

VPN Celepar

Leslie H. Watter

10 de abril de 2023

Sumário

1	Instruções Gerais	2
2	Esquema do Funcionamento VPN	2
3	Configuração do VNC na estação de trabalho	2
3.1	Gnome	2
3.2	Outros Gerenciadores de janela	2
4	Dicas para acelerar a conexão	4
5	Cliente VNC para acesso à máquina após fechar a VPN	4
5.1	Cliente Windows	4
5.2	Cliente Linux	4
5.3	Cliente Multi OS	4
6	Usando o SSH para acessar sua máquina remotamente	5
7	Fechando a VPN no SSLVPN na linha de comando	6
8	Configuração no Net Virtua	7
9	SSLVPN no MAC	8
10	Cliente de VPN Checkpoint	8
11	Criação de VPN CISCO no MAC	8
11.1	Crie uma conexão VPN	8
11.2	Informe os dados de Acesso	8
11.3	Complemente com Informações do Grupo	9
11.4	Autentique-se para fechar a conexão	9
12	Cliente Checkpoint para MAC	12
13	Cliente para Celular Android na Play Store	15

1 Instruções Gerais

- Link com as instruções para uso da vpn em casa: <http://www.pr.gov.br/vpn>

Alguns links que antes eram intranet e disponibilizaram temporariamente para internet.

- Para desvio de ramal: <http://www.pabx.celepar.pr.gov.br>
- Férias: <http://www.ferias.celepar.pr.gov.br>

Quem acessar da Celepar (usando a VPN), continuará a usar o endereço intranet.

2 Esquema do Funcionamento VPN

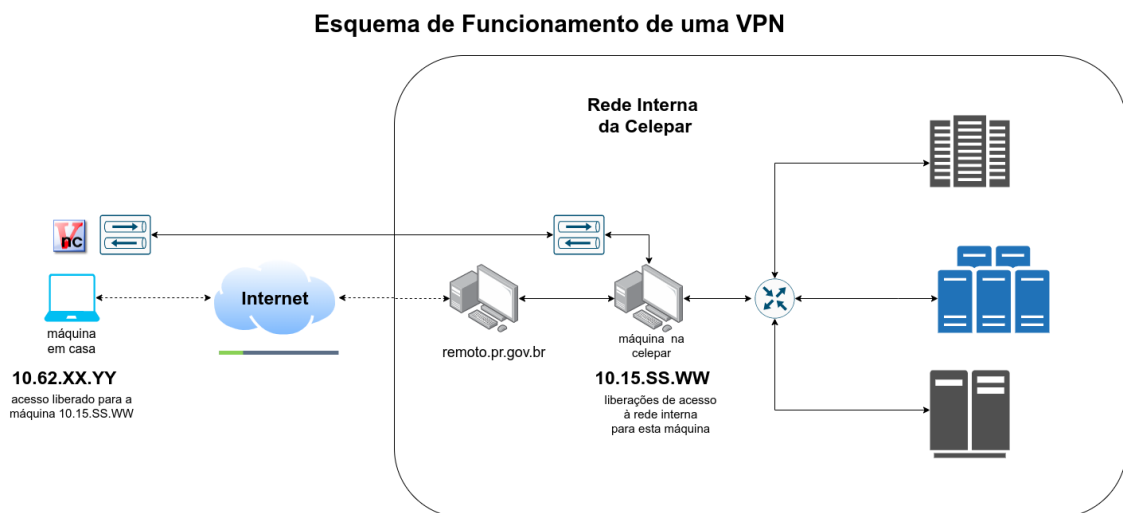


Figura 1: Esquema de Funcionamento VPN

3 Configuração do VNC na estação de trabalho

Para que o vnc funcione é necessário que o **vino-server** esteja rodando.

3.1 Gnome

Quem usa o gnome basta acionar o menu [F2] e digitar "Preferencias do Compartilhamento da area de trabalho".

- Marque "Permitir que outros usuários vejam a sua tela"
- Desmarque "Você deve confirmar cada acesso à essa máquina"
- Marque "Exigir que o usuário digite esta senha" e informe a senha que quiser
- Clique no botão *Fechar*

3.2 Outros Gerenciadores de janela

Caso você não tenha acesso gráfico, mas consiga acesso texto, execute os comandos abaixo:

```
# instala o servidor
sudo apt-get install vino-server
# habilita a chamada
gsettings set org.gnome.Vino enabled true
# retira necessidade de cripto
gsettings set org.gnome.vino require-encryption false
```

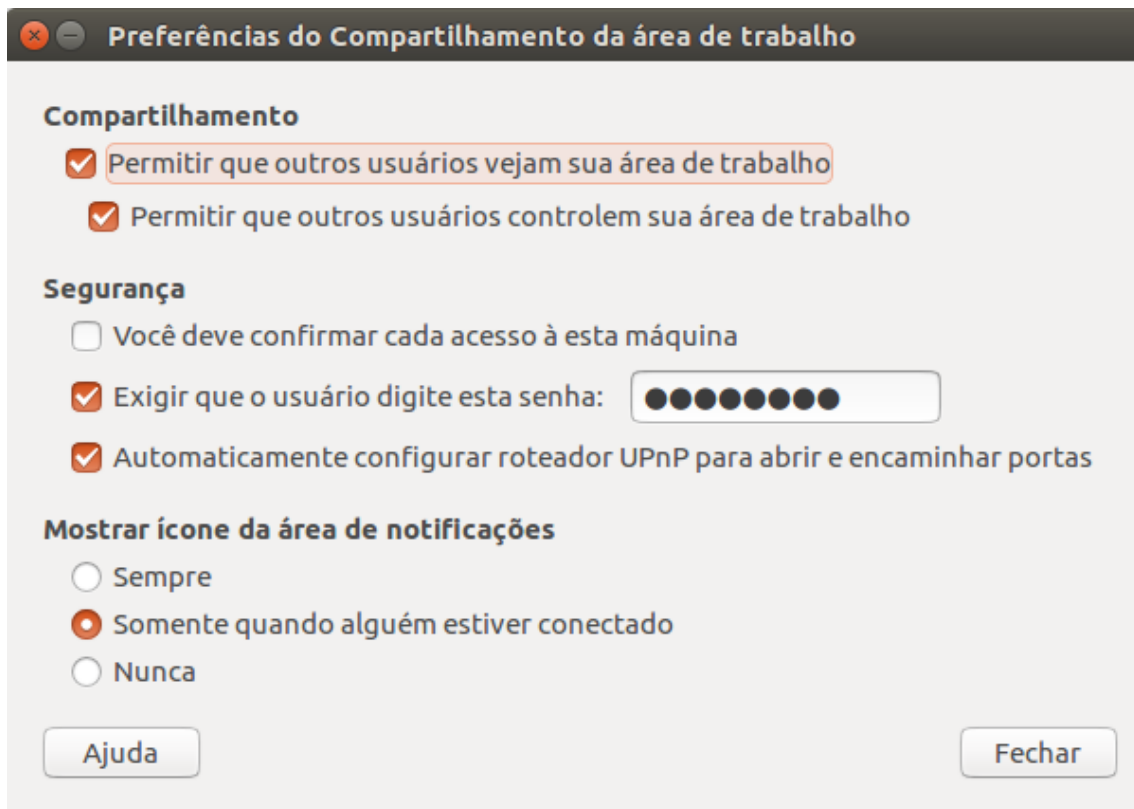


Figura 2: Preferencias de acesso do vino-server

```
# habilita a autenticação usando o vnc
gsettings set org.gnome.Vino authentication-methods "['vnc']"

# gera a senha em base64
echo -n 'vpasswd' | base64
dnBhc3N3ZA==

# configura a senha
gsettings set org.gnome.Vino vnc-password 'dnBhc3N3ZA=='
# remove o prompt local
gsettings set org.gnome.Vino prompt-enabled false
```

Caso consiga um terminal gráfico (`ssh -X usuario@ip`), você pode executar:

```
# export DISPLAY=:0.0
# xhost 10.20.30.40
vino-preferences &
```

E será mostrada a janela da figura 2:

- Marque "Permitir que outros usuários vejam a sua tela"
- Desmarque "Você deve confirmar cada acesso à essa máquina"
- Marque "Exigir que o usuário digite esta senha" e informe a senha que quiser
- Clique no botão *Fechar*
- Inicie o servidor manualmente

```
/usr/lib/vino/vino-server & # para iniciar o servidor vnc
```

4 Dicas para acelerar a conexão

1. Para quem tem dois monitores, desative um monitor.
2. Reduza a resolução do seu monitor de 1900x1080 para por exemplo 1600x837 (ou algo parecido)

Essas configurações podem ser feitas em 'Configurações do Sistema' -> 'Monitores'.

5 Cliente VNC para acesso à máquina após fechar a VPN

Após a conexão completa com a VPN, precisa usar um cliente VNC para acessar sua máquina na Celepar.

5.1 Cliente Windows

O Cliente VPN sugerido para uso (sem suporte) pode ser encontrado no link: <https://www.shrew.net/download> opção **Standard**

- Windows 8 e acima: <http://www.shrew.net/download/vpn/vpn-client-2.2.2-release.exe>

Para estabelecer a conexão é necessário importar o arquivo **.pcf** do perfil correspondente vpn no cliente; Utilize a sua autenticação (usuário e senha) LDAP/Expresso;

5.2 Cliente Linux

Um cliente mais *leve* (e normalmente já instalado) é o Remmina: <https://remmina.org/>

- Para instalar: <https://remmina.org/how-to-install-remmina/>

No Ubuntu:

```
sudo apt-get install remmina
```

O remmina permite selecionar a qualidade da imagem (baixa, média, alta) que vai influenciar diretamente na velocidade e quantidade de banda necessárias para a transmissão.

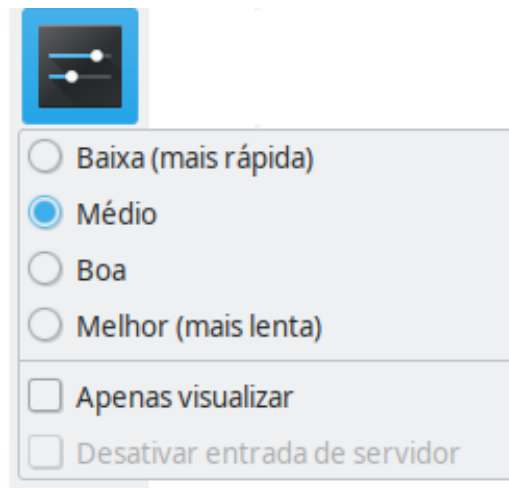


Figura 3: Qualidade da conexão

5.3 Cliente Multi OS

Caso não tenha um cliente instalado, baixe o realvnc no link: <http://www.realvnc.com/pt/connect/download/viewer/>

Após instalar o VNC Client, basta adicionar o IP da máquina.

6 Usando o SSH para acessar sua máquina remotamente

É possível também utilizar o `ssh` para conectar na sua máquina (caso vc tenha acesso ssh na sua máquina).

Após fechar a VPN, você pode fazer:

```
ssh -Y usuario@end_IP_sua_maquina comando
```

A opção a ser usada no ssh é `-Y` (`_Y Enables trusted X11 forwarding. Trusted X11 forwardings are not subjected to the X11 SECURITY extension controls._`)

O comando abaixo irá executar o `firefox` na sua máquina na empresa e mostrar a interface gráfica na sua máquina local (em casa).

```
ssh -Y usuario@end_IP_sua_maquina /usr/bin/firefox
```

Lembrete: é necessário ter a opção **X11Forwarding** habilitada na configuração do ssh (`/etc/ssh/sshd_config`)

```
~# cat /etc/ssh/sshd_config | grep X11F
X11Forwarding yes
~#
```

Caso não funcione de cara, lembre-se de executar o comando:

```
xhost +END.IP.EMPRESA
```

Troque `END.IP.EMPRESA` pelo endereço IP da sua máquina na empresa.

7 Fechando a VPN no SSLVPN na linha de comando

Existe um cliente linha de comando que funciona corretamente, é o **snx**. A orientação original pode ser encontrada em <https://unix.stackexchange.com/a/453727> e foi indicação do @leandroaraujo.

O @jurandirjcg precisou usar a versão E82.00 disponível no link com todas as versões.

Para instalar o **snx build 800007075**, baixe ele:

```
wget https://starkers.keybase.pub/snx_install_linux30.sh?dl=1 -O snx_install.sh
```

Para as estações baseadas em Debian/Ubuntu execute os seguintes comandos para adicionar a arquitetura 32-bits:

```
sudo dpkg --add-architecture i386
sudo apt-get update
```

Instale os seguintes pacotes:

```
sudo apt-get install libstdc++5:i386 libx11-6:i386 libpam0g:i386
```

Execute o script de instalação do snx:

```
chmod a+rx snx_install.sh
sudo ./snx_install.sh
```

Nesse ponto o binário do snx 32-bits está instalado no seu sistema. É necessário verificar se alguma biblioteca dinâmica está faltando usando o comando:

```
sudo ldd /usr/bin/snx
```

Só passe para o próximo passo se as dependências estiverem todas satisfeitas, por exemplo:

```
$ sudo ldd /usr/bin/snx
linux-gate.so.1 (0xf7f05000)
libX11.so.6 => /usr/lib/i386-linux-gnu/libX11.so.6 (0xf7d79000)
libpthread.so.0 => /lib/i386-linux-gnu/libpthread.so.0 (0xf7d5a000)
libresolv.so.2 => /lib/i386-linux-gnu/libresolv.so.2 (0xf7d42000)
libdl.so.2 => /lib/i386-linux-gnu/libdl.so.2 (0xf7d3d000)
libpam.so.0 => /lib/i386-linux-gnu/libpam.so.0 (0xf7d2d000)
libnsl.so.1 => /lib/i386-linux-gnu/libnsl.so.1 (0xf7d12000)
libstdc++.so.5 => /usr/lib/i386-linux-gnu/libstdc++.so.5 (0xf7c53000)
libc.so.6 => /lib/i386-linux-gnu/libc.so.6 (0xf7a77000)
libxcb.so.1 => /usr/lib/i386-linux-gnu/libxcb.so.1 (0xf7a4b000)
/lib/ld-linux.so.2 (0xf7f07000)
libaudit.so.1 => /lib/i386-linux-gnu/libaudit.so.1 (0xf7a21000)
libm.so.6 => /lib/i386-linux-gnu/libm.so.6 (0xf791d000)
libgcc_s.so.1 => /lib/i386-linux-gnu/libgcc_s.so.1 (0xf78ff000)
libXau.so.6 => /usr/lib/i386-linux-gnu/libXau.so.6 (0xf78fa000)
libXdmcp.so.6 => /usr/lib/i386-linux-gnu/libXdmcp.so.6 (0xf78f3000)
libcap-ng.so.0 => /lib/i386-linux-gnu/libcap-ng.so.0 (0xf78ed000)
libbsd.so.0 => /lib/i386-linux-gnu/libbsd.so.0 (0xf78d2000)
librt.so.1 => /lib/i386-linux-gnu/librt.so.1 (0xf78c8000)
```

Caso falte algum pacote, provavelmente ele está listado na lista de dependências do sslvpn no modo gráfico.

Para conectar na VPN manualmente use o comando:

```
snx -s sslvpn.pr.gov.br -u USER
```

Ao conectar você receberá uma saída parecida com a abaixo:

```
$ snx
Check Point's Linux SNX
build 800007075
Please enter your password:

SNX - connected.
```

Session parameters:

=====

Office Mode IP : 10.x.x.x
DNS Server : 10.x.x.x
Secondary DNS Server: 10.x.x.x
DNS Suffix : xxx.xx, xxx.xx
Timeout : 24 hours

Para desconectar execute o comando:

```
snx -d
```

8 Configuração no Net Virtua

Nota: A configuração abaixo somente deve ser feita caso não se consiga estabelecer a VPN normalmente.

Para alguns usuários do NET Virtua se faz necessário habilitar no modem as opções *IPSec PassThrough* e *PPTP PassThrough*:

Procedimentos:

- Modem da NET
 - Configurações Avançadas
 - Menu
 - * Avançado
 - Opções avançadas
 - Habilitar *IPSec PassThrough*
 - Aplicar
 - Resetar modem

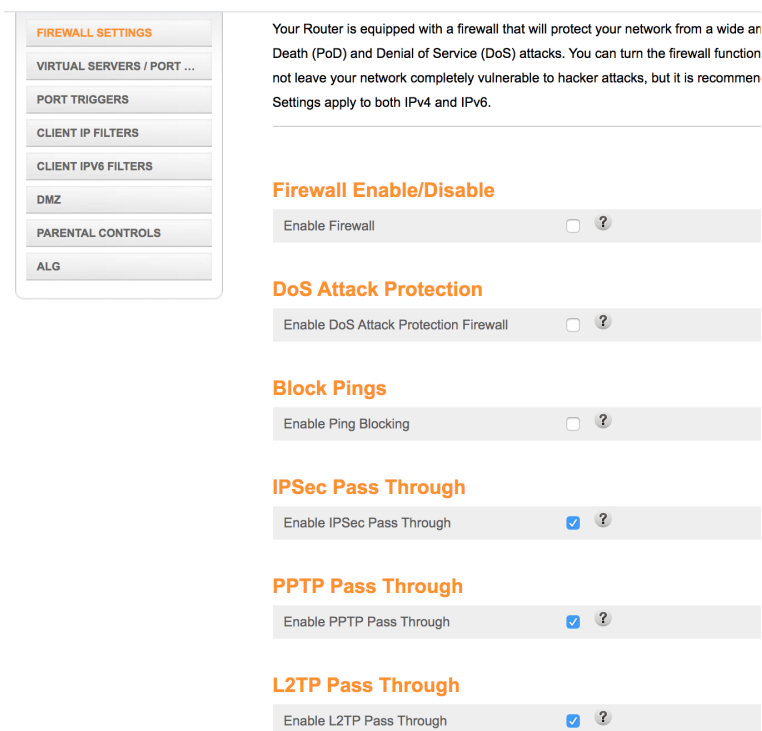


Figura 4: Configuração do Modem (cedido por @jakjr)

9 SSLVPN no MAC

Alguns usuários estão com problemas em estabelecer a VPN usando o `sslvpn` com o firefox no MAC.

