FICHA TRABALHO 6

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

OBJETIVOS

- Saber como instalar e configurar uma central telefónica VoIP com o software Asterisk (Ubuntu)

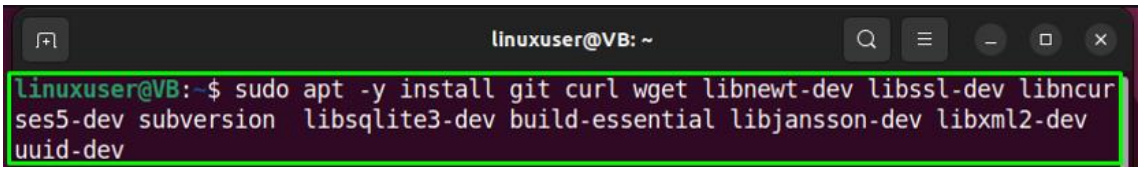
Passo 1: Atualização do sistema operativo Ubuntu

Atualizar o sistema operativo (repositórios e software do Ubuntu):

Passo 2: Instalação de pacotes essenciais

Em seguida, vá para a instalação de pacotes essenciais (copie e cole no terminal):

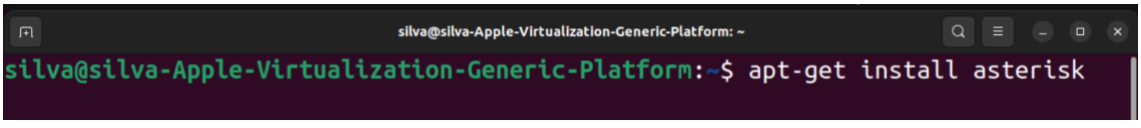
sudo apt -y install git curl wget libnewt-dev libssl-dev libncurses5-dev subversion libsqlite3-dev build-essential libjansson-dev libxml2-dev uuid-dev



Passo 3: Instalação do asterisk

Para instalar o software de central telefónica, vamos colocar o seguinte comando:

apt-get install asterisk (copie e cole no terminal)



Confirmar a instalação do software:

```
  libsox3 libspandsp2 libsrtp2-1 libsybdb5 libunbound8 liburiparser1
  libvo-amrwbenc0 mlock sox
0 pacotes actualizados, 29 pacotes novos instalados, 0 a remover e 3 não actuali
zados.
É necessário obter 13,0 MB de arquivos.
Após esta operação, serão utilizados 35,1 MB adicionais de espaço em disco.
Deseja continuar? [S/n]
```

No final, vamos aceder a pasta da instalação do asterisk. Para aceder a uma pasta colocamos o comando cd seguido da localização que queremos aceder. O comando ***ls*** (mostra o conteúdo da localização onde está atualmente):

```
silva@silva-Apple-Virtualization-Generic-Platform: /etc/asterisk
silva@silva-Apple-Virtualization-Generic-Platform:~$ cd /etc/asterisk/
silva@silva-Apple-Virtualization-Generic-Platform:/etc/asterisk$ ls
acl.conf                confbridge.conf         pjsip_notify.conf
adsi.conf               config_test.conf        pjsip_wizard.conf
agents.conf             console.conf            prometheus.conf
alarmreceiver.conf      dbsep.conf              queuerules.conf
alsa.conf               dnsmgr.conf             queues.conf
amd.conf                dsp.conf                res_config_mysql.conf
app_mysql.conf          enum.conf               res_config_sqlite3.conf
app_skel.conf           extconfig.conf          res_config_sqlite.conf
ari.conf                extensions.ael          res_corosync.conf
ast_debug_tools.conf    extensions.conf         res_curl.conf
asterisk.adsi           extensions.lua          res_fax.conf
asterisk.conf           extensions_minivm.conf  res_ldap.conf
calendar.conf           features.conf           res_odbc.conf
ccss.conf               festival.conf           resolver_unbound.conf
cdr_adaptive_odbc.conf  followme.conf           res_parking.conf
cdr_beanstalkd.conf     func_odbc.conf          res_pgsql.conf
cdr.conf                hep.conf                res_pktccops.conf
cdr_custom.conf         http.conf               res_snmp.conf
cdr_manager.conf        iax.conf                res_stun_monitor.conf
cdr_mysql.conf          iaxprov.conf            rtp.conf
cdr_odbc.conf           indications.conf        say.conf
cdr_pgsql.conf          logger.conf             sip.conf
cdr_sqlite3_custom.conf manager.conf            sip_notify.conf
cdr_syslog.conf         manager.d               sla.conf
```

