# FICHA TRABALHO 2

| | | | |
|---|---|---|---|
| MODALIDADE: | Aprendizagem + | Não aplicável | |
| CURSO: | Técnico/a de Cibersegurança | | |
| UC: | Gerir sistemas de deteção de intrusos (IDS) | CÓDIGO UC: | UC01486 |
| FORMADOR/A: | Bruno Silva | DATA: | |

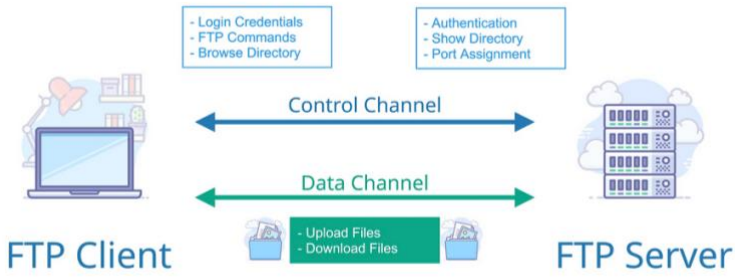
OBJETIVOS

- Saber como instalar e configurar um servidor de transferência de ficheiros
- Utilização do software VSFTPD e ligação com o Filezilla

## *FTP (File Transfer Protocol)*

Uma das primeiras e mais importantes aplicações em ambientes em rede e transferência de ficheiros (muito popular quando falamos de servidores online que alojam websites).

A importância desta aplicação prende-se ao facto dos ficheiros (que estão num determinado repositório de dados), serem objetos fundamentais de qualquer sistema informático, comportando não só dados do utilizador, mas também dados indispensáveis para o sistema operativo e aplicações.




2 exemplos de protocolos de transferência de ficheiros na Internet são o FTP (file transfer protocol) e o TFTP (trivial file transfer protocol), sendo este último uma versão simplificada do primeiro.

O HTTP é também um protocolo de transferência de ficheiros, embora de características bastante diferentes do FTP.

Já o FTP (file transfer protocol), permite a realização de um leque alargado de operações sobre ficheiros remotos, ou seja, ficheiros localizados em máquinas acessíveis através de uma rede, com o envio de informação (upload, put) ou a receção de informação (download, get), de um sistema ou múltiplos ficheiros localizados num servidor, bem como outras operações sobre sistema de ficheiros de máquinas remotas, quer sejam operações de navegação no sistema de ficheiros ou criação e gestão de diretorias.

O FTP é uma aplicação de utilizador, elástica, ***que funciona em modo cliente-servidor***.

Os utilizadores ligam-se ao serviço através de um programa de cliente que após a validação das credenciais de autenticação, envia pedidos ao servidor e recebe respetivas respostas. A comunicação entre o cliente e o servidor é feita usando várias ligações, isto é, uma para troca de comandos e respostas (ligação de controlo) e outras para a troca da informação de utilizador (ligações de dados), através das quais são transferidos os ficheiros.

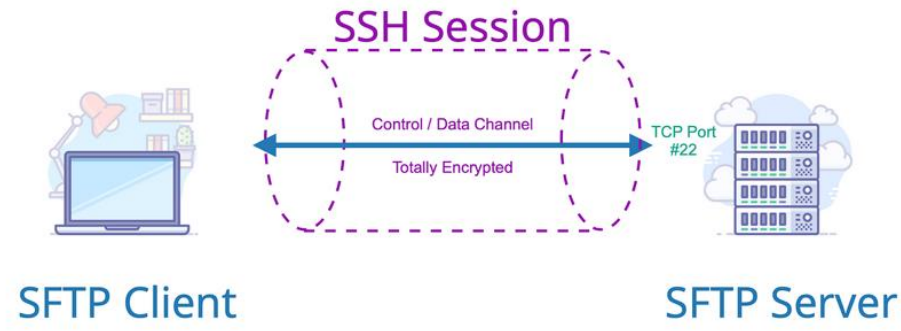
Não devemos esquecer que, para cada ficheiro transferido é estabelecida uma nova ligação de dados de forma a permitir a utilização concorrente do servidor. Quer a ligação do controlo quer as de dados funcionam sobre o protocolo TCP (transmission control protocol), nos portos de comunicação 21 e 20 respetivamente.

Em muitos casos, pretende-se que os servidores disponibilizem ficheiros à generalidade dos utilizadores na Internet. Como é impossível criar uma conta para cada um dos potenciais utilizadores desses servidores, o utilizador usou nome *anonymous* fornecendo, normalmente, com palavras-chave o seu endereço de correio eletrónico, passando a ter acesso às zonas públicas do servidor ao qual está ligado.

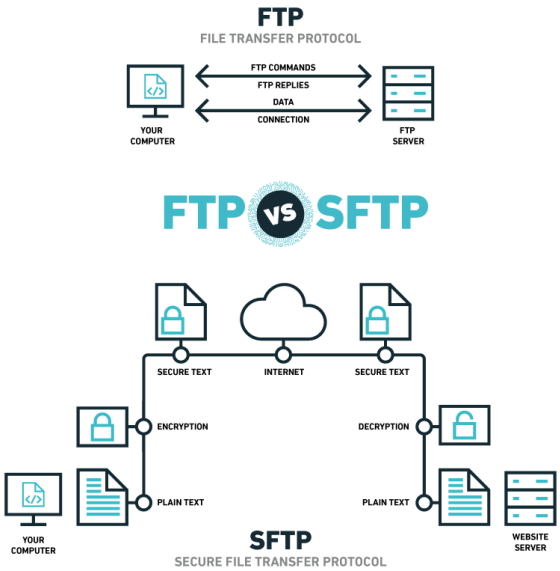
Atualmente, existem múltiplas aplicações com diferentes interfaces para utilização do protocolo FTP.

De visar que o FTP ***é um método não criptografado*** de transferência de arquivos entre dois sistemas remotos.

O SFTP, que significa “SSH File Transfer Protocol”, ou “Secure File Transfer Protocol”, é um protocolo separado incluído com o SSH que funciona de forma semelhante, mas com uma conexão segura. A vantagem é a capacidade de aproveitar uma conexão segura para transferir arquivos e percorrer o sistema de ficheiros tanto no sistema local quanto no remoto.