Faça o **downgrade do Firefox para a versão 51**. Segundo @jurandirjcg e @pcsantana, resolve a situação.

<https://www.techtudo.com.br/dicas-e-tutoriais/noticia/2017/03/atualizou-para-o-firefox-52-e-ficou-sem-html>

10 Cliente de VPN Checkpoint

Instale e configure o cliente do endereço:

https://supportcenter.checkpoint.com/supportcenter/portal/user/anon/page/default.psml/media-type/html?action=portlets.DCFileAction&eventSubmit_doGetdcdetails=&fileid=96032

Informando como ponto de chegada o endereço **sslvpn.pr.gov.br** e na última tela coloque autenticação com usuário e senha.

11 Criação de VPN CISCO no MAC

Procedimento para abrir a VPN no Mac:

11.1 Crie uma conexão VPN

- Vá nas configurações de rede como ilustrado na figura 5
 - acrescente uma interface: **VPN**
 - Tipo de VPN: **CISCO IPSec**
 - Nome do Serviço: **celepar** (nome da conexão)

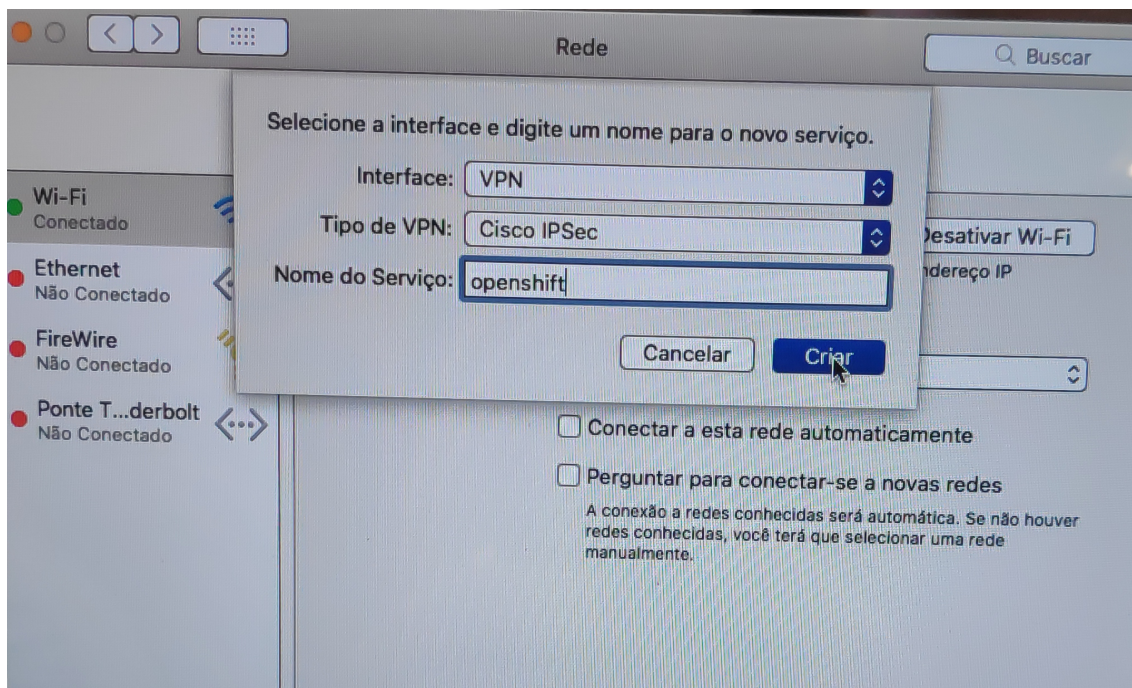


Figura 5:

11.2 Informe os dados de Acesso

- Após isso informe os dados conforme a figura 6
 - Endereço do Servidor: **remoto.pr.gov.br**

- Nome da Conta: **usuário do LDAP/Expresso**
- Senha: **senha do usuário LDAP/Expresso**