Passo 3: Configuração do ficheiro sip.conf (configurações de entidades e registos)

Sempre que a ideia seja modificar os ficheiros do programa, vamos sempre jogar pelo seguro e fazer backups. Para tal vamos fazer o comando mv (que serve para criar uma cópia do ficheiro):

sudo mv sip.conf sip.conf.backup

De seguida, vamos editar o ficheiro original sip.conf. Para tal, vamos pedir para abrir o ficheiro com a aplicação ***gedit*** (versão do notepad do Windows para Linux). Introduza o comando: ***sudo gedit sip.conf***

Dentro do ficheiro, vamos colocar a informação de configuração do servidor VoIP e respetivo funcionamento. O protocolo SIP é configurado no ficheiro ***/etc/asterisk/sip.conf*** e contém parâmetros relacionados à configuração dos telefones e operadoras SIP (local onde colocamos os utilizadores).

O ficheiro SIP é lido de cima para baixo.

A ***primeira seção*** do ficheiro contém as configurações globais [general] da central telefónica:

- ***bindaddr***: Endereço IP onde o Asterisk irá esperar pelas conexões SIP (endereço IP da máquina). O comportamento padrão é esperar em todas as interfaces e endereços secundários.
- ***bindport***: Porta que o Asterisk deve esperar por conexões de entrada SIP. O padrão é 5060.
- ***allowguest:*** se permite ligações convidadas, isto é, pessoas não autorizadas;
- ***context***: Configura o contexto padrão onde todos os clientes serão colocados, a menos que seja sobrescrito na definição da entidade, ou seja, podemos ter grupos diferentes;
- ***allow***: Permite que um determinado codec (qualidade de som) seja usado.
- ***disallow***: Proíbe um determinado codec (qualidade de som) seja usado.
- ***maxexpirey***: Tempo máximo para registo em segundos.
- ***defaultexpirey***: Tempo padrão para registo em segundos.
- ***register***: Regista o Asterisk com outro servidor. O formato é um endereço SIP opcionalmente seguido por uma barra normal (/) e a extensão.

Exemplo:

```
1 [general]
2 context=dummy
3 allowguest=yes
4 disallow=all
5 allow=ulaw
6 callevent=yes
7 notifyhold=yes
8 callcounter=yes
9
```

A seguir vamos colocar as pessoas que devem existir nas nossas entidades (ligações) SIP.

Para tal, vamos definir ***duas ligações*** com a extensão ***7001*** e ***7002***:

```
16 [7001]
17 type=friend
18 host=dynamic
19 secret=7001
20 context=internal
21
22 [7002]
23 type=friend
24 host=dynamic
25 secret=7002
26 context=internal
```

- ***[name]:*** Quando um dispositivo SIP é conectado ao Asterisk, ele utiliza a parte username do SIP URI para encontrar a entidade que está neste ficheiro (pode ser por números ou por nomes);
- ***type:*** Configura a classe de conexão, onde as opções são: ***peer***, ***user*** e ***friend***.
    - ***peer:*** Entidade para a qual o Asterisk envia chamadas;
    - ***user:*** Entidade que faz chamadas através do Asterisk;
    - ***friend:*** Os dois ao mesmo tempo (vamos optar por este);
- ***host:*** Configura o endereço IP ou o nome do host. Podemos usar também a opção '***dynamic'*** onde este espera que o computador onde está configurada a entidade faça o registo (é a opção mais comum);
- ***secret:*** Palavra-passe utilizada para autenticar a ligação da entidade para fazer uma chamada;
- ***context:*** Para indicar a que grupo pertence (como configurado na primeira parte do ficheiro);

Tabela resumida:

SIP.CONF	
[general]	Seção de configuração global. O que é inserido aqui é aplicado para todos os canais SIP criados
port=5060	O Asterisk escuta a porta 5060 para conexão
bindaddr=0.0.0.0	Escuta as solicitações de todas as interfaces
[1701] ou [ana]	Configura o canal SIP 1701. Também aceita valores alfanuméricos
type=friend	Configura o tipo de canal. Asterisk <=user; Asterisk =>peer e Asterisk = friend
username=1701	Nome do utilizador
secret=123456	senha do canal SIP para registo
host=dynamic	Define os endereços IP para o dispositivo SIP. A opção dynamic aceita todos os IPs
context=from-internal	Contexto utilizado quando o dispositivo abre o canal. Configurado em extensions.conf
qualify=yes	Monitora a latência
nat=yes	Suporte a NAT. Dica nas versões mais novas do Asterisk utilize: nat=force_rport,comedia

Passo 4: Configuração do ficheiro extensions.conf (funcionamento dos registos)

O plano das extensões define como o Asterisk irá gerir as chamadas que recebe.