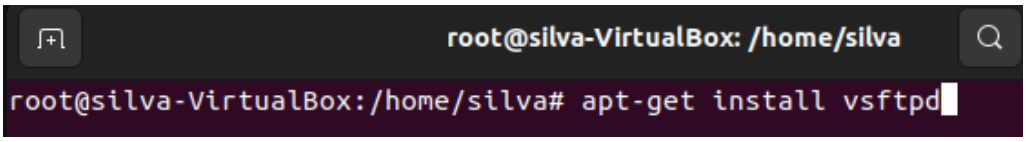



Em quase todos os casos, o SFTP é preferível ao FTP devido aos seus recursos de segurança e à capacidade de acompanhar uma conexão via protocolo SSH. O FTP é um protocolo inseguro que deve ser usado apenas em casos limitados ou em redes confiáveis.



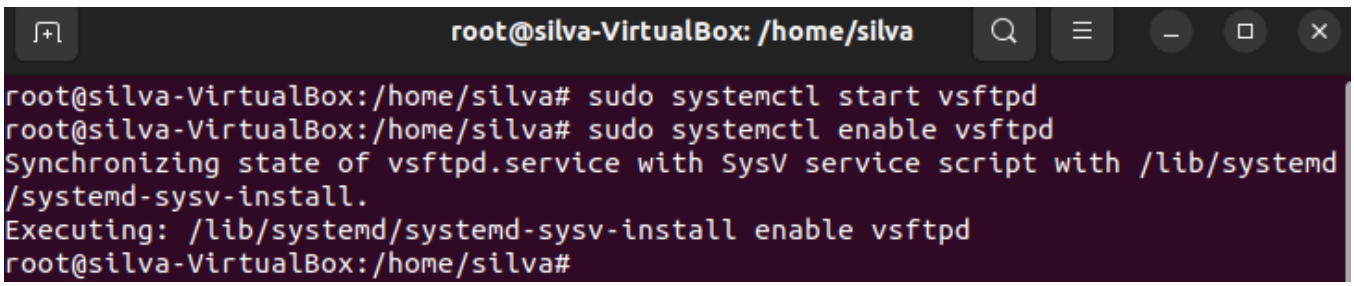

## *Parte 1 – Instalação do servidor FTP (VSFTPD)*

***Passo 1 –*** Instalar o servidor FTP no Ubuntu, mais especificamente, o servidor VSFTPD. Para tal, utilize o comando: **apt-get install vsftpd**



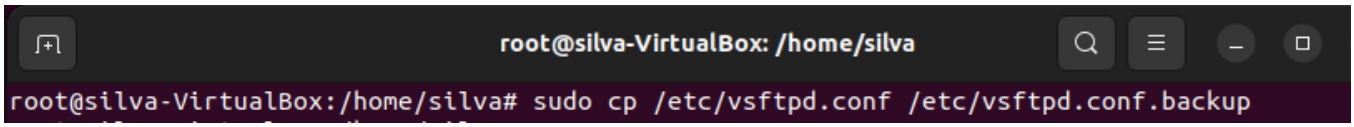

***Passo 2 –*** Vamos garantir que o serviço do servidor FTP esteja a funcionar e ativar o mesmo no iniciar do sistema operativo. Como tal vamos utilizar dois comandos:

- Comando para iniciar o serviço após instalação: **systemctl start vsftpd**
- Comando para iniciar serviço no arranque do S.O.: **systemctl enable vsftpd**



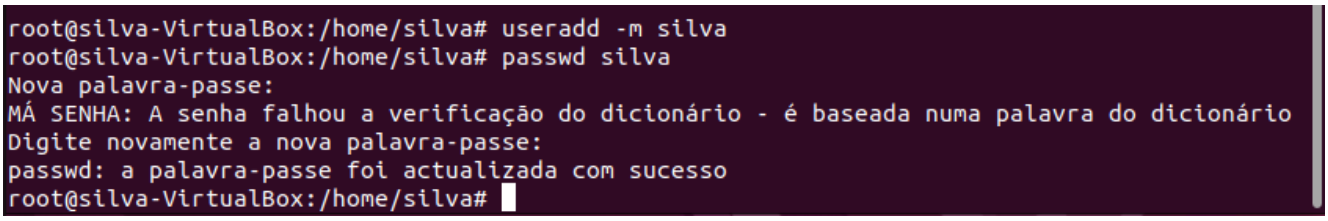
***Passo 3 –*** Sempre que possível vamos criar um backup do ficheiro das configurações do servidor FTP (para caso alguma coisa corra de errado). Para tal, vamos usar o comando para fazer cópia do ficheiro (cp) e indicar a localização original do ficheiro a copiar e o destino:

**cp /etc/vsftpd.conf /etc/vsftpd.conf.backup**




***Passo 4 –*** Vamos criar contas de utilizador para serem utilizadas no servidor FTP. Para tal, vamos criar uma conta que irá ficar no diretório HOME do Ubuntu (-m). Para tal, temos de criar o nome de utilizador e respetiva password com os comandos:

- Criar utilizador na pasta HOME: ***useradd -m <nome_utilizador>***
- Definir a password do utilizador: ***passwd <nome_utilizador>***




***Passo 5 –*** Um dos aspetos mais importantes é dar permissões na Firewall do Ubuntu, para que seja possível as aplicações conseguirem trabalhar sem restrições.

Numa máquina existem (teoricamente) 65.536 portos lógicos TCP que podem ser usados pelas mais diversas aplicações/serviços, o que (teoricamente) poderíamos ter 65.536 aplicações/serviços distintos a correr em simultâneo na nossa máquina. Além das portas TCP também temos 65.536 portas UDP (teoricamente).