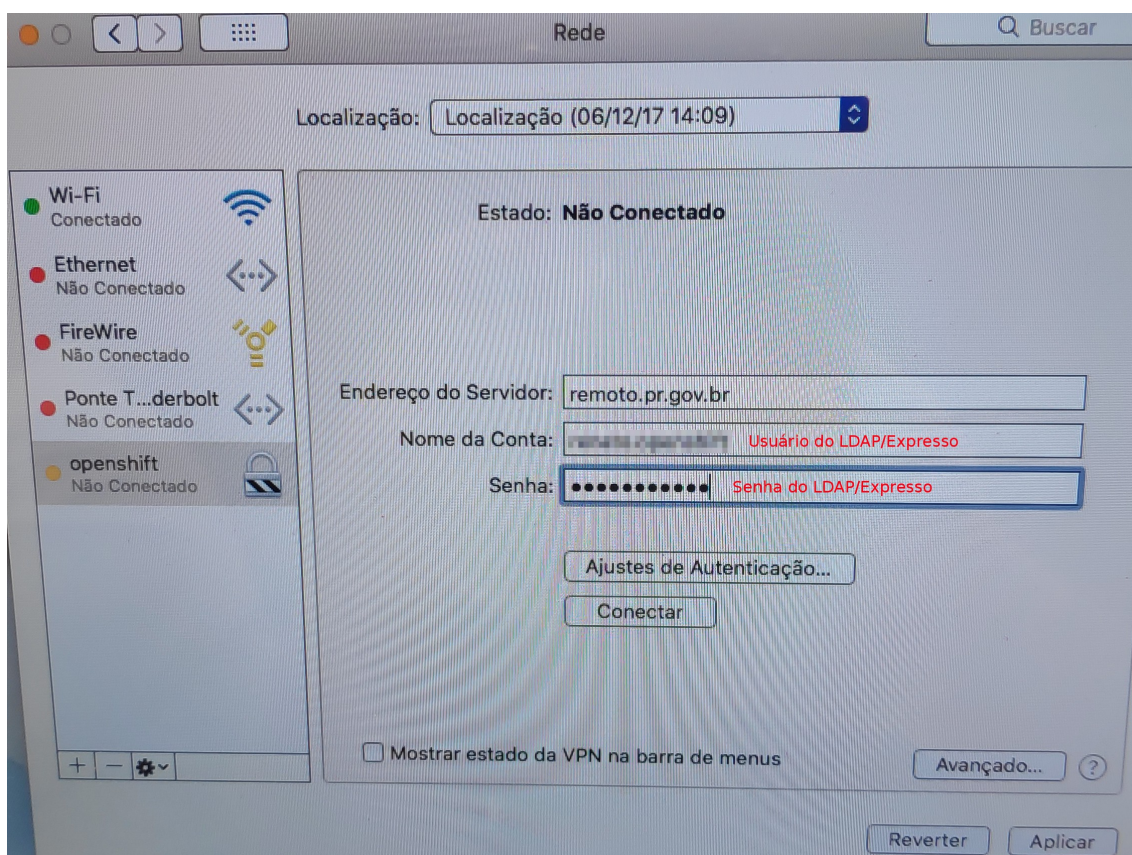


Figura 6:

11.3 Complemente com Informações do Grupo

- Clique em **Avançado** e informe os dados do grupo conforme figura 7:
 - Segredo Compartilhado: **senha do grupo**
 - Nome do Grupo: **nome do grupo vpn** - usualmente **vpn-celepar-...**
- Caso não saiba a senha do grupo (veja figura 8)
 - Abra o arquivo **.pcf** que você recebeu e copie o trecho que está na linha **enc_GroupPwd=...**
 - Acesse o site **cisco vpnclient password decoder** e cole somente o texto após o trecho **enc_GroupPwd=**
 - * A senha do grupo será mostrada na última linha: **Clear**

11.4 Autentique-se para fechar a conexão

- Clique em **Conectar** (figura 9).
 - Será solicitada sua credencial de acesso (usuário e senha LDAP/Expresso)
- Pronto! Você já pode navegar ;)

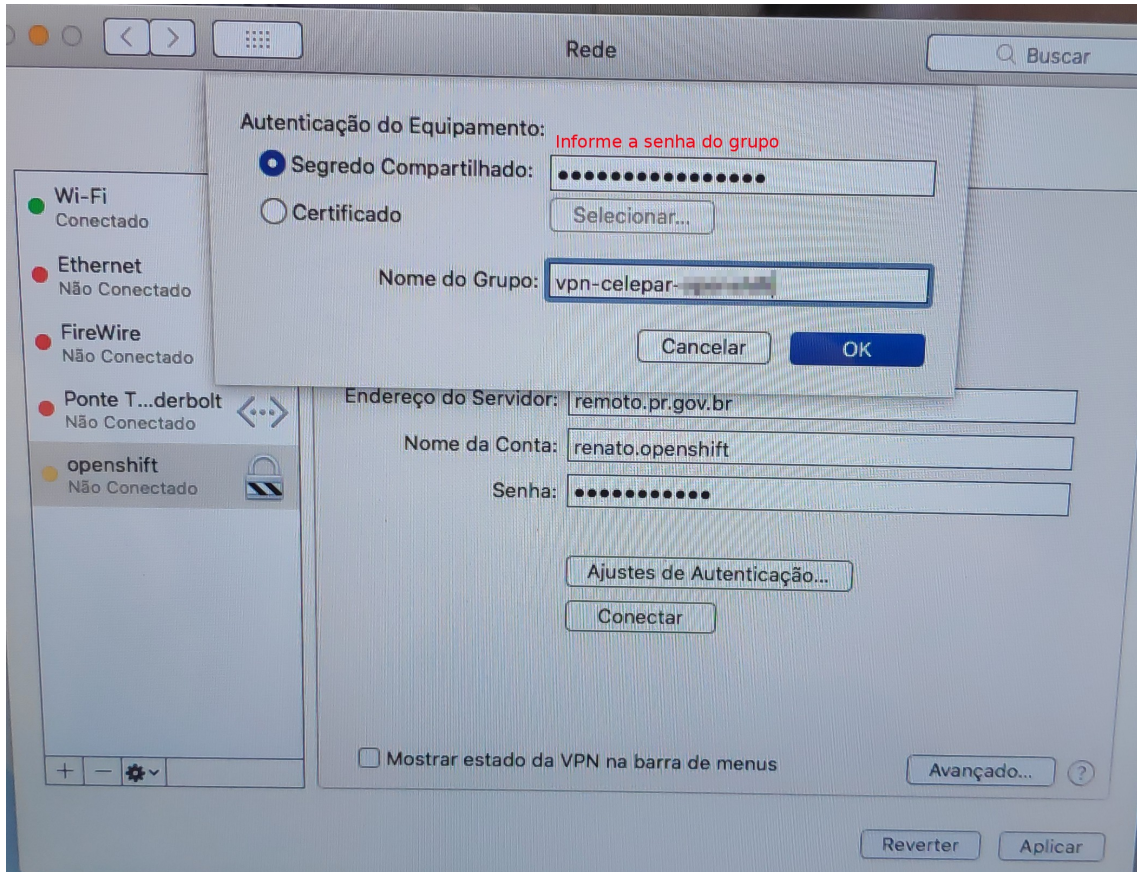


Figura 7:



Figura 8:

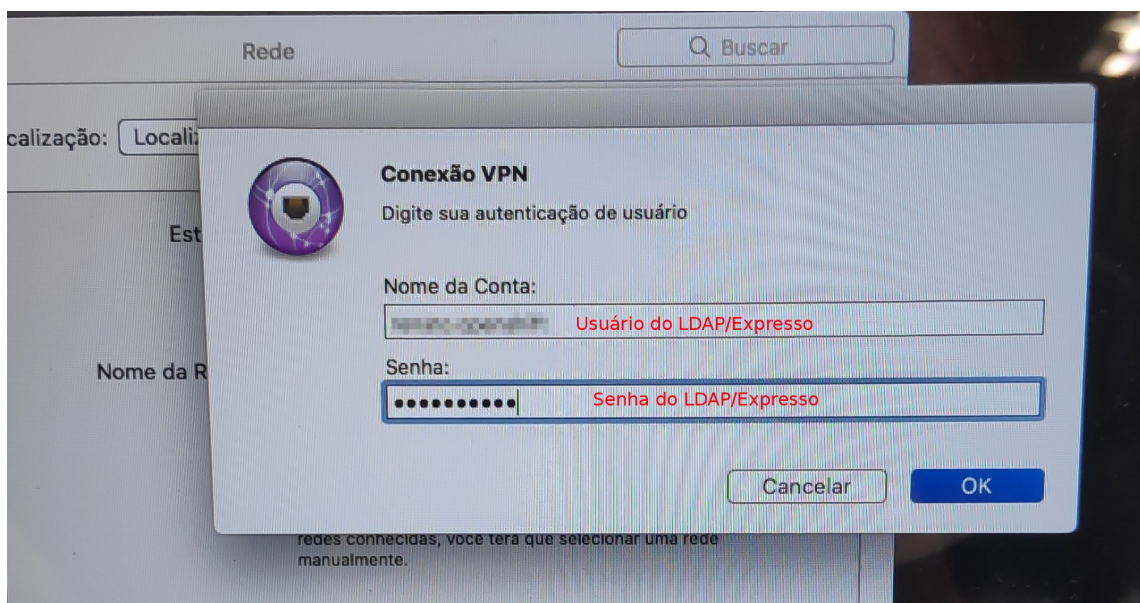


Figura 9:

12 Cliente Checkpoint para MAC

Contribuição do @pmenezes: Cliente pra MAC da checkpoint

https://supportcenter.checkpoint.com/supportcenter/portal/user/anon/page/default.psml/media-type/html?action=portlets.DCFileAction&eventSubmit_doGetdcdetails=&fileid=77603

Fica como opção ao navegador...

- Só conectar no endereço: **sslvpn.pr.gov.br**
- Vai dar erro de certificado, aí é só aceitar
- Escolher o método de autenticação: username and password

Basta seguir a sequência de imagens para fazer a configuração:

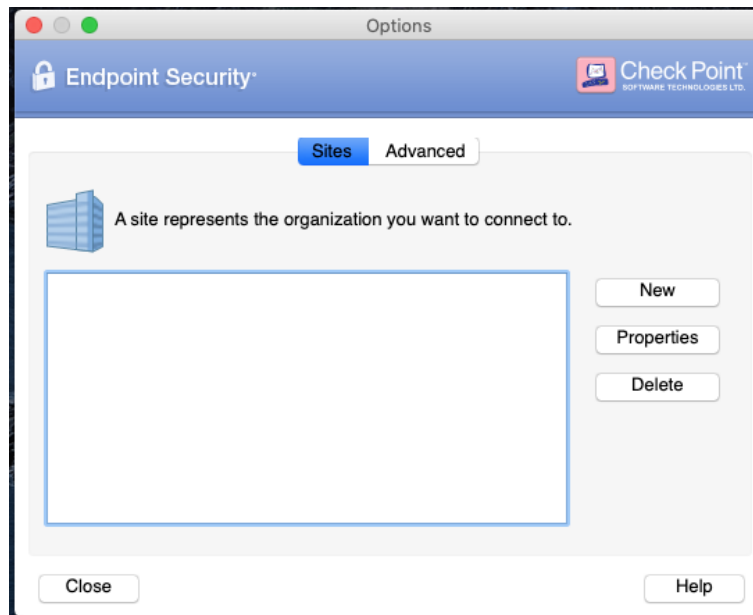


Figura 10:

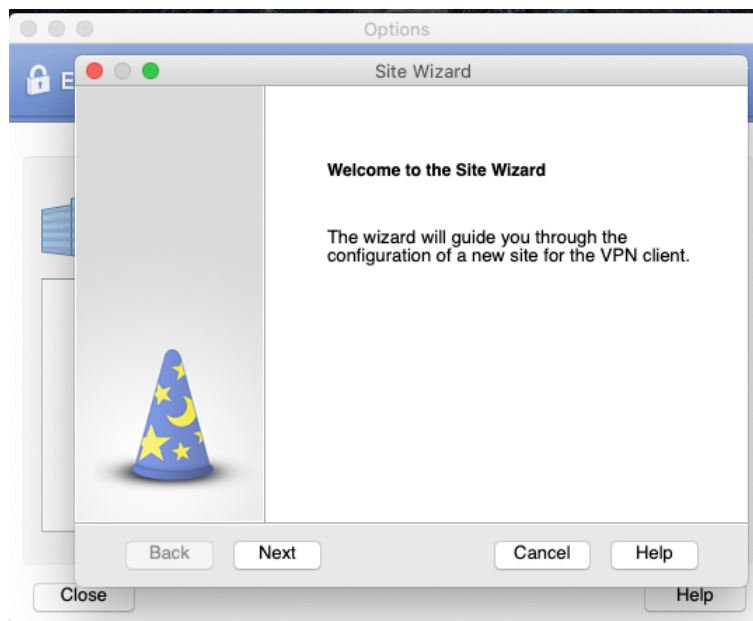


Figura 11:

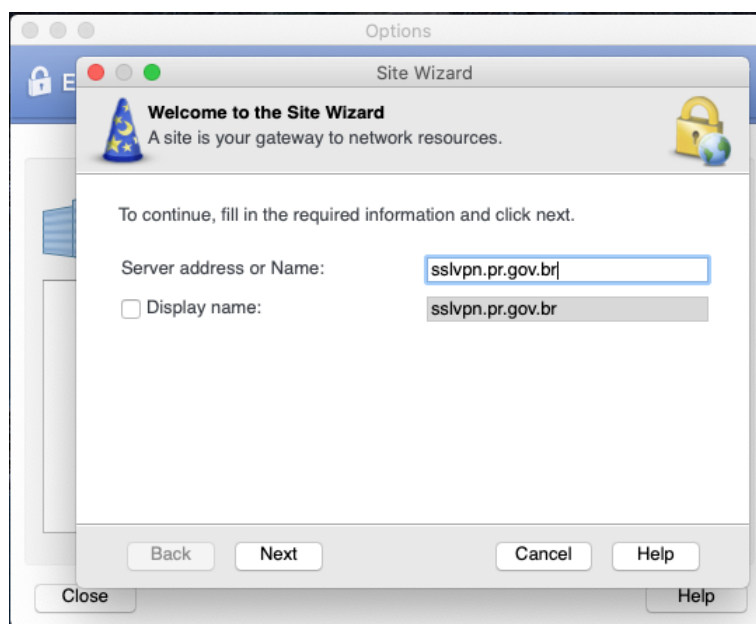


Figura 12:

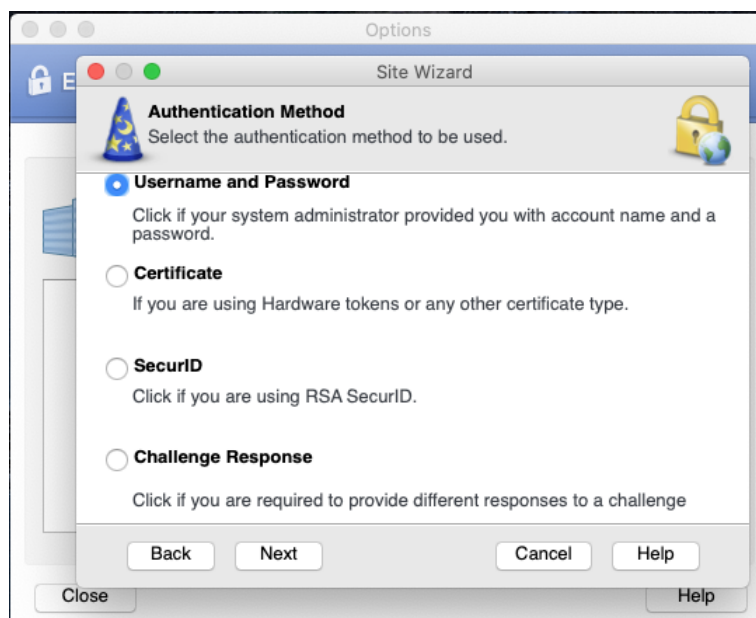


Figura 13:

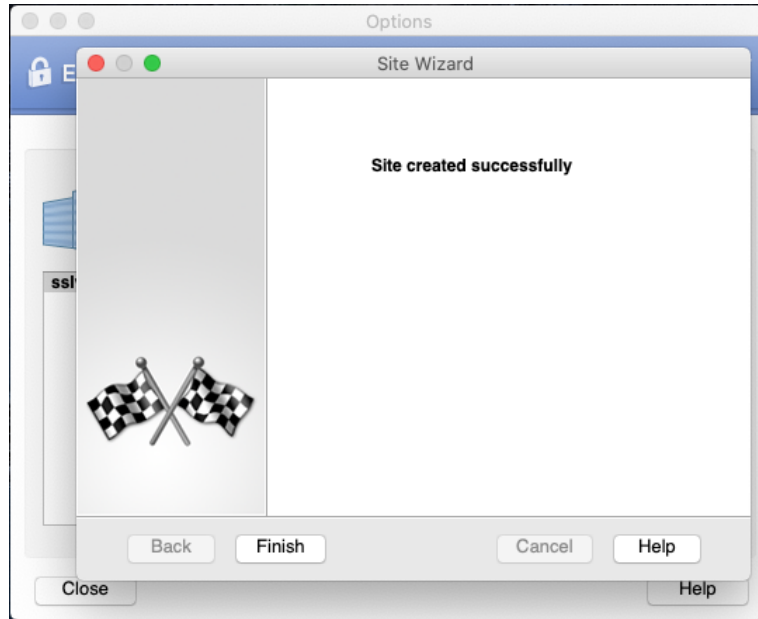


Figura 14:

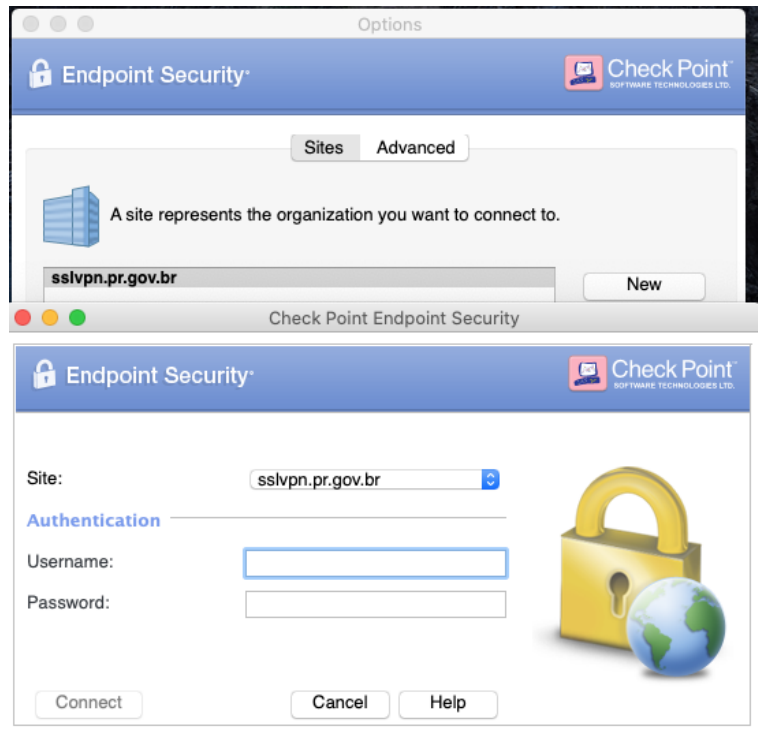


Figura 15:

13 Cliente para Celular Android na Play Store

Use o cliente Capsule VPN da Checkpoint disponível na playstore (link direto). Contribuições @alanzari e @luispaiva.

