FICHA TRABALHO 5

MODALIDADE:	Aprendizagem +	Não aplicável	
CURSO:	Técnico de Cibersegurança		
UC:	Instalar e configurar ferramentas de análise e recolha de logs e evidências	CÓDIGO UC:	UC01485
FORMADOR/A:	Bruno Silva	DATA:	

OBJETIVOS

- Saber como instalar e configurar um servidor OpenVPN Server e ligação com clientes

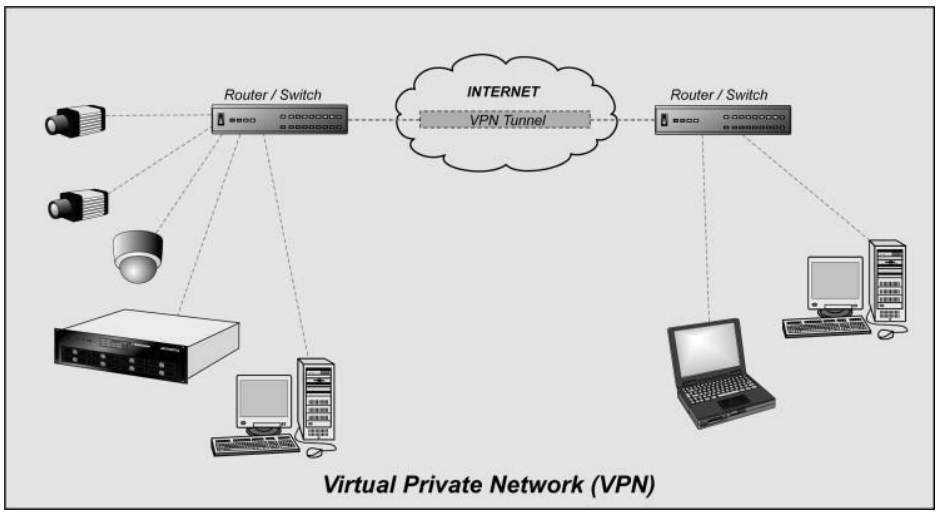
Introdução

A necessidade de Interligar redes ou sub-redes privadas utilizando outras redes para suporte de canais de comunicação seguros e virtualmente dedicados levou o conceito de redes privadas virtuais (VPN - virtual private networks).

A compreensão destes aspetos é essencial na tomada de decisões de projeto de qualquer rede informática, pois, hoje em dia, é vital ter uma comunicação segura entre diferentes sub-redes privadas utilizando infraestruturas públicas, em especial, nesta era digital, à medida que as empresas continuam a expandir as capacidades no trabalho remoto e existe uma necessidade de colocar a privacidade da transmissão de dados de forma segura.

Uma rede virtual privada é uma rede constituída por um conjunto de redes privadas interligadas por circuitos/canais virtuais suportados noutras redes (normalmente públicas, como por exemplo a Internet). De forma a garantir a segurança da comunicação, são utilizadas técnicas de encriptação e autenticação.

Para possibilitar a comunicação segura entre as 2 redes, ambas terão de perceber esquemas para encriptação e autenticação, através da configuração adequada dos sistemas nos extremos do canal que atravessa a rede Internet, que serão denominados, os concentradores de VPN.



Virtual Private Network (VPN)

Os concentradores de VPN podem assumir várias formas, como por exemplo, equipamentos físicos (computadores/servidores com hardware e software dedicados), ou software a correr num router/firewall (que já vem complementados com funcionalidades adicionais de segurança).

Benefícios da VPN

A utilização de VPN's tem benefícios significativos face a outras alternativas, como por exemplo utilização de redes ou circuitos dedicados. Mas como tudo, existe um custo a pagar por todos os benefícios, sendo uma boa parte desse custo alguma degradação do desempenho na comunicação, devido à utilização dos públicos (do qual, podem ter problemas em garantir o nível de qualidade de serviço), e à utilização de mecanismos de segurança.

- A redução de custos de telecomunicações dedicadas. A utilização de redes públicas, para interligar redes privadas e para permitir o acesso remoto tem custos consideravelmente menores do que a utilização de linhas dedicadas e a utilização de linhas telefónicas ou fibras óticas.
- A flexibilidade e da escalabilidade, pois, a utilização de soluções VPN baseadas na Internet são limitadas apenas pela largura de banda disponível e pela capacidade de processamento e não pelo número de utilizadores.
- A confidencialidade deverá ser garantida por encriptação e/ou tunneling, utilizando-se, mecanismos de encriptação comprovados e normas como o IPSec ou L2TP. Para além disso, de verão ter mecanismos de integridade (através de algoritmos hashing, como o SHA, MD5, entre outros), de autenticação (certificados e assinaturas digitais) De autenticação e controlo de acesso (LDAP, X.500, X.509, entre outros).
- Possibilidade de combinações de aplicações de VPN com firewall dedicados, como por exemplo, combinar Open VPN com PFSense;

OpenVPN Server – Instalação e configuração

As VPNs desempenham um papel fundamental na segurança das transmissões de dados, oferecendo experiências de navegação privadas e permitindo acesso a conteúdo restrito. Existe uma infinidade de soluções VPN disponíveis, como o OpenVPN que é uma opção de código aberto poderosa e flexível.

O OpenVPN Access Server (frequentemente abreviado como OpenVPN-AS), baseia-se na base estabelecida pelo projeto open-source da OpenVPN. Este fornece uma versão aprimorada do software com foco comercial, simplificando muitos dos desafios envolvidos na configuração e manutenção de uma VPN.

Embora o OpenVPN necessite configuração manual por meio de linhas de comando, o OpenVPN AS oferece uma interface web amigável, tornando todo o processo de gestão de VPN mais fácil.

Nesta ficha de trabalho, vamos realizar as etapas envolvidas na configuração do servidor de acesso OpenVPN no sistema operativo Ubuntu.