Tanto no protocolo TCP como no UDP, é comum o uso das portas de 1 a 1024, já que a aplicação destas é padronizada pela IANA (Internet Assigned Numbers Authority). De acordo com essa entidade, eis algumas das portas TCP mais utilizadas:

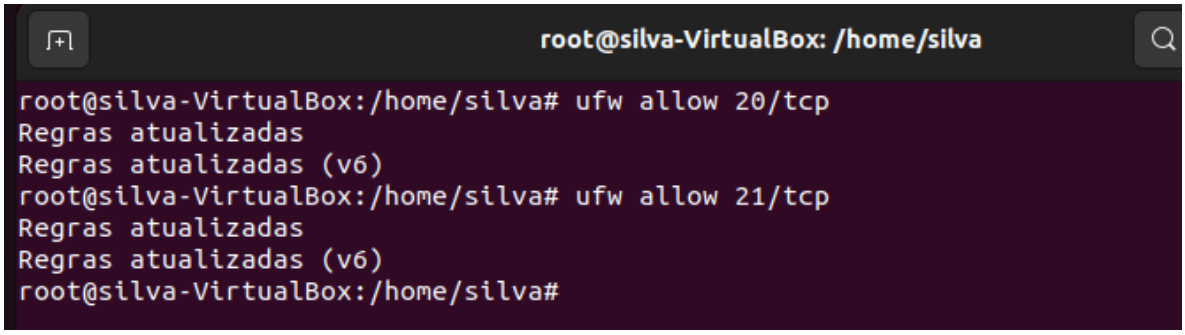
- 20 e 21 - FTP;
- 22 – SSH;
- 23 - Telnet;
- 25 - SMTP;
- 80 - HTTP;
- 110 - POP3;
- 143 - IMAP;
- 443 - HTTPS.

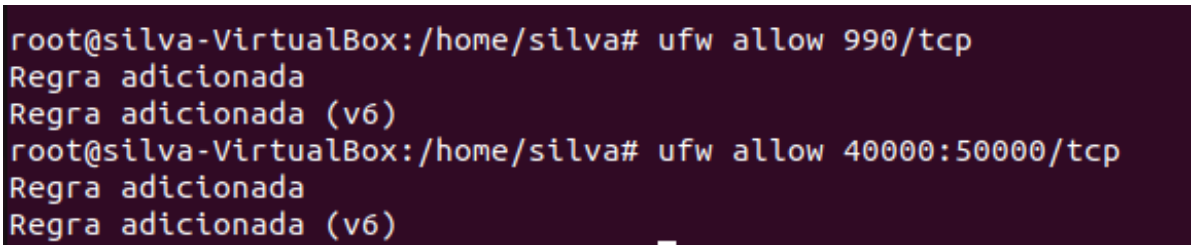
A IANA disponibiliza uma lista completa e atualizada da utilização das portas TCP e UDP nesta página: http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

***Muito Importante:*** Vamos instalar a aplicação de gestão de firewall no Ubuntu: ***apt install ufw***

Para este caso temos de dar permissões nos portos de comunicação TCP, mais especificamente, indicar ***qual o porto*** e ***qual o protocolo***:

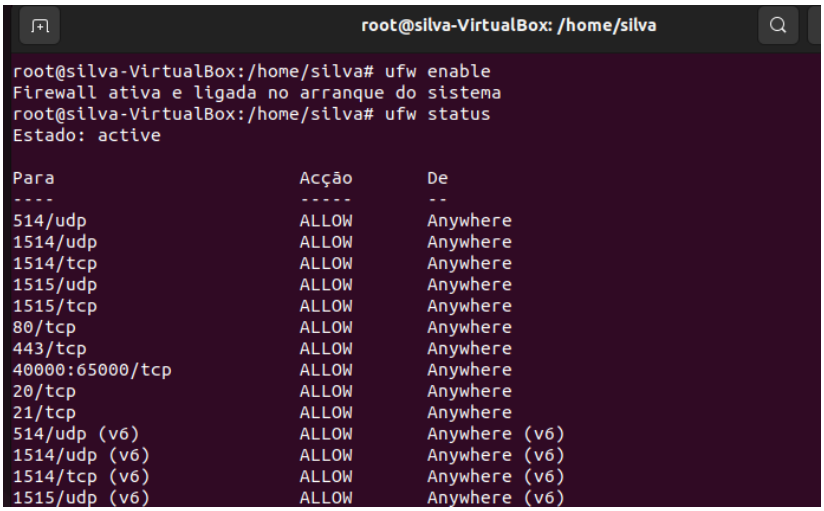
- 20/tcp (***comando:*** ufw allow 20/tcp);
- 21/tcp (***comando:*** ufw allow 21/tcp);
- 990/tcp (***comando:*** ufw allow 990/tcp);
- intervalo de portas entre 40000 e 50000 ambos em tcp ocupando apenas as necessárias para a aplicação (***comando:*** ufw allow 40000:50000/tcp);



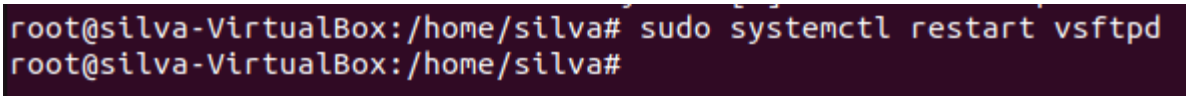




Para verificar as portas disponibilizadas na firewall, temos de ativar a firewall e só depois pedir a listagem das portas. Utilize os seguintes comandos:

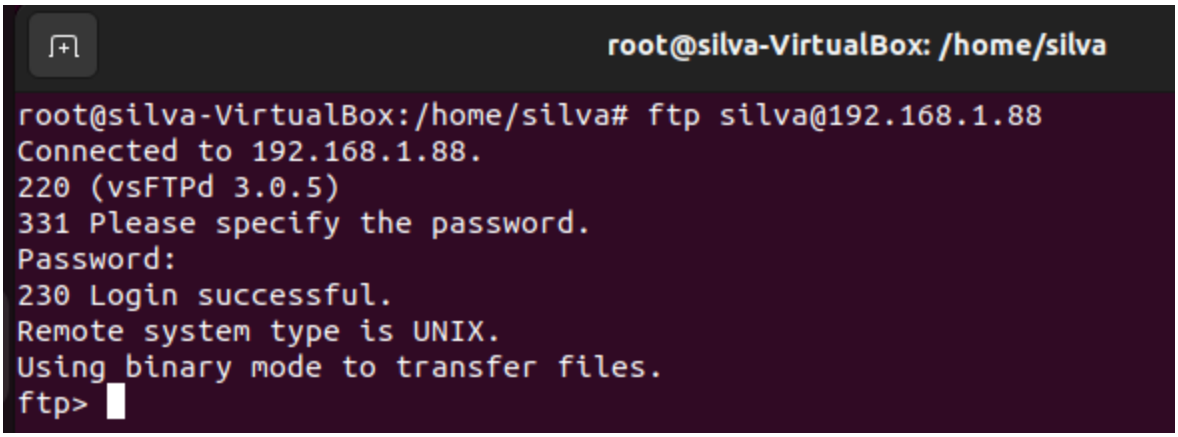
- ***ufw enable*** (ativar a firewall);
- ***ufw status*** (mostrar listagem das regras);




