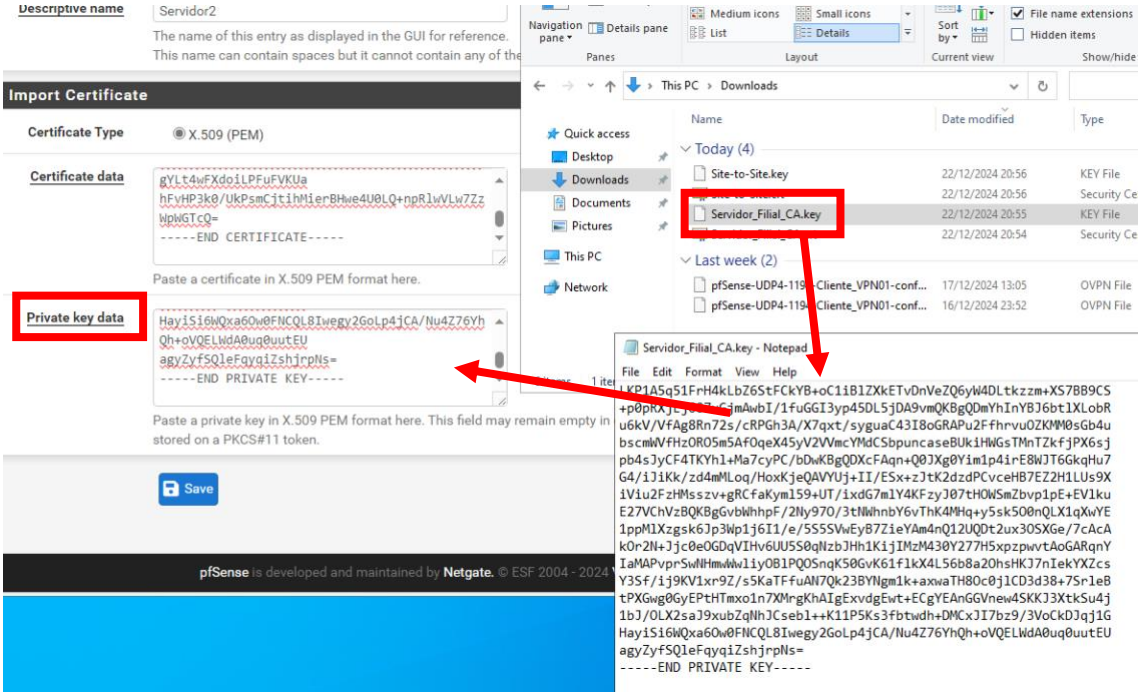


Passo 6 – Vamos importar os certificados que retirou do servidor. Coloque as seguintes opções:

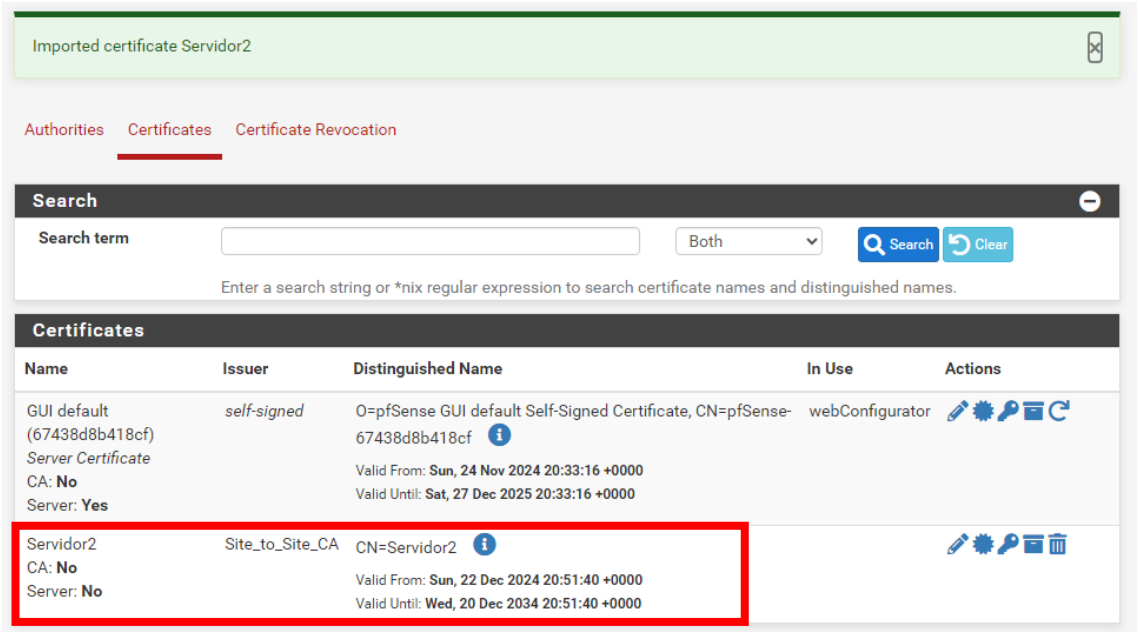
- **Method**: Import an existing Certificate (ao selecionar esta opção, mais abaixo vai aparecer um nova seção/caixa para colocar a informação do certificado)
- **Descriptive Name**: Servidor2
- Abra o ficheiro Servidor_Filial_CA.crt e copie a informação para o campo Certificate data:



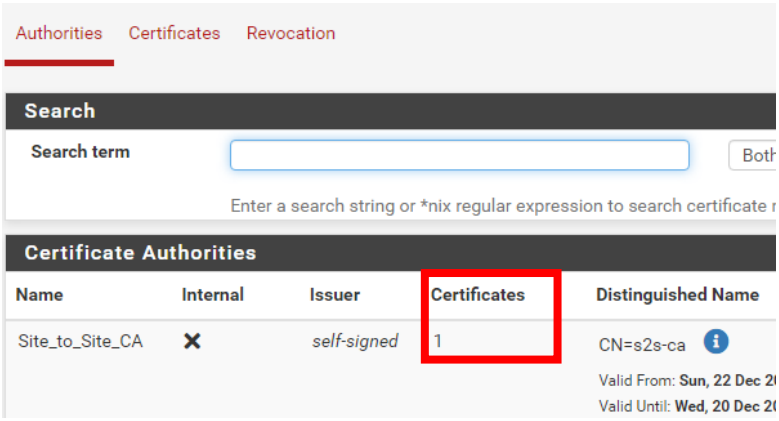
Passo 7 – Logo abaixo temos o campo Private Key data. Vamos abrir o ficheiro Servidor_filial_CA.eky e copiar a informação para esse campo:



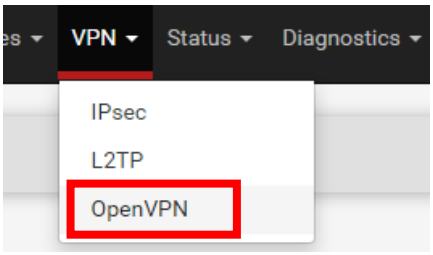
No final grave as novas alterações e veja o resultado:



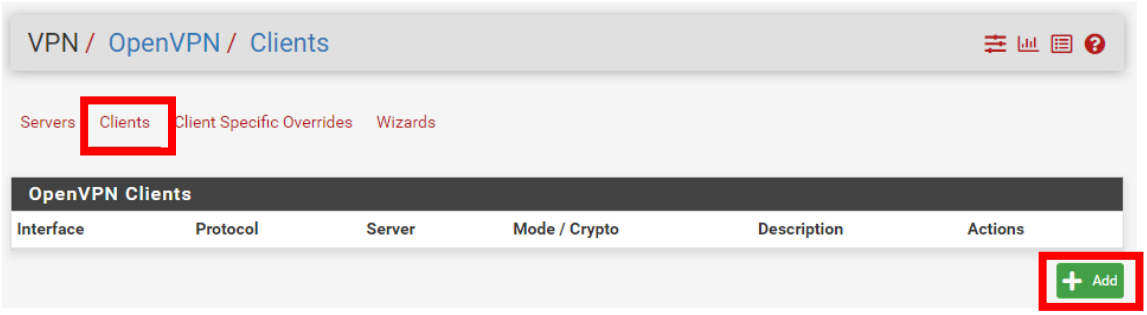
Passo 8 – Verifique que quando acabou de adicionar o certificado que importou anteriormente, o certificado da entidade autoritária acabou de associar automaticamente o novo certificado:



Passo 9 – Depois de importar os certificados, vamos criar a ligação cliente OpenVPN (para ligar com a ligação da Sede). Vamos ao menu VPN → OpenVPN

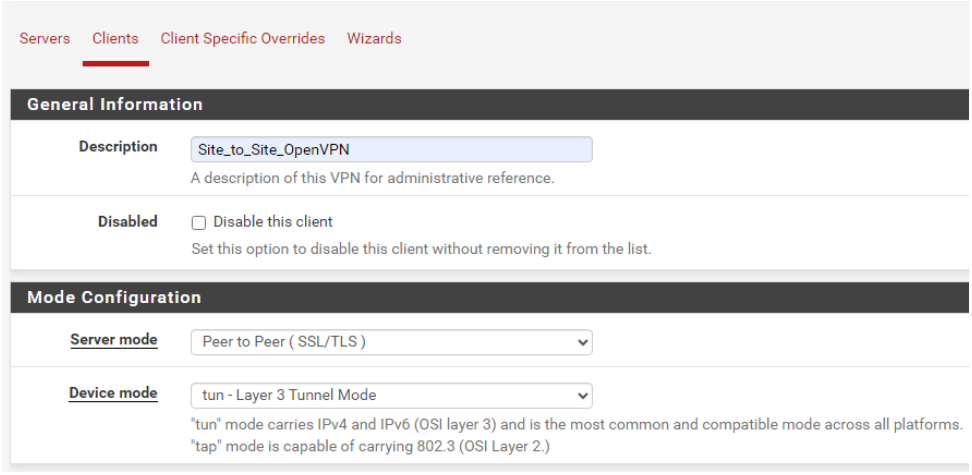


Selecione o separador Clients e clique no botão ADD:

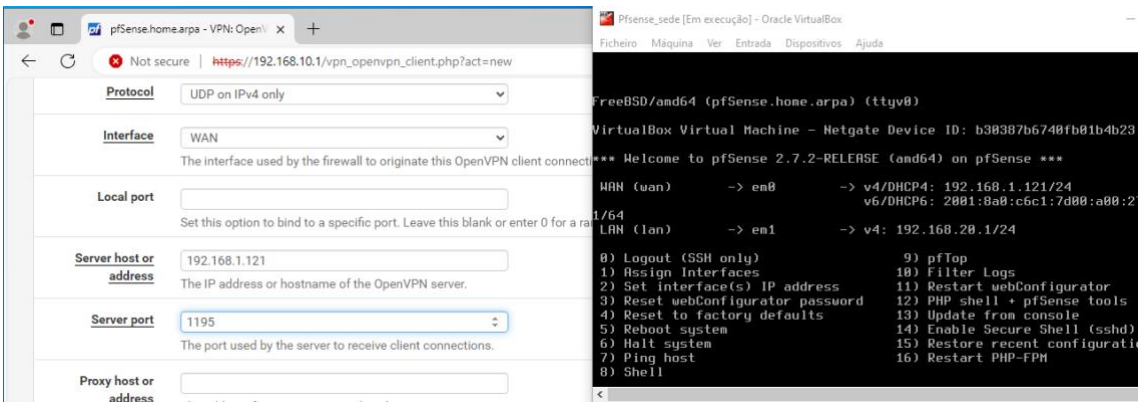


Passo 10 – Coloque as seguintes informações:

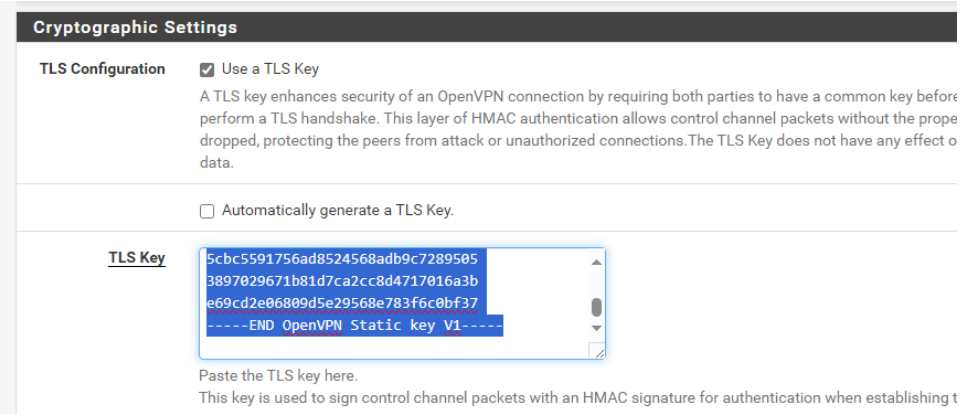
- **Description**: Site_to_Site_openVPN (o mesmo nome que deu no lado do servidor)
- **Server Mode**: Peer to Peer (SSL/TLS)
- **Device Mode**: tun – Layer 3 Tunnel Mode



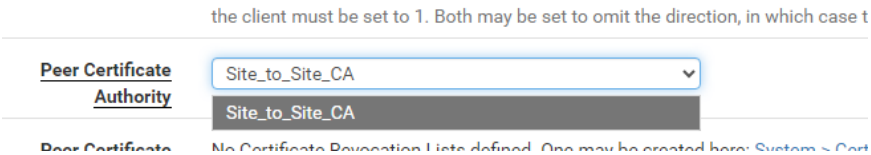
- Protocolo: UDP on IPv4 Only
- Interface: WAN
- Server host or address: 192.168.1.121 (endereço IP da rede WAN da filial)
- Server Port: 1195 (porta 1194 já está a ser utilizada no exercício anterior)



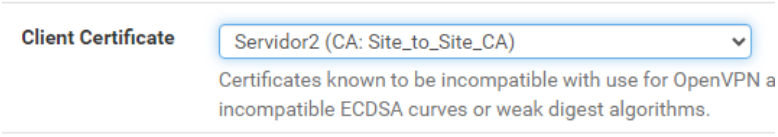
- TLS Configuration: ative esta opção
- Automatically generate a TLS Key: Desative esta opção e depois coloque a informação que copiou anteriormente para o bloco de notas para dentro do campo TLS Key (que foi realizado no passo da parte 8.1 – Passo 21):



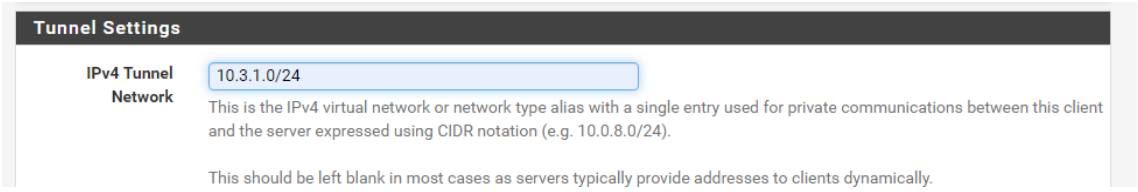
- **Peer Certificate Authority**: Site_to_Site_CA (entidade autoritária que importou do servidor)