Portanto, se desejam estabelecer uma infraestrutura de trabalho remota, proteger os nossos dados ou contornar restrições esta é uma boa solução para implementar.

Importante:* Antes de começar o tutorial, verifique se a placa de rede da máquina virtual está em *bridge mode!

Passo 1 – Entrar em modo de administrador (comando su e digitar a palavra-passe);

```
silva@silva-Apple-Virtualization-Generic-Platform:~$ su
Palavra-passe:
root@silva-Apple-Virtualization-Generic-Platform:/home/silva#
```

Passo 2 – Atualizar o repositório do sistema operativo e atualizar o sistema operativo (com o comando: ***apt-get update && apt-get upgrade***)

```
apt-get update && apt-get upgrade
```

Se aparecer uma mensagem a questionar se pretende continuar a operação de atualização, basta carregar na tecla y (de yes) e de seguida no enter:

```
xserver-xorg-core xserver-xorg-legacy xwayland
86 pacotes actualizados, 0 pacotes novos instalados, 0 a remover e 5 não actualizados.
É necessário obter 315 MB/421 MB de arquivos.
Após esta operação, serão utilizados 1246 kB adicionais de espaço em disco.
Deseja continuar? [S/n]
```

Passo 3 – Instalar os pacotes de certificados e segurança. Ao instalar os pacotes de segurança de certificados, estamos a fornecer ao nosso sistema a capacidade de obter pacotes com segurança de repositórios baseados em HTTPS. Muitas vezes, esta é uma etapa necessária antes de adicionar estes repositórios à lista de fontes do seu sistema. Use o comando:

apt -y install ca-certificates wget net-tools gnupg

```
root@silva-Apple-Virtualization-Generic-Platform:/home/silva# apt -y install ca-
certificates wget net-tools gnupg
```

Passo 4 – Instalar todas as bibliotecas necessárias para que a aplicação funcione sem problemas (caso contrário não deixa a aplicação instalar no sistema), com o comando:

apt install -y bridge-utils dmidecode iptables iproute2 libc6 libffi7 libgcc-s1 liblz4-1 liblzo2-2 libmariadb3 libpcap0.8 libssl3 libstdc++6 libsasl2-2 libsqlite3-0 net-tools python3-pkg-resources python3-migrate python3-sqlalchemy python3-mysqldb python3-ldap3 sqlite3 zlib1g python3-netaddr python3-arrow python3-lxml python3-constantly python3-hyperlink python3-automat python3-service-identity python3-cffi python3-defusedxml libcap-ng0 libnl-3-200 libnl-genl-3-200 python3-typing-extensions libxmlsec1-openssl libxmlsec1-openssl python3-zope python3-openssl python3-hamcrest python3-incremental

```
root@silva-Apple-Virtualization-Generic-Platform:/home/silva# apt install -y bri
dge-utils dmidecode iptables iproute2 libc6 libffi7 libgcc-s1 liblz4-1 liblzo2-2
 libmariadb3 libpcap0.8 libssl3 libstdc++6 libsasl2-2 libsqlite3-0 net-tools pyt
hon3-pkg-resources python3-migrate python3-sqlalchemy python3-mysqldb python3-ld
ap3 sqlite3 zlib1g python3-netaddr python3-arrow python3-lxml python3-constantly
 python3-hyperlink python3-automat python3-service-identity python3-cffi python3
-defusedxml libcap-ng0 libnl-3-200 libnl-genl-3-200 python3-typing-extensions li
bxmlsec1-openssl libxmlsec1-openssl python3-zope python3-openssl python3-hamcres
t python3-incremental
```

Passo 5 – Instalar a ferramenta curl (para fazer download dos dados através dos endereços das hiperligações via terminal), com o comando: ***apt-get install curl***

```
root@silva-Apple-Virtualization-Generic-Platform:/home/silva# apt-get install curl
```

Passo 6 – Obter a chave pública da aplicação para instalar o programa:

Modo 1 – Utilizar o comando ***curl*** para retirar a chave pública do servidor e colocar no diretório das chaves públicas:

curl -fsSL https://as-repository.openvpn.net/as-repo-public.asc > /etc/apt/trusted.gpg.d/as-repo-public.asc

```
root@silva-Apple-Virtualization-Generic-Platform:/home/silva# curl -fsSL https:/
/as-repository.openvpn.net/as-repo-public.asc > /etc/apt/trusted.gpg.d/as-repo-p
ublic.asc
```

Modo 2 – Caso o ***modo 1 não funcione***, temos de fazer a forma manual:

1. Fazer o download no navegador com a hiperligação: https://as-repository.openvpn.net/as-repo-public.asc

2. Mover o ficheiro das pasta das transferências (tem de estar na localização), para a pasta das chaves do Ubuntu com o comando: ***mv as-repo-public.asc /etc/apt/trusted.gpg.d***

Passo 7 – De seguida, adicione a ligação do repositório OpenVPN Access Server para Ubuntu para conseguir obter e instalar o software do servidor oficial:

- ***x86_64 (processadores 64 bits da Intel)***

  echo "deb [arch=amd64 signed-by=/etc/apt/trusted.gpg.d/as-repo-public.asc] http://as-repository.openvpn.net/as/debian jammy main">/etc/apt/sources.list.d/openvpn-as-repo.list

- ***arm64 (processador M1, M2 e M3 – Apple Silicon)***

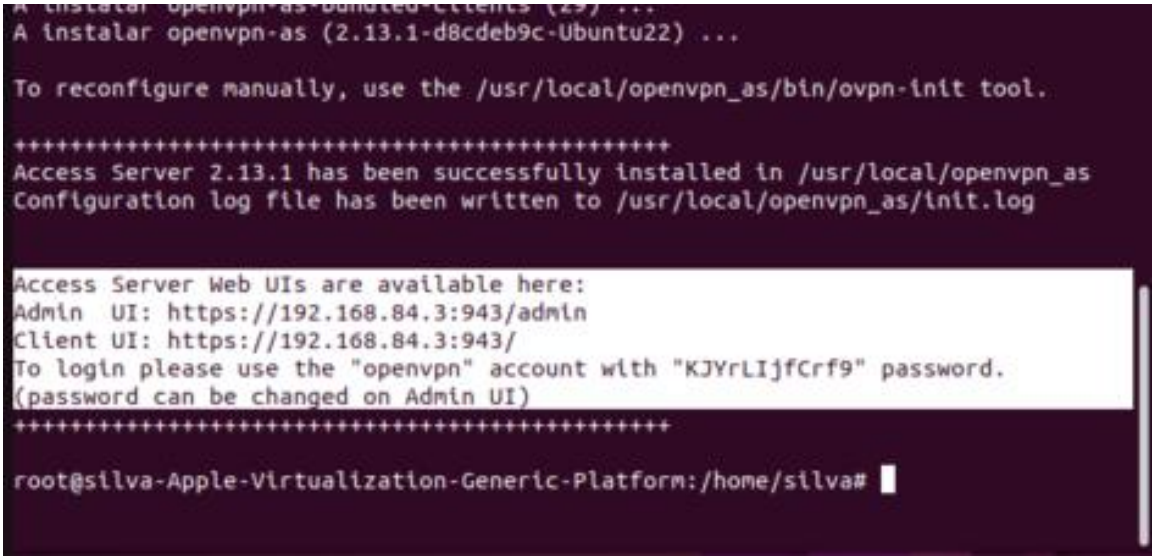
  echo "deb [arch=arm64 signed-by=/etc/apt/trusted.gpg.d/as-repo-public.asc] http://as-repository.openvpn.net/as/debian jammy main">/etc/apt/sources.list.d/openvpn-as-repo.list

```
root@silva-Apple-Virtualization-Generic-Platform:/home/silva# echo "deb [arch=ar
m64 signed-by=/etc/apt/trusted.gpg.d/as-repository.asc] http://as-repository.ope
nvpn.net/as/debian jammy main">/etc/apt/sources.list.d/openvpn-as-repo.list
```

Passo 8 – Prossiga com a instalação do OpenVPN Access Server, com o comando: ***apt update*** e depois o comando ***apt -y install openvpn-as***

```
root@silva-QEMU-Virtual-Machine:/home/silva# apt -y install openvpn-as
```

No final da instalação (se tudo correr bem), vai aparecer a seguinte mensagem, com os dados de acesso a plataforma OpenVPN:



MUITO IMPORTANTE: ***Deve selecionar os dados de acesso e gravar os dados num ficheiro de texto*** para mais tarde conseguir aceder a página de administração do openvpn na seção Admin UI. Se não fizer isto, ficará sem saber os dados de acesso da nossa plataforma

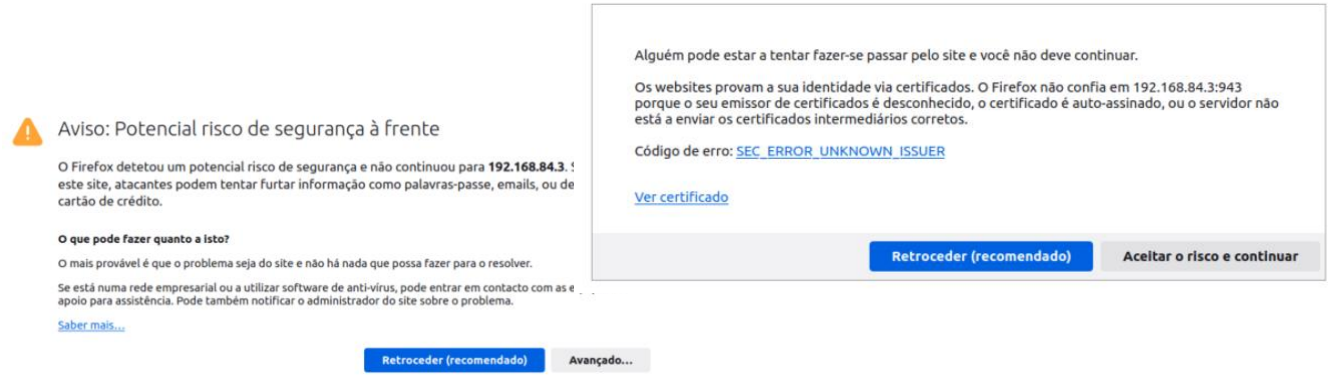
Passo 9 – No final da instalação deve verificar duas situações:

1. Saber qual o verdadeiro IP da máquina (caso só altere as propriedades da rede neste momento). Para tal use o comando ***ifconfig***;

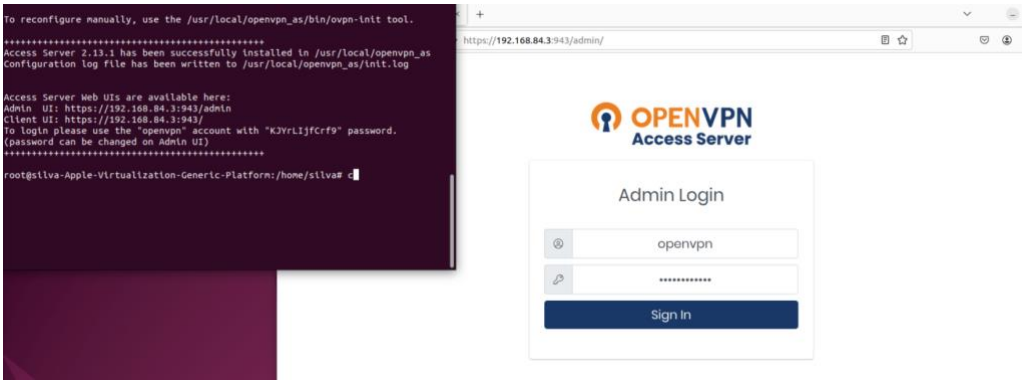
2. Saber se o serviço do OpenVPN está a correr no sistema (pois pode haver a necessidade de reiniciar a máquina para alguma operação posterior). Como tal pode usar os comandos:
   a. Para saber o estado do serviço: ***service openvpn status***
   b. Para ativar o serviço: ***service openvpn start***

No final da instalação deve saber qual o endereço IP e entrar com o seguinte formato: ***https://endereço_ip_da_máquina:943/admin → (exemplo: https://192.168.1.80:943/admin)***

Ao entrar na página, será questionado se pretende avançar (pois o certificado ainda é desconhecido e precisamos de avançar na confirmação):

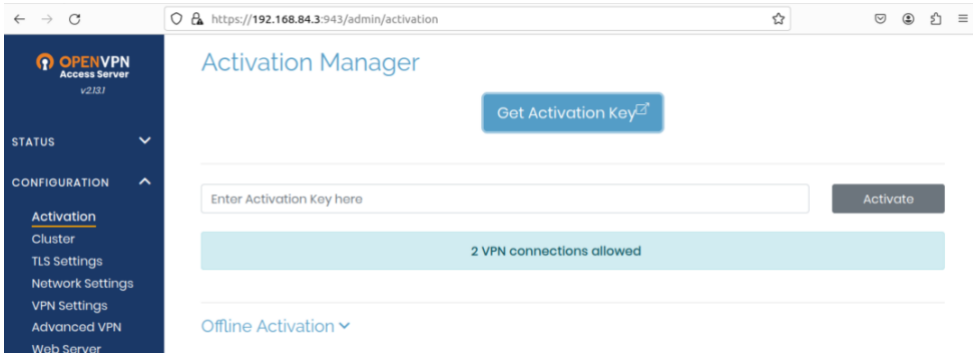


Passo 10 – Iniciar a sessão com os dados de acesso que foram fornecidos no terminal:

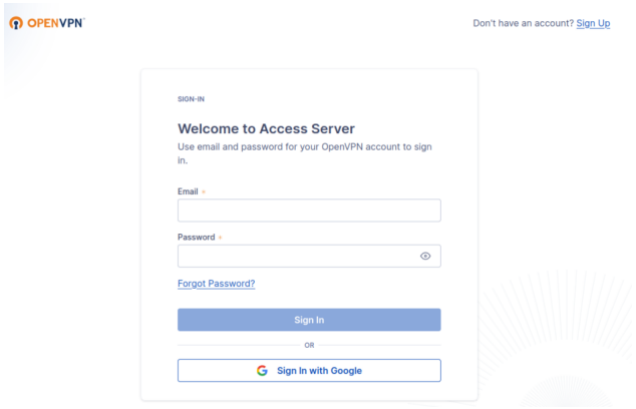


Passo 11 – Aceitar os termos e condições:

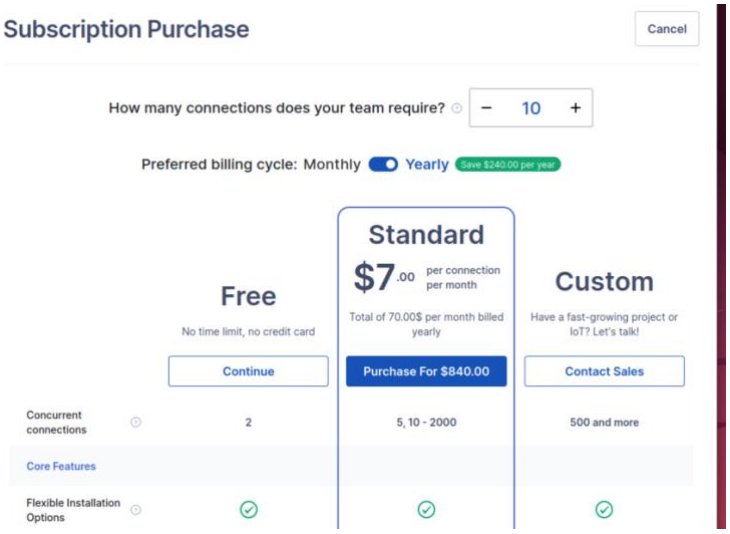
Passo 12 – Na página inicial, será pedida a chave de ativação do produto para conseguir utilizar o plano (que neste caso será o gratuito). O plano gratuito só permite 2 conexões ao mesmo tempo. Carregue no botão "***Get Activation Key***":



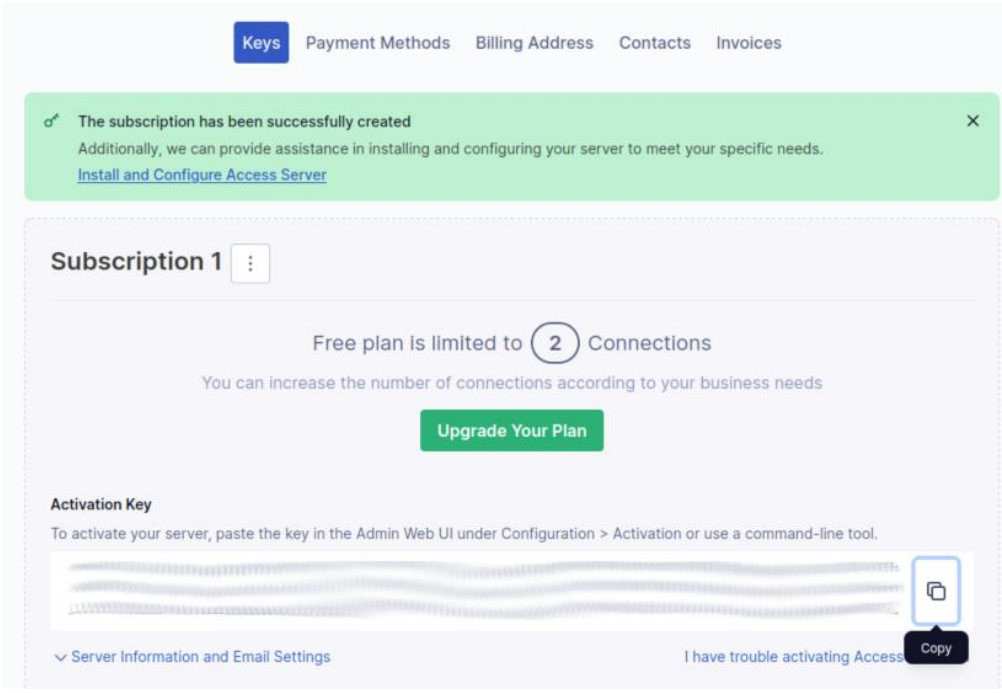
Deverá realizar a subscrição na página da OpenVPN:

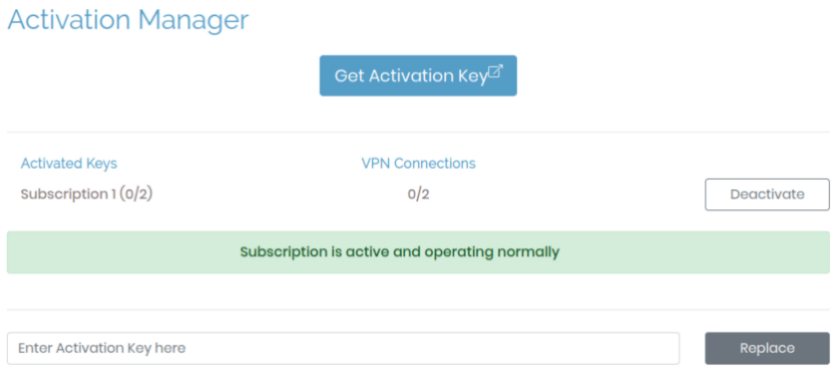


Na escolha do plano, selecione a opção Free:

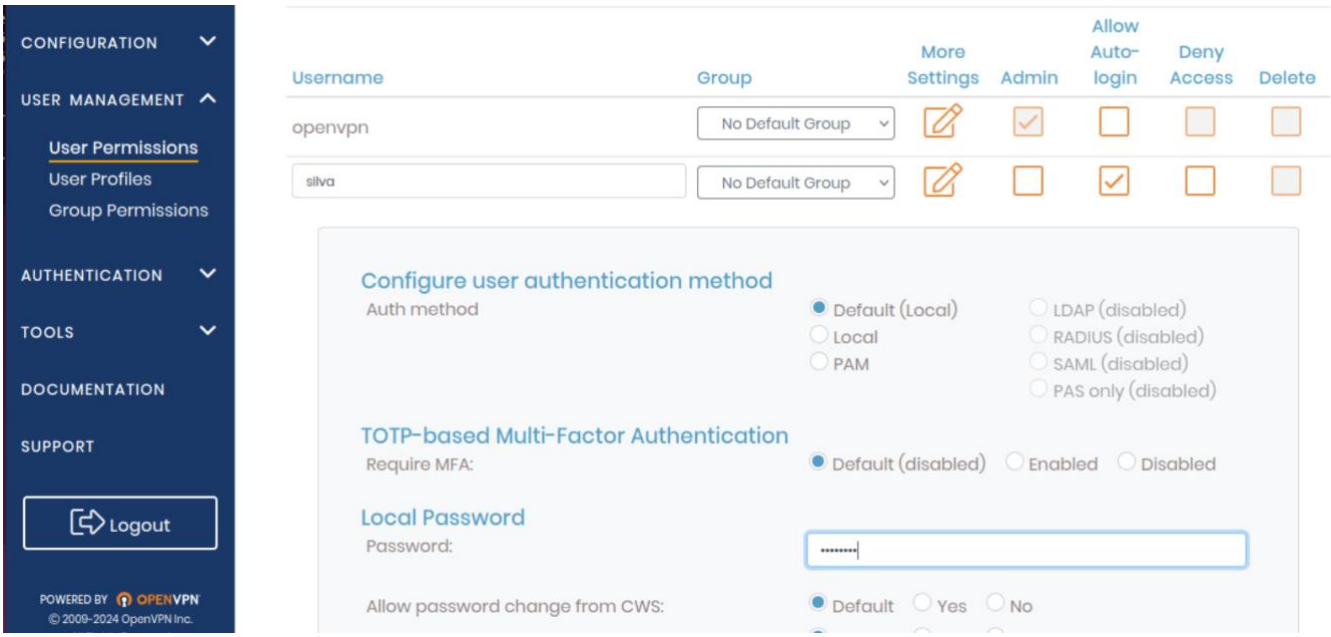


De seguida, copie a chave que foi oferecida:

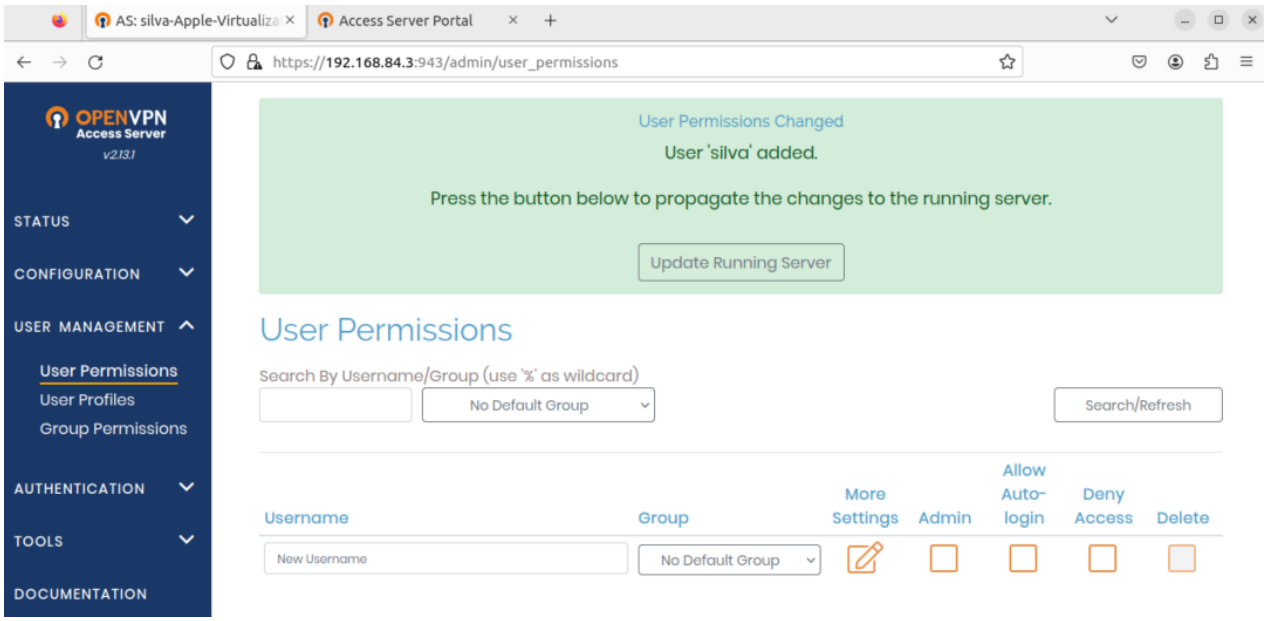




Passo 13 – Com o plano ativado, vamos ao menu lateral esquerdo da aplicação (aquela que instalamos) e selecione as opções User Managment → User Permissions. Por debaixo do utilizador OpenVPN, introduza um novo utilizador, selecionar a opção “Allow Auto-login” e depois clique no botão “More Settings” para definir a password:

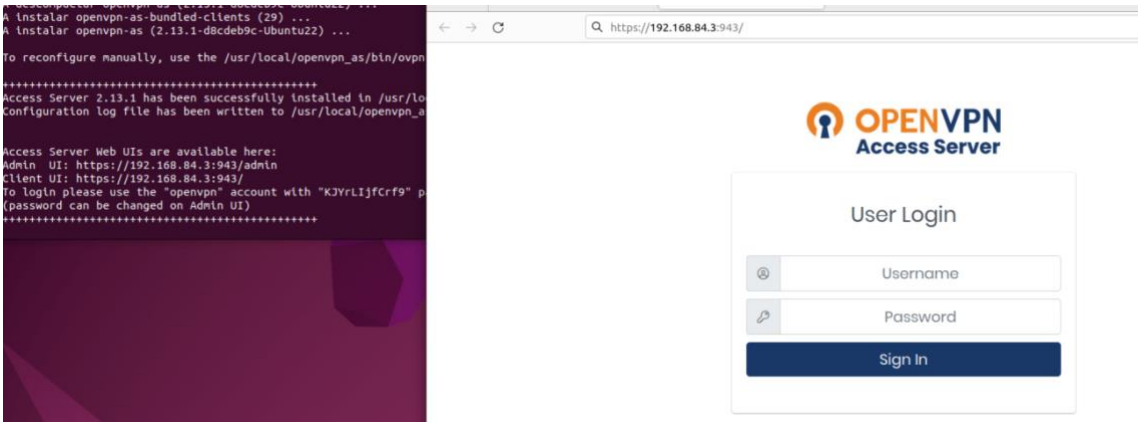


Passo 14 – Quando realizamos uma operação, temos de reiniciar o serviço para surtir os novos efeitos. Como tal, basta carregar no botão “Update Running Server”:



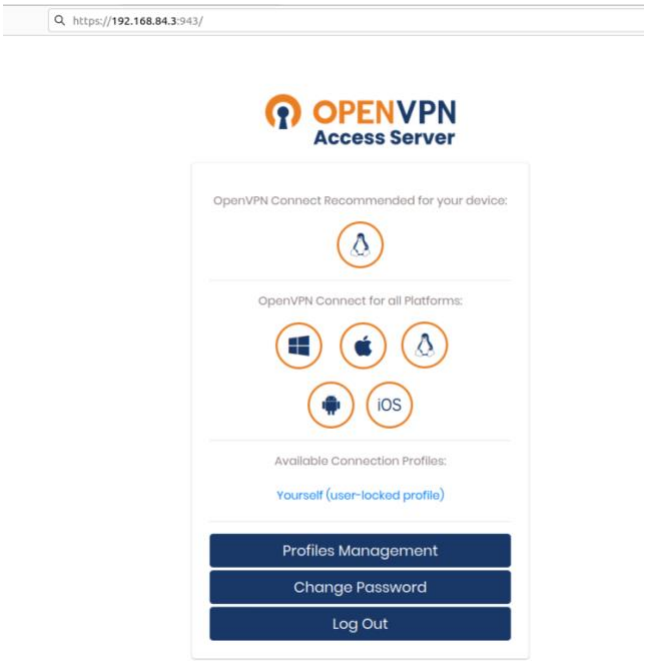
Download software cliente

Passo 1 – Quando instalou a máquina foi dado dois acessos, ou seja, um acesso para entrar na página de administração e outra hiperligação para entrar como cliente. Uma vez que já configurou a conta cliente no lado administrativo, vamos entrar na hiperligação do modo cliente, do qual, deve utilizar o nome de utilizador e password que criou na parte 1:

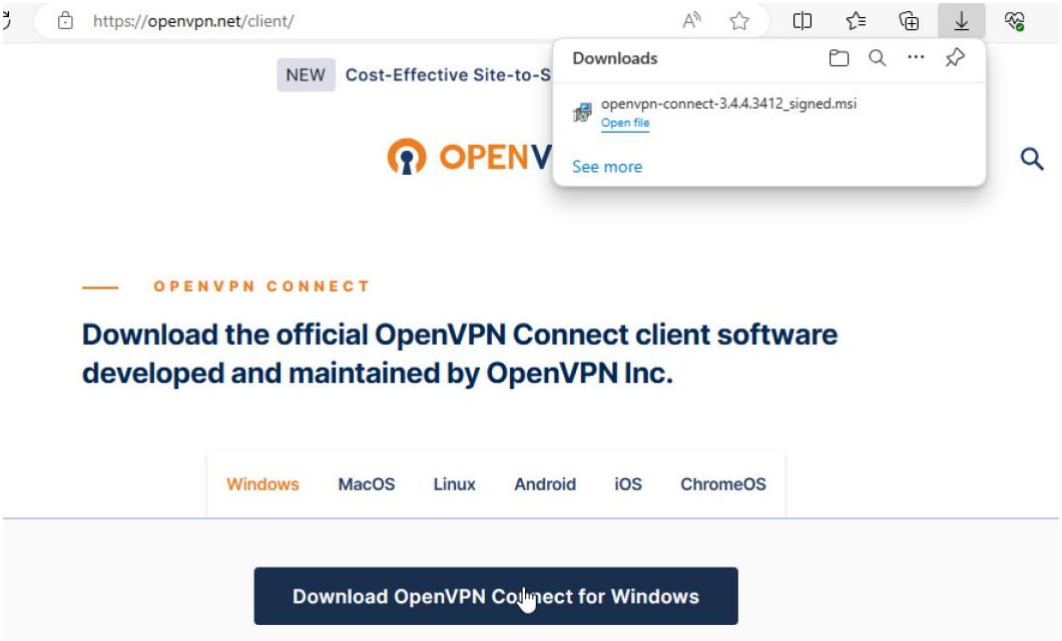


Passo 2 – Quando fizer o login, vai aparecer a recomendação para retirar o software para o sistema operativo que está a utilizar, mas, também poderá retirar outras formas de instalação (caso queira para outro sistema operativo). Vamos testar o mesmo no nosso telemóvel e verificar se este faz a associação.

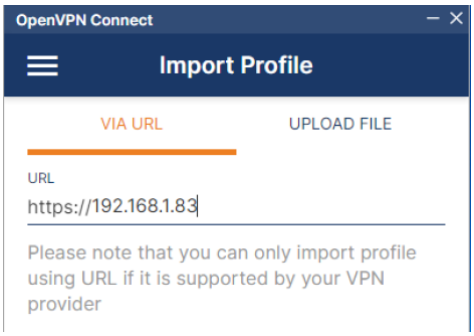
Nota importante: não esqueça de colocar o protocolo ***https://*** atrás do endereço ip, pois estamos a trabalhar com um servidor com certificado;



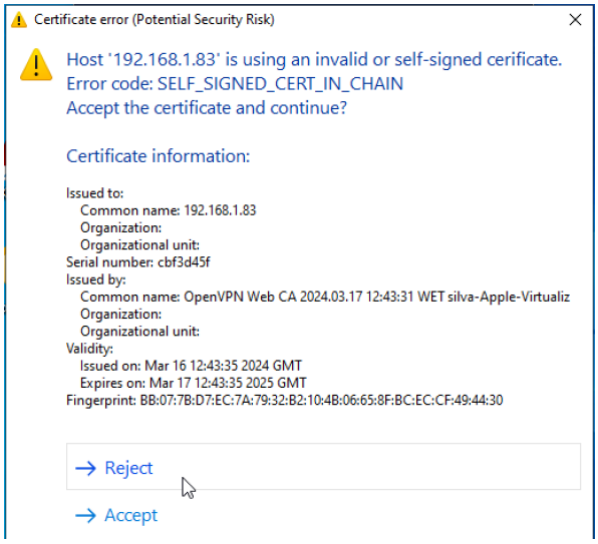
Em alternativa, podem ir ao website oficial do OpenVPN e descarregar o contudo manualmente: https://openvpn.net/client/



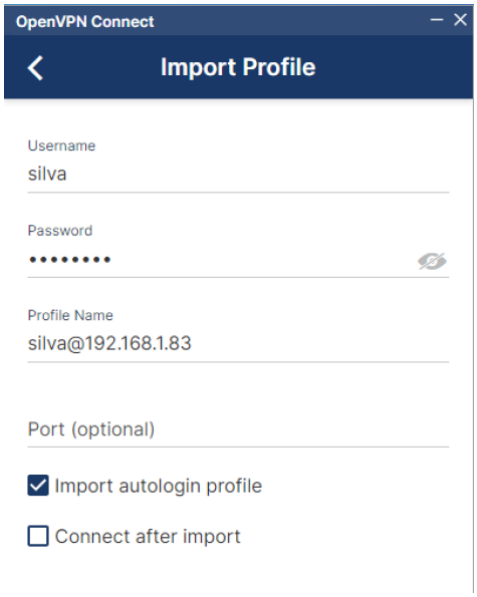
Passo 3 – Instalar o programa e quando este iniciar, devemos indicar a localização (endereço IP de onde esta o servidor OpenVPN ou serviço online):



