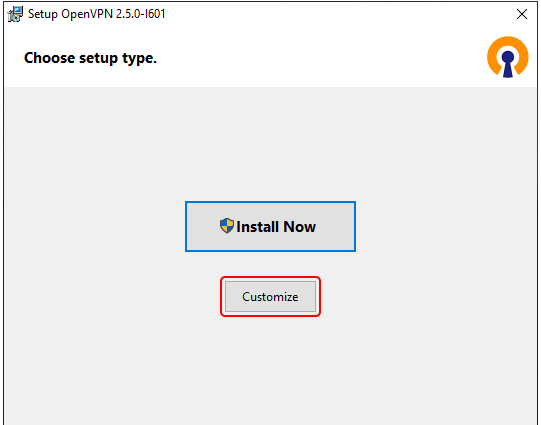
## **Tipo: PO – Procedimento Operacional**

**Grupo:**

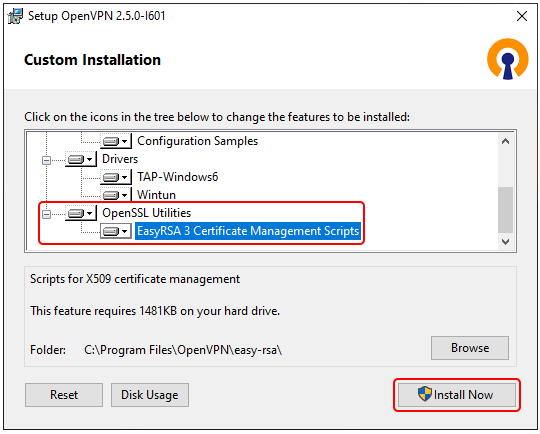
**SubGrupo:**

## **OBJETIVO: Ensinar a realizar a instalação do programa OpenVPN.**

1. Para darmos início a instalação do programa OpenVPN o instalador deverá ser baixado no seguinte site <https://openvpn.net/community-downloads/>
2. Após realizar o download do arquivo executável inicie o mesmo e siga os seguintes passos. Quando aberto, clique no botão “customize” para dar início a instalação do programa



1. Após clicar no botão “Custumize” a seguinte tela surgirá, e nela, deverá ser selecionada a opção “EasyRSA 3 Certificate Management Scripts”, após selecionar devidamente clique no botão “install now”.



A partir de agora será realizado o preparo da EasyRSA

1. Após clicar no botão “install now” o programa será instalado e deve ser configurado para o devido funcionamento. Para configurar deverá ser aberto o prompt de comando como administrador e os seguintes comandos em sequência deverão ser digitados:

º cd C:\Arquivos de programas\OpenVPN\easy-rsa

º EasyRSA-Start.bat

º./easyrsa init-pki

º notepad vars.bat (caso não abra siga o caminho C:\Program Files\OpenVPN\easy-rsa ) e abra manualmente com o bloco.

1. Após abrir o bloco localize as linhas

Definir KEY\_COUNTRY = US

Definir KEY\_PROVINCE = CA

Definir KEY\_CITY = SanFrancisco

Definir KEY\_ORG = OpenVPN definir [KEY\_EMAIL=mail@host.domain](mailto:KEY_EMAIL=mail@host.domain)

E as modifique de acordo com a sua necessidade.

1. Você também pode definir o tamanho da chave para os parâmetros Diffie Hellman utilizando o comando definir: DH\_KEY\_SIZE = 2048
2. Quando terminar, salve o arquivo e feche o editor; em seguida, execute os seguintes comandos no prompt:

ºvars.bat

º./easyrsa clean-all

1. Após a EasyRSA estar devidamente configurada partiremos para a configuração de certificados e chaves. Digite os comandos no prompt

./easyrsa build-ca nopass

./easyrsa build-server-full server nopass

./easyrsa build-client-full Client1 nopass (substitua cliente1 pelo nome do cliente)

E por último, digite:

./easyrsa gen-dh

Os arquivos gerados e assinados devem aparecer nos seguintes diretórios (por padrão):

Arquivos Localização

Certificado CA → C:\Arquivos de programas\OpenVPN\easy-rsa\pki

Parâmetros Diffie-Hellma→ C:\Arquivos de programas\OpenVPN\easy-rsa\pki

Chaves de cliente e servidor→ C:\Arquivos de programas\OpenVPN\easy-rsa\pki\private

Certificados de cliente e servidor→ C:\Arquivos de programas\OpenVPN\easy-rsa\pki\emitido

1. Após realizar os passos anteriores vamos dar inicio a configuração do servidor OpenVPN. Procure o arquivo:

C: \ Arquivos de programas \ OpenVPN \ sample-config ) sob o nome **server.ovpn** .