***Passo 6 –*** No final, vamos reiniciar o serviço FTP. Use o comando: **systemctl restart vsftpd**




***Passo 7 –*** Tente fazer a primeira conexão do utilizador que foi configurado anteriormente. Use o comando: ***ftp*** nome_utilizador**@**ip_maquina e coloque a password:



# *Parte 2 – Configurar as pastas de acesso*

Nesta etapa, vamos criar um utilizador FTP dedicado. No entanto, já pode ter utilizadores criados que precisam de acesso FTP. É sempre recomendado criar novos utilizadores FTP dedicados até configurar e testar a vossa configuração antes de reconfigurar qualquer utilizador que já criaram anteriormente.

***Passo 1 –*** Vamos criar contas de utilizador para serem utilizadas no servidor FTP. Para tal, vamos criar uma conta que irá ficar no diretório HOME do Linux (-m). Para tal, temos de criar o nome de utilizador e respetiva password com os comandos:

- Criar utilizador na pasta HOME: ***useradd -m <nome_utilizador>***
- Definir a password do utilizador: ***passwd <nome_utilizador>***

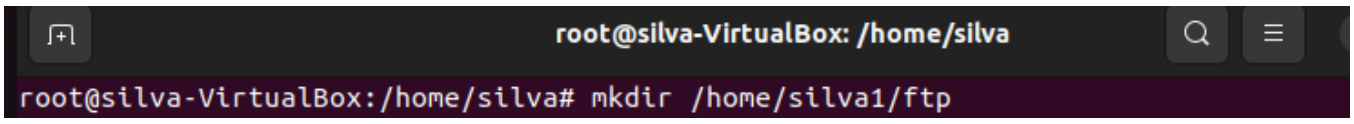
```
root@silva-VirtualBox:/home/silva# useradd -m silva1
root@silva-VirtualBox:/home/silva# passwd silva1
Nova palavra-passe:
MÁ SENHA: A senha falhou a verificação do dicionário - é baseada numa palavra do dicionário
Digite novamente a nova palavra-passe:
passwd: a palavra-passe foi actualizada com sucesso
root@silva-VirtualBox:/home/silva#
```

O FTP geralmente é mais seguro quando os utilizadores estão restritos a um diretório específico.

O servidor VSFTPD faz isso com o parâmetro **chroot** (como vamos ver no ficheiro de configuração da aplicação). Quando o chroot está ativo para utilizadores locais, estes ficam restritos ao seu diretório inicial por padrão e protege o diretório de uma maneira específica. Isso é adequado para um novo utilizador que deve conectar apenas via FTP, mas um utilizador existente pode precisar gravar na pasta pessoal se também tiver acesso ao terminal.

Neste exemplo, em vez de remover os privilégios de gravação do diretório inicial, vamos criar um diretório ftp para servir como chroot e um diretório de arquivos graváveis para armazenar os ficheiros reais.

***Passo 2 –*** Criar a pasta com o nome ftp no novo utilizador que acabou de criar no passo 1. Use o comando mkdir para criar pastas no sistema operativo: ***mkdir <localização>/ftp***



***Passo 3 –*** Definir a raiz da nossa pasta pessoal, com o comando sem atribuição a nenhum utilizador ou grupo: ***chown nobody:nogroup <localização>***

```
root@silva-VirtualBox:/home/silva# chown nobody:nogroup /home/silva1/ftp
```

***Passo 4 –*** Remover permissões de gravação na pasta da raiz (por segurança), com o comando ***chmod a-w <localização>***

```
root@silva-VirtualBox:/home/silva# chmod a-w /home/silva1/ftp/
```

***Passo 5 –*** Verificar permissões de gravação (após o passo 4), com o comando

***ls -la /home/***<utilizador>/<pasta>

```
root@silva-VirtualBox:/home/silva# ls -la /home/silva1/ftp/
total 8
dr-xr-xr-x 2 nobody nogroup 4096 abr  3 11:29 .
drwxr-x--- 3 silva1 silva1  4096 abr  3 11:29 ..
```

***Passo 6 –*** Criar a pasta ***files*** dentro da pasta ftp (criada anteriormente), para enviar os ficheiros (mas pode ser outro nome):

```
root@silva-VirtualBox:/home/silva# mkdir /home/silva1/ftp/files
```

***Passo 7 –*** Atribuir as ***propriedades de gestão*** da nova pasta ***ao utilizador que criou***:

chown ***<nome_utilizador>:<nome_utilizador> /home/***<utilizador>/<pasta>

```
root@silva-VirtualBox:/home/silva# chown silva1:silva1 /home/silva1/ftp/files/
```

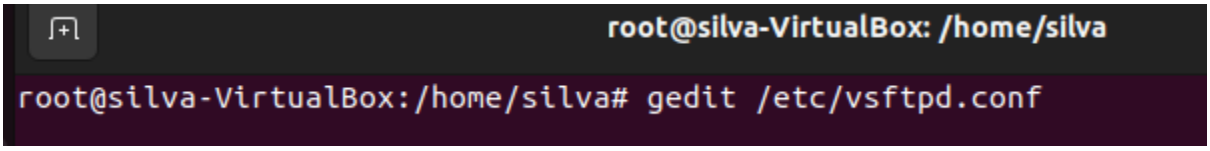
***Passo 8 –*** Verificar as ***permissões no diretório que criou***:

```
root@silva-VirtualBox:/home/silva# ls -la /home/silva1/ftp/
total 12
dr-xr-xr-x 3 nobody nogroup 4096 abr  3 11:32 .
drwxr-x--- 3 silva1 silva1  4096 abr  3 11:29 ..
drwxr-xr-x 2 silva1 silva1  4096 abr  3 11:32 files
```

# *Parte 3 – Configuração do ficheiro vsftpd.conf*

Nesta etapa, vamos fazer as configurações necessárias para aumentar o nível se segurança do nosso servidor FTP. As configurações já estão definidas no ficheiro vsftpd.conf localizado no diretorio /etc/vsftpd.conf.