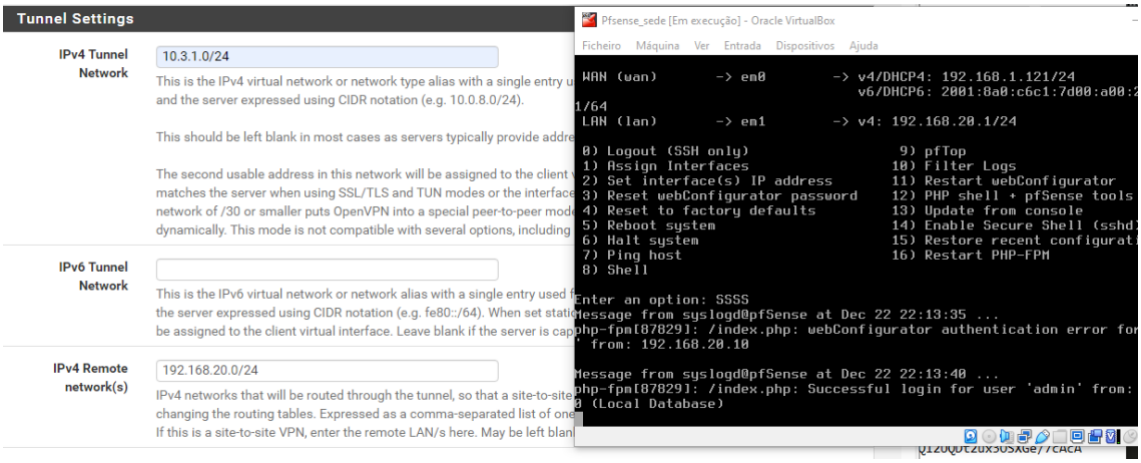
- **Client Certificate**: Servidor2 (CA: Site_to_Site_CA) (entidade autoritária e certificado que importou do servidor)



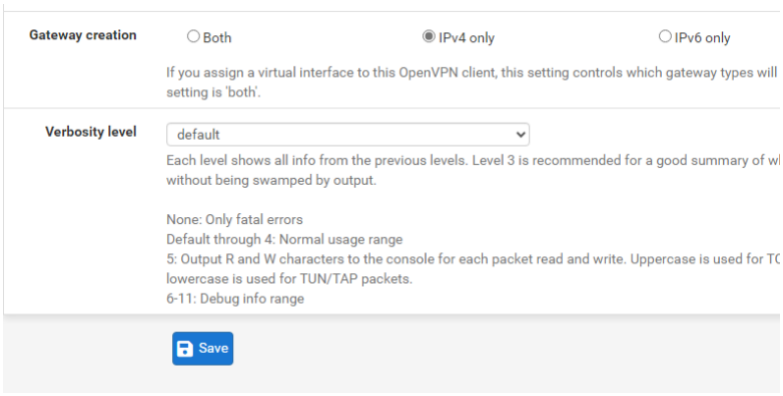
- **IPv4 Tunnel Network**: canal por onde vão navegar a ligação VPN até chegar a ambas as extremidades da LAN. Colocar o mesmo endereço IPv4 Tunnel como fez no servidor (ver Parte 8.1 - Passo 11), ou seja, o endereço 10.3.1.0/24



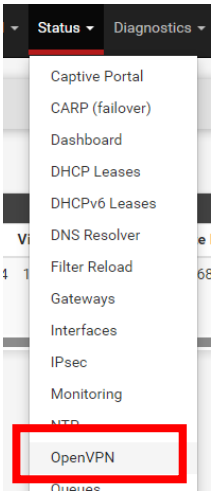
- **IPV4 Remote Network(s)**: colocar o domínio da rede LAN da máquina da firewall da SEDE e respetiva máscara de rede (neste caso é o 192.168.20.0/24) pertencente a máquina da firewall da SEDE firewall



- **Gateway creation:** IPv4 only
- **Verbosity level:** default

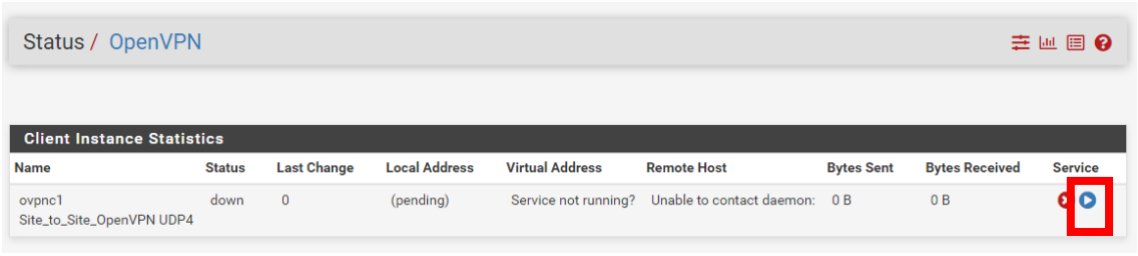


Passo 11 – Verificar se a ligação foi estabelecida. Vamos ao menu Status → OpenVPN:

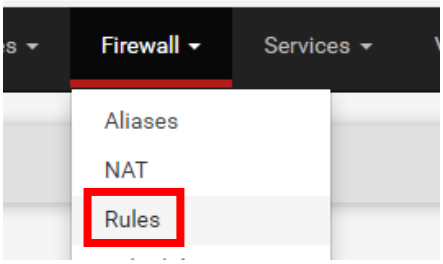




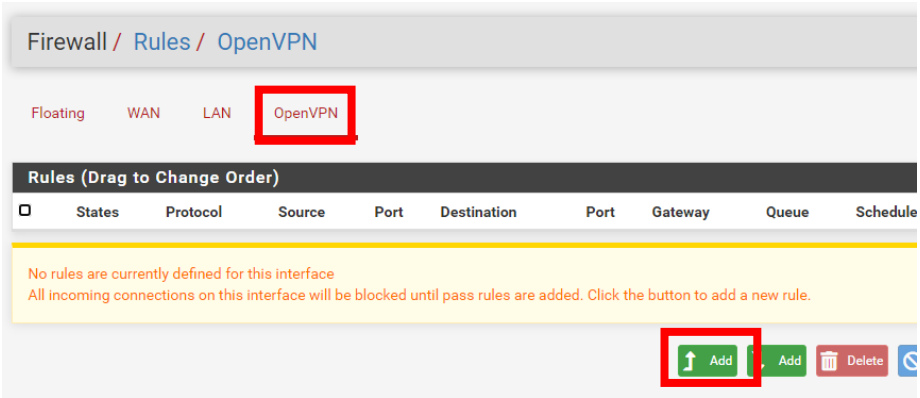
Nota Importante: por vezes o serviço pode estar parado. Clique no botão para ativar o serviço



Passo 12 – Mesmo com as configurações anteriores, ainda temos de adicionar a regra para passar o tráfico pela VPN desde o cliente até ao servidor. Como tal, vamos ao menu Firewall → Rules:



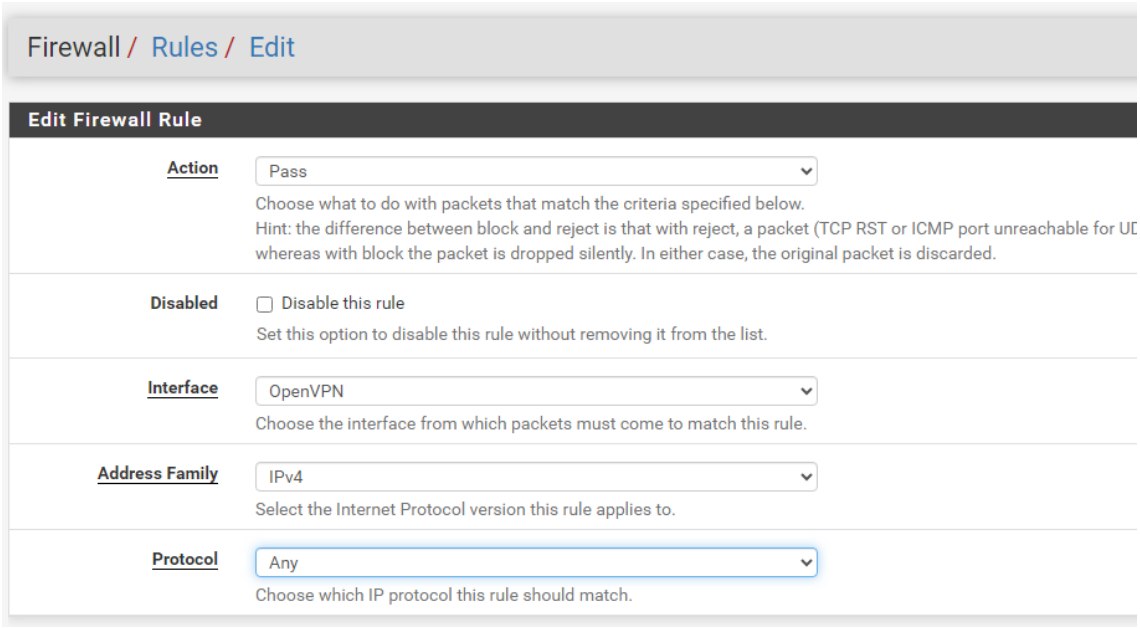
Selecionar o separador OpenVPN e clicar no botão ADD:



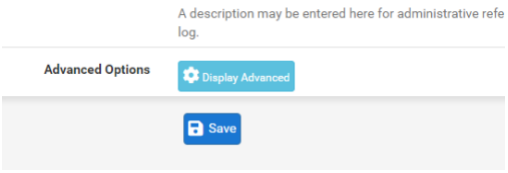
Nas regras, vamos colocar as seguintes informações:

- **Action**: Pass
- **Interface**: OpenVPN

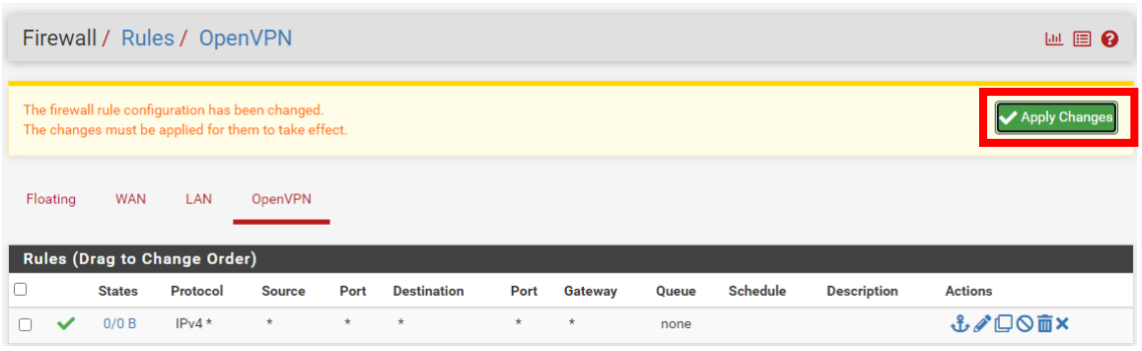
- **Address Family** IPv4
- **Protocol**: Any



No final não esqueça de gravar as novas informações.



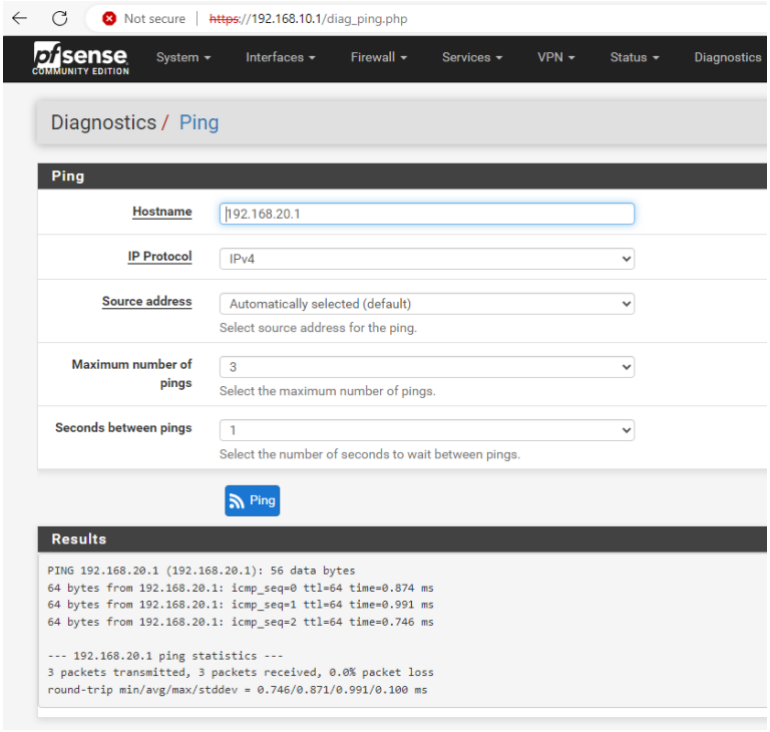
Passo 13 – Aplique as novas regras:



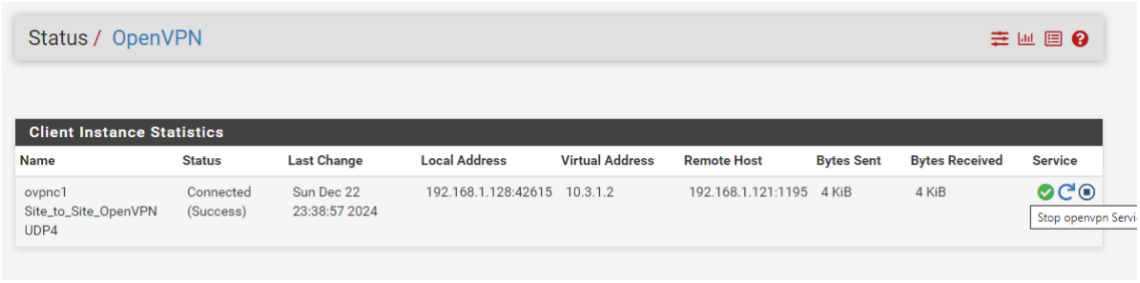
Passo 14 – Voltar a verificar o estado da OpenVPN

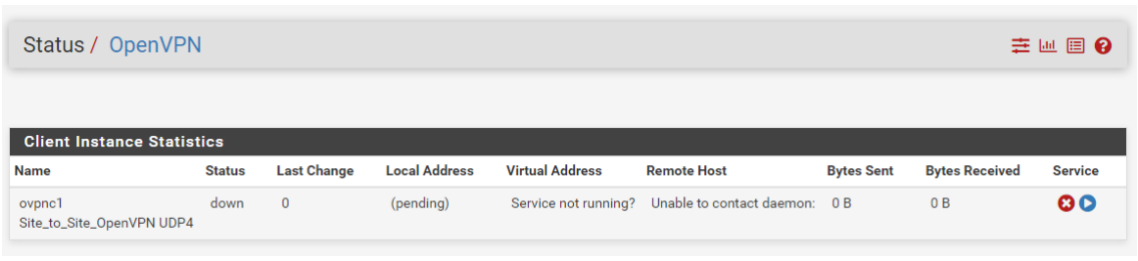


Passo 15 – Fazer ping entre se de e filial:

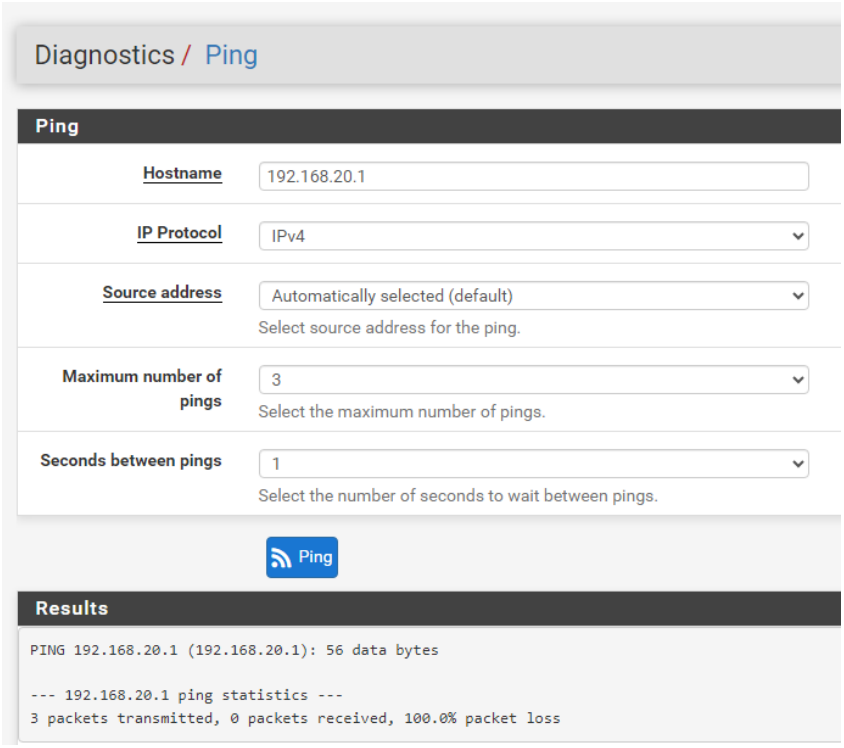


Se desligar o serviço da OpenVPN (sede-filial) veja que já não existe conexão:





Ao tentar fazer ping, não vai haver resposta:

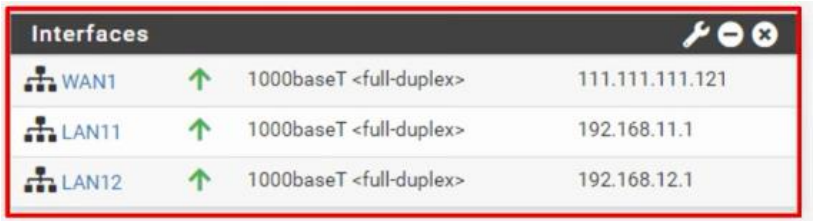


Limitar velocidade dentro da firewall



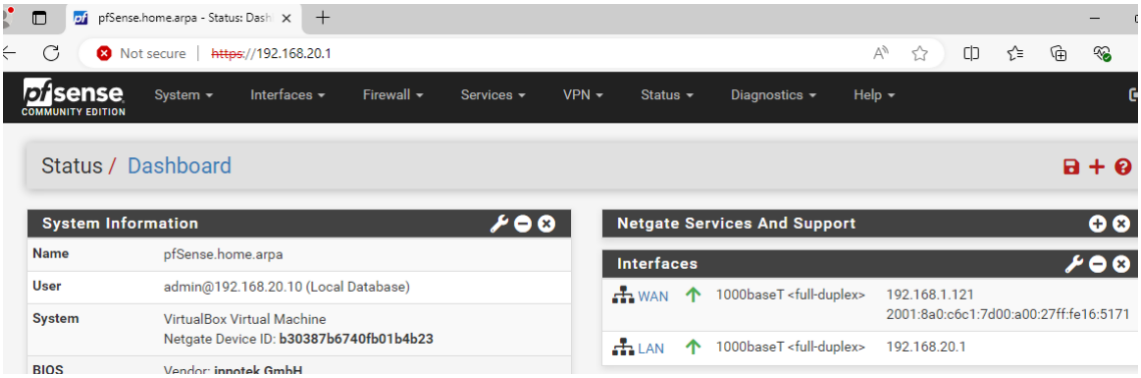
Imagine o seguinte cenário:

Temos a rede WAN que permite a entrada da internet na nossa firewall e assim comunicar com as redes internas (redes LAN, pois podemos ter mais do que uma, tal como demostra a seguinte imagem:

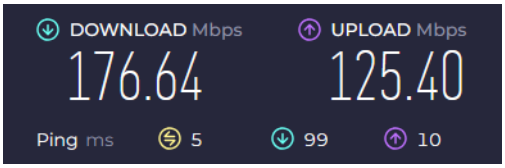


Como tal, podemos colocar limites no acesso a internet como uma norma de segurança adicional dentro da firewall.

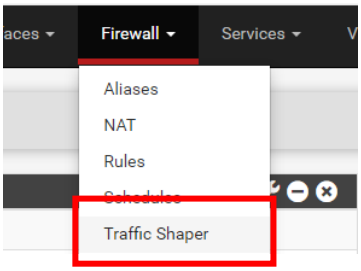
Como tal, vamos fazer os seguintes passos, mas neste caso prático, apenas vamos aplicar as regras numa rede LAN (com a máquina virtual da SEDE que temos trabalhado ao longo das fichas de trabalho):



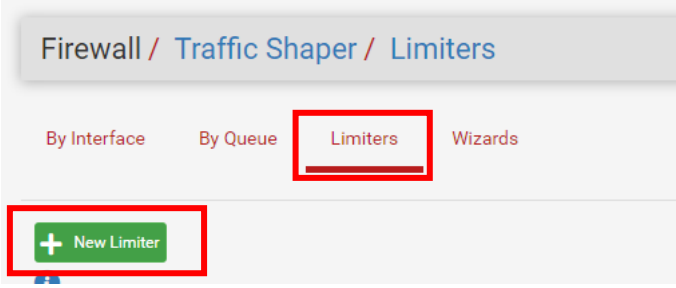
Suponha que estes são os valores da velocidade da sua Internet:



Passo 1 – Vamos até ao menu Firewall → Traffic Shaper

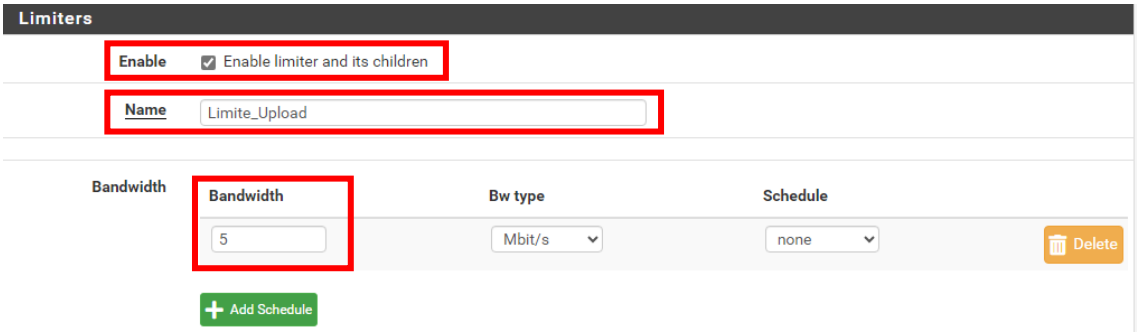


Passo 2 – Selecione o separador "Limiters" e depois carregue no botão New Limiter para adicionar uma nova limitação (neste passo apenas vamos dizer os parâmetros da configuração):



Passo 3 – Vamos criar as configurações para o Upload. Coloque as seguintes informações:

- **Enable**: ative esta opção
- **Name**: Limite_Upload
- **Brandwidth**: 5 (por defeito já vem Mbit/s)

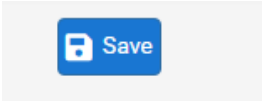


Passo 4 – No campo Mask, podemos escolher as opções "origem (source)" para definir que estamos a trabalhar o upload ou "destino (destiny)" para definir que estamos a trabalhar o download. Para tal, vamos:

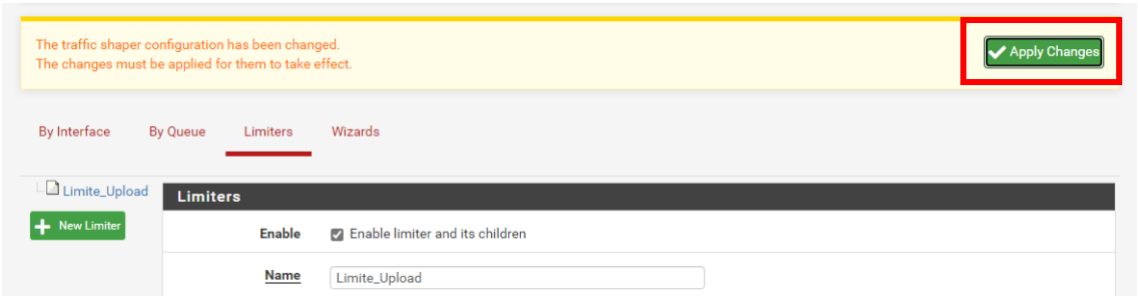
- **Mask**: selecionar a opção Source Address para indicar que quero trabalhar o Upload de dados;
  - Deixar os valores 32 e 128 para aplicar a regra em todos os hosts da LAN;
- **Description**: colocar a informação "Limitar Upload na rede LAN";



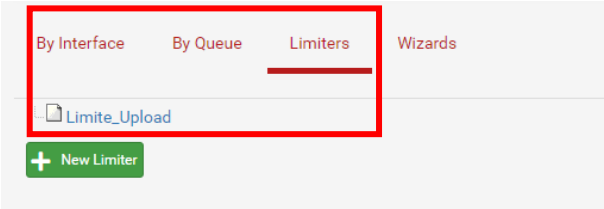
Passo 5 – Não esqueça de gravar as novas informações;



Passo 6 – Aplique as novas alterações:



Resultado da criação do limite:

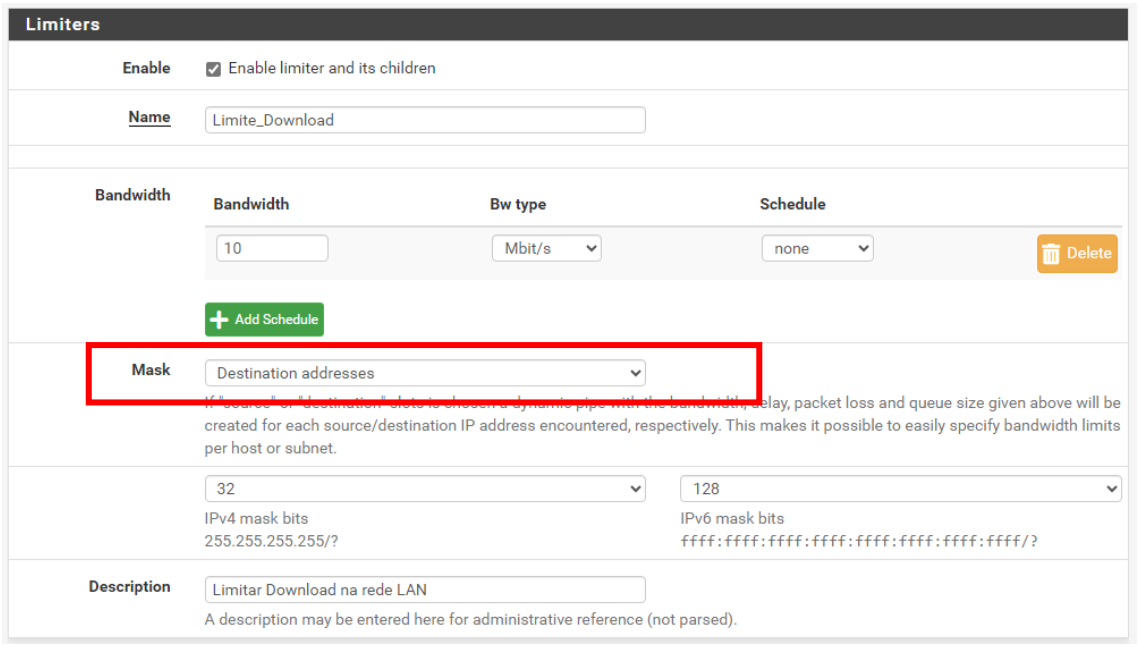


Passo 7 – Vamos fazer a mesma tarefa para o Download de ficheiros, mas com algumas modificações, em especial no campo Mask que ao contrário do Upload que usa Source Addresses o Dowload vai usar a opção Destination Addresses:

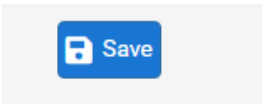
Vamos criar as configurações para o Download. Coloque as seguintes informações:

- **Enable**: ative esta opção

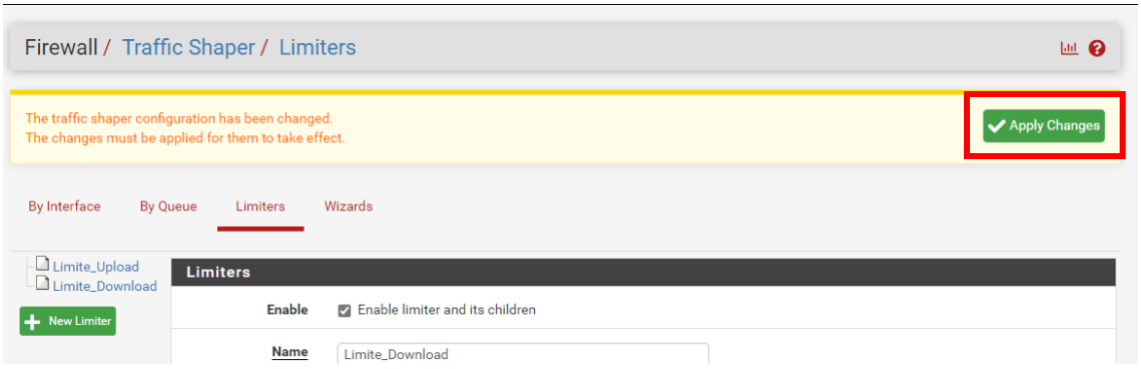
- **Name**: Limite_Download
- **Brandwidth**: 10 (por defeito já vem Mbit/s)
- **Mask**: selecionar a opção Destination Address para indicar que quero trabalhar o Download de dados;
    - Deixar os valores 32 e 128 para aplicar a regra em todos os hosts da LAN;
- **Description**: colocar a informação "Limitar Download na rede LAN";



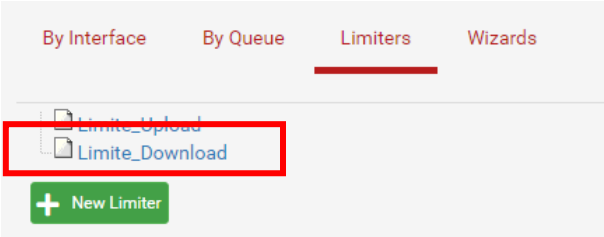
Passo 8 – Não esqueça de gravar as novas informações;



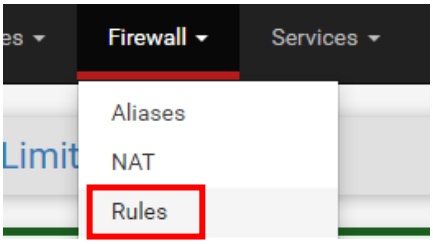
Passo 9 – Aplique as novas alterações:



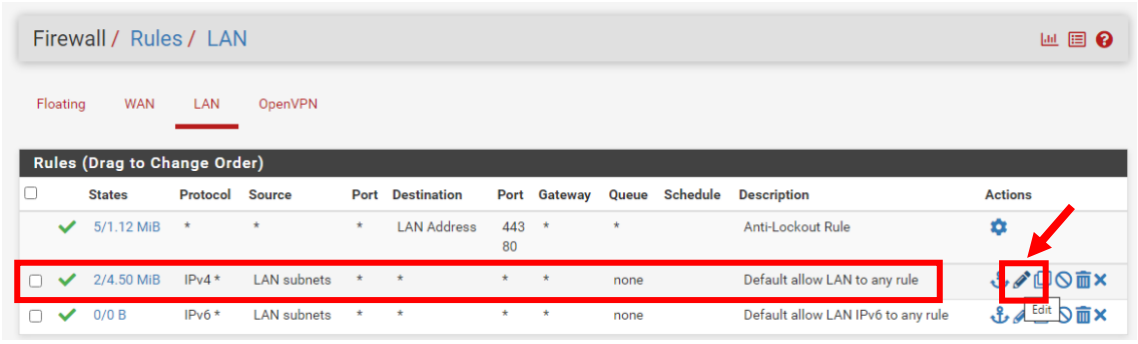
Resultado:



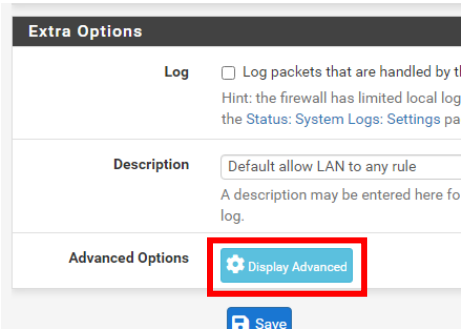
Passo 10 – No próximo passo, vamos associar a regra dos limites na rede LAN (pois apenas criamos as indicações, mas ainda falta associar as mesmas nas regras da firewall). Vamos ao menu **Firewall → Rules**:



Clique no separador LAN e de seguida, vamos clique no botão do lápis para alterar as definições da rede IPv4*:



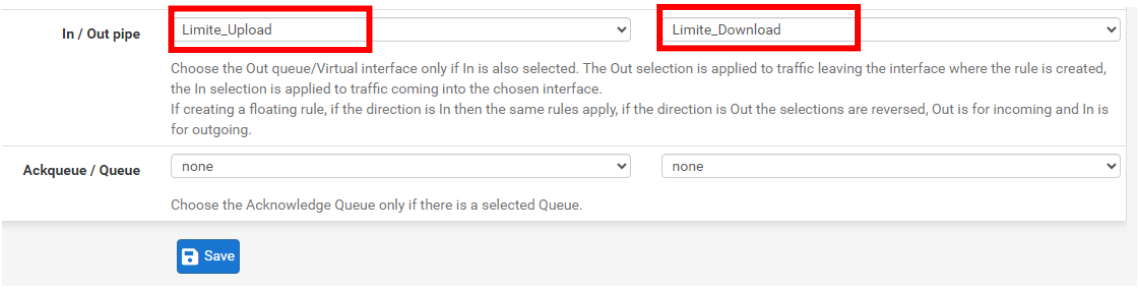
Dentro da regra, deve ir ao fundo da página e clicar no botão **Display Advanced** para aceder as propriedades avançadas das configurações da regra:



Este vai abrir várias opções, mas a que queremos está quase no fundo da página com o nome "In/Out Pipe". Deve aplicar as configurações que fez no limitador, mais especificamente:

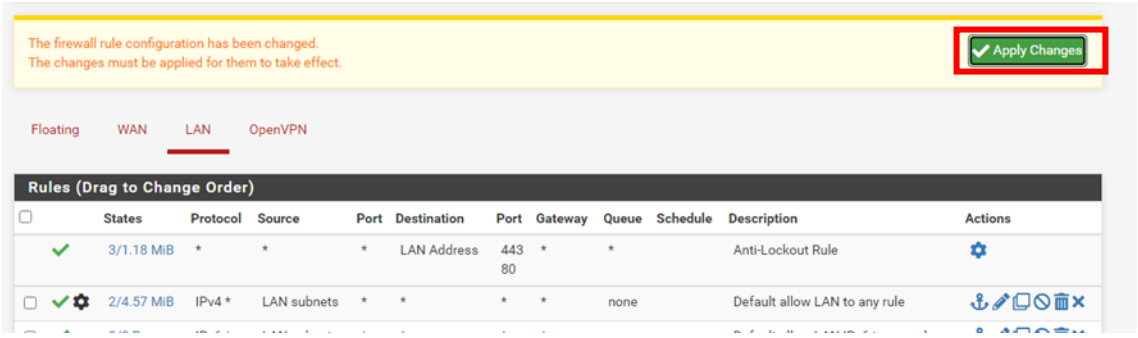
- 1º Campo → Colocar o limitador "Limite Upload"
- 2º Campo → Colocar o limitador "Limite Download"

Este por sua vez, vai definir a regra com base nos limitadores que serão impostos na rede da LAN.



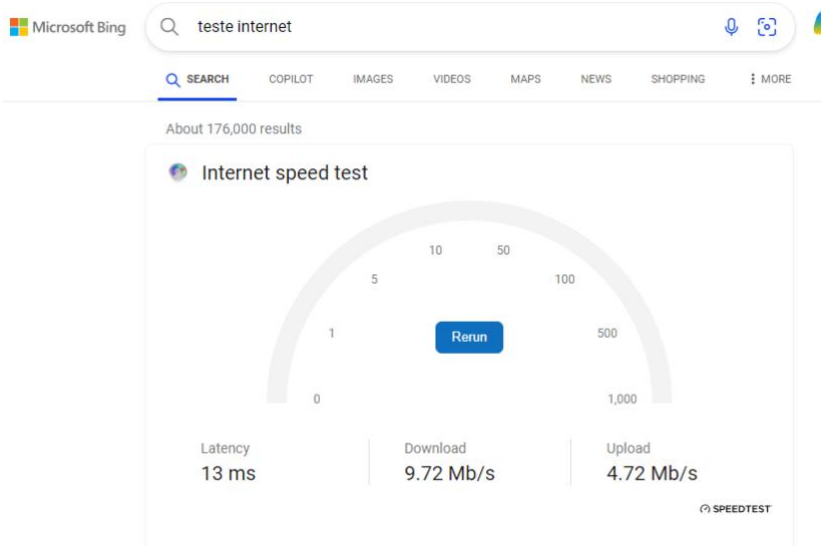
Não esquecer de gravar as novas alterações.

Passo 11 – Faça a aplicação das novas alterações e depois repare que vai aparecer uma roda dentada no início da regra:



Passo 12 – Teste a ligação da LAN na máquina virtual (que esteja ligada na rede LAN):

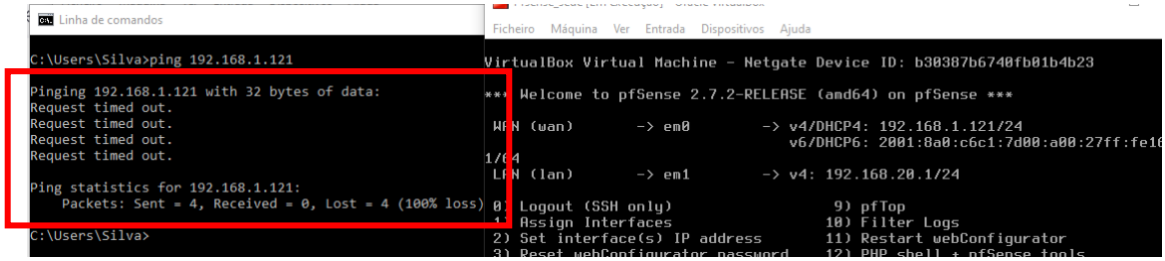
FICHA TRABALHO 4
PARTE 2



Permitir ping na rede WAN

De notar que, por defeito a firewall do PFsense bloqueia rodos os pacotes "ping", incluídos protocolos ICMP, por razoes de segurança. Contudo, pode haver situações que seja necessário verificar as conexões com a firewall, como por exemplo, nos programas de monitorização, como o Zabbix para verificar se a firewall está online ou offline.