1. Ao localizar o arquivo, faça uma cópia, renomeie-o e coloque-o no diretório de **configuração** da pasta OpenVPN (caminho padrão: C: \ Arquivos de programas \ OpenVPN \ config ). Você também deve copiar os certificados e as chaves para este diretório (arquivos necessários: ca.crt , server.crt , server.key , dh2048.pem )

Localize as seguintes linhas:

ca ca.crt

cert server.crt

key server.key

dh dh1024.pem

Edite as linhas de uma forma que corresponda aos caminhos de arquivo reais. Os padrões usados ​​neste exemplo são:

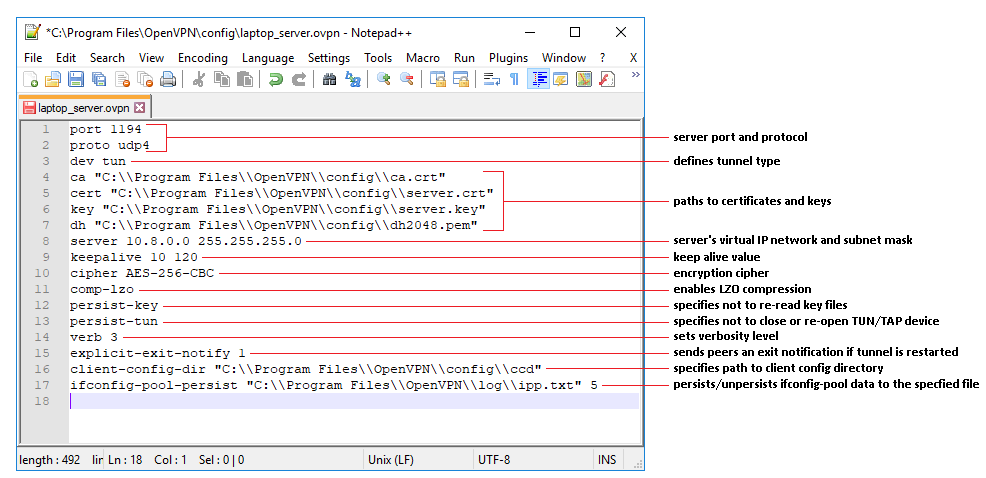
ca"C:\\Arquivos de programas\\OpenVPN\\config\\ca.crt"

cert"C:\\Arquivos de programas\\OpenVPN\\config\\server.crt"

chave"C:\\Arquivos de programas\\OpenVPN\\config\\server.key"

dh"C:\\Arquivos de programas\\OpenVPN\\config\\dh2048.pem"

1. Em seguida, vêm as configurações preferenciais, ou seja, se você deseja UDP ou TCP, Túnel ou Bridge, rede do servidor, keep alive, valores de cifra, etc. Você deve configurar essas opções de acordo com suas necessidades. Abaixo está uma imagem de como é a configuração final deste exemplo (com os comentários presentes no arquivo de amostra excluído para mais clareza):



As seguintes alterações foram feitas no arquivo de amostra:

* Alterado *udp* para *udp4* para indicar que a conexão deve usar apenas IPv4
* Adicionada opção *client-config-dir* para possível configuração de cliente TLS
* Alterado o caminho do arquivo *ifconfig-pool-persist*
* Mudanças nos caminhos do certificado e do arquivo de chave
* Nota: a cifra AES-256-CBC está obsoleta na v.2.5. Alterar CBC para GCM
* Você pode proteger (adicionar segurança) à VPN criando um arquivo ta.key no servidor, colocando-o na pasta config e copiando-o para a pasta config de todas as máquinas clientes.
* Edite o arquivo server.ovpn encontrado na pasta OpenVPN / sample-config. Linhas que começam com # ou; será ignorado.) Sinta-se à vontade para alterá-lo como quiser.

1. Agora, para configurar os clientes, Instale o OpenVPN em todas as máquinas clientes, mas omita as etapas 4 a 12 acima. Basta copiar os arquivos ca.crt, client.crt e client.key já criados na máquina do servidor na Etapa 9 e 10 acima para a pasta de configuração da máquina do cliente relevante.

A próxima etapa é criar um arquivo de configuração para os clientes. Edite o arquivo client.ovpn encontrado na pasta sample-config e salve-o. Agora abra o artigo separado: [**Cliente OpenVPN no Windows**](https://wiki.teltonika-networks.com/view/OpenVPN_client_on_Windows)**,** mas observe que apenas a última parte é relevante para esta página. Comece na linha "• Salve o arquivo com uma extensão **.ovpn** ."

Nota: O arquivo client.ovpn editado pode ser copiado para todas as máquinas clientes, a menos que mudanças específicas precisem ser feitas.

1. Se você seguiu todas as etapas até agora, a configuração do servidor OpenVPN está concluída! A próxima coisa a fazer é simplesmente iniciar o servidor.

Execute o aplicativo **OpenVPN GUI como administrador** para que o aplicativo possa preencher os arquivos de log.

Localize OpenVPN GUI na bandeja do sistema do Windows. Clique com o botão direito e clique em **Conectar** :