Este consiste de uma lista de instruções ou passos que o Asterisk deverá seguir. Essas instruções são disparadas a partir dos dígitos recebidos de um canal ou aplicação.

A maior parte do plano das extensões está configurada no ficheiro ***/etc/asterisk/extensions.conf***.

Sempre que a ideia seja modificar os ficheiros do programa, vamos sempre jogar pelo seguro e fazer backups. Para tal vamos fazer o comando mv (que serve para criar uma cópia do ficheiro):

sudo mv extensions.conf extensions.conf.backup

De seguida, vamos editar o ficheiro original extensions.conf. Para tal, vamos pedir para abrir o ficheiro com a aplicação ***gedit*** (versão do notepad do Windows para Linux).

Introduza o comando: ***sudo gedit extensions.conf***

Dentro do ficheiro, vamos organizar o conteúdo e indicar como é processada cada extensão:

Exemplo de Configuração:

Tabela resumida:

EXTENSIONS.CONF	
[general]	Configurações gerais do plano de extensões
static=yes	Configuração estática
writeprotect=yes	Não permite alterações do plano de discagem sejam realizadas a partir do console (CLI)
[globals]	Seção de variáveis
[name]	Define um nome contexto. Poderíamos utilizar um contexto chamado de [from-internal] ou simplesmente [joao]
dial(tech/u:p@host)	Conecta com um host / utilizador usando um canal
answer()	Abre um canal
hangup()	Encerra um canal
wait(n)	Espera por **n** segundos
goto(n)	Salta de uma prioridade **n** na mesma extensão. Goto(100,12) aqui o salto é para extensão e prioridade 12.
gotoif($[${X}=1]?,1:5)	Salta para prioridade 1 se a variável X for igual a 1. Caso contrário salta para prioridade 5 da extensão
gotoiftime(9:00-17:00|monfri|1-31|*?dia,s,1)	Salta para o contexto dia na extensão **s** , prioridade 1 caso seja entre 9h:00 e 17h:00. De segunda a sexta.
voicemail()	Conectar uma chamada ao correio de voz. Utilizar as opções u: unavailble, b: busy e s: gravação
voicemailmain()	Conectar um utilizador ao menu principal do sistema de correio de voz

Passo 5: Configuração do ficheiro voicemail.conf (funcionamento da gravação)

O ficheiro voicemail, permite criar um correio de gravação de voz, caso não consiga efetuar a chamada de voz.

Sempre que a ideia seja modificar os ficheiros do programa, vamos sempre jogar pelo seguro e fazer backups. Para tal vamos fazer o comando mv (que serve para criar uma cópia do ficheiro):

sudo mv voicemail.conf voicemail.conf.backup

De seguida, vamos editar o ficheiro original voicemail.conf. Para tal, vamos pedir para abrir o ficheiro com a aplicação ***gedit*** (versão do notepad do Windows para Linux).

Introduza o comando: ***sudo gedit voicemail.conf***

Dentro do ficheiro, apenas vamos indicar as ligações do nome de utilizador para que caixa a caixa de correio:

Passo 6: Iniciar servidor Asterisk

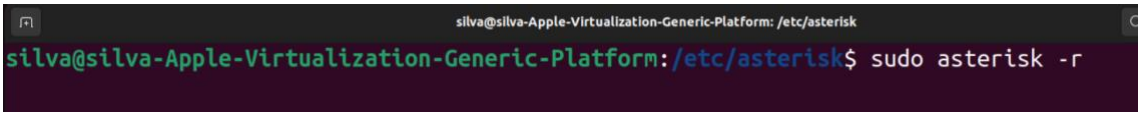
Depois de tudo configurado, vamos iniciar o nosso servidor em causa. Antes de mais, temos de fazer as novas atualizações que foram realizados nos outros ficheiros.