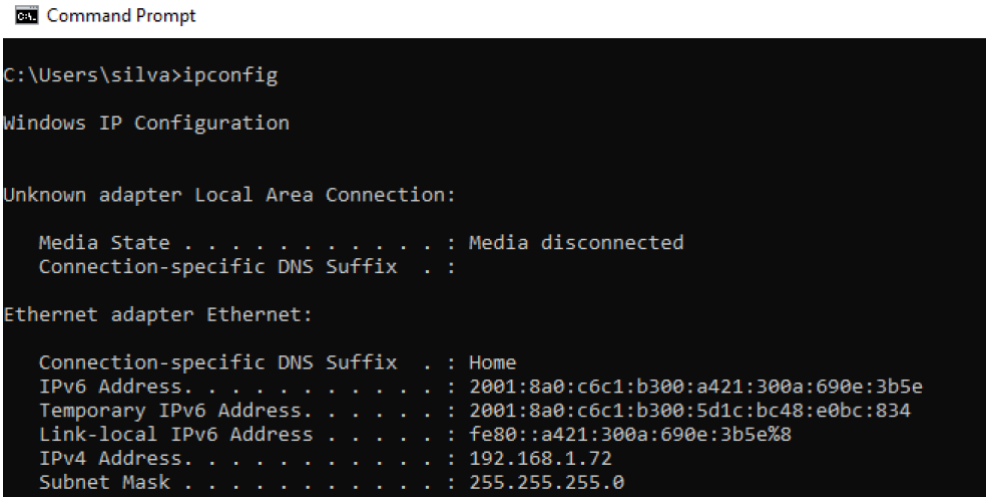
Passo 4 – Aceitar o certificado de segurança da ligação:



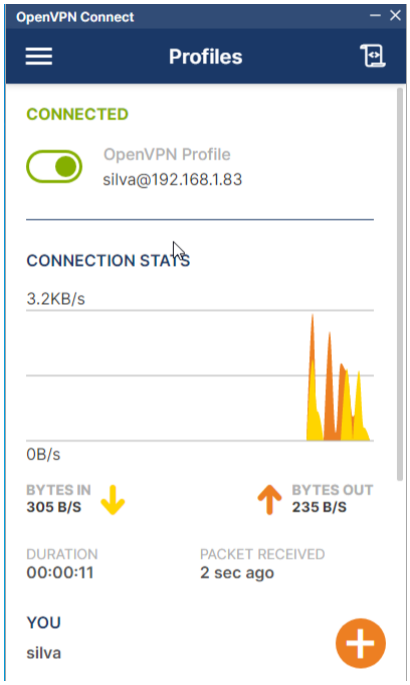
Passo 4 – Indicar os dados de acesso da nova conta que foi criada (cuidados para não haver espaços nos endereços ou outras informações):

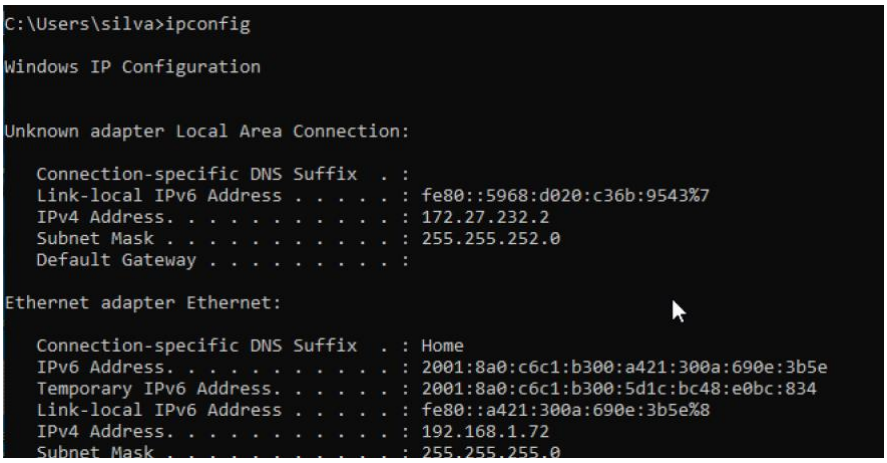


Passo 5 – Ir ao terminal do Windows e fazer ipconfig para verificar qual o endereço atual da placa de rede (local ou wireless)

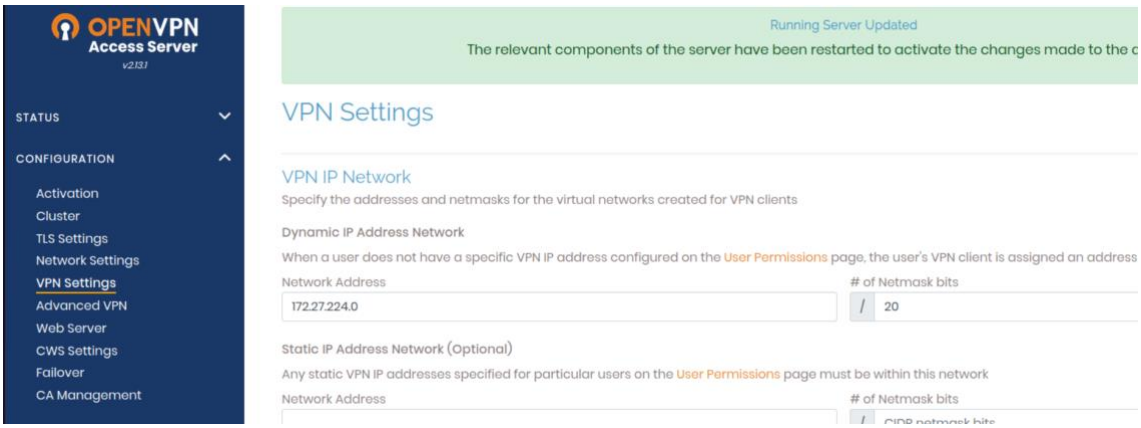


Passo 6 – Ativar a conexão VPN e verificar de seguida os endereços no terminal:





Passo 7 – Se não tiver acesso a Internet no servidor OpenVPN, pode ser por causa dos servidores DNS ainda não estarem definidos. Como tal, deve ir ao menu lateral esquerdo e clicar nas opções VPN Settings e mais abaixo tem o grupo DNS Settings:



Nesta área coloque os seguintes dados:

- Primary DNS Server: 8.8.8.8 (DNS Google)
- Secondary DNS Server: 4.4.4.4 (DNS Google)