
# MANUAL DE PROCEDIMENTOS DE INSTALAÇÃO OPENVPN E CRIAÇÃO DE CHAVES

**VERSÃO 1.2**

# Índice

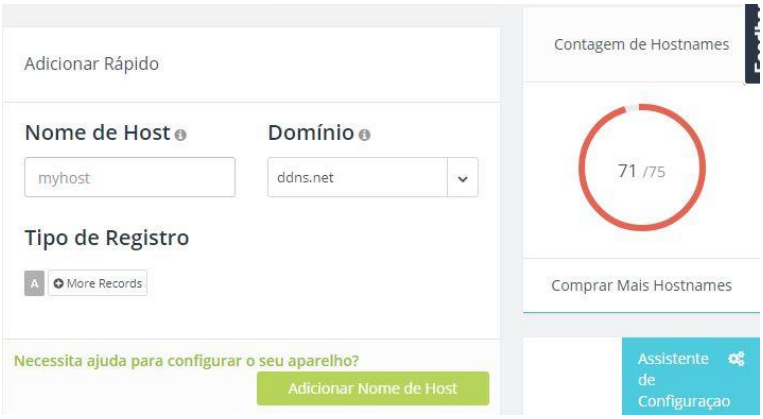
# 1. CONTEXTO

O presente documento pretende ser um guia para a instalação de postos de acesso remoto aos softwares Tactis (NoviGest, NoviPem), requerendo a existência de um DDNS (no nosso caso o fornecedor será NO-IP), a instalação de um programa para gerir o acesso, o OpenVPN e a criação de chaves para o server e cliente OpenVPN.

## 2. NO-IP

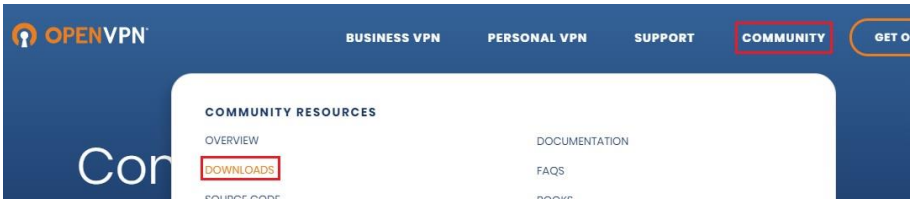
Caso a clínica ainda não tenha um DDNS criado, devemos aceder ao site https://www.noip.com/ fazendo log-in com a conta Tactis.

Encontramos depois do login várias opções onde para nós serão relevantes duas, adicionar rápido ou contagem de hostnames, que ao clicar no gráfico nos dá acesso à listagem de hostnames e possibilidade de pesquisar ou criar um novo hostname.



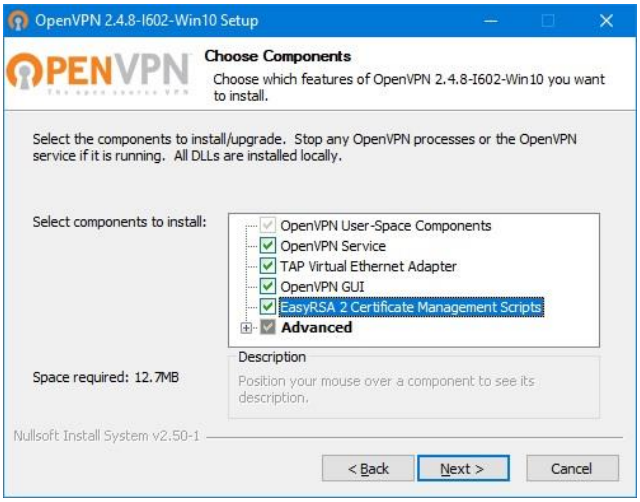

## 3. INSTALAÇÃO OPENVPN

Para a criação de chaves, caso ainda não esteja instalado devemos proceder a instalação do OpenVPN no nosso PC, acedendo a www.openvpn.pt, no separador community encontram a opção downloads onde encontram algumas versões, devemos fazer o download da última versão.





Depois do dowload do instalador, executamos o mesmo e vamos selecionando seguinte, à exceção da escolha dos componentes, que requer que se selecione a opção **EasyRSA**, por defeito não é instalada, mas no nosso caso em que pretendemos a criação de Keys, precisamos deste componente.




Os restantes passos não requerem alteração, clicamos em seguinte ate a conclusão da instalação.

## 4. CRIAR KEYS

Para a criação de chaves vamos precisar de alguns ficheiros disponíveis na partilha Tactis (\\192.168.70.70\partilha\HELPDESK\MANUAIS\OpenVPN\), **remake.bat** e **vars.bat**.

O ficheiro **remake.bat**, vai eliminar as chaves existentes e criar uma nova. O ficheiro **vars.bat** vai preencher por defeito alguns dados pedidos na criação das chaves.

Estes ficheiros devem se copiados para o vosso PC para a pasta C:\Program Files\OpenVPN\easy-rsa (este caminho poderá variar caso instalem o programa noutro diretório)

Apos a cópia destes ficheiros estamos prontos a criar uma chave para um novo acesso.

Para isso abrimos a linha de comando como administrador e vamos até ao caminho da pasta easy-rsa:

**cd**

**cd "Program Files\OpenVPN\easy-rsa"**

**C:\Program Files\OpenVPN\easy-rsa>remake.bat**

**Processo concluído, podes agora fazer build-key-server ou build-key.**

**Press any key to continue . . .**

Apos executarmos estes comandos vamos começar a criar a chave para o servidor

Para isso da mesma forma que excutamos o remake.bat, executamos **build-key-server.bat**:

**C:\Program Files\OpenVPN\easy-rsa>build-key-server.bat "nome do server"**

Aqui acrescentamos o nome que vamos atribuir ao server. O nome atribuído deverá ser o nome do domínio criado no NO-IP "-" srv. Por exemplo se o domínio fosse xpto.no-ip.net o server seria xpto-srv

Apos darmos enter vai surgir o seguinte texto:

Generating a RSA private key

.....++++

.....+
+++

writing new private key to 'keys\teste.key'

---

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

---

Country Name (2 letter code) [PT]:

A partir deste ponto vamos dar 5 enters, as várias linhas que vão surgindo vão ser preenchidas automaticamente com os dados que aparecem entre parenteses retos. Apos os 5 enters encontram a linha:

**Common Name (eg, your name or your server's hostname) [OVPN-TACTIS]: "nome do server"**

Aqui preenchemos mais uma vez o nome server e damos mais cinco clics na tecla enter, até que surge a linha de comando:

**Sign the certificate? [y/n]:**

Onde devemos inserir a letra Y e dar enter, dando origem a linha de comando:

**1 out of 1 certificate requests certified, commit? [y/n]**

Onde devemos também inserir a letra **Y** e dar enter. desta forma encontramos no diretório **C:\Program Files\OpenVPN\easy-rsa\keys** as chaves que acabamos de gerar.

O processo de criação de Keys para os postos clientes é semelhante, mas em vez de executarmos o bat build-key-server executamos **build-key.bat**.

Fazemos na mesma o **remake.bat** e **build-key.bat** substitui o build-key-server.bat, sendo que os passos são exatamente iguais alterando apenas para nome cliente em vez de servidor, à semelhança do que fizemos com o server o nome atribuído deverá ser o nome do domínio criado no NO-IP "-" clt"número do cliente" . Por exemplo se o domínio fosse xpto.no-ip.net o server seria xpto-clt01 e caso necessário mais acessos alteramos o número (clt02, clt03, clt04…)

Para alem das Keys precisamos dos ficheiros da configuração OVPN.

Os ficheiros de exemplo podem ser encontrados em \\192.168.70.70\partilha\HELPDESK\MANUAIS\OpenVPN\uteis\base.ovpn devem ser editados para que se adaptem à ligação que estamos a criar. Abrimos o ficheiro com Notepad e encontramos algo como:

port 1194 **Pode ser editado se entrar em conflito com outros programas**

proto udp **Pode ser alterado para tcp**

dev tun

;dev-node MyTap

ca ca.crt

cert "nome do ficheiro crt".crt **Tem de ser editado para o ficheiro ,crt que criamos**

key "nome do ficheiro key".key **Tem de ser editado para o ficheiro ,crt que criamos**

dh dh1024.pem

server 10.8.0.0 255.255.255.0 **Pode ser editado para alterar a gama de IP's a distribuir**

ifconfig-pool-persist ipp.txt

keepalive 10 120

comp-lzo

;max-clients 100

persist-key

persist-tun

status openvpn-status.log

verb 3

;mute 20

Os campos comentados terão de ser editados seguindo as instruções em frente, os restantes campos não devem ser alterados.