***Passo 1 –*** Abra o ficheiro com o comando: ***gedit /etc/vsftpd.conf***




***Passo 2 –*** A partir da linha 25 vamos verificar/indicar:

- a opção ***anonymous_enable*** está com o valor ***NO,*** pois não queremos pessoas anónimas a fazer acesso ao servidor FTP;
- a opção ***local_enable*** está com o valor ***YES***, para permitir que os utilizadores do sistema operativo possam aceder aos serviços FTP;
- **comentar** a opção write_enable (com o símbolo #), para não permitir escrever informação na pasta (**mais tarde vamos desativar**);

```
23 #
24 # Allow anonymous FTP? (Disabled by default).
25 anonymous_enable=NO
26 #
27 # Uncomment this to allow local users to log in.
28 local_enable=YES
29 #
30 # Uncomment this to enable any form of FTP write command.
31 #write_enable=YES
32 #
```

***Passo 2 –*** Na linha 40 vamos comentar a opção **anon_upload_enable=YES**:

```
37 # Uncomment this to allow the anonymous FTP user to upload files. This only
38 # has an effect if the above global write enable is activated. Also, you will
39 # obviously need to create a directory writable by the FTP user.
40 #anon_upload_enable=YES
41 #
```

***Passo 3 –*** Na linha 114 ***vamos ativar*** a opção ***chroot_local_user*** com o valor ***YES***. Isto vai permitir restringir os utilizadores para navegar apenas nas pastas onde tem permissões, sem a possibilidade de estes acederem a outros diretórios:

```
111 # You may restrict local users to their home directories.  See the FAQ for
112 # the possible risks in this before using chroot_local_user or
113 # chroot_list_enable below.
114 chroot_local_user=YES
115 #
```

***Passo 4 –*** A partir da linha 157 vamos ***operações adicionais de segurança***:

- Adicione a opção ***user_sub_token*** cujo valor é a variável de ambiente do utilizador que estiver a trabalhar naquele momento ***$USER;***
- Adicione a opção ***local_root*** e configure-a para o diretório do qual deve ser sempre inciado de cada vez que faz login no servidor FTP (que também inclui a variável de utilizador $USER). Esta configuração garante que a configuração permitirá que o utilizador e futuros utilizadores sejam indicados para o diretório inicial do utilizador apropriado ao efetuar login;
- Limite o intervalo dos portos de comunicação que podem ser usadas para o FTP passivo de forma a garantir conexões suficientes (como configurado anteriormente na firewall do linux, mais especificamente, o intervalo de porta 40000:50000). Para tal, definimos o intervalo mínimo (***pasv_min_port***) e máximo (***pasv_max_port***);
- Para permitir o acesso ao FTP caso-a-caso, defina a configuração para que os utilizadores tenham acesso somente quando forem explicitamente adicionados a uma lista:
    - ***Para ativar a lista***, ative a opção ***userlist_enable*** com o valor ***YES***;
    - Indicar ***onde fica a lista de utilizadores autorizados***, ative a opção ***userlist_file*** com o valor ***/etc/vsftpd.userlist*** (local onde vai ficar o ficheiro com as autorizações);
    - A opção ***userlist_deny*** vamos definir o ***valor NO***. Quando o valor está definido ***como YES***, os utilizadores da lista ***têm acesso negado ao FTP***; quando definido ***como NO***, ***somente*** os utilizadores da lista é que vão ***ter acesso***.

```
157 ########################
158 #operações adicionais
159
160 user_sub_token=$USER
161 local_root=/home/$USER/ftp
162
163 pasv_min_port=40000
164 pasv_max_port=50000
165
166 userlist_enable=YES
167 userlist_file=/etc/vsftpd.userlist
168 userlist_deny=NO
169
```

Para além destas permissões podemos indicar operações adicionais, tais como:

| Option | Default value | Description |
|---|---|---|
| download_enable | YES | Specifies whether downloads from the Ubuntu FTP server are possible |
| ssl_enable | NO | Offers the possibility to enable SSL encryption for FTP access |
| anon_max_rate | 0 | Sets the maximum transfer speed (bytes per second) for anonymous users; 0 stands for an unlimited rate |
| local_max_rate | 0 | Sets the maximum transfer speed (bytes per second) for local users; 0 stands for an unlimited rate |
| max_clients | 0 | Maximum value for the number of clients logged on to the FTP server at the same time; 0 means no restriction |
| anon_root | /home/ftp | Directory to which anonymous users are automatically sent |
| log_ftp_protocol | NO | Logs all FTP requests and responses |
| connect_timeout | 60 | Defines the time span (in seconds) after which the connection between the server and the client is interrupted in the absence of communication |
| ftpd_banner | | Welcome text |
| guest_enable | NO | Allows you to unblock the anonymous access profile defined in guest_username |
| guest_username | ftp | Username for anonymous login |

***Passo 5*** **–** No final, vamos reiniciar o serviço FTP. Use o comando: **systemctl restart vsftpd**

```
root@silva-VirtualBox:/home/silva# sudo systemctl restart vsftpd
root@silva-VirtualBox:/home/silva#
```

***Passo 6 –*** De seguida, vamos testar o acesso ao servidor ftp, só que desta vez este vai ser negado, pois ainda não definimos os nomes de utilizadores autorizados no ficheiro de autorizações. Use o comando: **ftp** utilizador**@**ip_maquina

```
root@silva-VirtualBox:/home/silva# ftp silva@192.168.1.88
Connected to 192.168.1.88.
220 (vsFTPd 3.0.5)
530 Permission denied.
ftp: Login failed
ftp>
```

***Passo 7 –*** De seguida, vamos editar o ficheiro da lista com os utilizadores autorizados (do qual temos de criar o ficheiro). Para tal use o comando: ***gedit /etc/vsftpd.userlist***

```
root@silva-VirtualBox:/home/silva# gedit /etc/vsftpd.userlist
```

Dentro deste ficheiro, coloque apenas o nome do último utilizador que criou nesta ficha de trabalho.