Comandos básicos da aplicação:

INICIAR E PARAR O ASTERISK	
asterisk	Arrancar o Asterisk
asterisk -c	Iniciar o Asterisk e abrir o consola (CLI)
asterisk -r	Ingressar na consola remota
asterisk -vvvvvr	Inciar o asterisk em modo de detalhado

COMANDOS IMPORTANTES - CLI	
reload	Recarrega todas as definições e alterações
Set debug	Ativa o modo de depuração no CLI
sip show peers	Listar todas contas SIP's do Asterisk
sip show channels	Listar todos os canais e conexões ativos

Passo 1 – Iniciar o servidor asterisk em modo de consola:

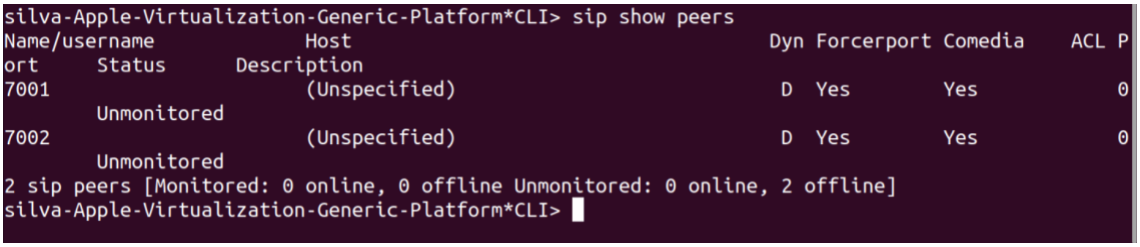


Passo 2 – Pedir para recarregar todas as alterações efetuadas com o comando "reload":

Passo 3 – Sair do modo de consola com o comando ***exit*** e de seguida, executar em modo de depuração (para ter os detalhes da aplicação ao nosso dispor).

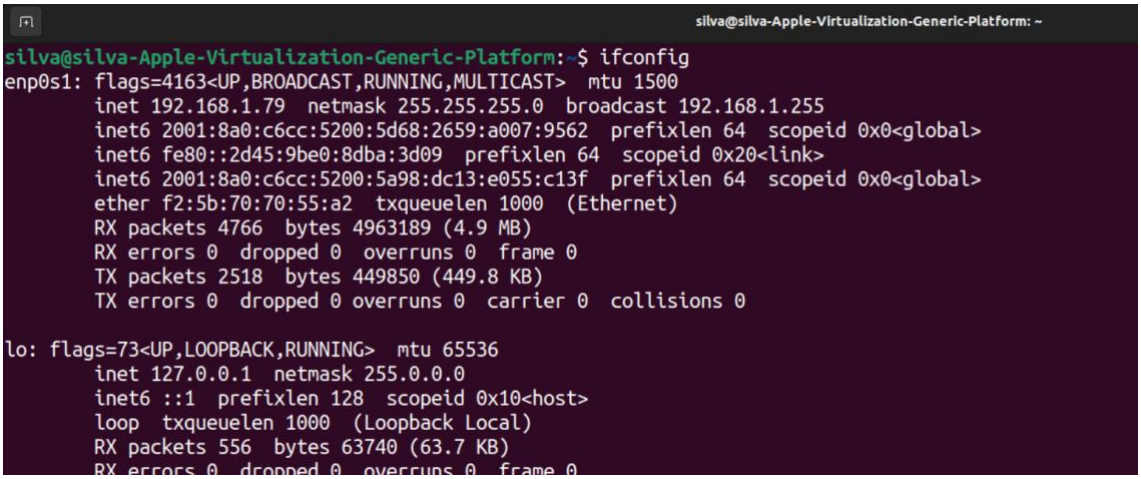
Escreva o comando: ***sudo asterisk -vvvvvr***

Passo 4 – Pedir para mostrar quais são as entidades que estão registados e qual o estado. Escreva o comando "***sip show peers***":



Passo 4 – No entanto, a ligação da nossa máquina tem de ser alterada.

Muito importante: as configurações da máquina virtual ***devem passar ter uma ligação do tipo Bridge Mode*** (senão temos de andar a fazer reencaminhamentos), para depois conseguir comunicar com dispositivos externos (como telemóveis). Se utilizar apenas máquinas virtuais internas, não precisa deste ponto.