O exemplo anterior refere-se ao .opn do servidor, no caso do cliente o processo é semelhante:

client

dev tun

;dev-node MyTap

proto udp **Tem de ser igual ao protocolo utilizado pelo servidor**

remote "enderelo ddns" 1194 **Temos de inserir o endereço do DDNS**

resolv-retry infinite

nobind

persist-key

persist-tun

ca ca.crt

cert "nome do ficheiro crt".crt **Tem de ser editado para o ficheiro .crt que criamos**

key "nome do ficheiro crt".key **Tem de ser editado para o ficheiro .crt que criamos**

ns-cert-type server

comp-lzo

verb 3

;mute 20

# 5. CONFIGURAÇÃO NO CLIENTE

## 5.1 OPENVPN

O processo de instalação do OpenVPN é semelhante ao explicado a pagina 5, no entanto não ativamos a instalação do Easy-RSA, uma vez que no PC na clínica, não vai ser utilizado este componente.

Após a instalação do programa, copiamos os ficheiros para dentro da pasta **C:\Program Files\OpenVPN\config**

Ficheiros necessários:

- **ca.crt**
- **dh1024.pem**
- **server.ovpn / cliente.ovpn**
- **server.crt / cliente.crt**
- **server.key / cliente.key**

Os ficheiros que indiquei como server oc cliente devem ser nomeados de acordo com o acesso, pegando no exemplo do acesso xpto: xpto-srv.ovpn, xpto-srv.crt, xpto-srv.key e para o cliente xpto-clt0x.ovpn, xpto-clt0x.crt, xpto-clt0x.key.

## 5.2 FIREWALL

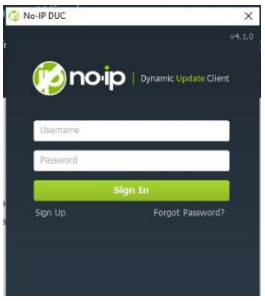
No caso do servidor devemos abrir na firewall do Windows ou do antivírus permissão para os executáveis do OpenVPN e para a porta utilizada pela ligação VPN.

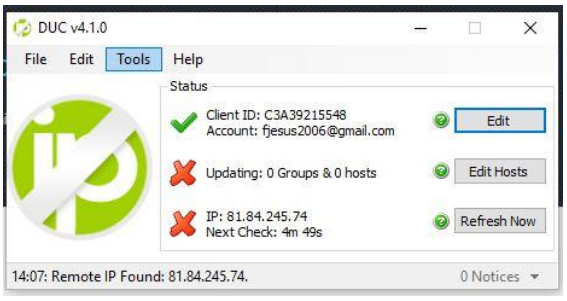
## 5.3 CONFIGURAÇÃO DE DDNS

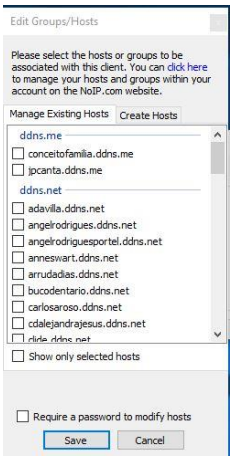
Temos duas alternativas para a configuração do DDNS, uma será acedendo à página interna do router da clínica e procurar uma ferramenta relativa a DDNS, onde configuramos endereço DDNS e a conta Tactis no NO-IP. Outra será através da instalação do DUC.

https://www.noip.com/pt-BR/download?page=win

A instalação resume-se a ir selecionando seguinte até concluir a mesma, em relação a configuração apos a abertura do programa fazemos login com os dados da conta Tactis e selecionamos o domínio que vamos utilizar, devemos selecionar a opção para requerer password para alterar os hosts para que a clínica não o faça.



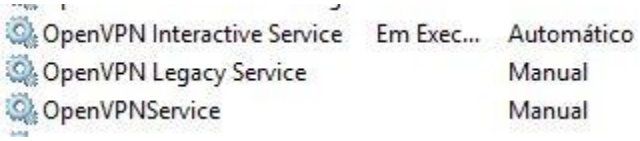



Mesmo que a opção seja a configuração através do DUC é necessário que a clínica nos dê aceso para configurar a abertura de porta utilizada pelo OpenVPN para o IP do servidor, ou que alguém responsável na clínica o faça.

## 5.4 ARRANQUE DO OPENVPN

Caso tenha apenas um servidor e uma VPN para se ligue automaticamente devemos ir aos serviços do Windows através das teclas **Win+R** e na janela para executar escrevemos **services.msc**, procuramos os serviços OpenVPNServiceInteractive e OpenVPNService, iniciamos estes serviços e caso o arranque esteja manual, alteramos para automático.




Ao arrancar os serviços o PC vai ganhar IP da gama distribuída pela VPN e podemos configurar o NoviGest nos PC's clientes, para que se liguem ao IP de VPN do servidor, concluindo assim o processo.