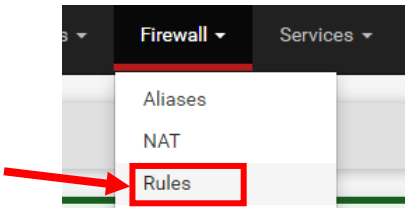
Passo 1 – Abra uma linha de comandos (cmd) e faça ping na firewall da sede (neste exemplo o IP é o 192.168.1.121):



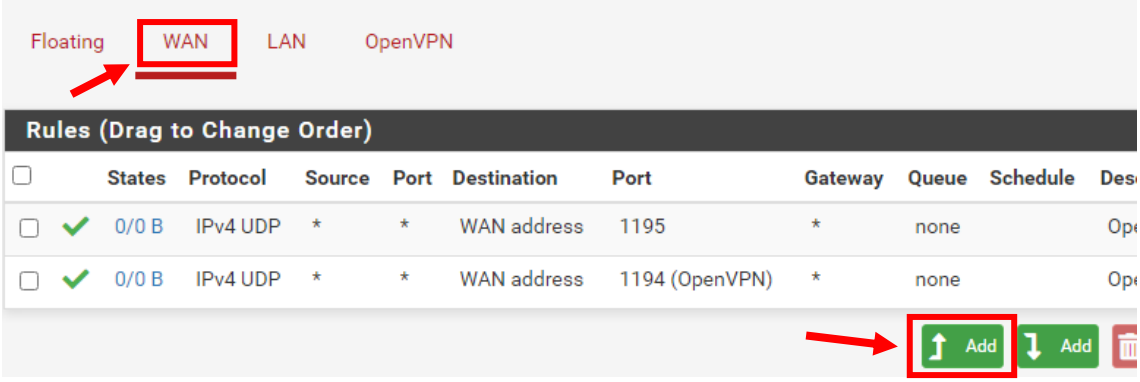
Repare que a resposta foi negativa e os pacotes não obtiveram qualquer resposta!

Vamos adicionar uma nova regra na interface WAN para permitir o protocolo ICMP:

Passo 1 – Vamos ao menu da firewall e selecione as opções Firewall → Rules:

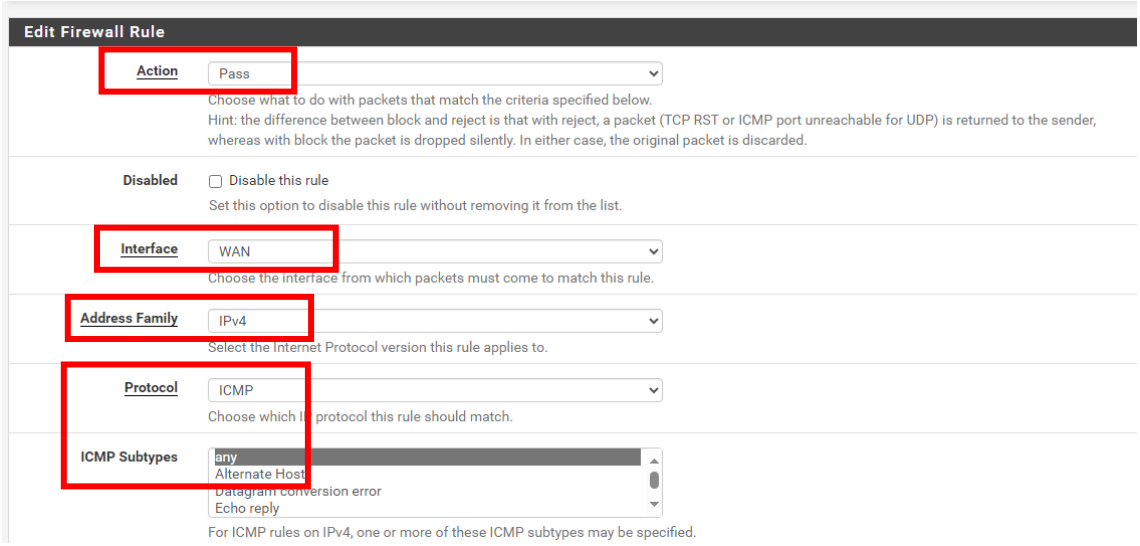


Passo 2 – Selecione o separador WAN e clique no botão ADD para adicionar nova regra:



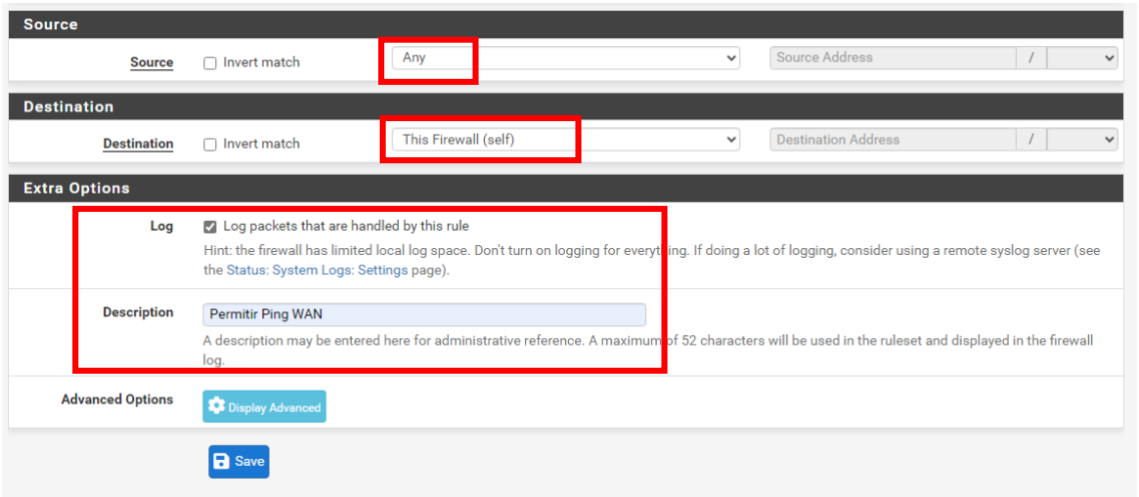
Passo 3 – Coloque as seguintes opções:

- **Action**: Pass
- **Interface**: WAN
- **Address Family**: IPv4
- **Protocol**: ICMP
- **ICMP Subtypes**: Any



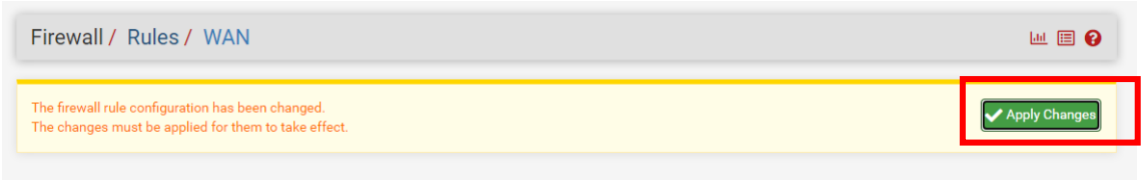
Passo 4 – Nas próximas seções deve fazer as seguintes ações:

- Seção Origem (Source) deve selecionar a opção ANY;
- Seção Destino (Destination), deve selecionar a opção This Firewall (self);
- Seção Extra Options:
  - Selecionar a opção Log, para permitir os registos de atividade;
  - Colocar a descrição "Permitir Ping Wan";



No final não esqueça de gravar as novas alterações.

Passo 5 – Aplique as novas alterações:



Passo 6 – Recebida a confirmação da aplicação da regra, vamos fazer novamente o PING ao servidor da firewall da SEDE e veja a reposta com sucesso:

