Network

- DDNS (Dynamic Domain Name System)
- DDNS gratuito do No-IP
- Como Instalar e Configurar Cliente com VPN Zerotier
- tryideas atualizador DNS
- Manual de Instalaçãodo OpenVPN Client
- TraceTCP v1.0.3

DDNS (Dynamic Domain Name System)

1. DNS: Antes de entender o DDNS, é importante conhecer o DNS. O DNS é um sistema que traduz nomes de domínio, como exemplo.com, em endereços IP, que são números únicos atribuídos a dispositivos conectados à Internet. O DNS permite que os usuários acessem sites digitando nomes de domínio em vez de números IP complicados.
2. Endereços IP dinâmicos: Em algumas situações, os endereços IP atribuídos a dispositivos podem ser dinâmicos, o que significa que podem mudar periodicamente. Isso é comum em conexões de Internet residenciais ou em alguns tipos de conexões de Internet móvel. Quando o endereço IP de um dispositivo muda, pode ser difícil acessá-lo usando um nome de domínio, já que o DNS está mapeado para um endereço IP antigo.
3. Problema de atualização: O problema surge quando você precisa acessar um dispositivo com um endereço IP dinâmico usando um nome de domínio. Se você simplesmente mapear o nome de domínio para o endereço IP atual, ele ficará desatualizado assim que o endereço IP mudar.
4. Solução: É aqui que o DDNS entra em cena. O DDNS é um serviço que permite atualizar automaticamente o registro DNS sempre que o endereço IP de um dispositivo muda. Ele permite que você atribua um nome de domínio fixo a um endereço IP dinâmico.
5. Cliente DDNS: Para usar o DDNS, você precisa de um cliente DDNS em execução no

dispositivo cujo endereço IP está mudando. Esse cliente é geralmente um software ou aplicativo que se comunica com o provedor DDNS.

6. Provedor DDNS: Existem vários provedores DDNS disponíveis, que fornecem o serviço de atualização do DNS quando um endereço IP muda. Esses provedores geralmente exigem que você se registre e configure uma conta com eles.
7. Configuração: Após criar uma conta com um provedor DDNS, você geralmente precisa configurar o cliente DDNS para se comunicar com o provedor. Isso envolve fornecer suas credenciais de conta e configurar o nome de domínio que deseja associar ao seu endereço IP.
8. Atualização automática: Uma vez configurado, o cliente DDNS monitora o endereço IP do dispositivo e, sempre que detecta uma alteração, notifica o provedor DDNS. O provedor DDNS, por sua vez, atualiza o registro DNS para que o nome de domínio aponte para o novo endereço IP.
9. Acesso remoto: Com o DDNS configurado corretamente, você pode acessar seu dispositivo remotamente usando o nome de domínio atribuído, em vez de precisar digitar o endereço IP atualizado manualmente.

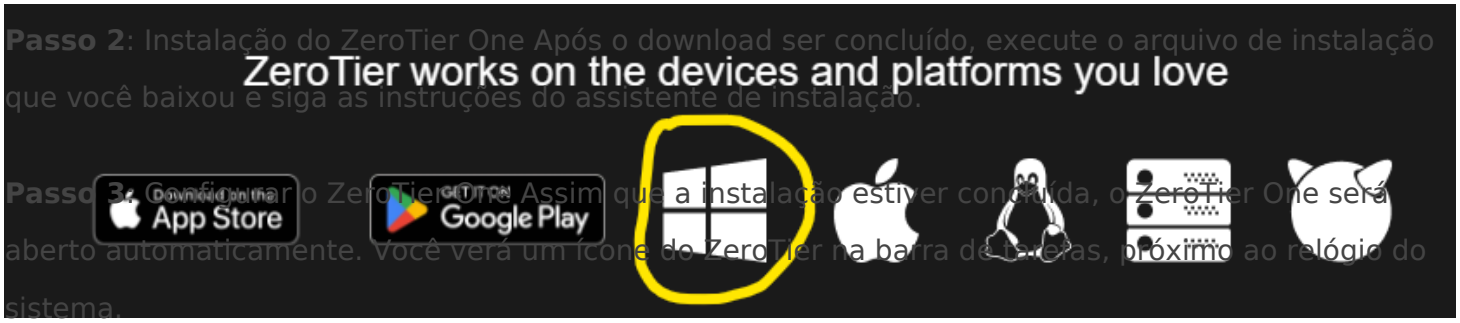
DDNS gratuito do No-IP

1. Cadastro: Primeiro, você precisa criar uma conta no site do No-IP. Acesse www.noip.com e clique em "Sign Up" ou "Registre-se". Preencha o formulário de registro com suas informações pessoais e escolha um nome de usuário e senha.
2. Adicionar um host: Após fazer login na sua conta, vá para o painel de controle do No-IP. Na seção "Dynamic DNS", clique em "Add a Host" ou "Adicionar um Host". Digite o nome do host que deseja usar (por exemplo, "meuhost.ddns.net"). Em seguida, selecione o domínio que deseja usar (geralmente no-ip.org). Deixe a opção "DNS Host (A)" selecionada.
3. Configuração do cliente DDNS: Agora você precisa configurar o cliente DDNS no seu dispositivo. O No-IP oferece seu próprio cliente DDNS chamado DUC (Dynamic Update Client), que você pode baixar e instalar. Certifique-se de escolher a versão correta para o seu sistema operacional. Após a instalação, abra o cliente DUC.
4. Configurar o DUC: No DUC, faça login usando suas credenciais do No-IP (nome de usuário e senha). Selecione o host que você criou anteriormente na lista suspensa. Verifique se a opção "Use Wildcards" está desmarcada, a menos que você precise especificamente de wildcards. Clique em "Save" ou "Salvar" para salvar as configurações.
5. Verificação e atualização: O cliente DUC agora estará em execução e se comunicará automaticamente com o No-IP para verificar e atualizar seu endereço IP dinamicamente. Certifique-se de que o cliente DUC esteja sempre em execução no seu dispositivo para garantir que o endereço IP seja atualizado corretamente.

Lembre-se de que, para o serviço gratuito do No-IP, é necessário confirmar sua conta a cada 30 dias, caso contrário, seu host será desativado. Eles normalmente enviam um e-mail de confirmação para você renovar o host.

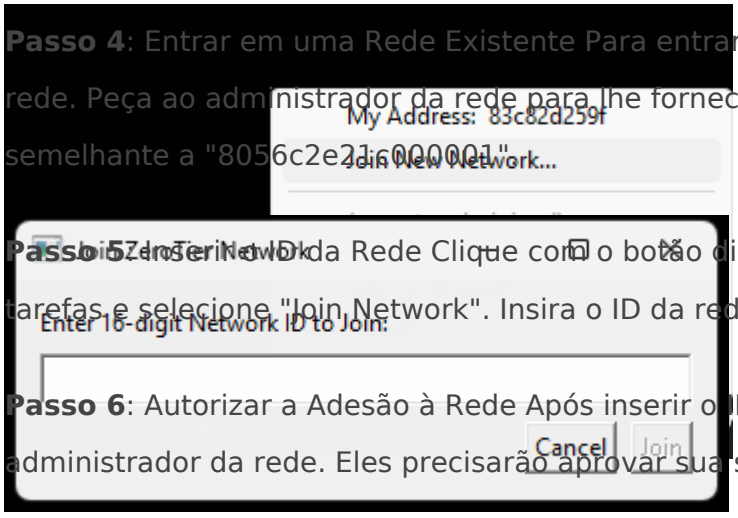
Como Instalar e Configurar Cliente com VPN Zerotier

Passo 1: Baixar o ZeroTier One Acesse o site oficial do ZeroTier (https://www.zerotier.com/download) e baixe a versão apropriada para o seu sistema operacional Windows.



Passo 2: Instalação do ZeroTier One Após o download ser concluído, execute o arquivo de instalação que você baixou e siga as instruções do assistente de instalação.

Passo 3: Configurar o ZeroTier One Assim que a instalação estiver concluída, o ZeroTier One será aberto automaticamente. Você verá um ícone do ZeroTier na barra de tarefas, próximo ao relógio do sistema.



Passo 4: Entrar em uma Rede Existente Para entrar em uma rede já criada, você precisará do ID da rede. Peça ao administrador da rede para lhe fornecer o ID, que é um código único de 16 caracteres, semelhante a "8056c2e21c000001".

Passo 5: Inserir o ID da Rede Clique com o botão direito do mouse no ícone do ZeroTier na barra de tarefas e selecione "Join Network". Insira o ID da rede fornecido pelo administrador e clique em "Join".