***Nota importante:*** coloque cada nome de utilizador por linha (nunca ficam juntos);

***Passo 8 –*** Use o comando: **ftp** utilizador**@**ip_maquina e verifique se consegue aceder a sua conta ftp;

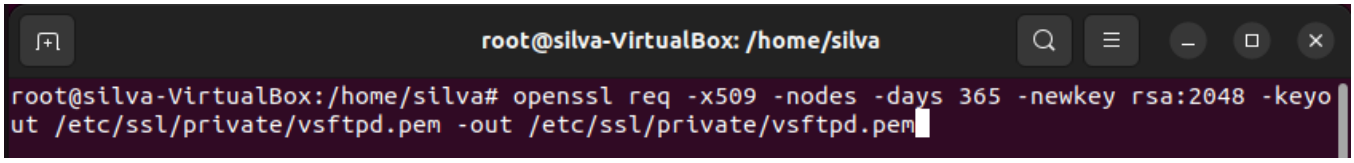
# *Parte 4 – Encriptação e Proteção das ligações FTP*

Nesta etapa, vamos fazer as configurações necessárias para aumentar o nível se segurança do servidor FTP, mais especificamente, ao nível da transmissão da informação

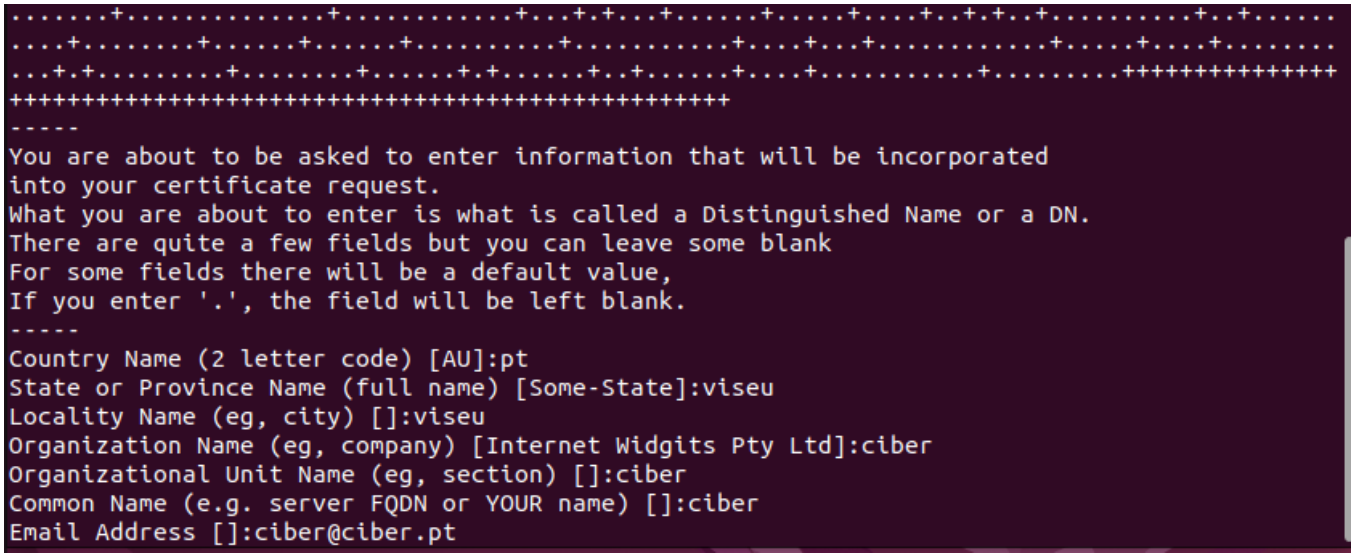
Como o FTP não faz a criptografia (incluindo as credenciais do utilizador), vamos ativar o TLS/SSL para fornecer essa criptografia. A primeira etapa é criar os certificados SSL para utilizar com o servidor vsftpd.

***Passo 1 -*** Vamos utilizar o ***openssl*** para criar um novo certificado e use o parâmetro -days para torná-lo válido por um ano (365 dias). No mesmo comando, adicione uma chave RSA privada com 2.048 bits de codificação. Ao definir os parâmetros -keyout e -out com o mesmo valor, a chave privada e o certificado estarão localizados no mesmo arquivo:

***openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem***




***Passo 2 –*** Ao executar o comando, este vai gerar os certificados e chave privada. Ao mesmo tempo, vai pedir dados adicionais para ajudar a construir o certificado:



***Passo 3 –*** Depois de gerada toda a informação, vamos listar o diretório do qual criou o conteúdo do passo anterior, com o comando: ***ls -l /etc/ssl/private*** (como indicado no passo 1):

```
root@silva-VirtualBox:/home/silva# ls -l /etc/ssl/private/
total 8
-rw-r----- 1 root ssl-cert 1704 mar 28 09:54 ssl-cert-snakeoil.key
-rw------- 1 root root     3099 abr  3 20:43 vsftpd.pem
```

***Passo 3 –*** Confirmado o passo2, vamos indicar as novas configurações no ficheiro de configuração do vsftpd. Use o comando ***gedit /etc/vsftpd.conf*** e dirige-se para a linha 147.

