



Manual VPN do P.PORTO – Acesso remoto aos serviços de rede do P.PORTO

↩ Versão	↩ Data	↩ Autores	↩ Aprovação (Sigla e data)	↩ Descrição
1.0	2016/04/26	Bruno Silva, Serviços da Presidência		Versão Inicial
1.1	2016/12/16	Bruno Silva, Serviços da Presidência	"jestrela@sc" a 2016/12/19	Alterações à estrutura do manual; Adicionada a configuração no Windows 10
1.2	2017/01/03	Bruno Silva, Serviços da Presidência	"jestrela@sc" a 2017/01/23	Corrigida a configuração para o Windows 10
1.4	2020/04/30	Ricardo Cardoso. Serviços da Presidência		Adicionada informações para SO's Mac recentes
1.5	2023/01/13	Ricardo Cardoso. Serviços da Presidência		Reformulação do Documento para a Fortinet



ÍNDICE

ÍNDICE.....	2
1. Introdução.....	3
2. Instalação e Configuração	4
2.1. Definições Gerais de configuração.....	4
2.1.1. Perfis registados	4
2.1.2. Perfis Não Registados	4
2.2. Windows 10 e Superior	5
2.2.1. Instalação software FortiClient.....	5
2.2.2. Configuração software FortiClient.....	6
2.3. macOS.....	14
2.3.1. macOS Catalina 10.15.....	14
2.3.2. macOS Big Sur 11.....	25
2.3.3. macOS Monterey 12.....	31
2.4. Linux	36
2.4.1. Ubuntu e derivados	37

1. Introdução

O serviço de Rede Privada Virtual (VPN – *Virtual Private Network*), disponibilizado pelo P.PORTO, permite que utilizadores registados acedam remotamente a recursos da rede do P.PORTO. O tipo de acesso é definido pelo perfil atribuído individualmente ou a um determinado grupo de utilizadores.

Após a ativação do serviço, o computador remoto, i.e. do utilizador, passa a efetuar as ligações para a Internet através da rede do P.PORTO. Todas as ligações entre o computador remoto e a rede do P.PORTO passam a ser efetuadas de forma encriptada.

Para utilizar o serviço de VPN é necessário possuir e utilizar as credenciais (utilizador e palavra-passe) que atempadamente lhe foram atribuídas pelo P.PORTO, incluindo as suas Unidades Orgânicas (UO).

2. Instalação e Configuração

Para a configuração da VPN disponibilizada pelo P.PORTO é necessária a instalação no computador do utilizador de um software específico, denominado genericamente de Cliente VPN, para o estabelecimento de VPNs. Para este efeito, no caso do P.PORTO é exigida a utilização do software FortiClient disponibilizado pela empresa Fortinet¹.

2.1. Definições Gerais de configuração

A luz do que já existia com a vpn da Checkpoint, existem 2 modos de acessos com a VPN.

Perfis registados: contas de funcionários, docentes que tem acessos privilegiados aos sistemas internos do P.Porto.

Perfis não registados: são sobretudo contas de alunos e ou utilizadores não registados apenas com acessos genéricos aos sistemas internos do P.Porto

Qualquer que seja o tipo de acesso, o acesso carece sempre da autenticação com a conta do P.Porto.

Assim sendo, agora com a nova VPN da Fortinet, existem 2 conjuntos de configurações distintas uma para cada tipo de acesso.

Estas configurações serão utilizadas na configuração de clientes nativos mais a frente neste manual.

2.1.1. Perfis registados

Para perfis registados, a configuração é a seguinte:

- Endereço do Servidor: vpns.sl.ipp.pt
- Segredo Partilhado (Pre-Shared key): qrml2fpa8.@L?0IHKi1\
- Nome do grupo: VPN_REGISTERED
- Utilizador: email do P.Porto
- Password: password do email do P.Porto

2.1.2. Perfis Não Registados

Para não perfis registados, a configuração é a seguinte:

- Endereço do Servidor: vpns.sl.ipp.pt
- Segredo Partilhado (Pre-Shared key): u0;w/7uT0`#D43YTn6~e
- Nome do grupo: VPN_GENERIC
- Utilizador: email do P.Porto
- Password: password do email do P.Porto

¹ <https://www.fortinet.com>

2.2. Windows 10 e Superior

2.2.1. Instalação software FortiClient

O primeiro passo é descarregar (*download*) o software FortiClient VPN para Windows , disponível neste [link direto²](#), ou pela página geral da Fortinet³ (cf. Figura 1).

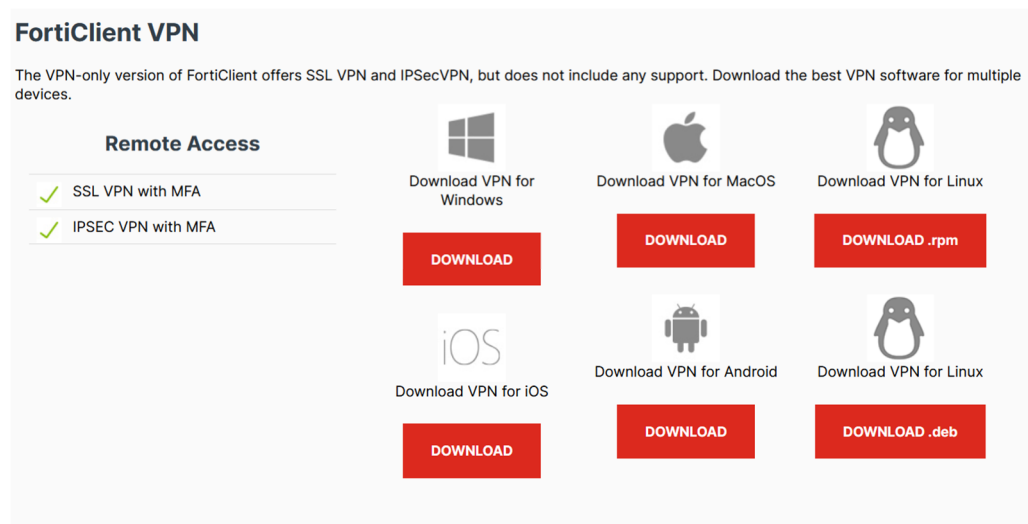


Figura 1 – Sistemas operativos suportados para instalação de Forticlient VPN.



Chamada de atenção!

Na página geral da Fortinet existem vários clientes! Para o caso, deve ser utilizado o FortiClient VPN que está ao meio da página

Depois de ter concluído com sucesso o download do FortiClient, deve proceder à sua instalação através do ficheiro que ficou disponível na pasta das Transferências. O nome deste ficheiro, será algo como:

- “FortiClientOnlineInstaller.exe” para o sistema operativo Windows;

A instalação é normalmente iniciada através de um duplo *click* no respetivo ficheiro. Durante a instalação deve seguir as indicações apresentada por omissão. Desde já, salienta-se que este processo, nalgumas circunstâncias, pode demorar algum tempo.

Findo o processo de instalação com sucesso, a aplicação FortiClient ficará em execução na bandeja do sistema (*system tray*).

² <https://links.fortinet.com/forticlient/win/vpnagent>

³ <https://www.fortinet.com/support/product-downloads#vpn>

2.2.2. Configuração software FortiClient

Na página de internet onde este manual está disponível⁴, estão também disponíveis dois ficheiros de configuração:

- *perfilRegistado.conf* – destinado a utilizadores da comunidade P.PORTO com acessos privilegiados tais como, por exemplo, acesso remoto a um posto de trabalho ou acesso a um servidor web para carregamento de ficheiros;
- *perfilNãoRegitado.conf* – destinado a todos os restantes utilizadores da comunidade P.PORTO.

Antes de prosseguir, o utilizador deve efetuar o *download* do ficheiro que se enquadra no seu perfil. Em caso de dúvida, deve contactar os serviços informáticos de suporte existentes no P.PORTO.



Ficheiro a utilizar

A utilização de um ficheiro de configuração inadequado levará, em último recurso, a utilizar o serviço de VPN do P.PORTO com restrições de acesso não pretendidas ou até mesmo a não conseguir utilizar de todo o serviço de VPN do P.PORTO.

Após o descarregamento do ficheiro de configuração adequado, para proceder à configuração da ligação VPN à rede do P.PORTO, deve aceder ao *icon* do FortiClient na bandeja do sistema e seleccionar a opção "**Open FortiClient Console**".

Primeiramente, surgirá uma janela a solicitar a confirmação de que o cliente é um software gratuito e, com suporte limitado. Deve ser colocado o visto na caixa de seleção e deveser clicado no botão "I accept" cf. Figura 2

4

<https://www.ipp.pt/faqs/index.php?sid=571129&lang=pt&action=artikel&cat=2&id=1&artlang=p/index.php?sid=571129&lang=pt&action=artikel&cat=2&id=1&artlang=pt>

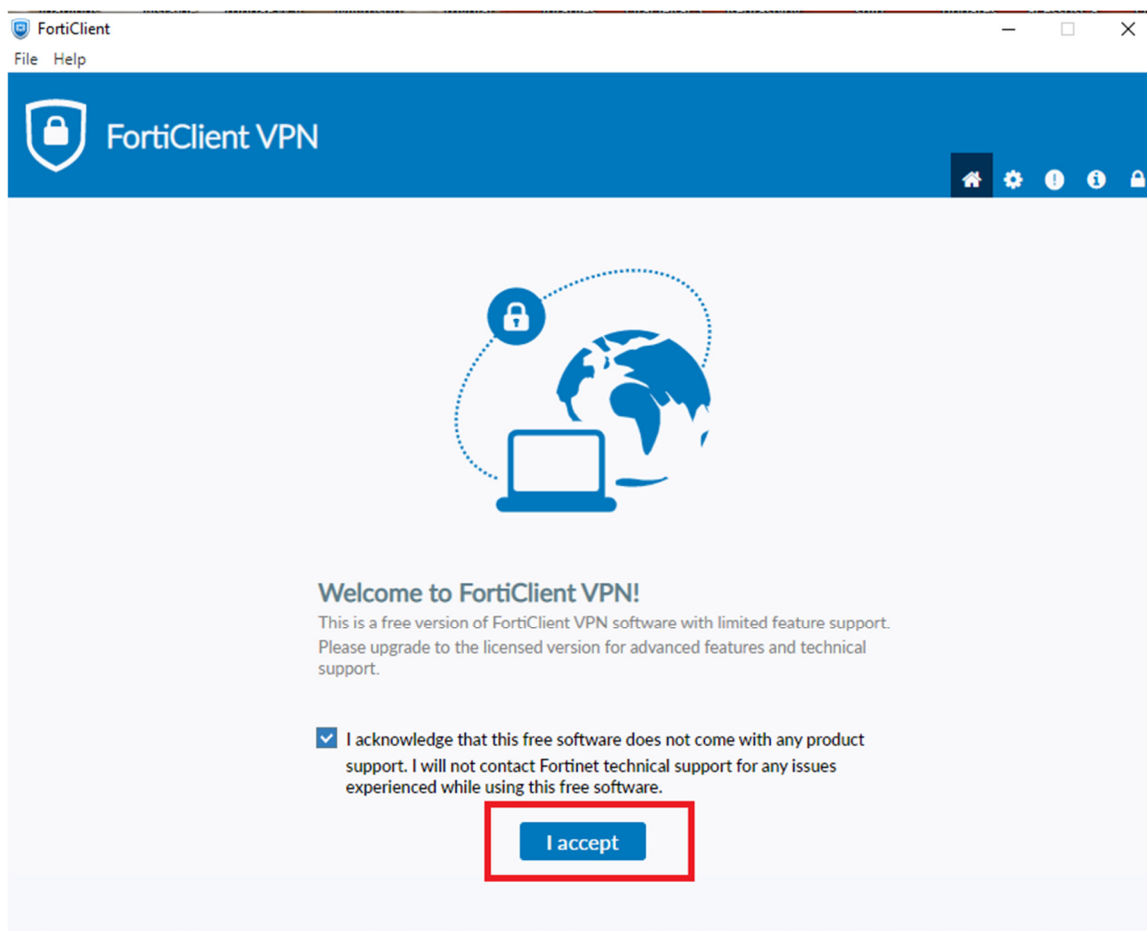


Figura 2 – Aceitação das condições do cliente da Fortinet

De seguida surgirá uma nova janela, na qual deverá selecionar a opção ***“Unlock Settings”***, clicando no ícone do cadeado disponível no canto superior direito (cf. Figura 3). Em seguida, deve selecionar a opção ***“Settings”*** clicando no ícone da roda dentada e, logo depois a opção ***“Restore”*** (cf. Figura 4).

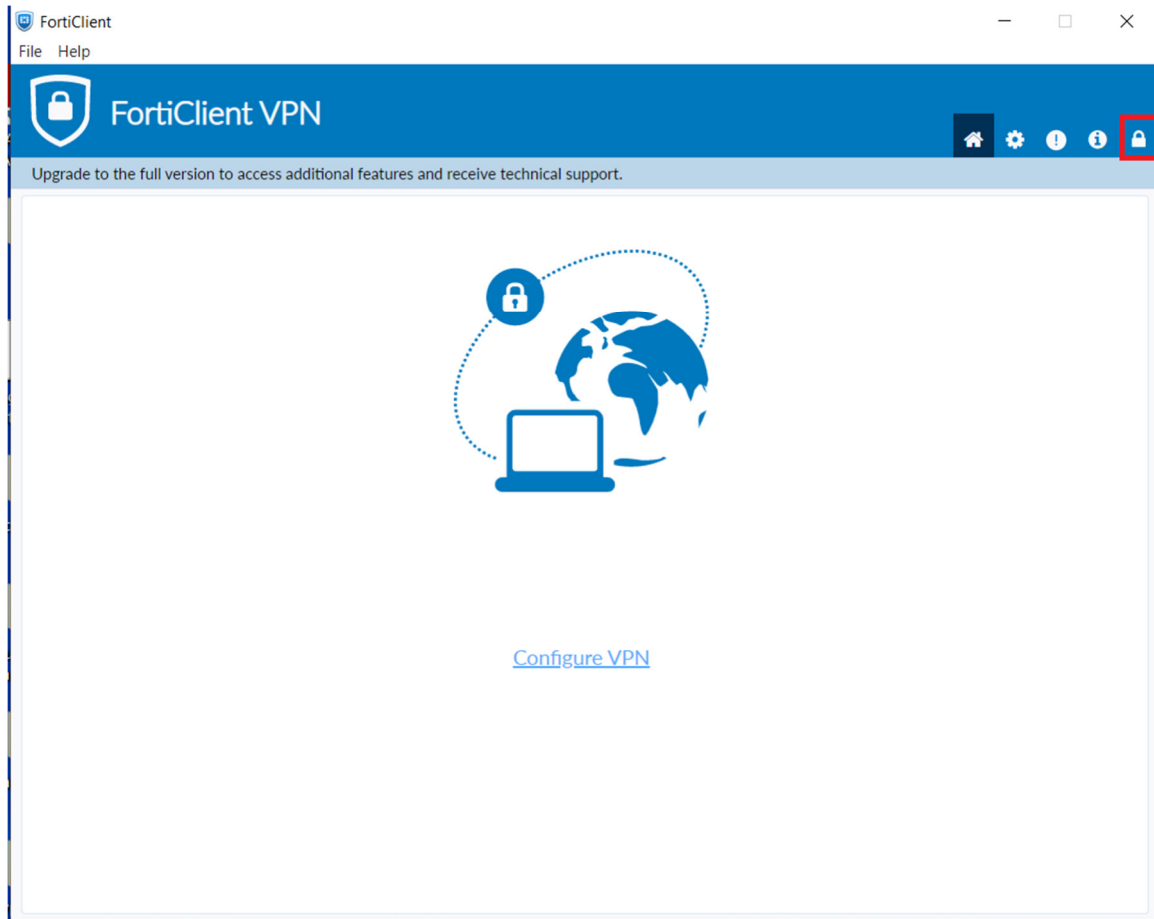


Figura 3 – Opção “Unlock Settings” no Forticlient

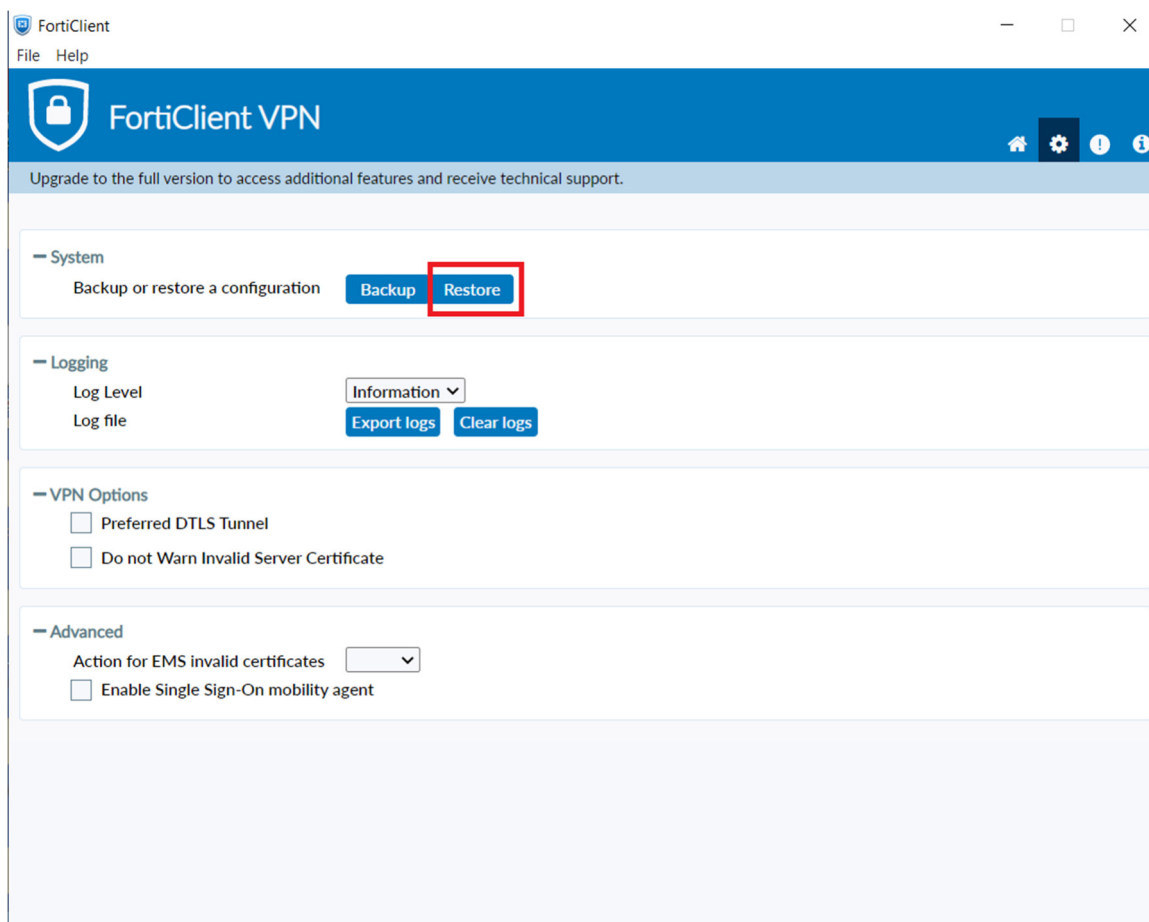


Figura 4 – Opções “Settings” e “Restore” no Forticlient

Agora, selecione o ficheiro de configuração anteriormente descarregado, insira a palavra-passe: **Fort134\$#** e selecione a opção **OK**. Imediatamente, deverá aparecer a mensagem que indica que o ficheiro foi importado corretamente (cf. Figura 5 e Figura 6).

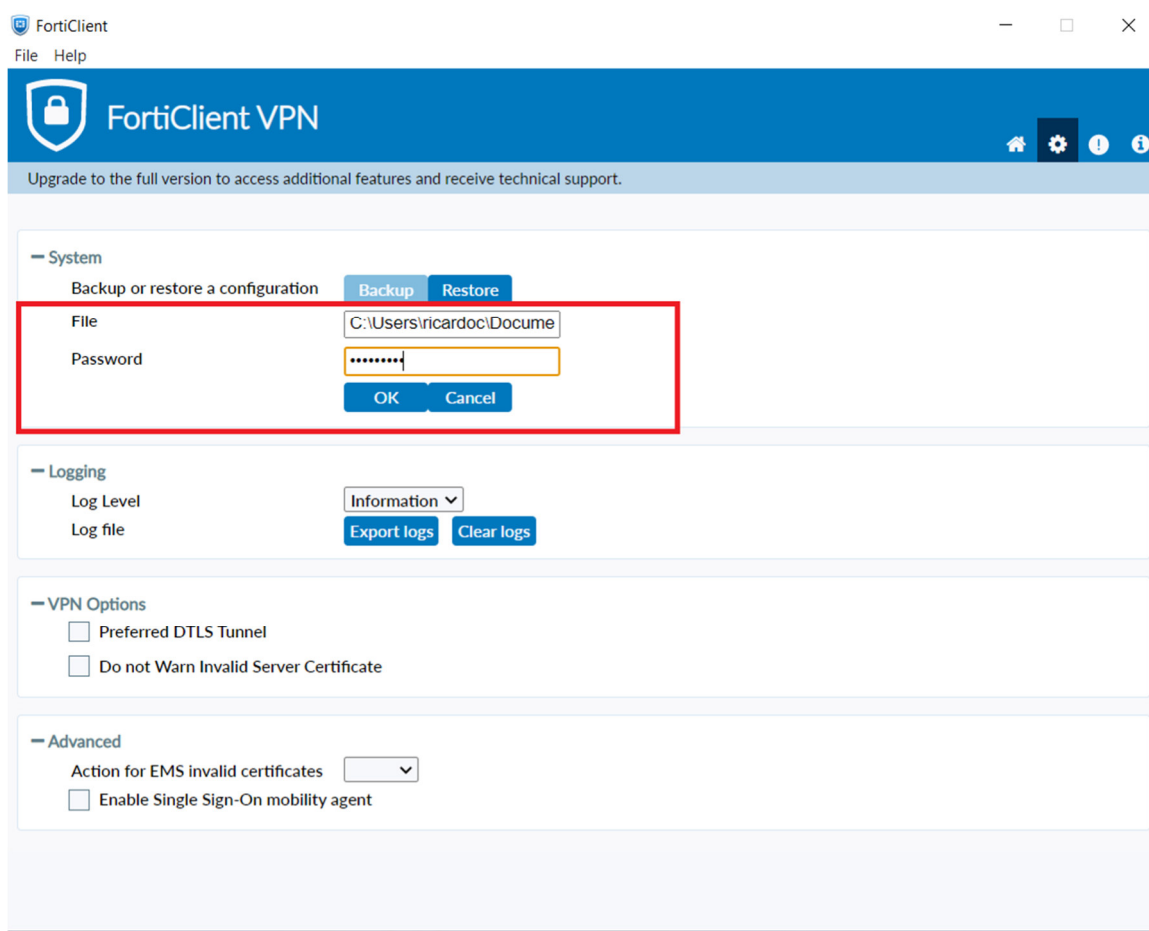


Figura 5 – Introdução de dados na opção "Restore" no Forticlient



Chamada de atenção!

O ficheiro a importar deve ser selecionado de acordo com o tipo de utilizador. Ou seja, o ficheiro *perfilRegistado.conf* apenas serve para utilizadores registados e o ficheiro *perfilNaoRegistado.conf* para todos os restantes utilizadores.

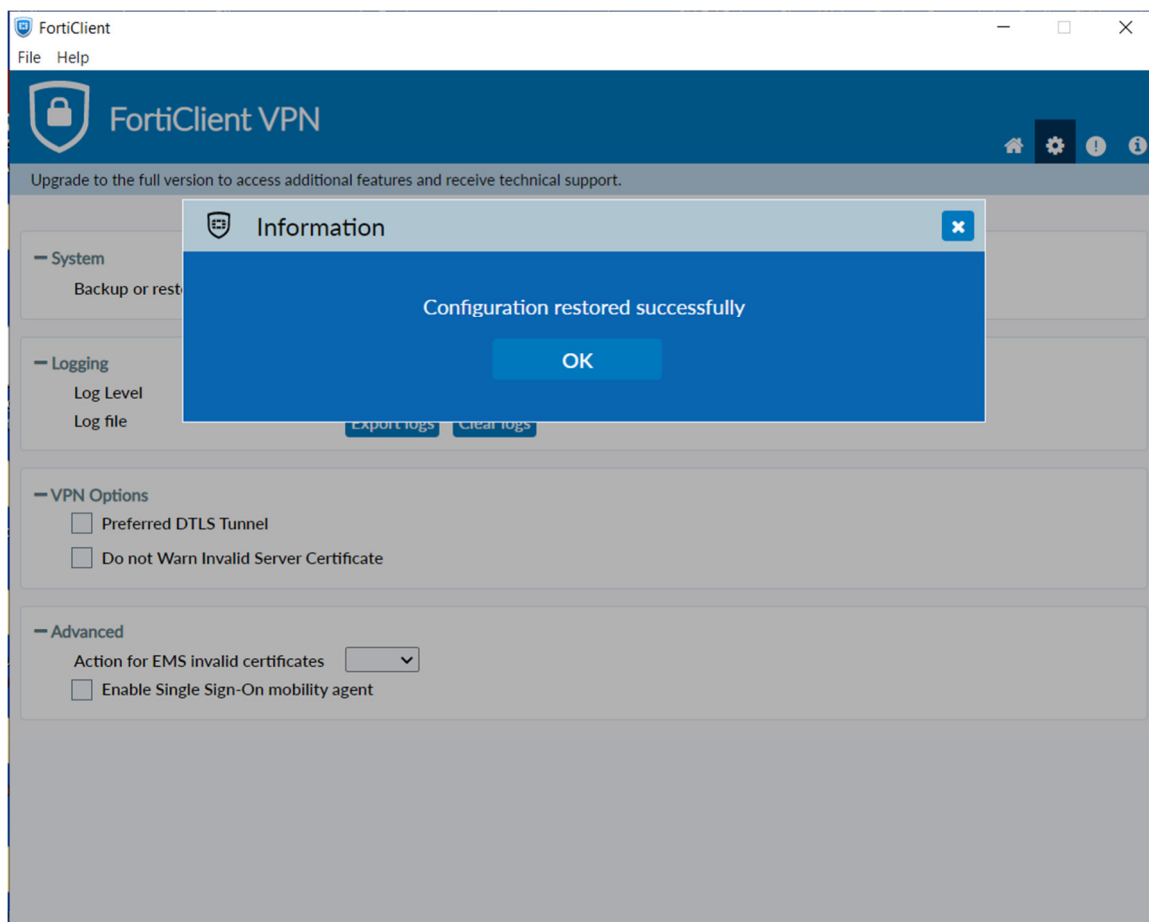


Figura 6 – Ficheiro de configuração importado com sucesso.

Posto isto, deve ser clicado no ícone da casa, no canto superior direito cf. Figura 7, de seguida, devem ser introduzidos os seus dados de autenticação (Utilizador e Palavra-Passe) e ligar a VPN, utilizando o botão **Connect**(cf. Figura 8).

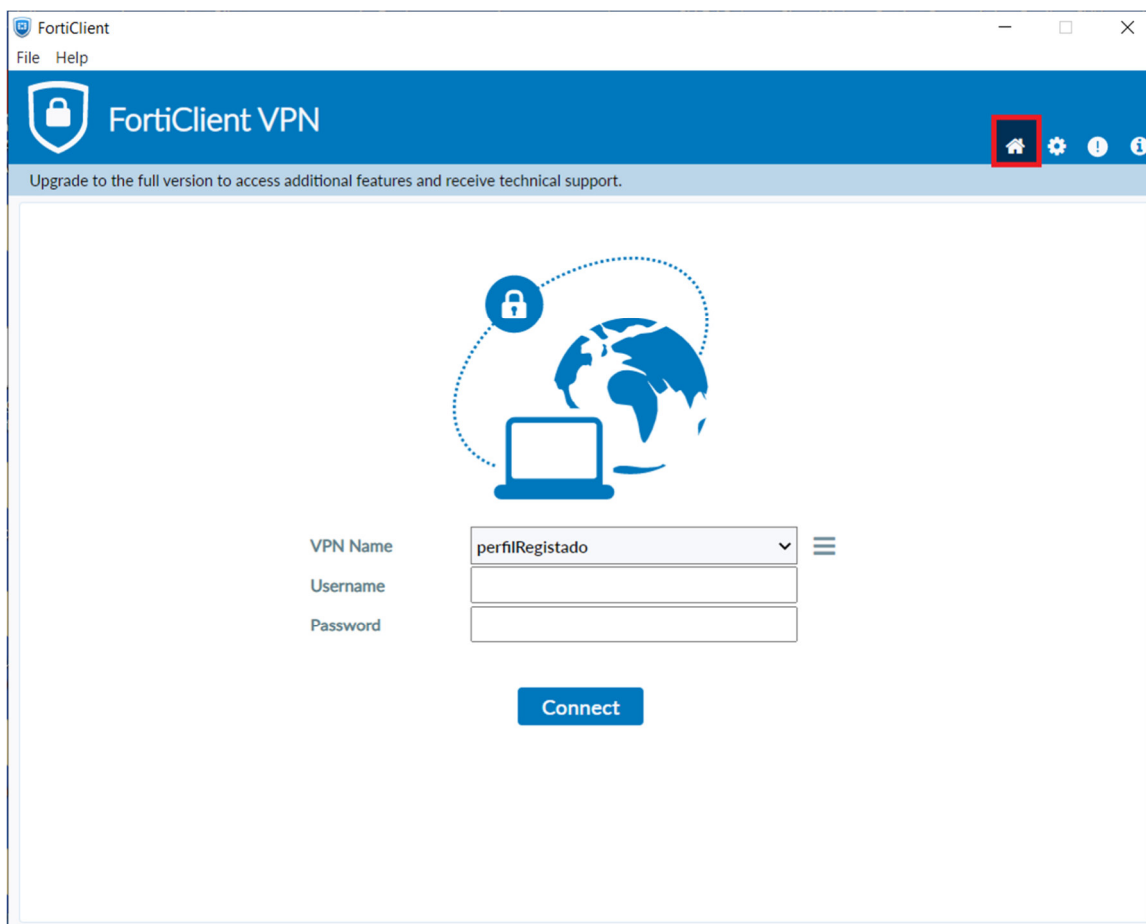


Figura 7 – Janela de introdução de credenciais da VPN

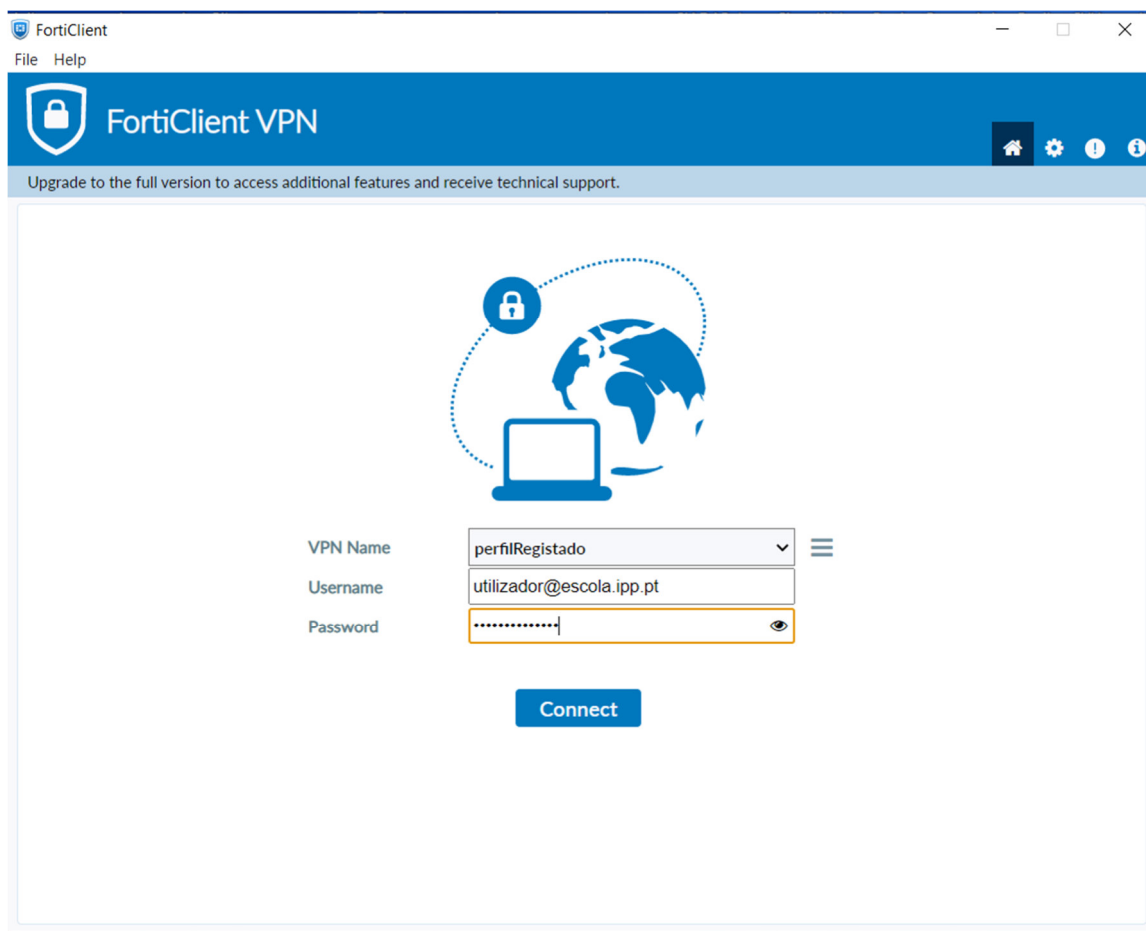


Figura 8 – Estabelecer a conexão ao serviço VPN com o Forticlient

Por fim, pode verificar que a ligação ao serviço de VPN do P.PORTO se encontra ativa abrindo a aplicação Forticlient (cf. Figura 9).

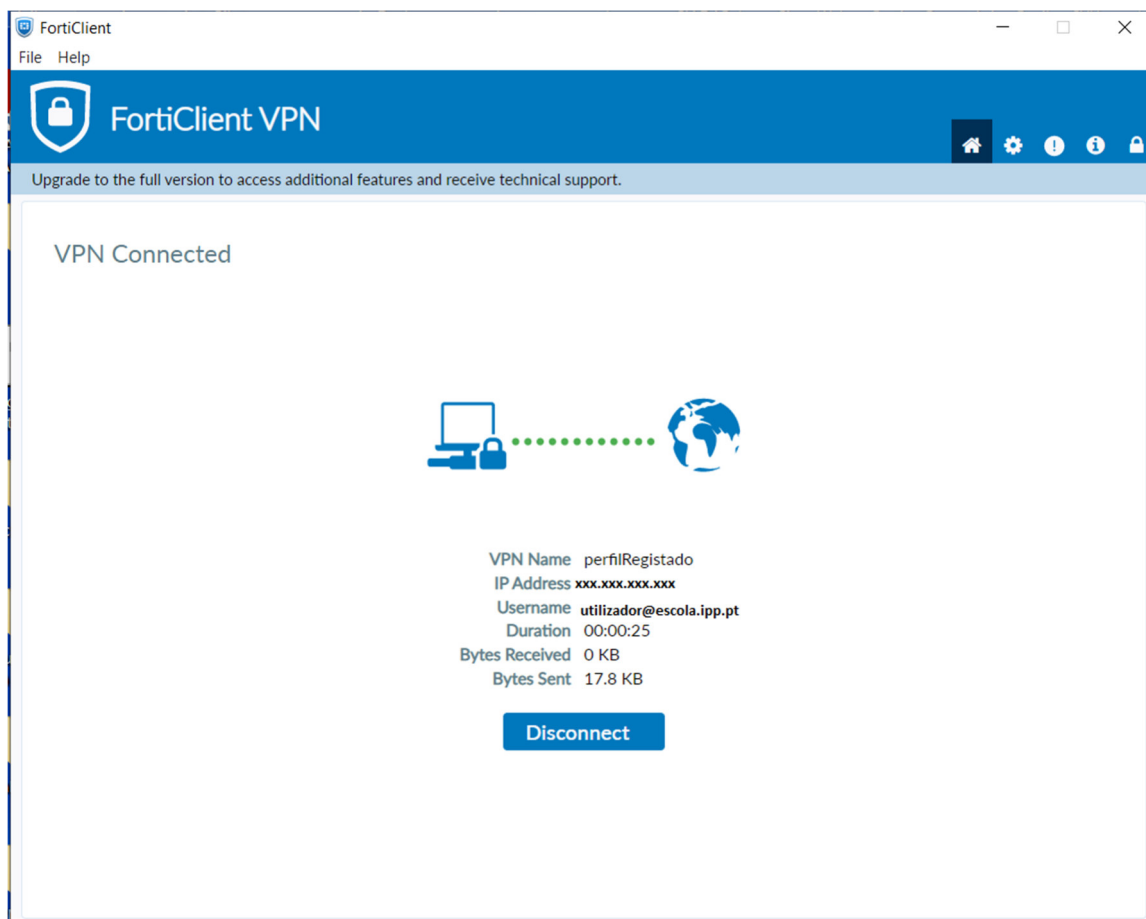


Figura 9 – Conexão ativa ao serviço VPN com o Forticlient

2.3. macOS

Nos sistemas operativos Apple, o cliente proprietário da Fortinet não é necessário.

É possível fazer a configuração da VPN apenas com o cliente nativo presente no macOS e as definições gerais cf. ponto 2.1.

2.3.1. macOS Catalina 10.15

Em primeiro lugar, é necessário abrir as preferências de sistema clicando no ícone destacado cf. Figura 10



Figura 10 – Ícone das preferências de sistema no macOS Catalina

De seguida, é necessário clicar nas definições de rede, clicando para isso no ícone Rede destacado cf. Figura 11

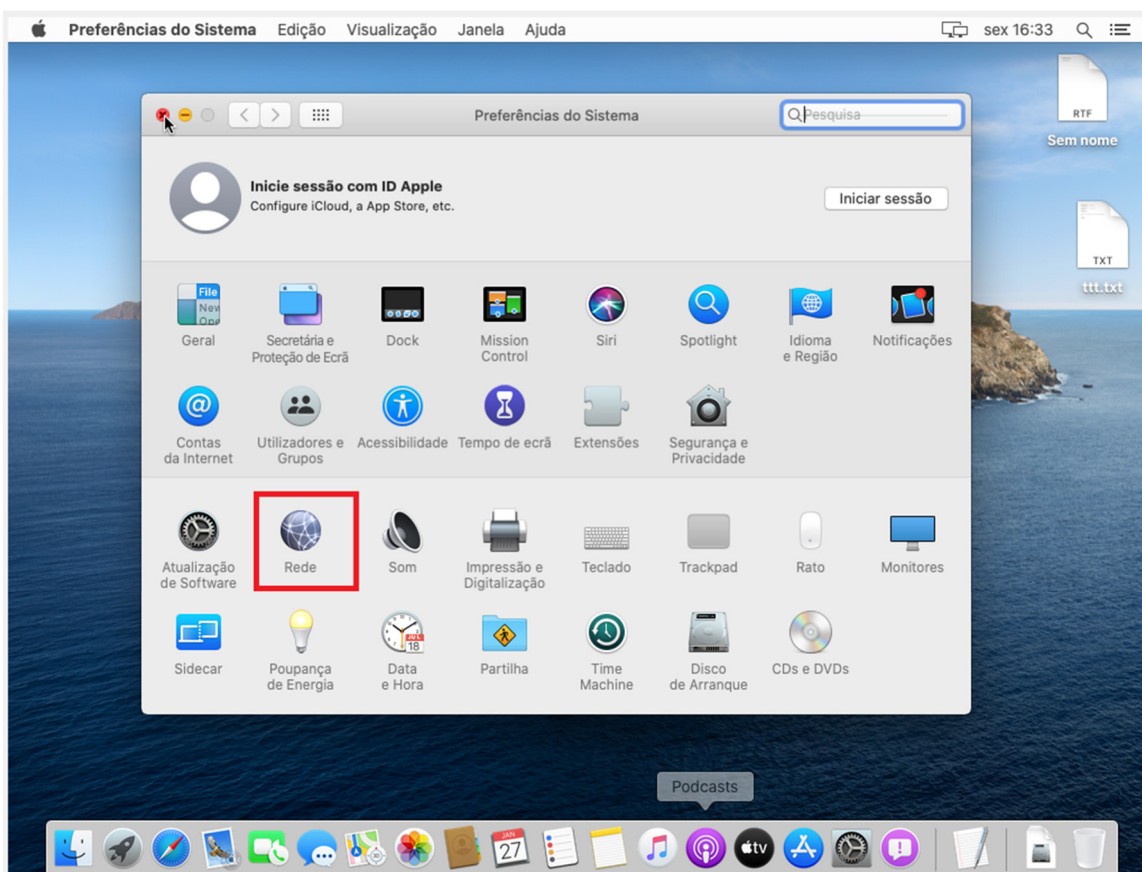


Figura 11 – Ícone da Rede no macOS Catalina

De seguida, deve ser seleccionada a opção de adicionar mais uma ligação, clicando assim na opção + cf. Figura 12

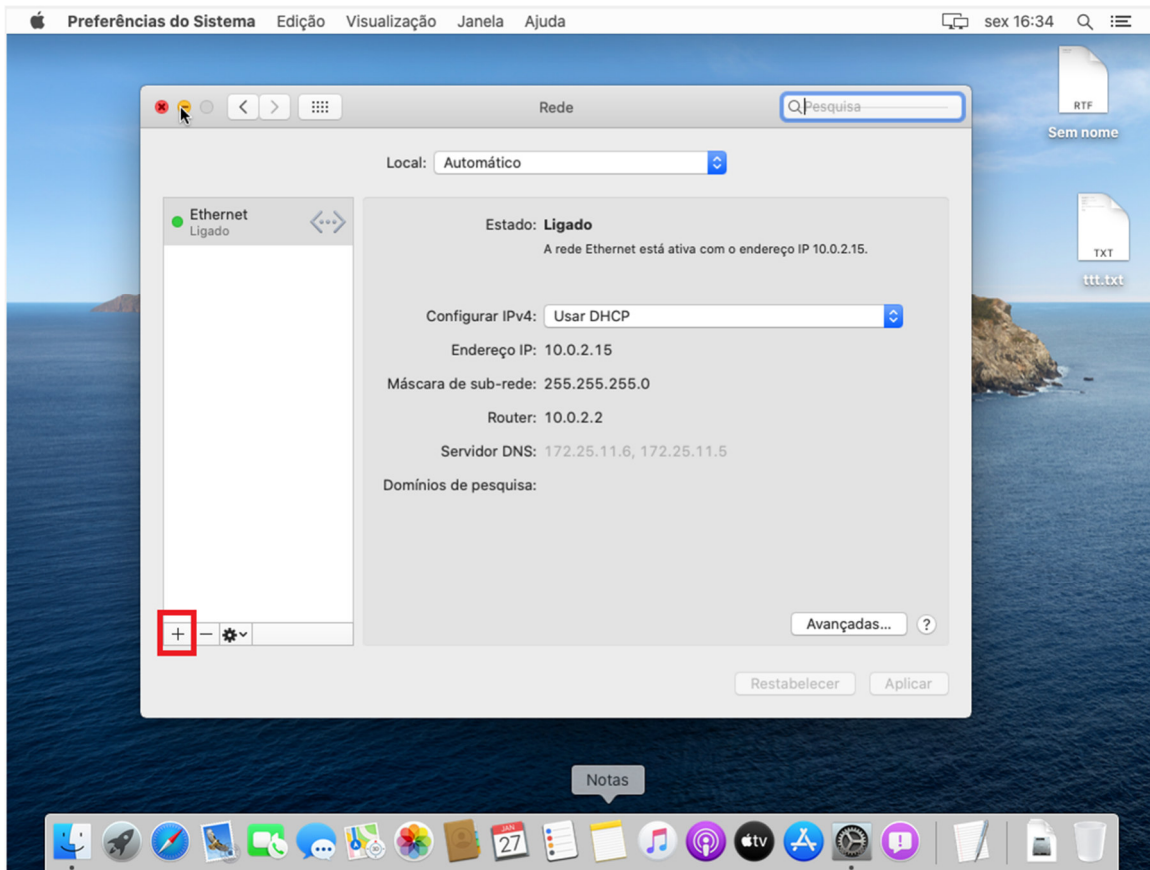


Figura 12 – Opção de adicionar uma nova ligação no macOS Catalina

Devem ser preenchidos os campos conforme a Figura 13

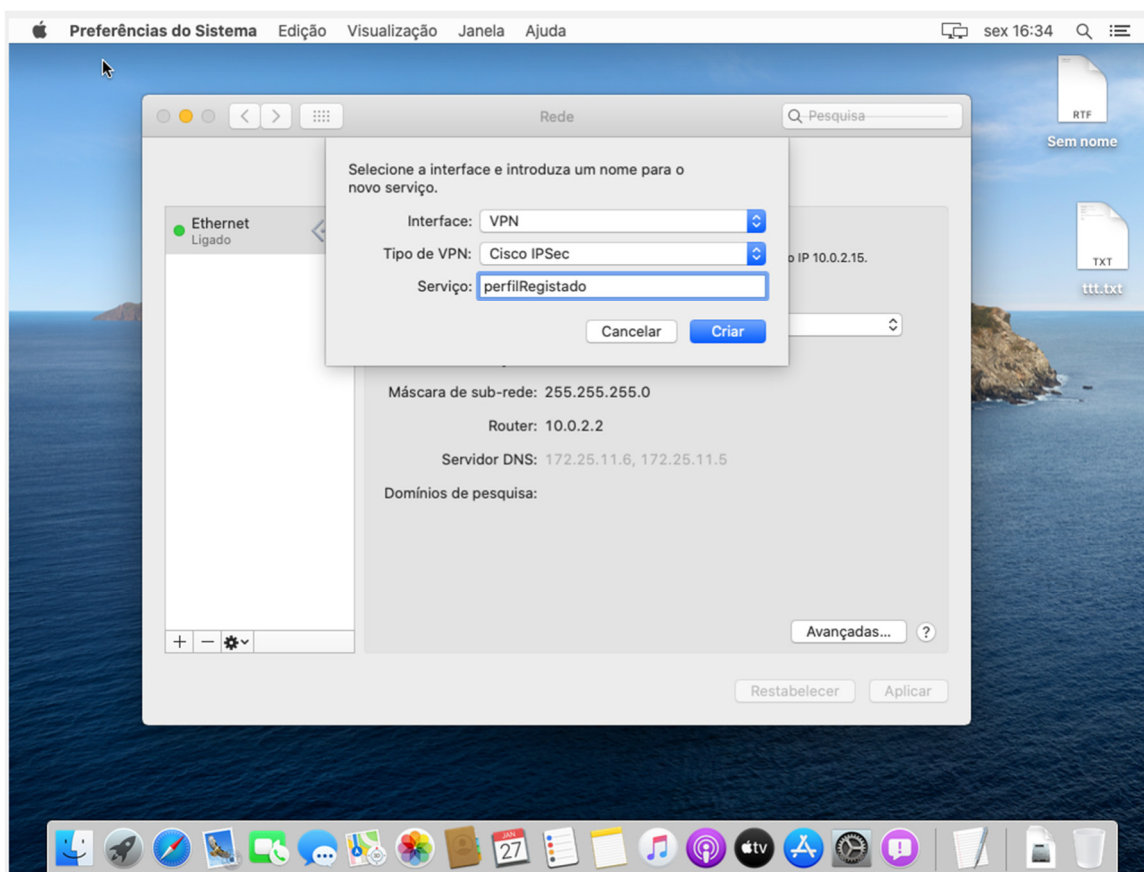


Figura 13 – Definições de VPN no macOS Catalina

O campo Serviço, pode ser preenchido com qualquer texto a escolha, no entanto foi escolhida a designação “perfilRegistrado” para ser mais parecido com o exemplo do Windows.

De seguida deve ser seleccionada a opção criar cf. Figura 14

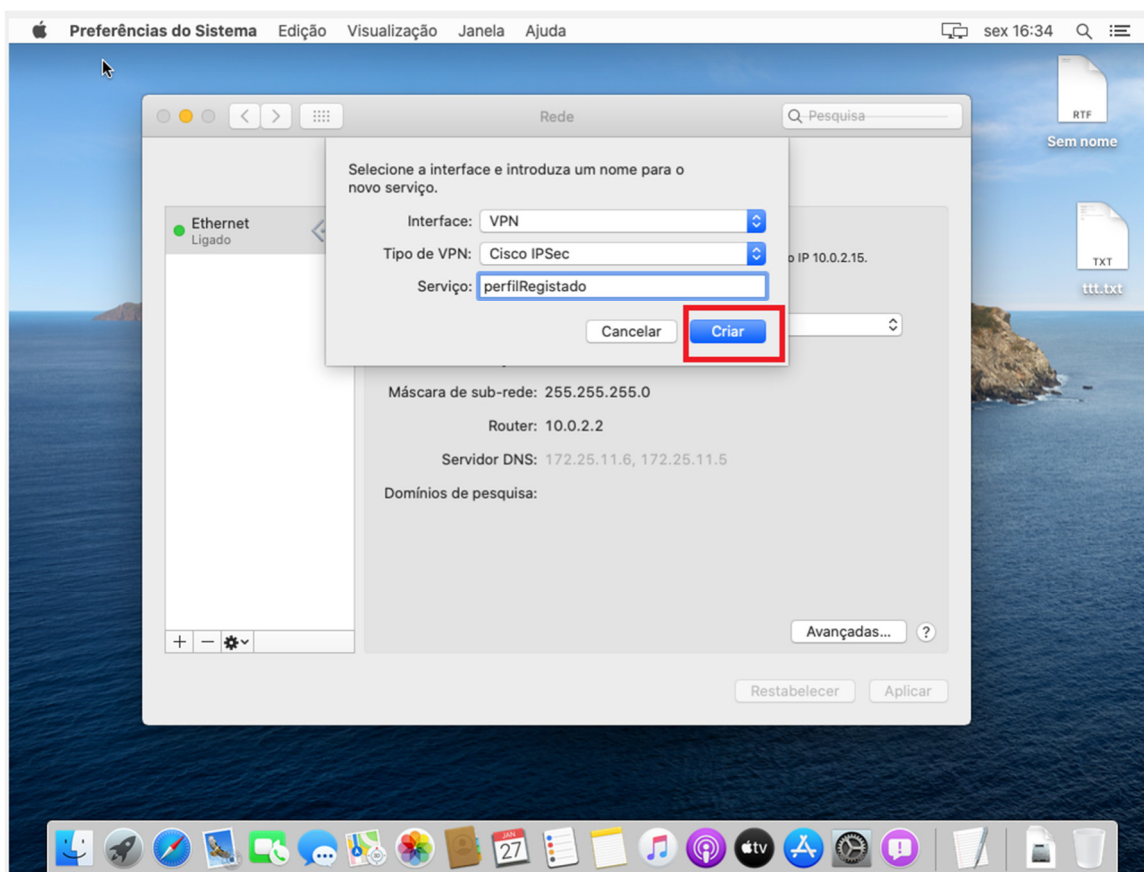


Figura 14 – Criação de nova ligação no macOS Catalina

Posteriormente, devem ser preenchidos os campos de autenticação com as credenciais do P.Porto e, o endereço do servidor cf. Figura 14

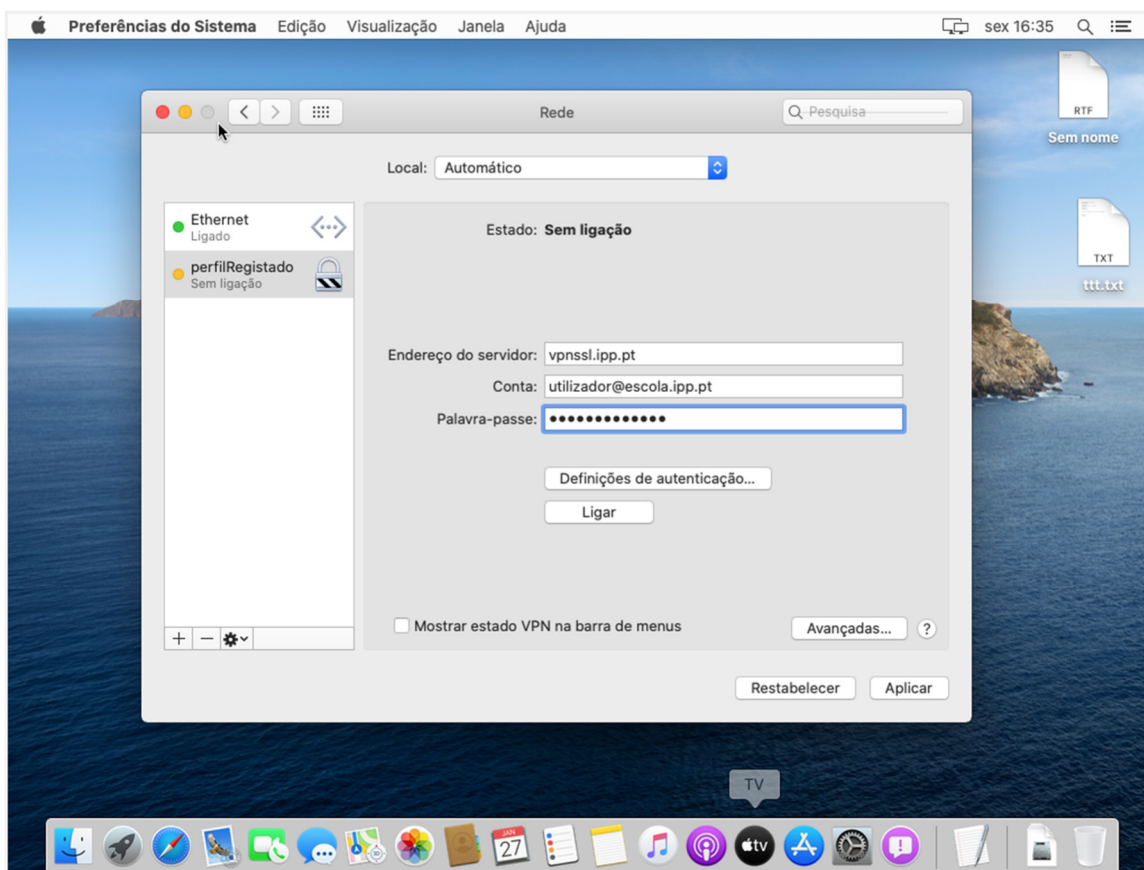


Figura 15 – Introdução de credenciais no macOS Catalina

Finalmente e, antes de fazer a ligação é necessário preencher as Definições de autenticação. Para isso deve ser escolhida a opção “Definições de autenticação” cf. Figura 16

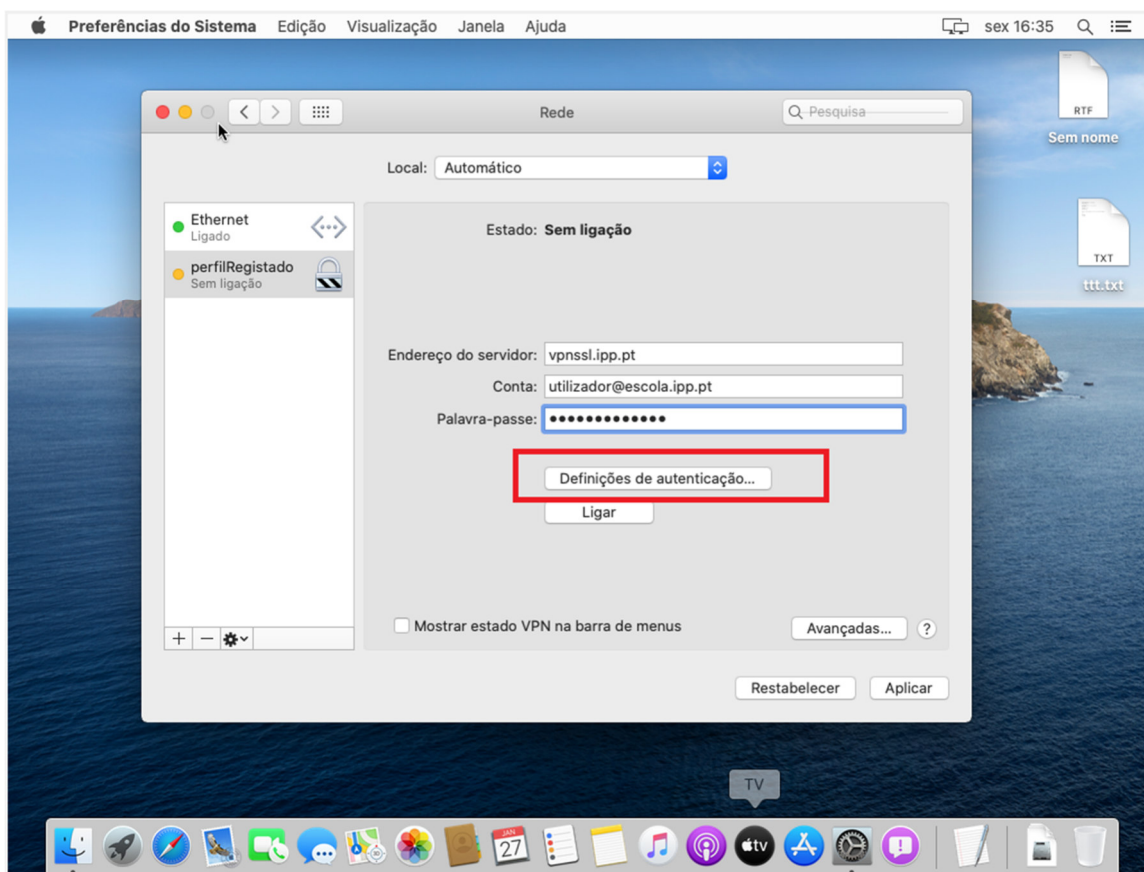


Figura 16 – Definições de Autenticação macOS Catalina

No ecrã das definições de autenticação, devem ser preenchidos os campos segredo partilhado e Nome do grupo conforme o tipo de utilizador registado ou não cf o ponto 2.1.

A título de exemplo foram usadas as definições de um perfil registado cf. Figura 17

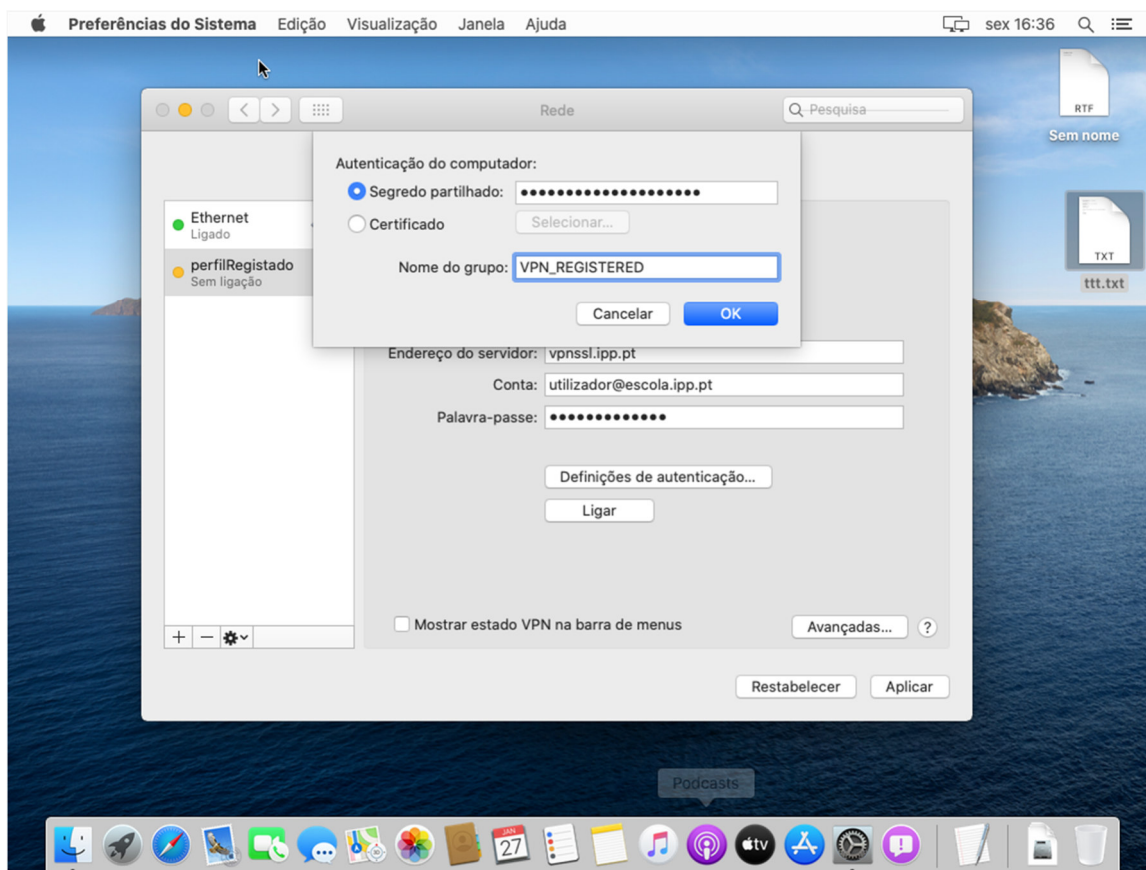


Figura 17 – Definições de perfil registado no macOS Catalina

Posto isto, é apenas necessário clicar no botão aplicar cf. Figura 18

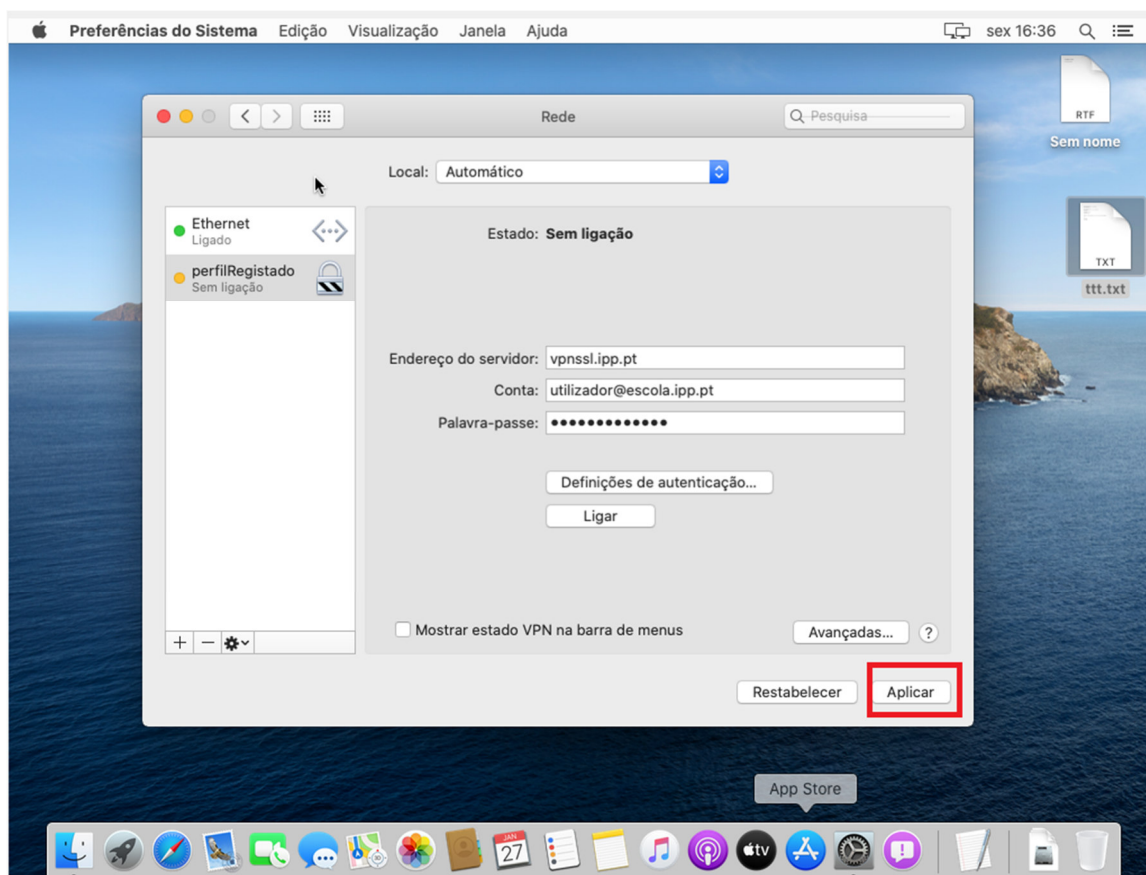


Figura 18 – Passo final da configuração no macOS Catalina

De seguida a ligação está pronta a ser usada basta apenas clicar no botão ligar cf. Figura 19:

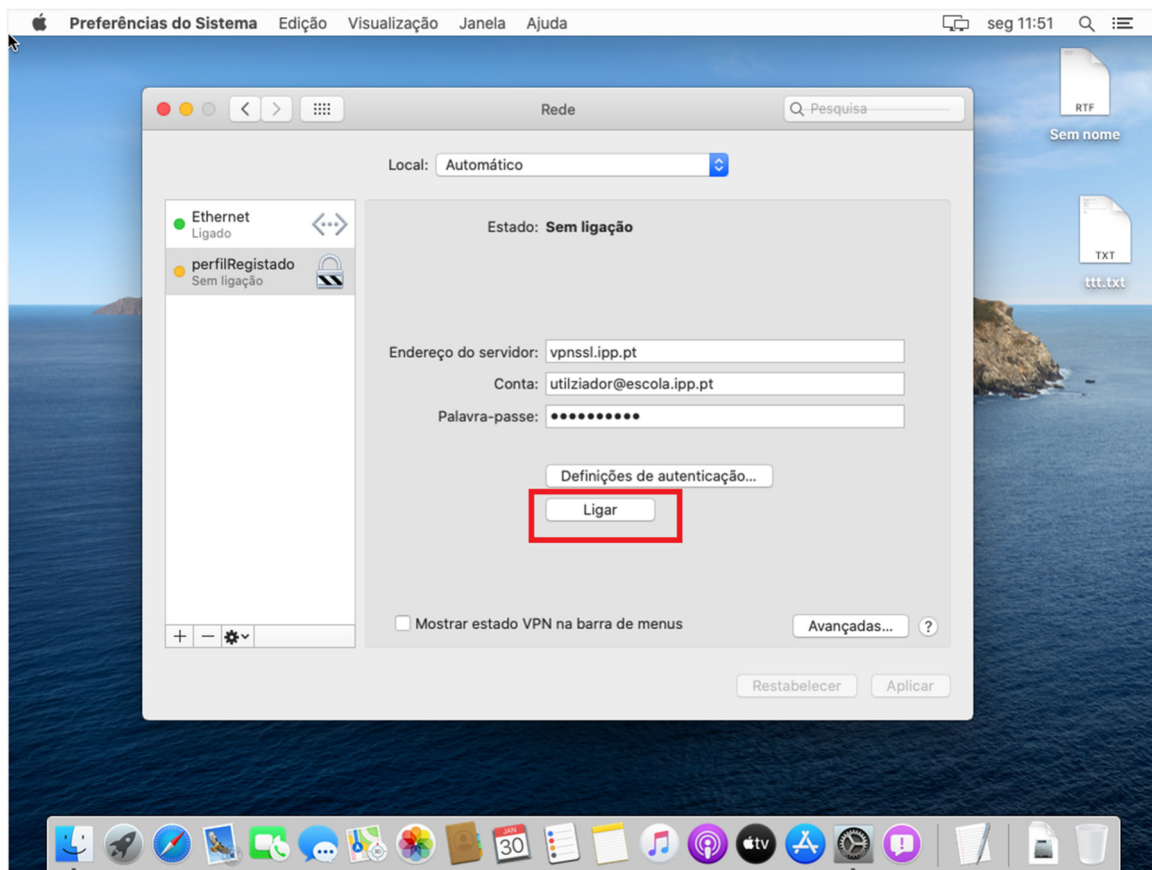


Figura 19 – Ligação pronta a ligar no macOS Catalina

Depois da ligação ser estabelecida, será apresentado o ecrã cf. Figura 20

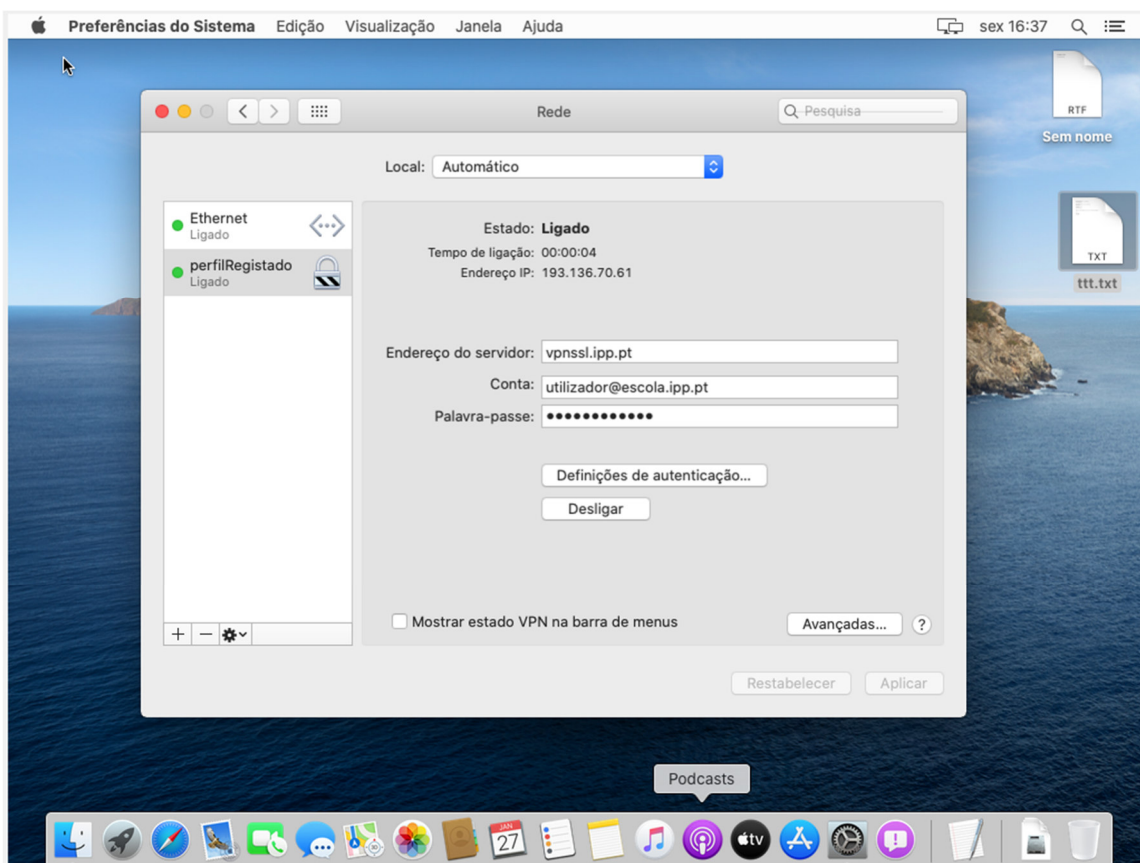


Figura 20 – Ligação estabelecida no macOS Catalina

2.3.2. macOS Big Sur 11

Em primeiro lugar, é necessário abrir as Preferências do Sistema, para isso deve ser clicado o ícone correspondente cf. Figura 21:



Figura 21 – Ícone das preferências de sistema no macOS BigSur

Posto isto, no ecrã de preferências de sistema deve ser selecionado o ícone da Rede cf.

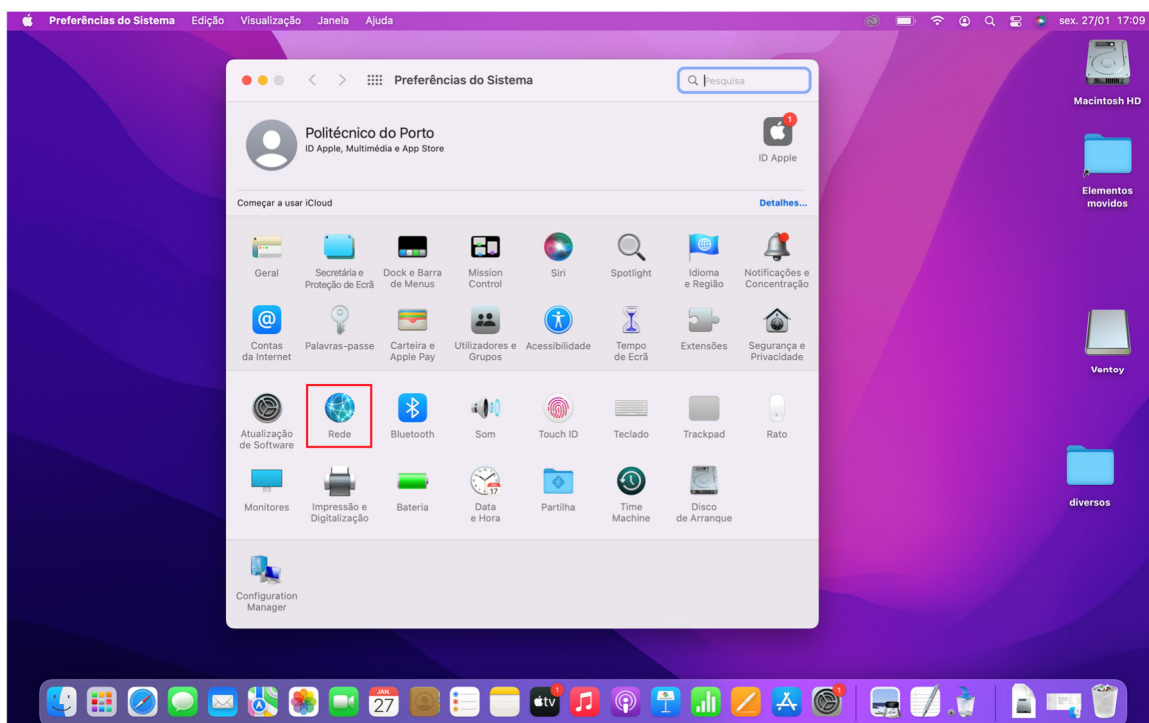


Figura 22 – Seleção da Rede no macOS BigSur

No ecrã de configuração da rede, deve ser adicionada uma nova ligação clicando no botao + cf. Figura 23

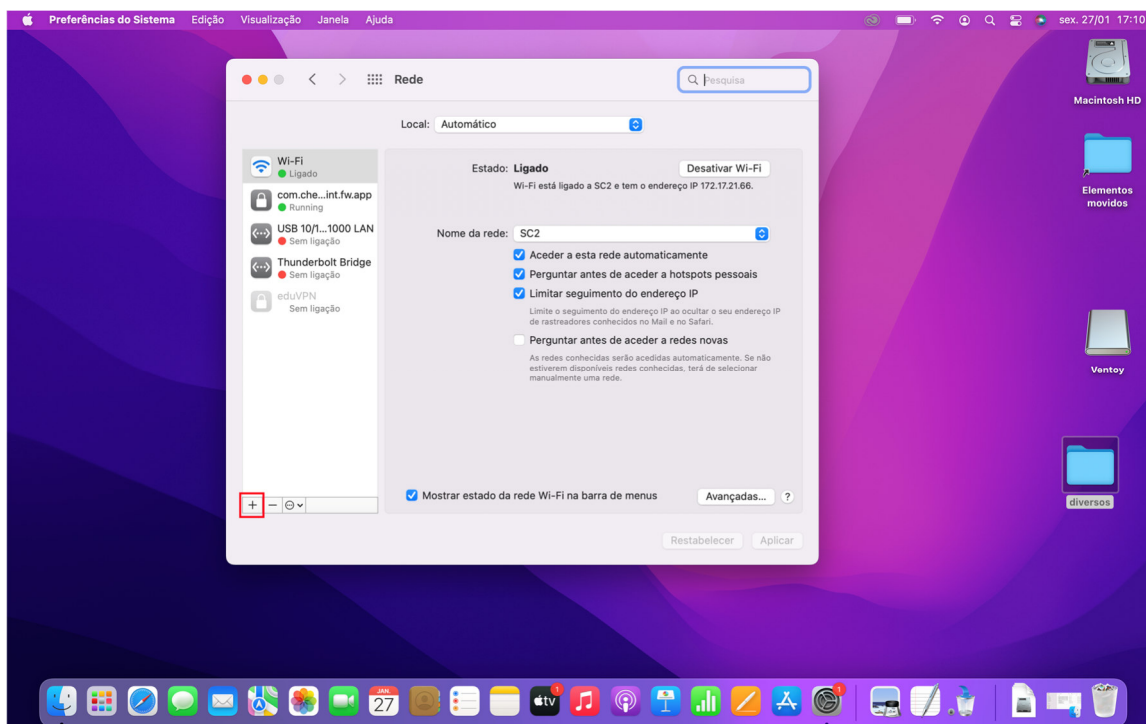


Figura 23 – Adicionar nova ligação no macOS BigSur

Devem ser preenchidos os campos conforme a Figura 24

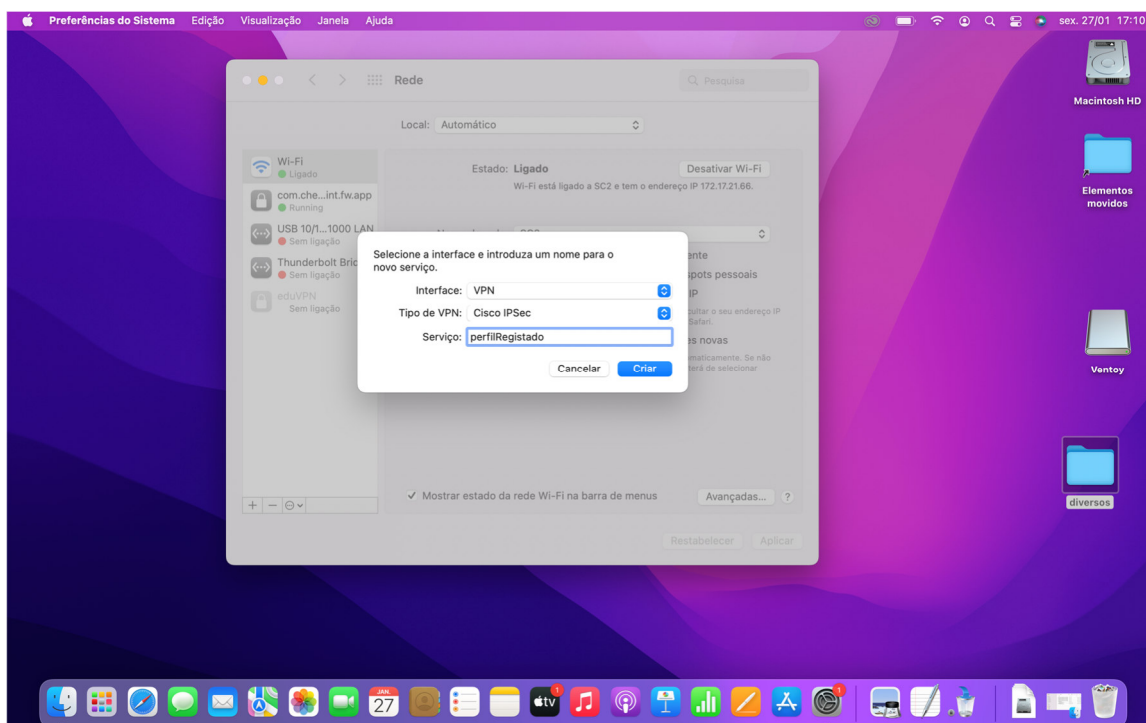


Figura 24 – Nova ligação VPN no macOS BigSur

Em seguida, deve ser clicado no botão “Criar” e devem ser preenchidos os campos de autenticação com as credencias do P.Porto e o endereço do servidor cf. Figura 25

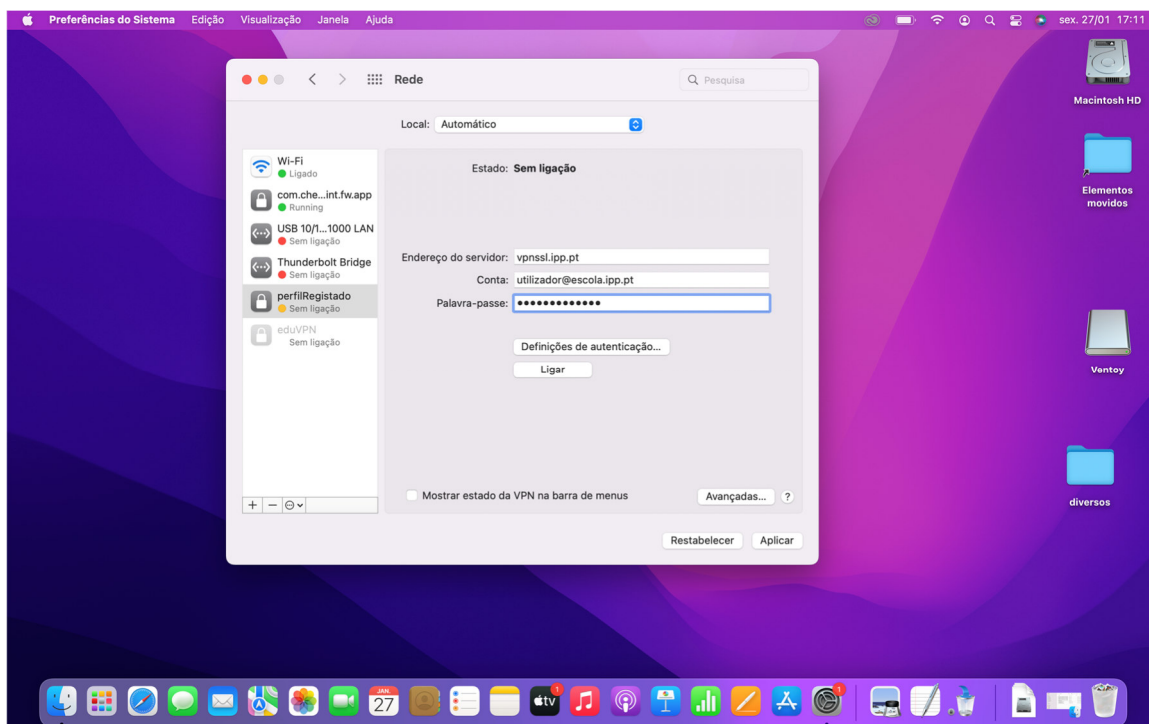


Figura 25 – Definições da VPN no macOS BigSur

Finalmente e antes de estabelecer a ligação, é ainda necessário preencher as definições de autenticação. Definições de autenticação. Para isso deve ser escolhida a opção “Definições de autenticação” cf. Figura 26

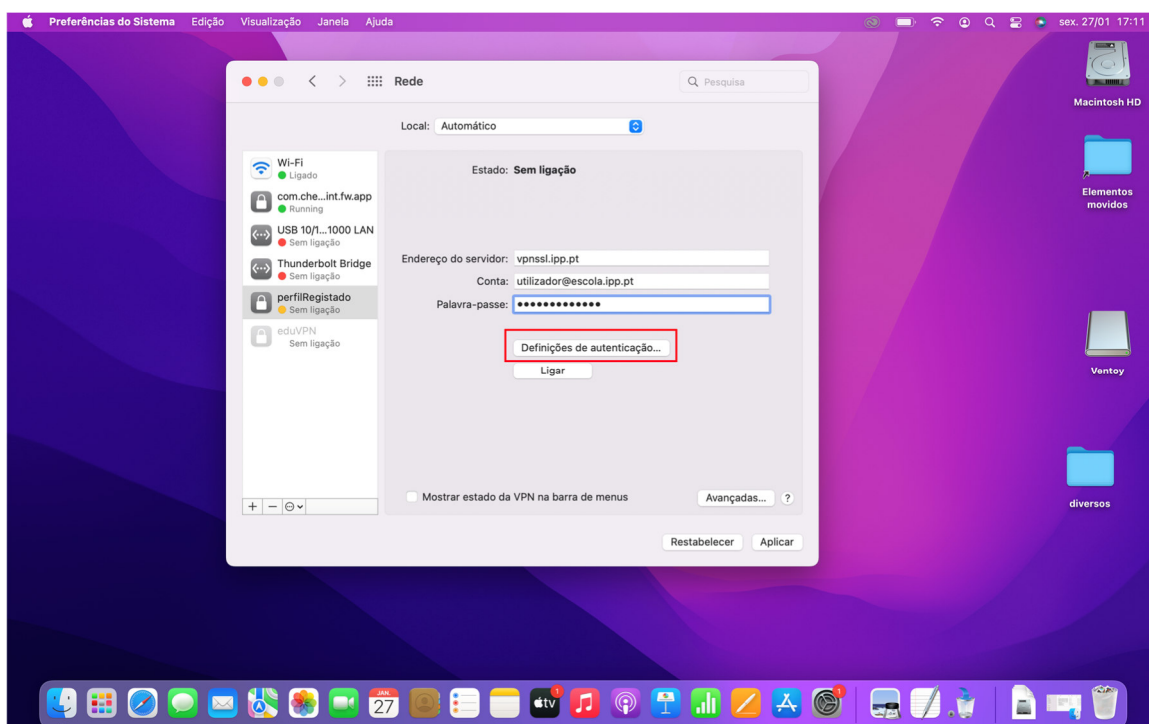


Figura 26 - Definições de Autenticação macOS no macOS BigSur

No ecrã das definições de autenticação, devem ser preenchidos os campos segredo partilhado e Nome do grupo conforme o tipo de utilizador registado ou não cf o ponto 2.1

A título de exemplo foram usadas as definições de um perfil registado cf. Figura 27

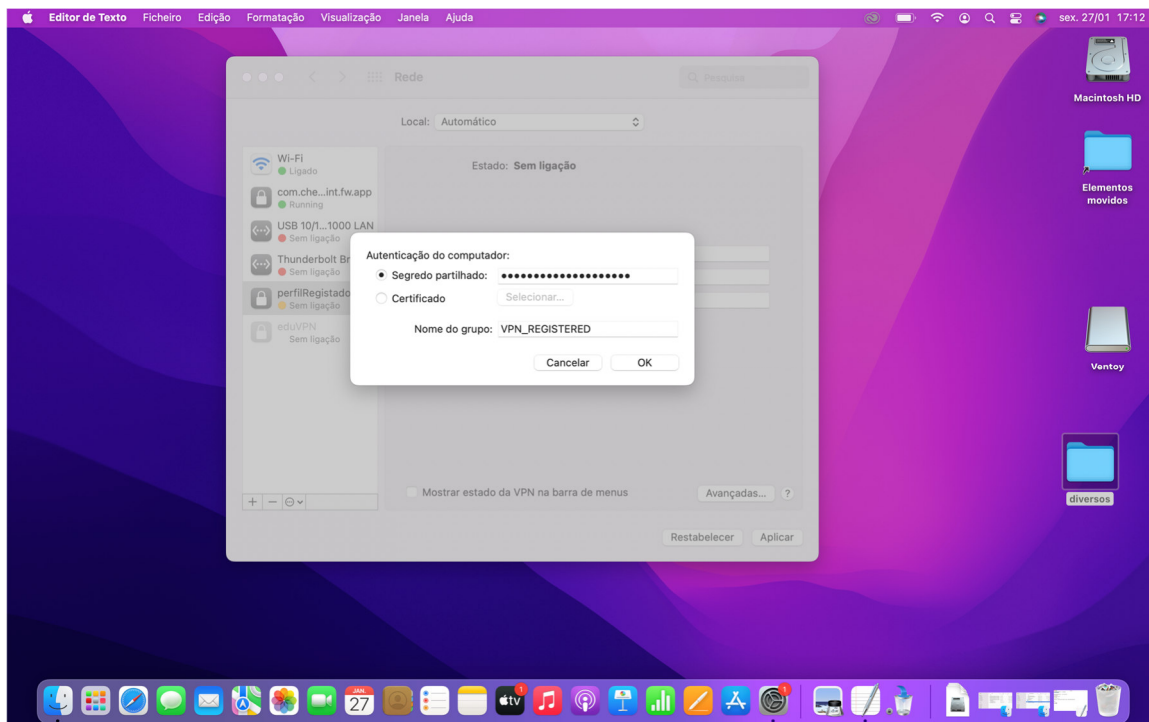


Figura 27 - Definições de perfil registado no macOS BigSur

Posto isto, é apenas necessário clicar no botão aplicar cf. Figura 28

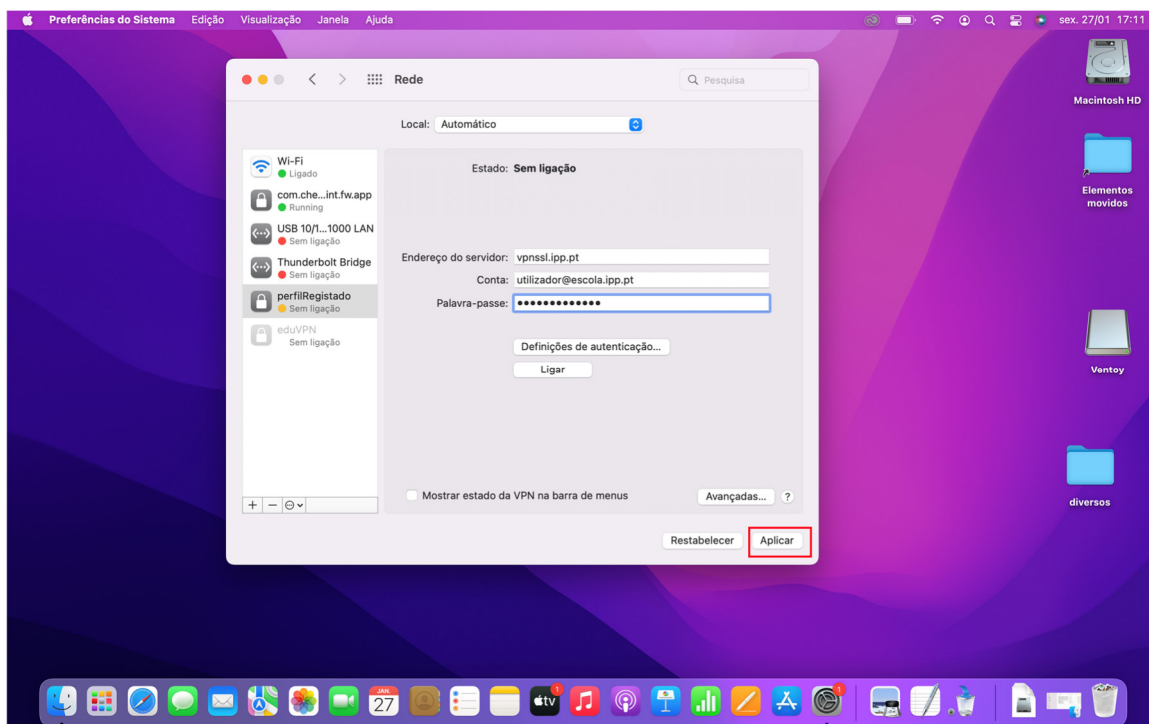


Figura 28 - Passo final da configuração no macOS BigSur

De seguida a ligação está pronta a ser usada basta apenas clicar no botão ligar cf. Figura 29

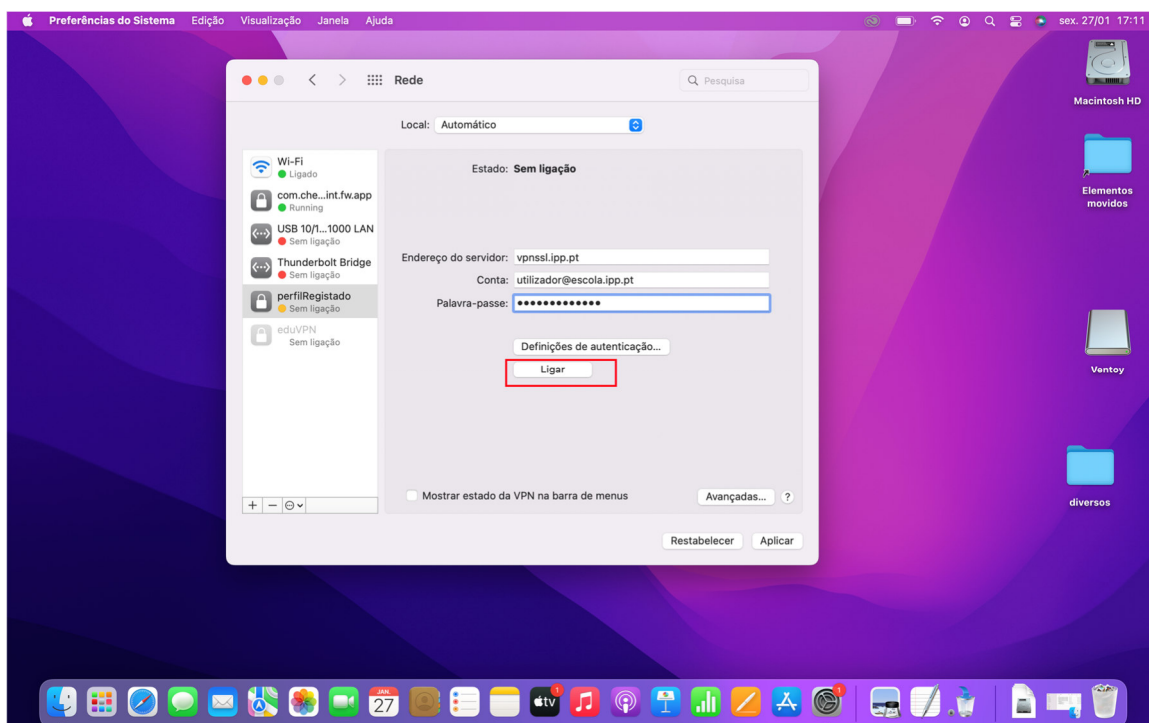


Figura 29 - Ligação pronta a ligar no macOS BigSur

Depois da ligação ser estabelecida, será apresentado o ecrã cf. Figura 30

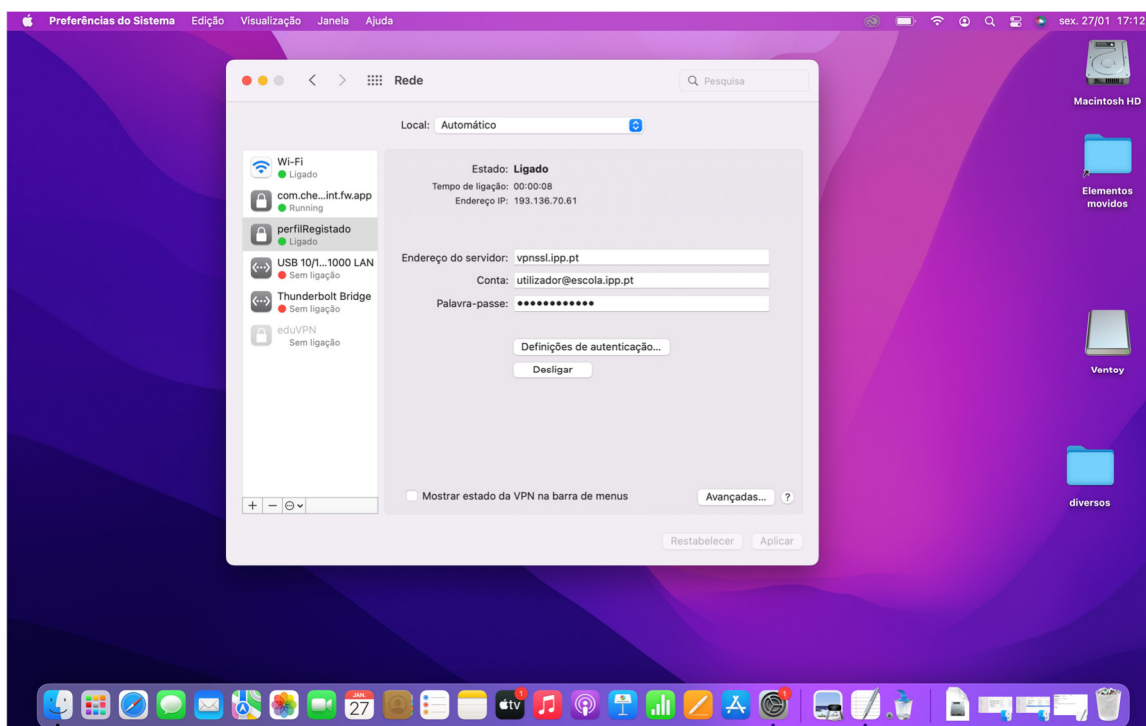


Figura 30 - Ligação estabelecida no macOS BigSur

2.3.3. macOS Monterey 12

Antes de tudo, é necessário abrir as preferências de sistema clicando no ícone destacado cf. Figura 31

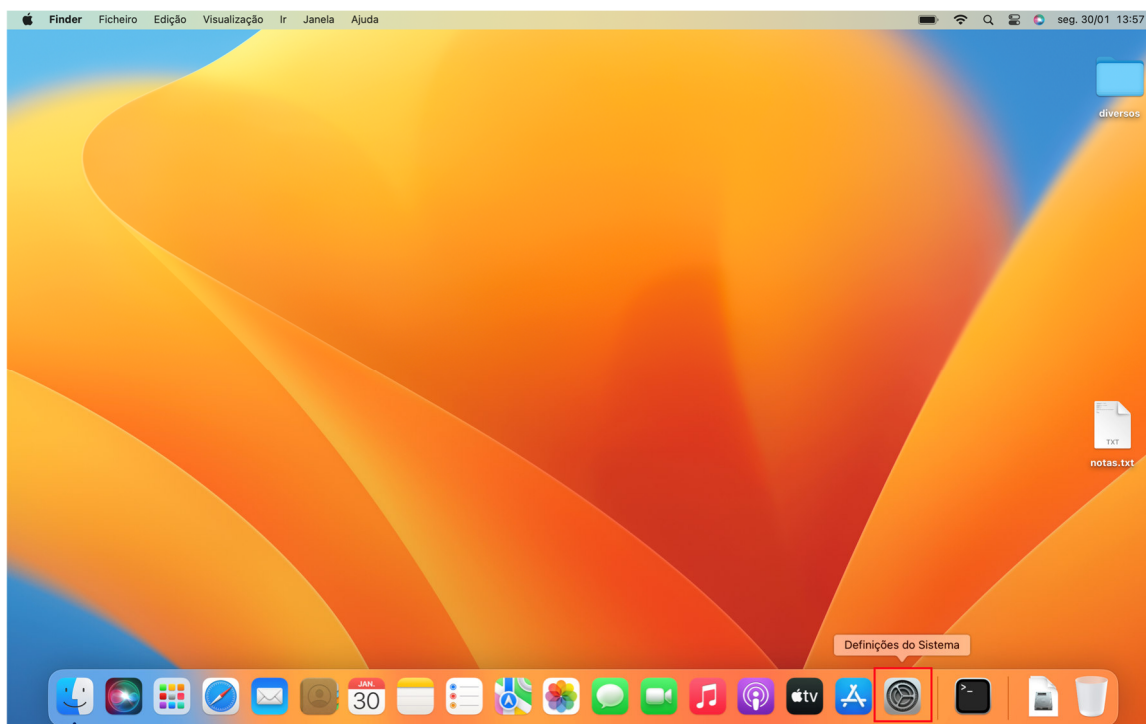


Figura 31 - Ícone das preferências de sistema no macOS Monterey

De seguida, é necessário clicar nas definições de rede, clicando para isso no ícone Rede destacado cf. Figura 32

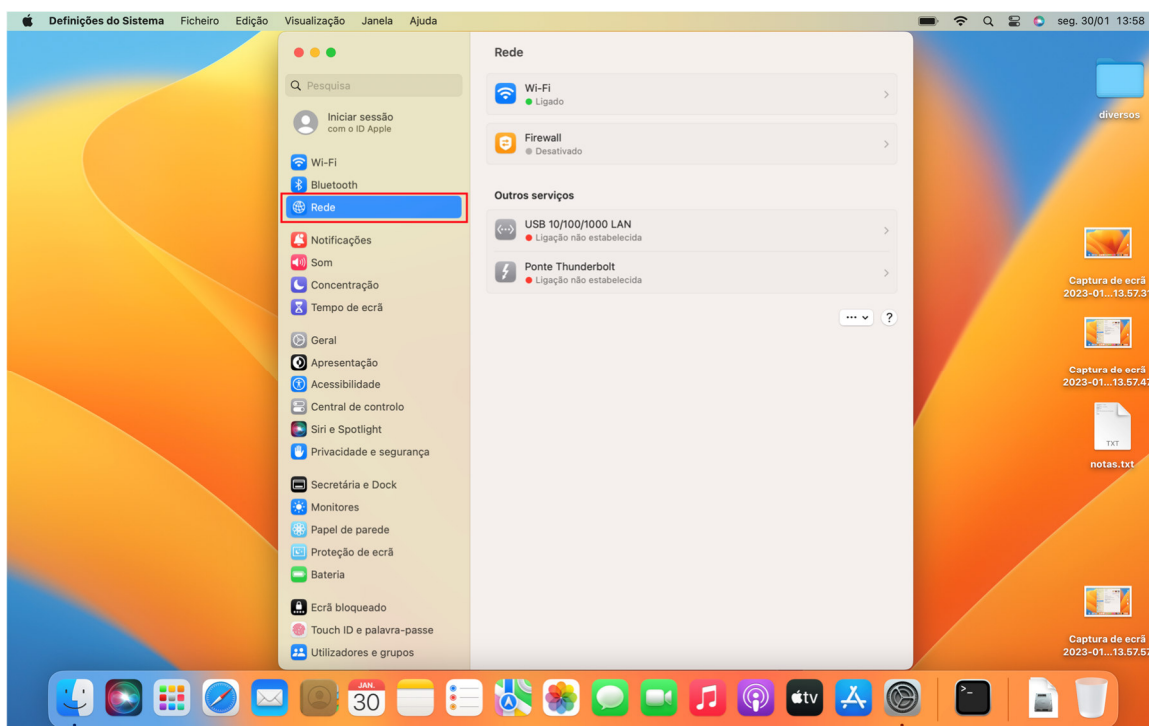


Figura 32 - Ícone da Rede no macOS Monterey

De seguida, deve ser selecionada a opção de adicionar mais uma ligação, clicando assim na opção ... cf. Figura 33

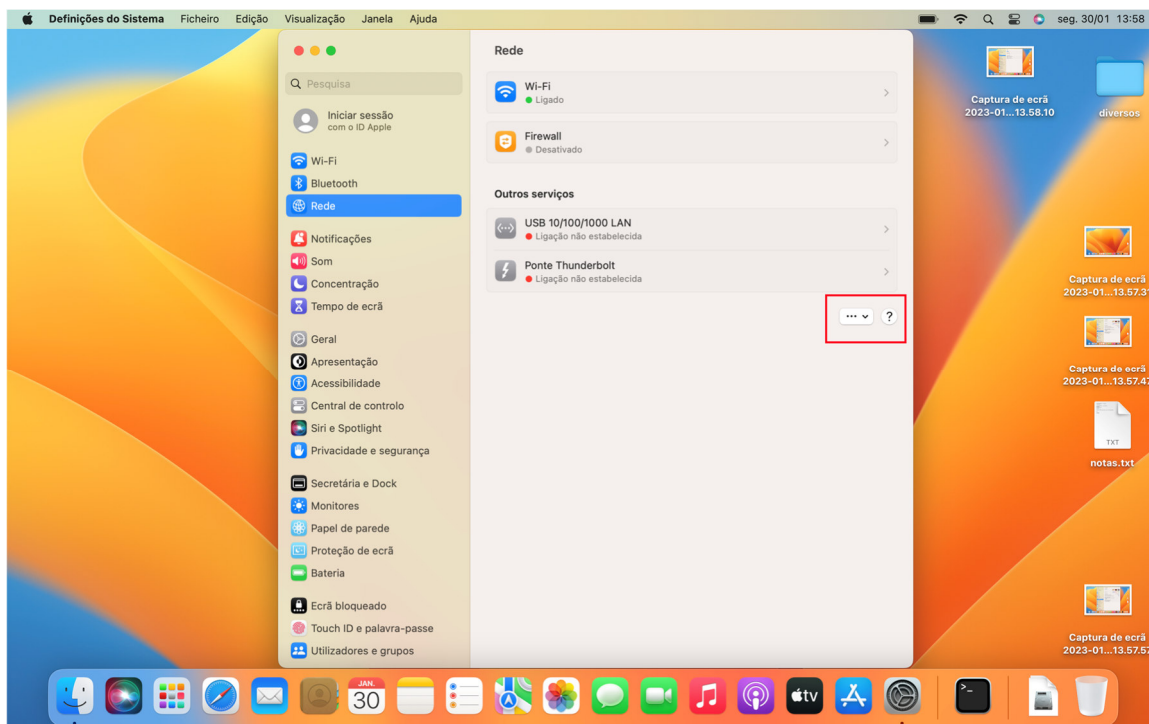


Figura 33 - Opção de adicionar uma nova ligação no macOS Monterey

Deve ser seleccionada a opção “Adicionar configuração de VPN” → Cisco IPSec cf. Figura 34

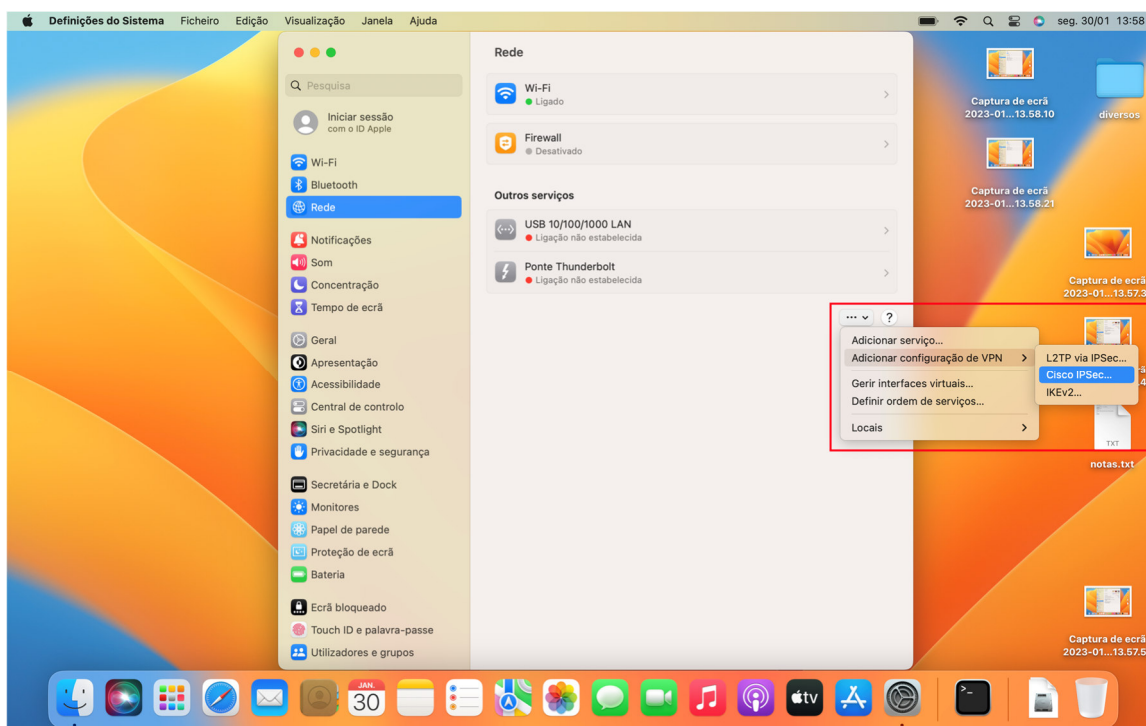


Figura 34 – Seleção do tipo de VPN no macOS Monterey

Devem ser preenchidos os campos Nome da conta, Palavra-passe com a credencial do P.Porto, os campos Nome a apresentar, endereço do servidor devem ser preenchidos cf. Figura 35

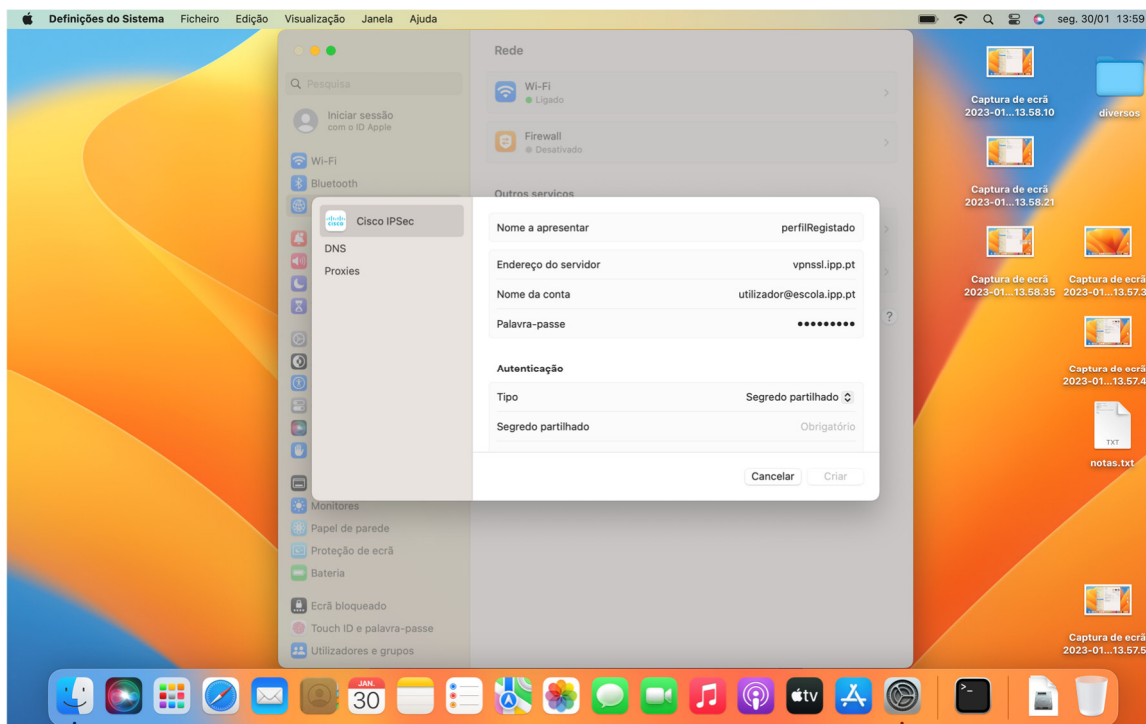


Figura 35 – Preenchimento dos dados da VPN no macOS Monterey

Os campos segredo partilhado e Nome do grupo conforme o tipo de utilizador registado ou não cf o ponto 2.1.

A título de exemplo foram usadas as definições de um perfil registado cf. Figura 36

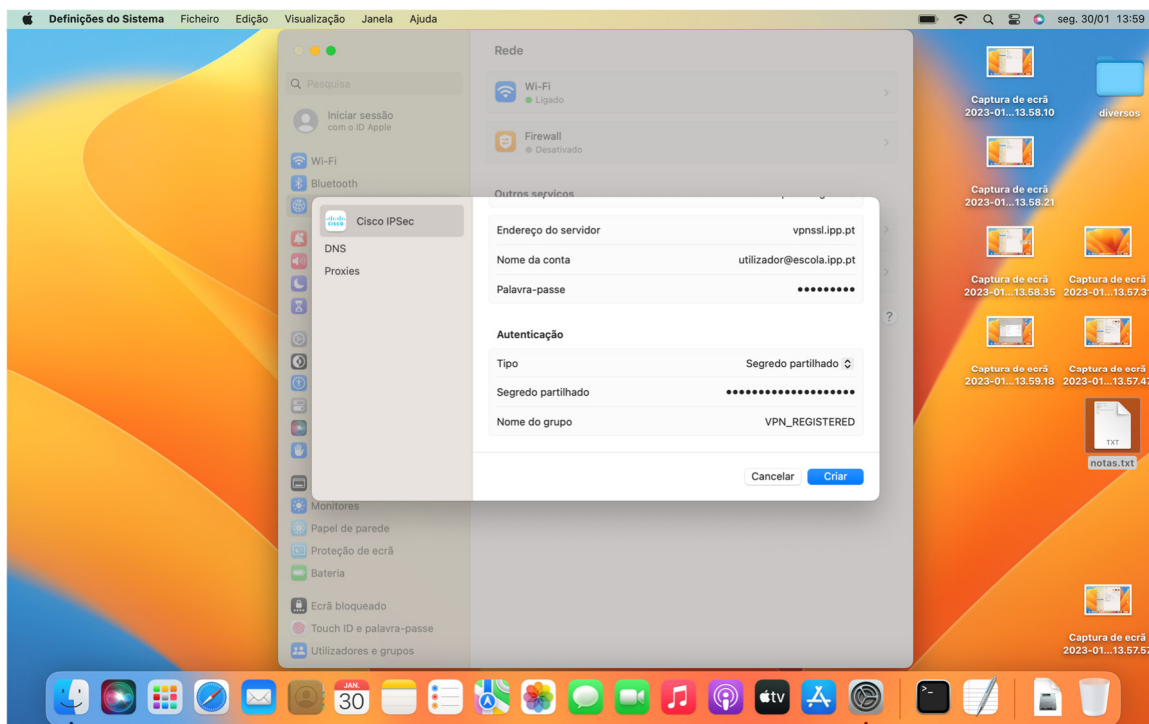


Figura 36 - Definições de perfil registado no macOS Monterey

Posto isto, é apenas necessário clicar no botão criar cf. Figura 37

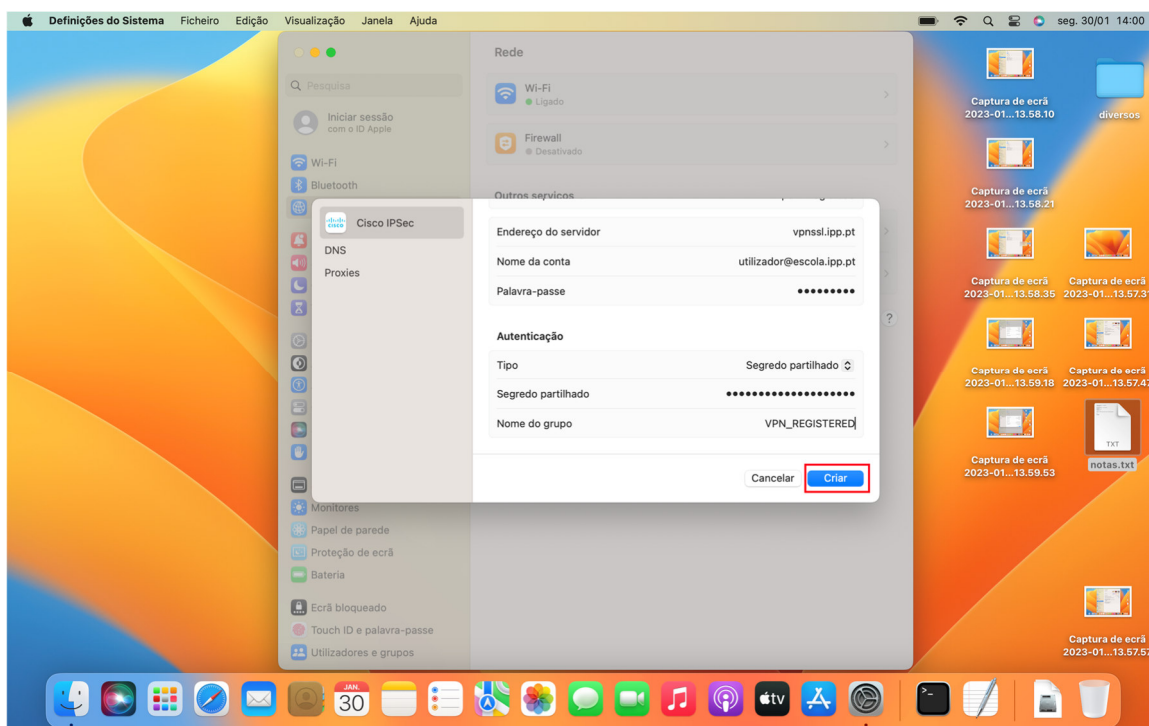


Figura 37 - Passo final da configuração no macOS Monterey

De seguida a ligação está pronta a ser usada. Para isso é necessário escolher a opção VPN cf.

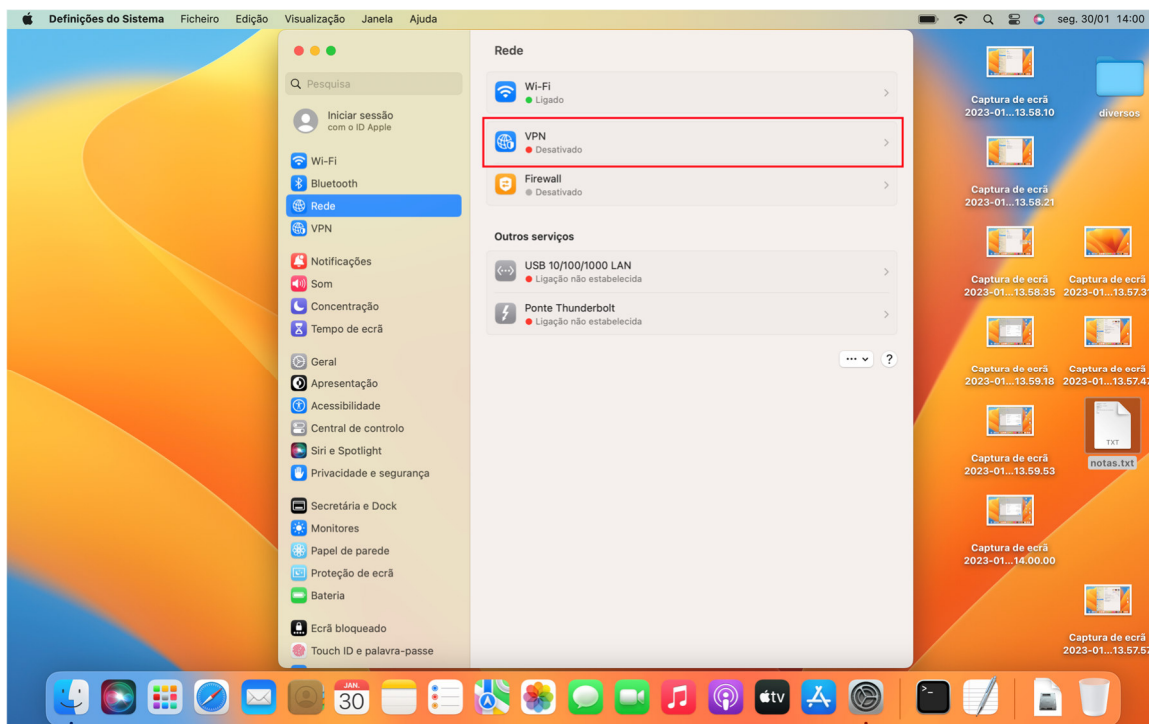


Figura 38 – Selecionar opção VPN no macOS Monterey

E de seguida, ativar a VPN recém-criada, neste caso “Perfil Registrado” cf Figura 39

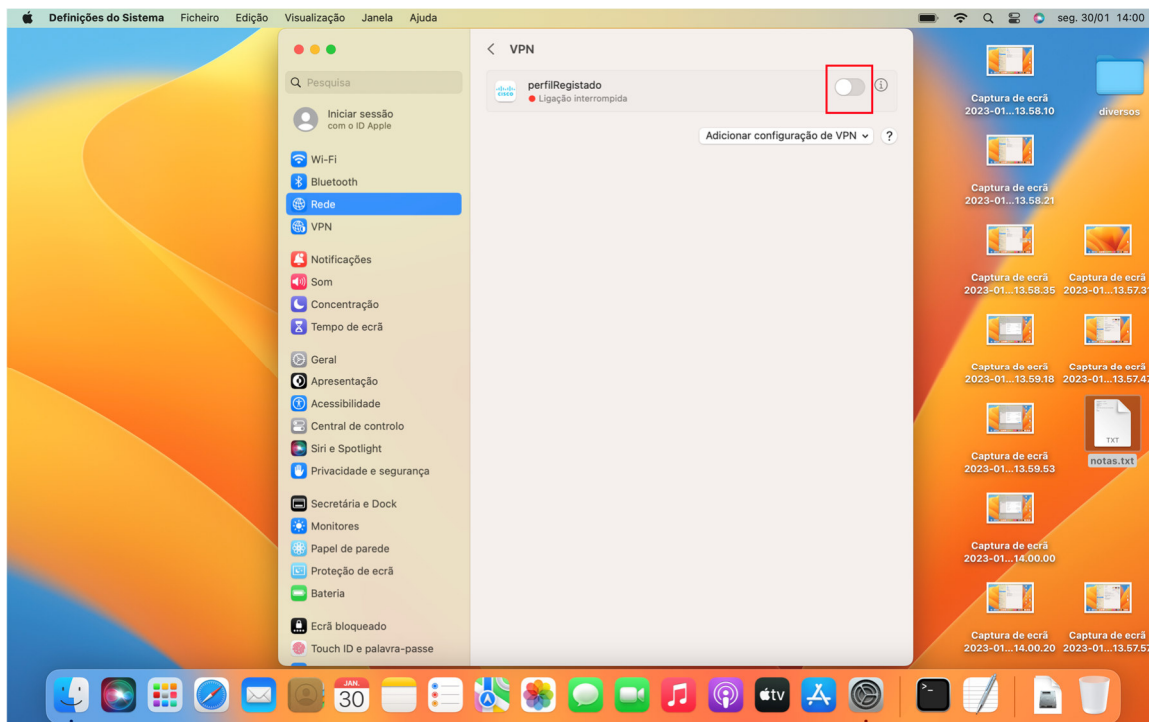


Figura 39 – Ativação da VPN no macOS Monterey

Depois da ligação ser estabelecida, será apresentado o ecrã cf. Figura 40

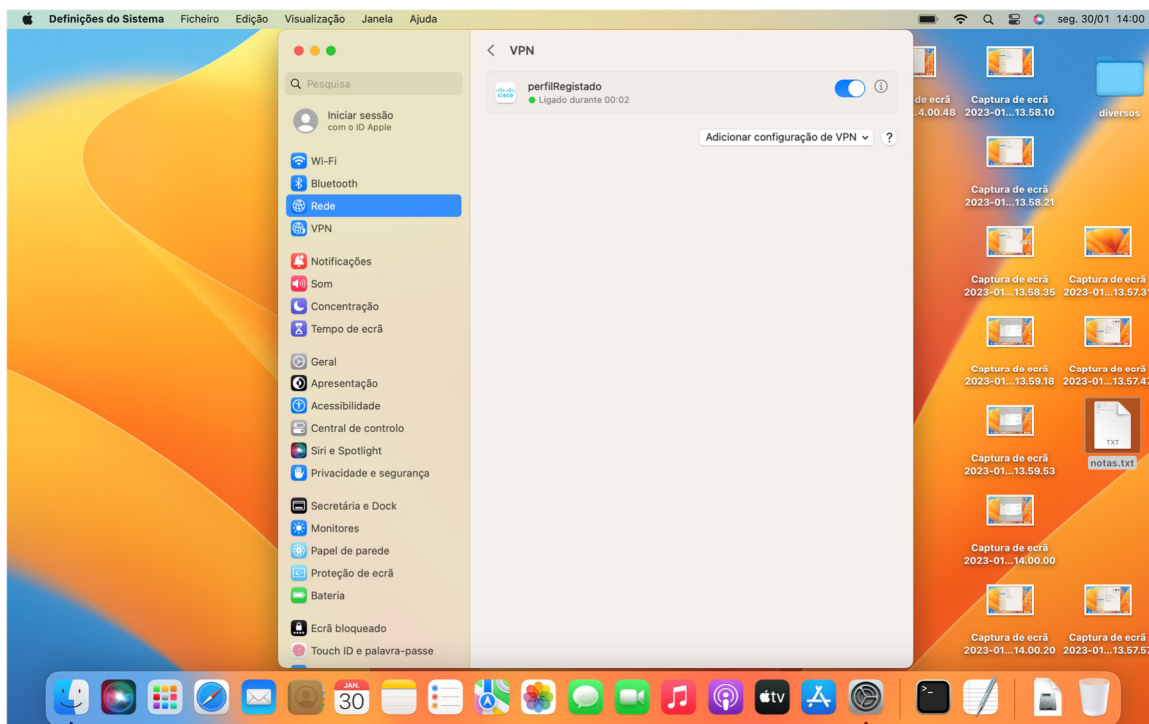


Figura 40 – VPN Ligada no macOS Monterey

2.4. Linux

Nos sistemas Linux o cliente da Fortinet não suporta o Dialup IPsec.

Assim sendo é necessário utilizar alguns pacotes auxiliares como por exemplo o strongswan.