Para configurar, basta informar o ponto de chegada do SSLVPN: **sslvpn.pr.gov.br** na tela do capsule conforme sequência de imagens:

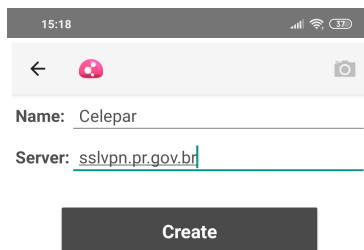


Figura 16: Informe o Servidor

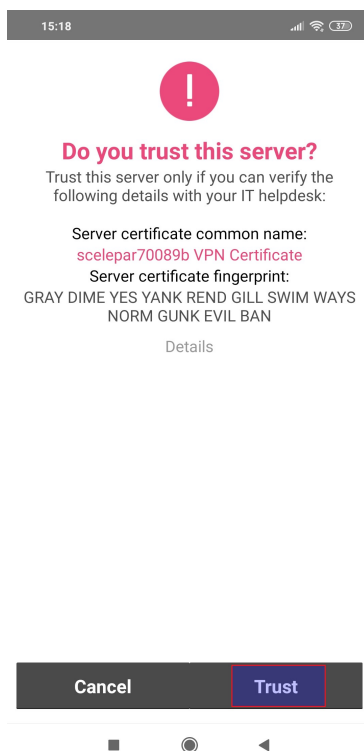


Figura 17: Aceite o Certificado

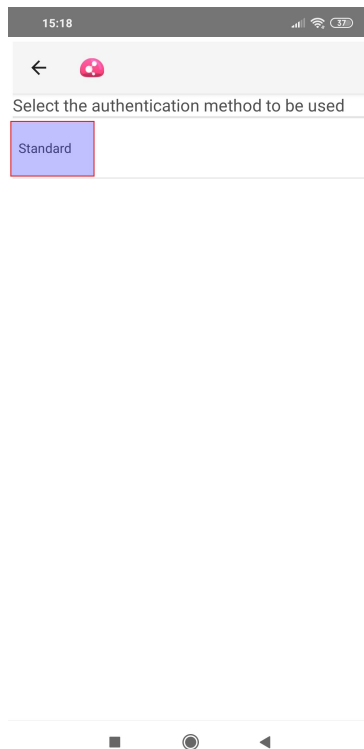


Figura 18: Seleccione Standard como Método de Autenticação

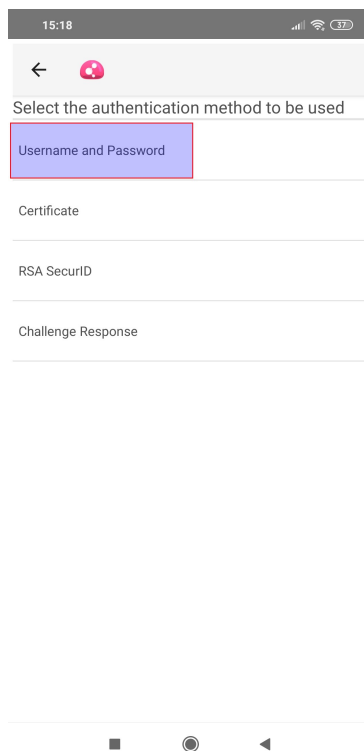


Figura 19: Seleccione Username and Password

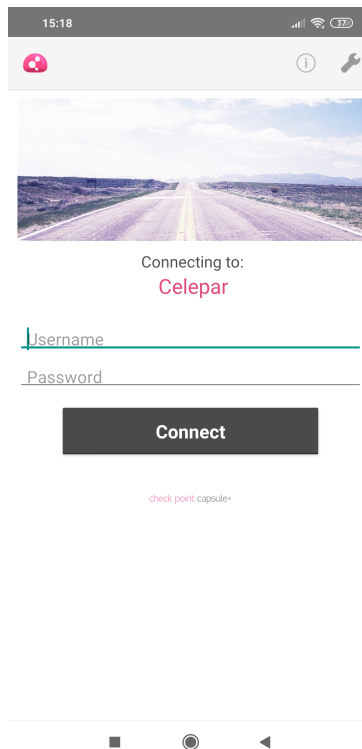


Figura 20: Informe suas Credenciais

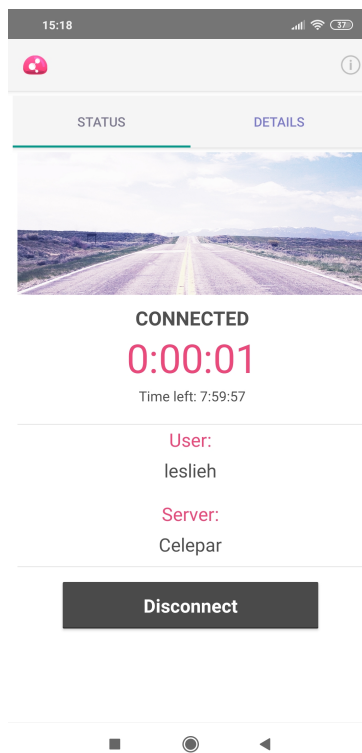


Figura 21: Você está conectado!