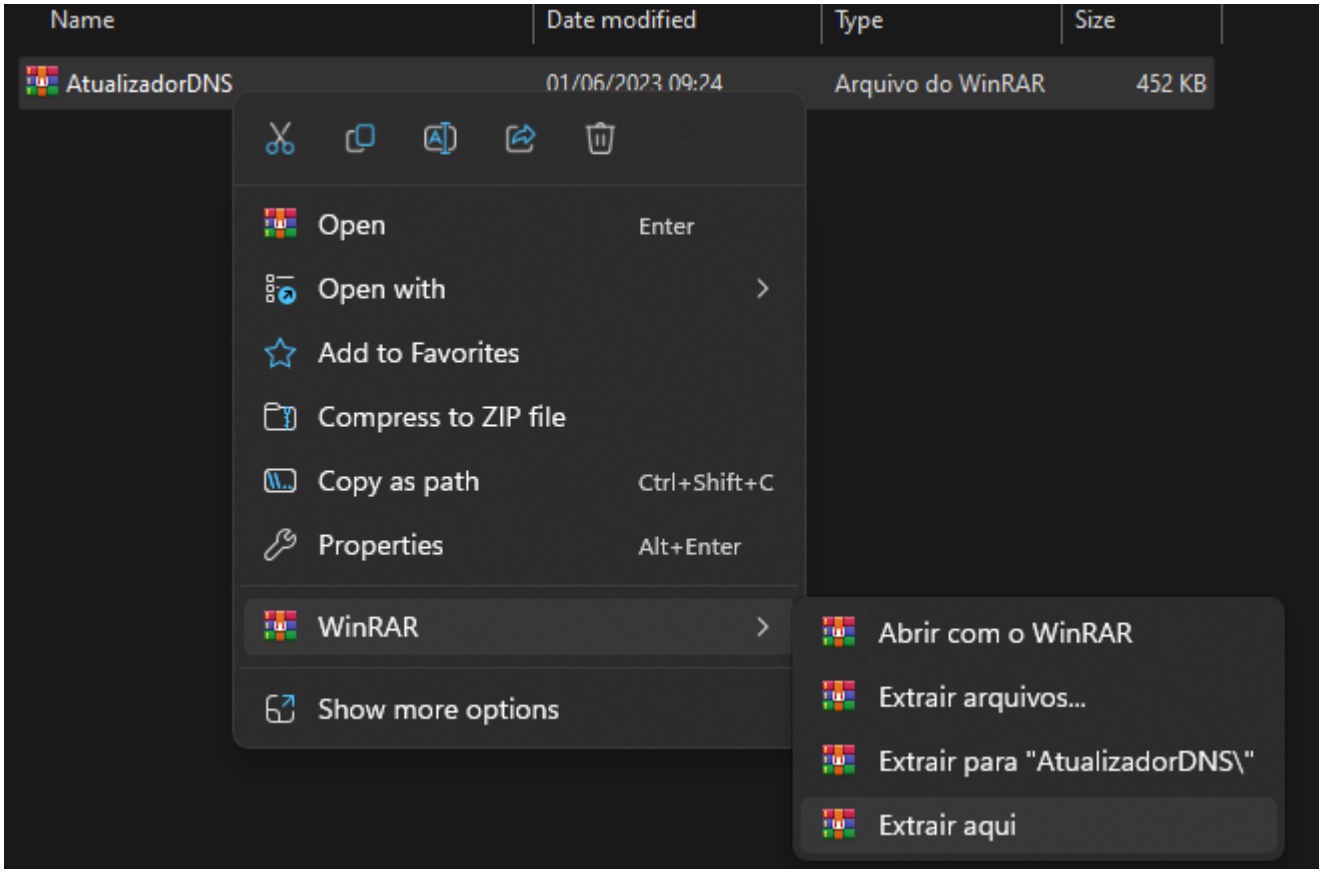
Passo 6: Autorizar a Adesão à Rede Após inserir o ID da rede, aguarde a autorização do administrador da rede. Eles precisarão aprovar sua solicitação de adesão.

Passo 7: Verificar a Conexão Quando a autorização for concedida, o status do ZeroTier mudará para "ONLINE" e você estará conectado à rede.

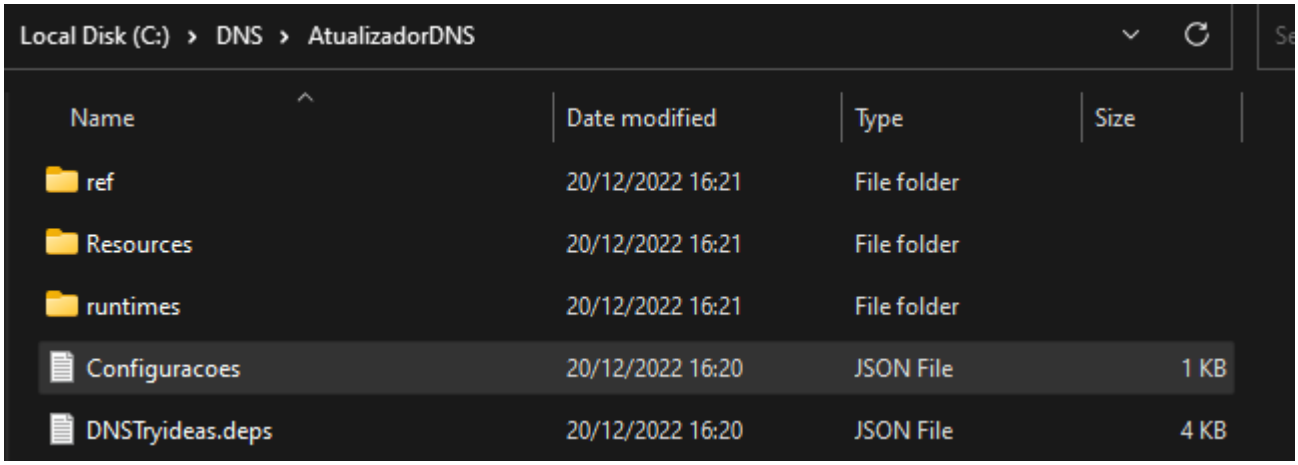
Agora você está conectado à rede ZeroTier e pode acessar recursos e dispositivos na rede conforme

configurado pelo administrador.

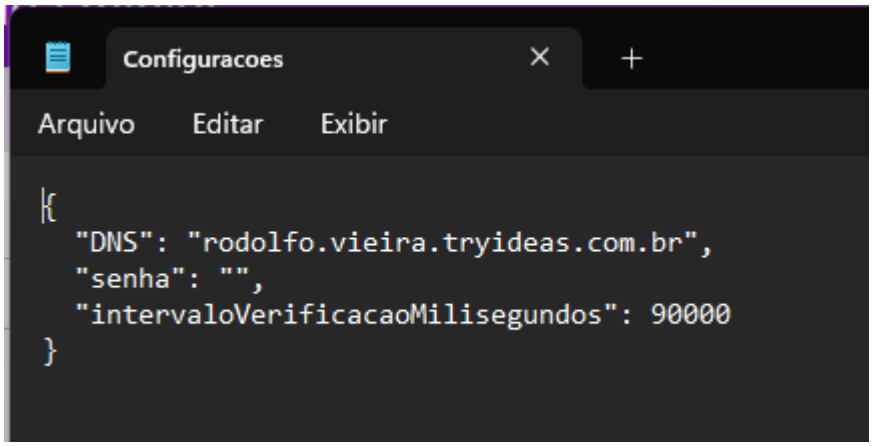
tryideas atualizador DNS



3 - Edite o arquivo Configurações.



4 - Alterar os campos DNS e senha, preencha com os seus e salve o arquivo.

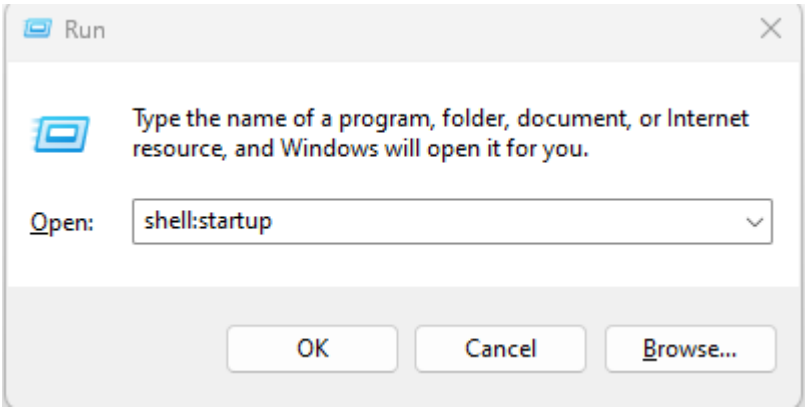


5 - Abra o DNSTryideas.exe.

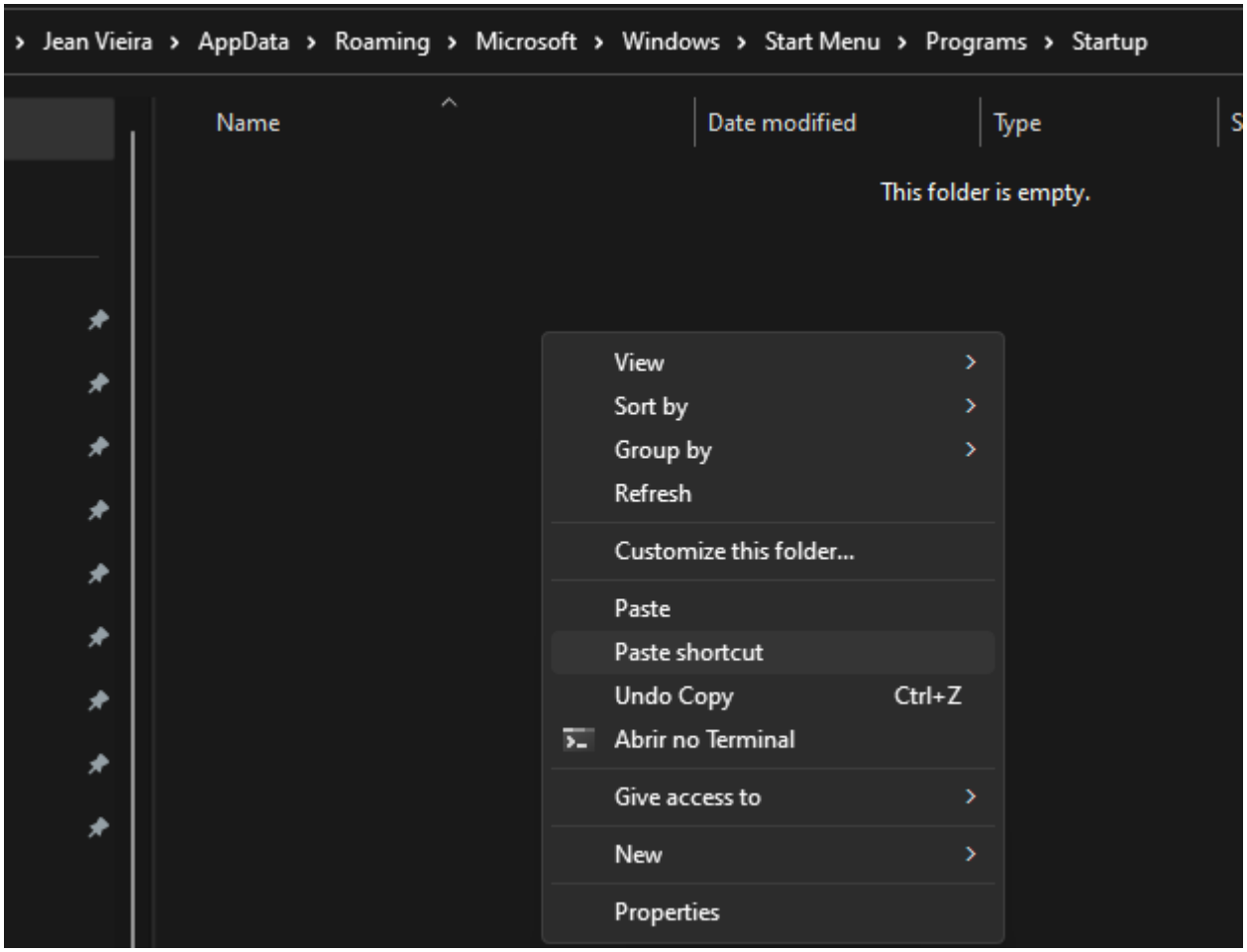
6 - Deve aparecer assim se der tudo certo.

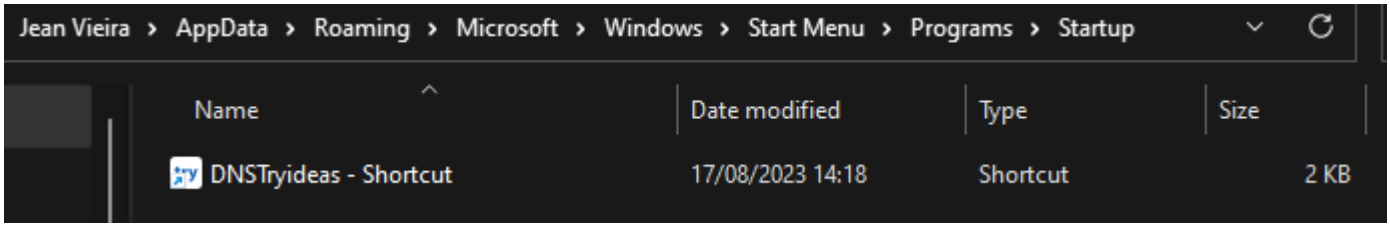
7 - Pode adicionar no iniciar do Windows, copie o DNSTryideas.exe na pasta dele.

8 - Abra o executar do Windows e digite 'shell:startup'.



9 - Na pasta que abrir, clique com botão direto do mouse e vai em colocar atalho.


Jean Vieira › AppData › Roaming › Microsoft › Windows › Start Menu › Programs › Startup
Name
Date modified
Type
This folder is empty.
View
Sort by
Group by
Refresh
Customize this folder...
Paste
Paste shortcut
Undo Copy Ctrl+Z
Abrir no Terminal
Give access to
New
Properties


Jean Vieira › AppData › Roaming › Microsoft › Windows › Start Menu › Programs › Startup
Name
Date modified
Type
Size
DNSTryideas - Shortcut
17/08/2023 14:18
Shortcut
2 KB

Fim.

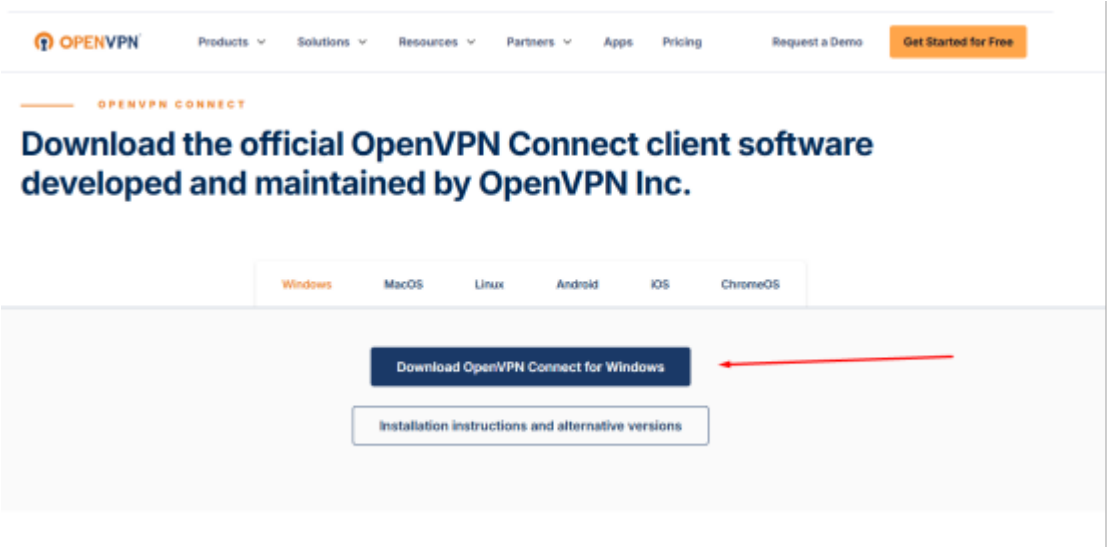
Manual de Instalaçãodo

OpenVPN Client

1. Download do OpenVPN Client

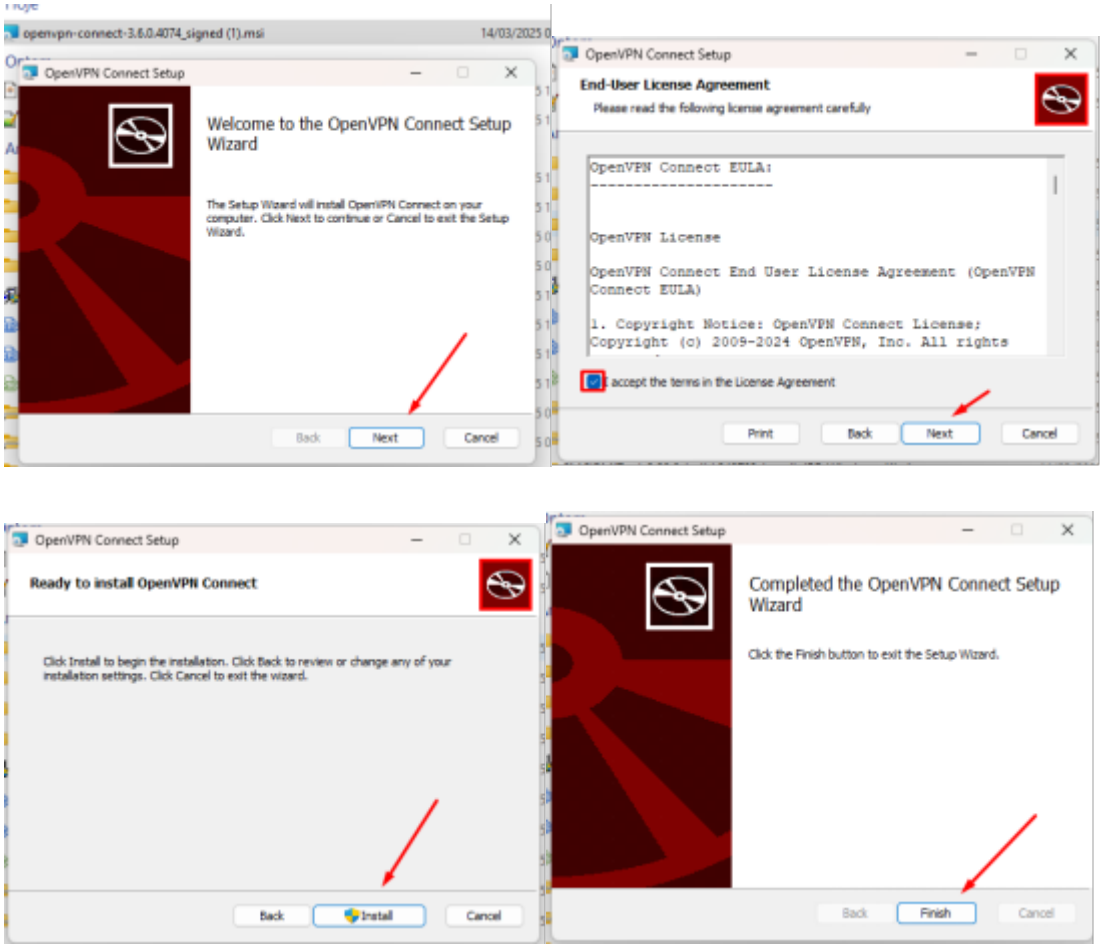
Acesse o site oficial do OpenVPN para baixar o cliente: https://openvpn.net/client/

Ou baixe diretamente pelo link: https://openvpn.net/downloads/openvpn-connect-v3-windows.msi

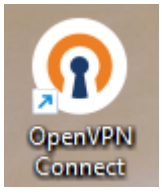


2. Instalação do OpenVPN Client

- Depois de concluir o download, execute o arquivo para iniciar a instalação.
- Siga as instruções do assistente de instalação até a conclusão do processo.
- Após a instalação, o aplicativo será aberto automaticamente. Caso não abra, localize o ícone "OpenVPN Connect" na área de trabalho e abra manualmente.

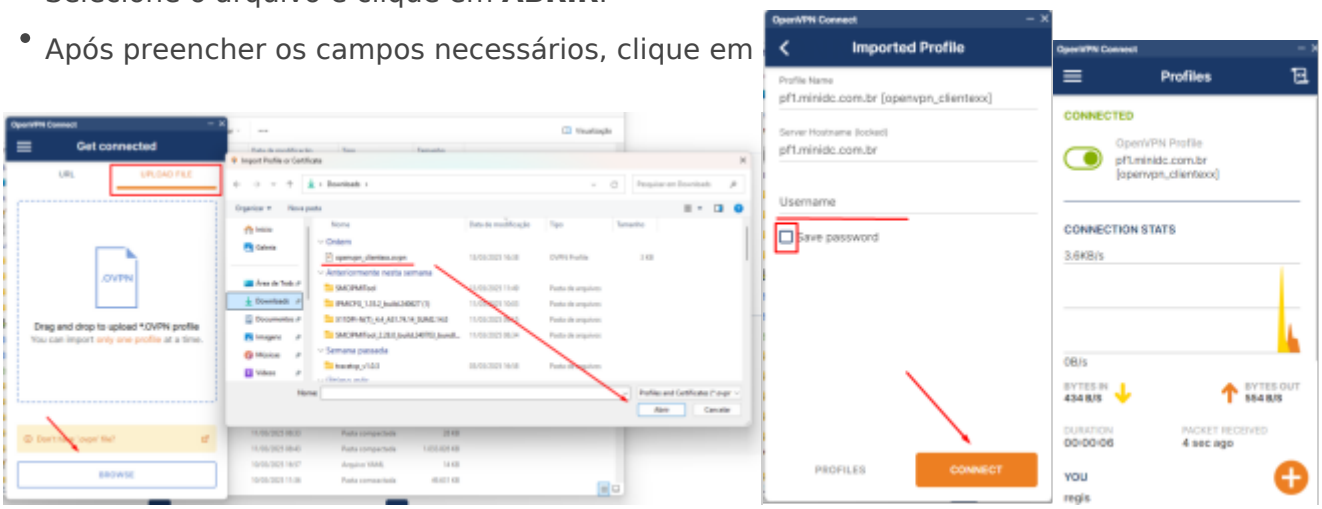


Após a finalizar a instalação o aplicativo abrira automaticamente, caso não abra procure na área de trabalho pelo icone OpenVPN Connect:



3. Configuração do OpenVPN

- Com o OpenVPN Connect aberto, selecione a opção **UPLOAD FILE**.
- Clique em **BROWSE**e localize o arquivo de configuração recebido.
- Selecione o arquivo e clique em **ABRIR**.
- Após preencher os campos necessários, clique em

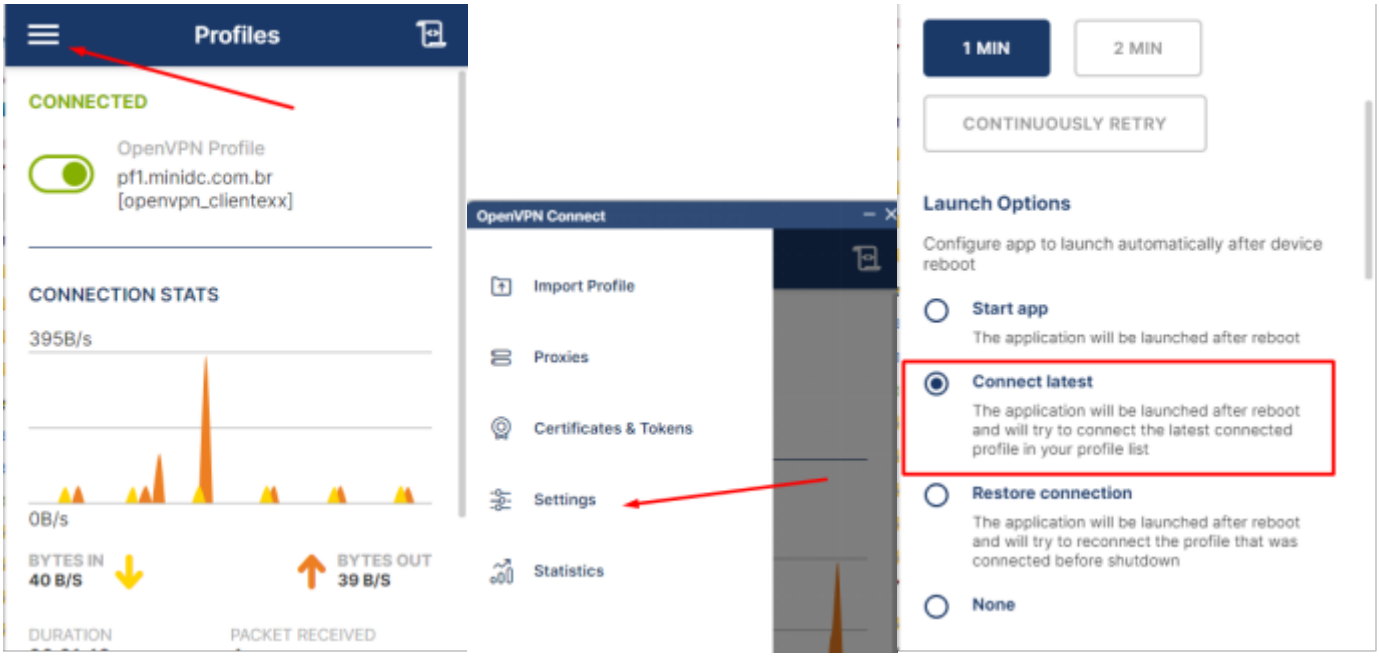


Se tudo estiver correto, você estará conectado à VPN.

4. Configuração para Início Automático

Para garantir que a VPN seja conectada automaticamente ao iniciar o computador, siga os passos abaixo:

- Abra o OpenVPN Connect.
- Acesse as configurações do aplicativo.
- Ative a opção **Auto-connect on startup**.



Agora, toda vez que o computador for ligado, a VPN será ativada automaticamente.

TraceTCP v1.0.3

□□ Manual TraceTCP v1.0.3 — Windows CMD

□□ 1. Downloads necessários

Arq	Lin	Obs
tracetcp v1.0.3	Baixar `tracetcp.exe`	https://github.com/0xcafed00d/tracetcp/releases/tag/v1.0.3
WinPcap 4.1.3	DLL	https://www.winpcap.org/install/default.htm obrigatória

> ⚠ **O WinPcap é OBRIGATÓRIO.** O tracetcp não funciona sem ele — ele substitui o uso de raw sockets que a Microsoft removeu a partir do XP SP2.

□□ 2. Instalação passo a passo

Passo 1 — Instalar o WinPcap

1. Baixe o instalador do WinPcap no link acima
2. Execute `WinPcap_4_1_3.exe` como **Administrador**
3. Siga o assistente de instalação (Next → Next → Finish)
4. Reinicie o computador se solicitado

Passo 2 — Instalar o tracetcp.exe

1. Baixe o arquivo `tracetcp.exe` na página de releases do GitHub
2. Copie o executável para uma pasta no PATH do sistema, por exemplo:

   ```
   C:\Windows\System32\
   ```

   Ou crie uma pasta dedicada e adicione ao PATH manualmente:

   ```
   C:\Tools\tracetcp\
   ```

□□ 3. Executando via CMD

> ⚠ **Sempre abra o CMD como Administrador** — o tracetcp exige privilégios elevados para capturar pacotes.

Sintaxe geral

```
tracetcp.exe host[:porta|:serviço] [opções]
```

- Se nenhuma porta for informada, assume **porta 80 (HTTP)** por padrão.

□□ 4. Opções disponíveis

Opçã	Descrição
`-?`	Exibe a ajuda

Opçã	Descrição
`-c`	Modo condensado (saída resumida)
`-h N`	Inicia o trace a partir do hop N
`-m N`	Máximo de hops até o destino
`-n`	Desativa resolução reversa de DNS em cada nó

Opçã	Descrição
`-p N`	Número de pings por hop (padrão: 3)
`-r p1 p2`	Múltiplos traces de porta p1 até p2
`-t N`	Timeout em milissegundos para cada resposta
`-v`	Exibe a versão

Opçã	Descrição
`-F`	Desativa o timer anti-flood (traces mais rápidos)
`-s p1 p2`	Modo scan de porta fácil (equivale a `-cnr p1 p2 -h 128 -m 1 -p 1`)
`-g endereço`	Usa um host específico como gateway

□□ 5. Exemplos práticos — Trace com porta para DNS

O DNS usa a **porta 53**. Abaixo exemplos reais para testar conectividade TCP na porta 53 até servidores DNS.

▶ Teste para o DNS público do Google (8.8.8.8) na porta 53

```
tracetcp.exe 8.8.8.8:53
```

▶ Teste para o DNS público da Cloudflare (1.1.1.1) na porta 53

```
tracetcp.exe 1.1.1.1:53
```

▶ Teste para o seu DC/DNS interno (exemplo minidc.int)

```
tracetcp.exe 192.168.1.1:53
```

▶ Sem resolução reversa de DNS (mais rápido)

```
tracetcp.exe 8.8.8.8:53 -n
```

□□ 6. Interpretando a saída

```
Tracing route to 8.8.8.8 on port 53
Over a maximum of 30 hops.
1    1 ms    1 ms    1 ms   192.168.1.1          <- Gateway local2    9 ms   10 ms    8 ms
10.0.0.1             <- Roteador do ISP3   11 ms   12 ms   11 ms   189.x.x.x           <- Nó
intermediário
...
N   Destination Reached in 25 ms.               <- Destino alcançado    Connection established
to 8.8.8.8           <- Conexão TCP estabelecida
    Trace Complete.
```

Resul	Significado
`Destination Reached`	Porta aberta e conexão TCP estabelecida
`Destination Reached` + `port is closed`	Host alcançado mas porta fechada ou filtrada ⚠

Resul	Significado
`* * * Request timed out`	Hop bloqueando ICMP ou firewall dropando o pacote

⚠ 7. Observações importantes

- **Execute sempre como Administrador** — sem isso o WinPcap não consegue capturar pacotes
- O tracetcp **não funciona via dial-up** (limitação do WinPcap)
- Testado no Windows XP, Vista, 7, 10 e 11
- DNS na porta 53 TCP é para transferência de zona e consultas grandes — alguns firewalls bloqueiam TCP/53 mas liberam UDP/53 (o tracetcp usa TCP)
- Se o destino for alcançado mas a porta aparecer como fechada, pode ser que o host não aceite conexões com TTL=0; o tracetcp v1.0.3 reenvia automaticamente com TTL alto para confirmar