Estes parâmetros impedirão que clientes que não conseguem lidar com TLS conectem ao servidor FTP. Isso é necessário para garantir que todo o tráfego seja criptografado.

```
147 # This option specifies the location of the RSA certificate to use for SSL
148 # encrypted connections.
149 #rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
150 #rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
151 #ssl_enable=NO
152
153 rsa_cert_file=/etc/ssl/private/vsftpd.pem
154 rsa_private_key_file=/etc/ssl/private/vsftpd.pem
155 ssl_enable=YES
156
```

Copie as linhas 149 até 151 e cole mais abaixo (onde está o texto assinalado com laranja). Descomete as linhas no início de cada uma (retirando o símbolo #) e nos parâmetros:

- ***Localização do certificado:*** rsa_cert_file = /etc/ssl/private/vsftpd.pem
- ***Localização da chave privada:*** rsa_private_key_file = /etc/ssl/private/vsftpd.pem
- ***Ativar o modo SSL:*** ssl_enable=YES

***Passo 4 –*** Para além do passo anterior, vamos ativar mais alguma funcionalidade adicionais para acrescer a segurança da ligação, tais como:

- Adicione as seguintes linhas para negar explicitamente conexões anônimas por SSL e exigir SSL para transferência de dados e logins:

  ***allow_anon_ssl=NO***

  ***force_local_data_ssl=YES***

  ***force_local_logins_ssl=YES***

- Configure o servidor para usar TLS, o sucessor preferencial do SSL, adicionando a seguinte linha:
  ***ssl_tlsv1=YES***

- Finalmente, adicione duas opções finais. O primeiro não exigirá a reutilização de SSL porque pode quebrar as ligações muitos clientes FTP. O segundo exigirá conjuntos de cifras de criptografia "alta", o que atualmente significa comprimentos de chave iguais ou superiores a 128 bits (HIGH):

  ***require_ssl_reuse=NO***
  ***ssl_ciphers=HIGH***

***Formato com todos os parâmetros:***

```
152
153 rsa_cert_file=/etc/ssl/private/vsftpd.pem
154 rsa_private_key_file=/etc/ssl/private/vsftpd.pem
155 ssl_enable=YES
156
157 #opções adicionais para aumentar a segurança do FTP
158 allow_anon_ssl=NO
159 force_local_data_ssl=YES
160 force_local_logins_ssl=YES
161 ssl_tlsv1=YES
162
163 require_ssl_reuse=NO
164 ssl_ciphers=HIGH
165
```

***Passo 5 –*** Vamos reiniciar o serviço FTP. Use o comando: **systemctl restart vsftpd**

```
root@silva-VirtualBox:/home/silva# sudo systemctl restart vsftpd
root@silva-VirtualBox:/home/silva#
```

***Passo 6 –*** No final, teste a conexão. Use o comando: **ftp** utilizador**@**ip_maquina. Mas, agora não vai conseguir fazer login, pois acabou de criar regras de sessões encriptadas e a ligação que está a efetuar é por entrada sem ligação cifrada:

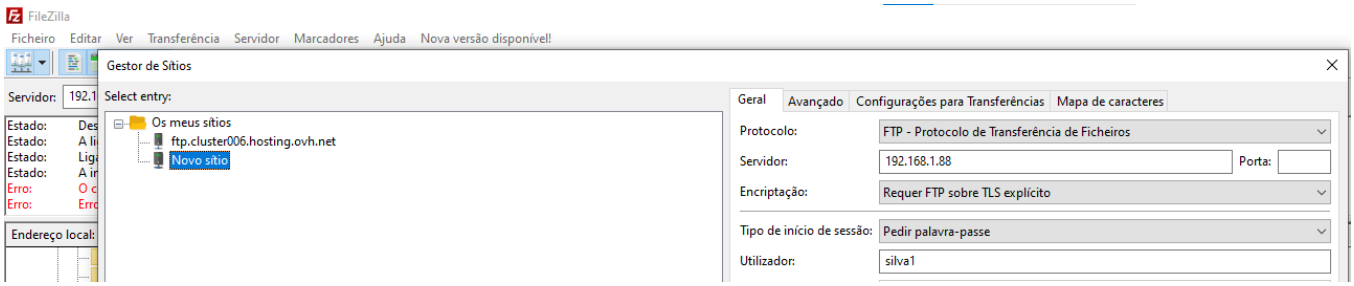
```
root@silva-VirtualBox: /home/silva
root@silva-VirtualBox:/home/silva# ftp silva1@192.168.1.88
Connected to 192.168.1.88.
220 (vsFTPd 3.0.5)
530 Non-anonymous sessions must use encryption.
ftp: Login failed
ftp>
```

# *Parte 5 – Acesso ao FTP com o programa Filezilla (com TLS/SSL)*

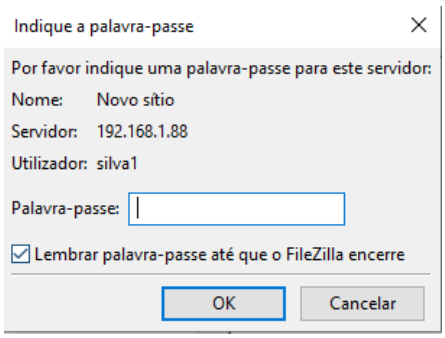
A maioria dos clientes FTP modernos pode ser configurada para usar criptografia TLS. Para tal, vamos utilizar uma aplicação muito popular com o nome FileZilla do qual tem suporte multiplataforma.

Ao abrir o FileZilla pela primeira vez, encontre o ícone do ***Site Manager*** localizado abaixo da palavra Ficheiro, o ícone mais à esquerda na linha superior. Ao clicar nesse botão, vamos na opção mais abaixo "Criar novo sitio" e introduzir os seguintes dados:

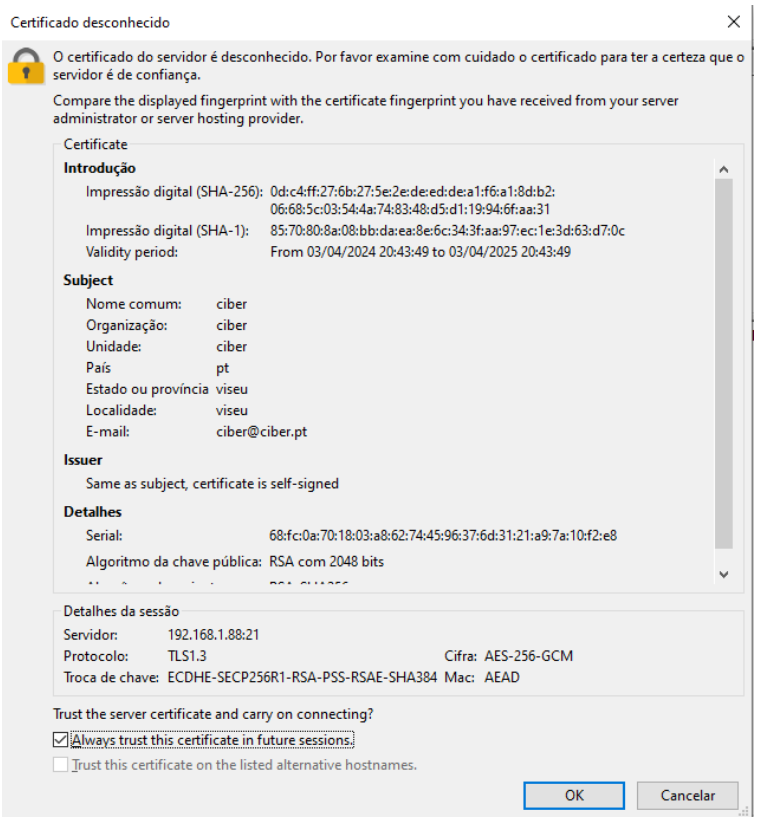
- ***Protocolo:*** FTP – Protocolo de Transferencia de ficheiros
- ***Servidor:*** Endereço IP da máquina com o servidor VSFTPD
- ***Encriptação:*** Requer FTP sobre TLS explícito
- ***Tipo de início de sessão:*** Pedir palavra-passe
- ***Utilizador:*** nome do utilizador autorizado



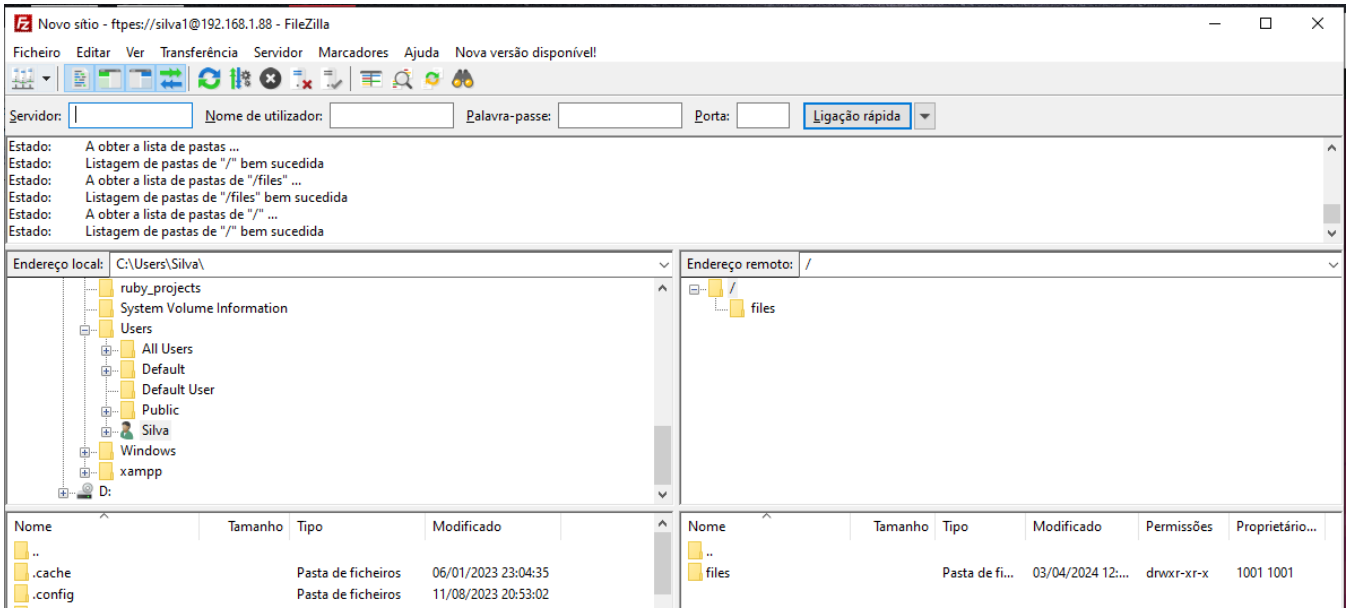

De seguida clique no botão ligar/conectar e será exibida uma caixa para introduzir a password:




Se for feita a autenticação com segurança, será exibido a confirmação do certificado de segurança que gerou anteriormente ***e antes de confirmar***, clique na opção "Always trust this certificate in future sessions" e clicar OK:

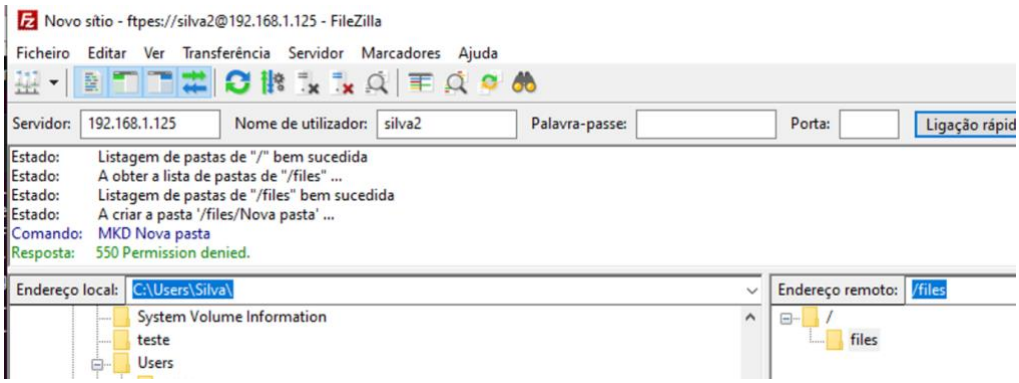



**Resultado final:**




**MUITO IMPORTANTE:**

Ao tentar criar uma pasta, pode dar erro de criação de conteúdos.




Caso aconteça, volte ao ficheiro de configurações do vsftpd.conf e ***ative a opção "write_enable***" (que costuma estar perto do início do ficheiro, normalmente na linha 31) e coloque o valor YES. Volte a reiniciar o serviço.

No final das alterações, reinicie o servidor do ftp e volte a testar a criação dos conteúdos.