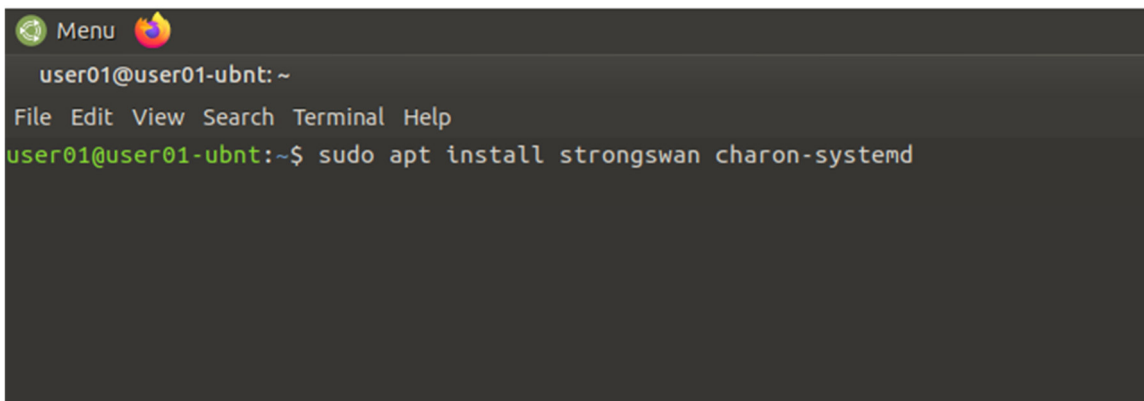
Informação

O exemplo de configuração seguinte, tem por base uma *Technical Tip* da Fortinet⁵

⁵ <https://community.fortinet.com/t5/FortiGate/Technical-Tip-IPsec-connection-between-FortiGate-and-Ubuntu-via/ta-p/207149>

2.4.1. Ubuntu e derivados

Primeiramente, é necessário abrir a consola e instalar os dois pacotes do strongswan cf. Figura 41



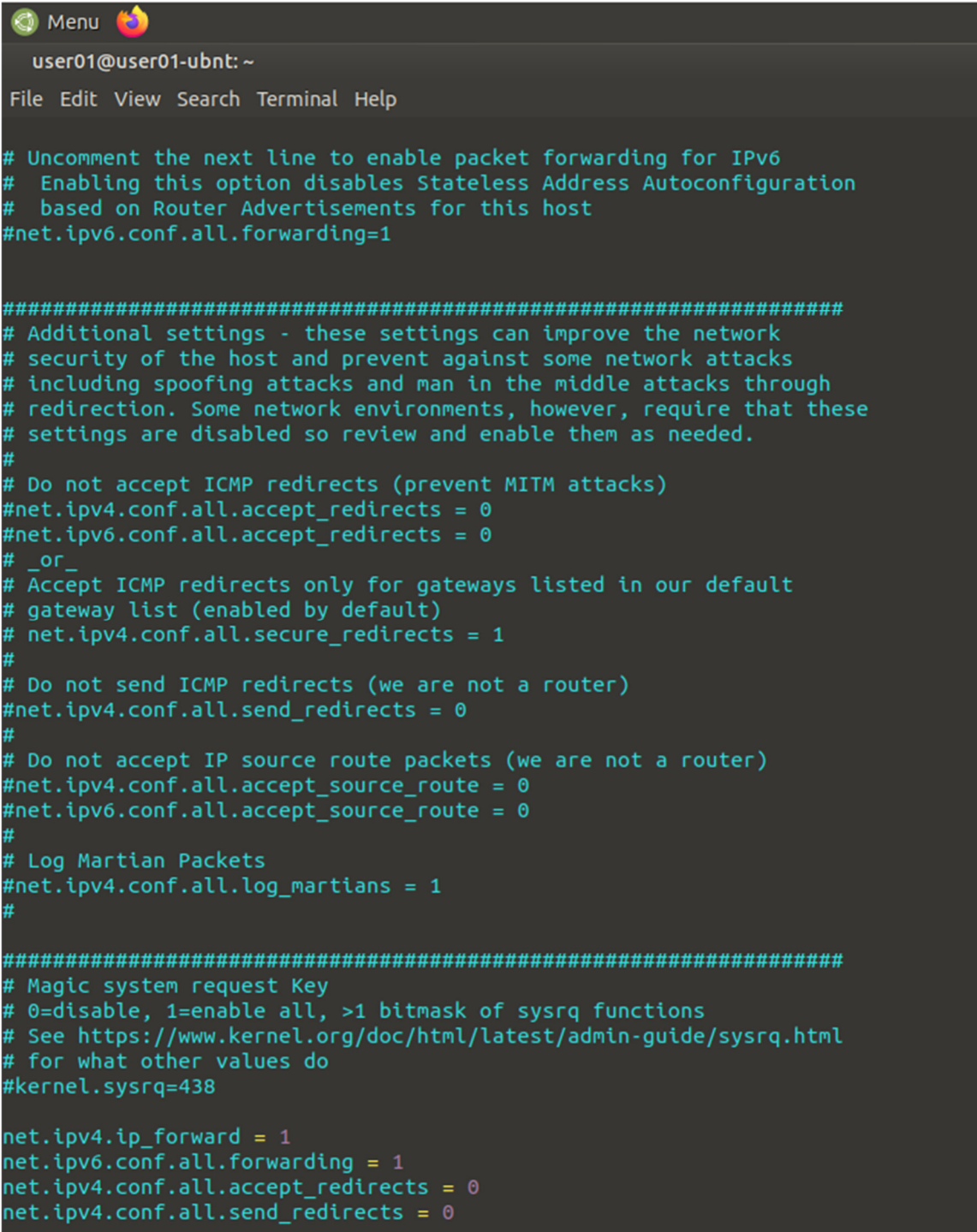
```
user01@user01-ubnt: ~  
File Edit View Search Terminal Help  
user01@user01-ubnt:~$ sudo apt install strongswan charon-systemd
```

Figura 41 – Instalação dos pacotes do strongswan no Ubuntu 20.04

Posto, isto é, necessário ativar o encaminhamento de pacotes. Para isso é necessário acrescentar estas linhas:

```
net.ipv4.ip_forward = 1  
net.ipv6.conf.all.forwarding = 1  
net.ipv4.conf.all.accept_redirects = 0  
net.ipv4.conf.all.send_redirects = 0
```

no final do ficheiro `/etc/sysctl.conf` cf. Figura 42



```
user01@user01-ubnt: ~
File Edit View Search Terminal Help

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1

#####
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.
#
# Do not accept ICMP redirects (prevent MITM attacks)
#net.ipv4.conf.all.accept_redirects = 0
#net.ipv6.conf.all.accept_redirects = 0
# _or_
# Accept ICMP redirects only for gateways listed in our default
# gateway list (enabled by default)
# net.ipv4.conf.all.secure_redirects = 1
#
# Do not send ICMP redirects (we are not a router)
#net.ipv4.conf.all.send_redirects = 0
#
# Do not accept IP source route packets (we are not a router)
#net.ipv4.conf.all.accept_source_route = 0
#net.ipv6.conf.all.accept_source_route = 0
#
# Log Martian Packets
#net.ipv4.conf.all.log_martians = 1
#

#####
# Magic system request Key
# 0=disable, 1=enable all, >1 bitmask of sysrq functions
# See https://www.kernel.org/doc/html/latest/admin-guide/sysrq.html
# for what other values do
#kernel.sysrq=438

net.ipv4.ip_forward = 1
net.ipv6.conf.all.forwarding = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
```

Figura 42 – Ficheiro de configuração de variáveis do kernel do Ubuntu 20.04

De seguida, deve ser executado o seguinte comando:

```
sudo sysctl --system
```

Para recarregar as variáveis recém acrescentadas ao ficheiro /etc/sysctl.conf cf. Figura 43

```

Menu
user01@user01-ubnt: ~
File Edit View Search Terminal Help
user01@user01-ubnt:~$ sudo sysctl --system
* Applying /etc/sysctl.d/10-console-messages.conf ...
kernel.printk = 4 4 1 7
* Applying /etc/sysctl.d/10-ipv6-privacy.conf ...
net.ipv6.conf.all.use_tempaddr = 2
net.ipv6.conf.default.use_tempaddr = 2
* Applying /etc/sysctl.d/10-kernel-hardening.conf ...
kernel.kptr_restrict = 1
* Applying /etc/sysctl.d/10-link-restrictions.conf ...
fs.protected_hardlinks = 1
fs.protected_symlinks = 1
* Applying /etc/sysctl.d/10-magic-sysrq.conf ...
kernel.sysrq = 176
* Applying /etc/sysctl.d/10-network-security.conf ...
net.ipv4.conf.default.rp_filter = 2
net.ipv4.conf.all.rp_filter = 2
* Applying /etc/sysctl.d/10-pttrace.conf ...
kernel.yama.pttrace_scope = 1
* Applying /etc/sysctl.d/10-zero-page.conf ...
vm.mmap_min_addr = 65536
* Applying /usr/lib/sysctl.d/50-default.conf ...
net.ipv4.conf.default.promote_secondaries = 1
sysctl: setting key "net.ipv4.conf.all.promote_secondaries": Invalid argument
net.ipv4.ping_group_range = 0 2147483647
net.core.default_qdisc = fq_codel
fs.protected_regular = 1
fs.protected_fifos = 1
* Applying /usr/lib/sysctl.d/50-pid-max.conf ...
kernel.pid_max = 4194304
* Applying /etc/sysctl.d/99-sysctl.conf ...
net.ipv4.ip_forward = 1
net.ipv6.conf.all.forwarding = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
* Applying /usr/lib/sysctl.d/protect-links.conf ...
fs.protected_fifos = 1
fs.protected_hardlinks = 1
fs.protected_regular = 2
fs.protected_symlinks = 1
* Applying /etc/sysctl.conf ...
net.ipv4.ip_forward = 1
net.ipv6.conf.all.forwarding = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
user01@user01-ubnt:~$

```

Figura 43 – Recarregamento de variáveis do Kernel no Ubuntu

Em seguida, deve ser verificado se o serviço do strongswan esta a correr com o comando: `systemctl status strongswan.service` cf. Figura 44

```

Menu
user01@user01-ubnt: ~
File Edit View Search Terminal Help
user01@user01-ubnt:~$ sudo systemctl status strongswan.service
● strongswan.service - strongSwan IPsec IKEv1/IKEv2 daemon using swanctl
   Loaded: loaded (/lib/systemd/system/strongswan.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2023-01-31 14:44:11 MET; 7m1n ago
     Main PID: 1998 (charon-systemd)
       Status: "charon-systemd running, strongSwan 5.8.2, Linux 5.15.0-58-generic, x86_64"
        Tasks: 17 (limit: 9888)
       Memory: 2.1M
       CGroup: /system.slice/strongswan.service
              └─1998 /usr/sbin/charon-systemd

Jan 31 14:44:11 user01-ubnt systemd[1]: Starting strongSwan IPsec IKEv1/IKEv2 daemon using swanctl...
Jan 31 14:44:11 user01-ubnt charon-systemd[1998]: loaded plugins: charon-systemd aesni aes rc2 sha2 sha1 md5 mgf1 random nonce x509 revocation constraints
Jan 31 14:44:11 user01-ubnt charon-systemd[1998]: dropped capabilities, running as uid 0, gid 0
Jan 31 14:44:11 user01-ubnt charon-systemd[1998]: spawning 16 worker threads
Jan 31 14:44:11 user01-ubnt swanctl[2017]: no files found matching '/etc/swanctl/conf.d/*.conf'
Jan 31 14:44:11 user01-ubnt swanctl[2017]: no authorities found, 0 unloaded
Jan 31 14:44:11 user01-ubnt swanctl[2017]: no pools found, 0 unloaded
Jan 31 14:44:11 user01-ubnt swanctl[2017]: no connections found, 0 unloaded
Jan 31 14:44:11 user01-ubnt systemd[1]: Started strongSwan IPsec IKEv1/IKEv2 daemon using swanctl.
user01@user01-ubnt:~$

```

Figura 44 – Verificação do serviço do strongswan

A configuração do strongswan, assenta em dois ficheiros:

- /etc/ipsec.conf
- /etc/ipsec.secrets

De forma a configurar por exemplo um utilizador registado, deve ser acrescentado o seguinte conteúdo ao ficheiro: /etc/ipsec.conf

```
config setup
    charondebug="dmn 2, mgr 2, ike 2, chd 2, job 2, cfg 2, knl 2, net 2, enc2, lib 2"
    nat_traversal = yes
```

```
conn IPP-Registado
    keyexchange=ikev1
    ikelifetime=1440m
    keylife=720m
    aggressive=yes
    ike=aes256-sha512-modp2048
    esp=aes256-sha512-modp2048
    xauth=client
    leftid=VPN_REGISTERED
    left=%defaultroute
    leftsourceip=%config
    modeconfig=pull
    leftauth=psk
    leftauth2=xauth
    right=vpnssl.ipp.pt
    rightauth=psk
    rightid=vpnssl.ipp.pt
    rightsubnet=0.0.0.0/0
    xauth_identity=escola@utilizador.ipp.pt
    auto=add
```

Deve também ser acrescentado as seguintes linhas ao ficheiro: /etc/ipsec.secrets

```
utilizador@escola.ipp.pt : XAUTH "password"
vpnssl.ipp.pt : PSK "qrml2fpa8.@L?OIHKi1\"
```



Chamada de atenção!

As configurações acima, incluem as definições genéricas presentes no ponto 2.1 bem como a credencial do P.Porto

Devem ser ajustados os parâmetros, do utilizador e palavra passe com a credencial do P.Porto

De seguida, devem ser reiniciados os serviços e, recarregadas as novas configurações com o comando:

```
sudo systemctl restart strongswan && sudo ipsec update && sudo ipsec reload
```


Conforme cf. Figura 45

```
user01@user01-ubnt: ~
┌───┴───┐
│ Menu  │
└───┴───┘
user01@user01-ubnt: ~
File Edit View Search Terminal Help
user01@user01-ubnt:~$ sudo vim /etc/ipsec.conf
user01@user01-ubnt:~$ vim /etc/ipsec.secrets
user01@user01-ubnt:~$ sudo vim /etc/ipsec.conf
user01@user01-ubnt:~$ sudo vim /etc/ipsec.secrets
user01@user01-ubnt:~$ sudo systemctl restart strongswan && sudo ipsec update && sudo ipsec reload
Updating strongSwan IPsec configuration...
Reloading strongSwan IPsec configuration...
user01@user01-ubnt:~$
```

Figura 45 – Reiniciar o serviço e recarregar definições do strongswan no Ubuntu 20.04

Finalmente, para efetuar a ligação é necessário correr o comando:

```
sudo ipsec up IPP-Registado
```

Conforme Figura 46

```
user01@user01-ubnt: ~
┌───┴───┐
│ Menu  │
└───┴───┘
user01@user01-ubnt: ~
File Edit View Search Terminal Help
user01@user01-ubnt:~$ sudo ipsec up IPP-Registado
initiating Aggressive Mode IKE_SA IPP-Registado[1] to 193.136.56.27
generating AGGRESSIVE request 0 [ SA KE No ID V V V V ]
sending packet: from 10.0.2.15[4500] to 193.136.56.27[500] (570 bytes)
received packet: from 193.136.56.27[500] to 10.0.2.15[500] (725 bytes)
parsed AGGRESSIVE response 0 [ SA KE No ID HASH V NAT-D NAT-D V V V V ]
received NAT-T (RFC 3947) vendor ID
received DPD vendor ID
received XAuth vendor ID
received unknown vendor ID: 82:99:03:17:57:a3:60:82:c6:a6:21:de:00:00:00:00
received FRAGMENTATION vendor ID
received FRAGMENTATION vendor ID
selected proposal: IKE:AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/MODP_2048
local host is behind NAT, sending keep alives
generating AGGRESSIVE request 0 [ HASH NAT-D NAT-D ]
sending packet: from 10.0.2.15[4500] to 193.136.56.27[4500] (236 bytes)
received packet: from 193.136.56.27[4500] to 10.0.2.15[4500] (124 bytes)
parsed TRANSACTION request 2436631114 [ HASH CPRQ(X_TYPE X_USER X_PWD) ]
generating TRANSACTION response 2436631114 [ HASH CPRP(X_USER X_PWD) ]
sending packet: from 10.0.2.15[4500] to 193.136.56.27[4500] (156 bytes)
received packet: from 193.136.56.27[4500] to 10.0.2.15[4500] (124 bytes)
parsed TRANSACTION request 3276165429 [ HASH CPS(X_STATUS) ]
XAuth authentication of 'ricardoc@sc.ipp.pt' (myself) successful
IKE_SA IPP-Registado[1] established between 10.0.2.15[VPN_REGISTERED]...193.136.56.27[vpnssl.ipp.pt]
scheduling reauthentication in 85479s
maximum IKE_SA lifetime 86019s
generating TRANSACTION response 3276165429 [ HASH CPA(X_STATUS) ]
sending packet: from 10.0.2.15[4500] to 193.136.56.27[4500] (124 bytes)
generating TRANSACTION request 1034959570 [ HASH CPRQ(ADDR DNS) ]
sending packet: from 10.0.2.15[4500] to 193.136.56.27[4500] (124 bytes)
received packet: from 193.136.56.27[4500] to 10.0.2.15[4500] (140 bytes)
parsed TRANSACTION response 1034959570 [ HASH CPRP(ADDR DNS DNS) ]
installing DNS server 193.136.56.10 to /etc/resolv.conf
installing DNS server 193.136.56.9 to /etc/resolv.conf
installing new virtual IP 193.136.70.61
generating QUICK_MODE request 1923350932 [ HASH SA No KE ID ID ]
sending packet: from 10.0.2.15[4500] to 193.136.56.27[4500] (492 bytes)
received packet: from 193.136.56.27[4500] to 10.0.2.15[4500] (492 bytes)
parsed QUICK_MODE response 1923350932 [ HASH SA No KE ID ID ]
selected proposal: ESP:AES_CBC_256/HMAC_SHA2_512_256/MODP_2048/NO_EXT_SEQ
CHILD_SA IPP-Registado[1] established with SPIs c79f81e2_i 064eb9ce_o and TS 193.136.70.61/32 == 0.0.0.0/0
connection 'IPP-Registado' established successfully
user01@user01-ubnt:~$
```

Figura 46 – Ligação da VPN no Ubuntu 20.04

É possível também desligar a vpn com o comando:

```
sudo ipsec down IPP-Registado
```

Conforme Figura 47

```
user01@user01-ubuntu:~$ sudo ipsec down IPP-Registado
closing CHILD_SA IPP-Registado[1] with SPIs c79f81e2_i (0 bytes) 064eb9ce_o (1303 bytes) and TS 193.136.70.61/32 == 0.0.0.0/0
sending DELETE for ESP_CHILD_SA with SPI c79f81e2
generating INFORMATIONAL_V1 request 1000701468 [ HASH D ]
sending packet: from 10.0.2.15[4500] to 193.136.56.27[4500] (124 bytes)
deleting IKE_SA IPP-Registado[1] between 10.0.2.15[VPN_REGISTERED]...193.136.56.27[vpnssl.ipp.pt]
sending DELETE for IKE_SA IPP-Registado[1]
generating INFORMATIONAL_V1 request 2588596883 [ HASH D ]
sending packet: from 10.0.2.15[4500] to 193.136.56.27[4500] (140 bytes)
removing DNS server 193.136.56.9 from /etc/resolv.conf
removing DNS server 193.136.56.10 from /etc/resolv.conf
IKE_SA [1] closed successfully
user01@user01-ubuntu:~$
```

Figura 47 – Desligar a VPN no Ubuntu 20.04



Chamada de atenção!

As configurações acima, incluem as definições genéricas presentes no ponto 2.1

Devem ser ajustados os parâmetros, do utilizador e palavra passe com a credencial do P.Porto