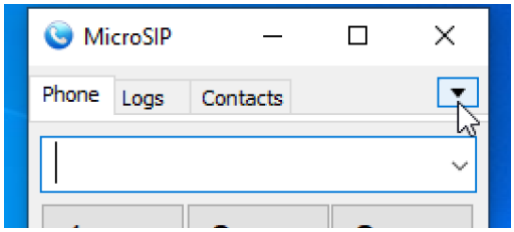


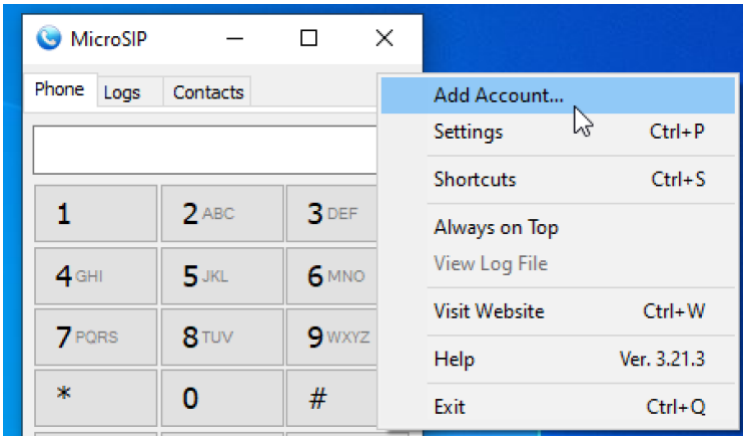
Passo 7: Associar conta na aplicação MicroSIP (cliente VoIP)

Para conseguir interligar com o servidor Asterisk, necessitamos de uma aplicação que permita registar as nossas entidades (que foram criados no ficheiro sip.conf). A aplicação a usar vai ser o MicroSIP.

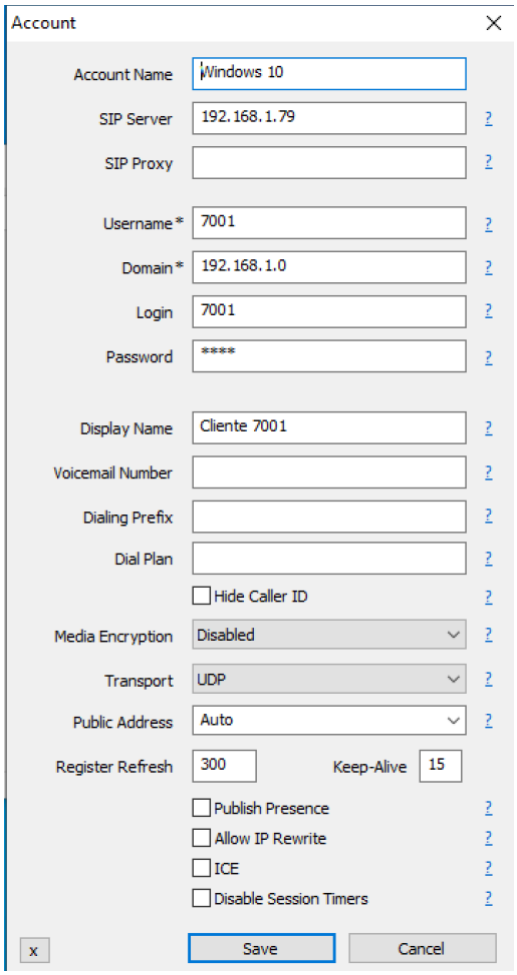
Para tal, poderá iniciar uma máquina virtual com Windows 10 ou Windows 7, mas também pode usar a máquina física onde esta a máquina virtual do Ubuntu.

Passo 1 - Na parte superior do ecrã, vamos clicar no botão da seta para baixo (que está no canto direito da aplicação) e clicar na opção “Add Account...”:

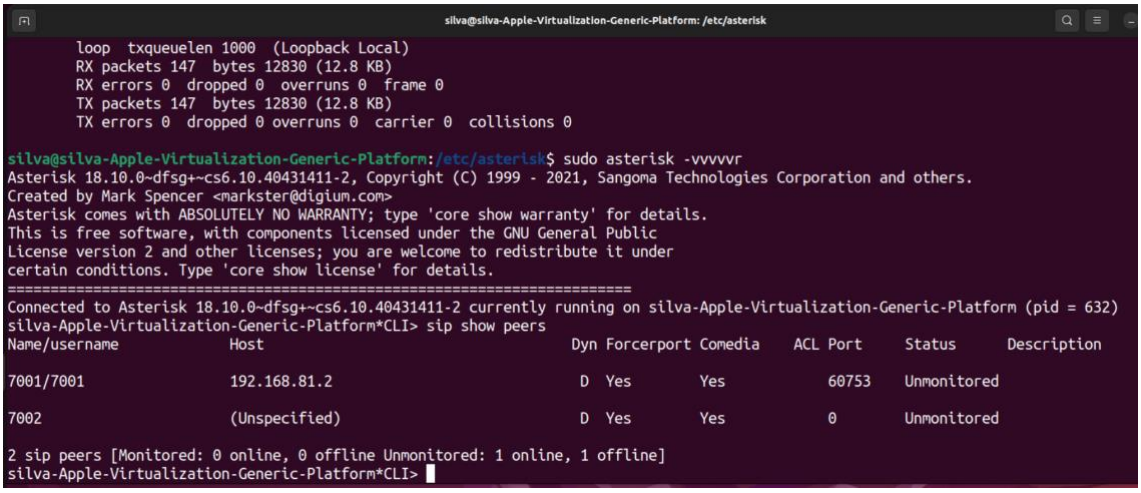




Passo 2 – Colocar as informações de acordo com as entidades que forma definidas:



Passo 3 – Se tudo correr bem e no programa do MicroSIP o estado ficar online, vá até ao servidor do asterik no Ubuntu e faça o comando “sip show peers” e verifique se já foi atribuído um IP e porta de comunicação:

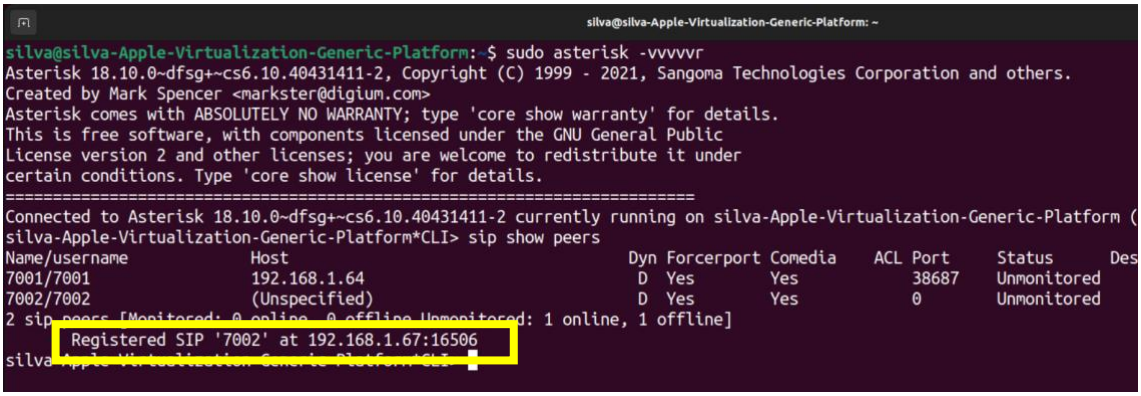


Passo 8: Associar conta na aplicação MicroSIP (smartphones)

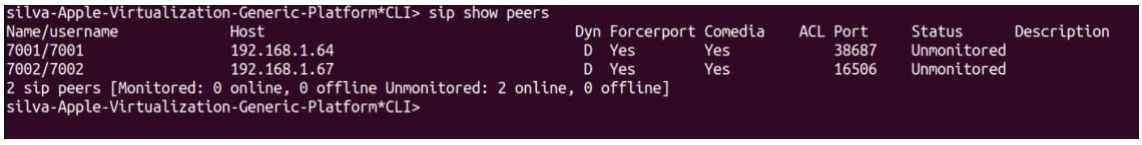
Passo 1 – Retirar o software Mizudroid

Passo 2 – Configurar conta (colocar print)

Passo 3 – Quando a aplicação conectar o telemóvel a máquina virtual, reparem que é exibida uma nova conexão (tal como nos programas):



Passo 4 - Fazer novamente o comando “sip show peers”:



Passo 5 – Teste a realização de uma chamada de áudio com a aplicação Mizudroid entre dois smartphones;

Passo 9: Proteção das passwords dos utilizadores com o algoritmo md5 (md5secret)

Vamos implementar medidas de segurança adicionais para impedir que alguém veja as nossas senhas no Asterisk. No entanto, temos de verificar um facto importante: o uso do algoritmo de encriptação de dados MD5 fornece pouca segurança nos dias atuais. A menos que estejam a usar conexões criptografadas, a senha ainda é enviada em texto claro (algo que já vamos implementar mais a frente com os certificados TLS)

Como tal, vamos utilizar o algoritmo md5 para ajudar a proteger a password.

1 – Gerar password com algoritmo MD5

Uma vez que temos a função md5sum na linha de comandos, podemos construir uma senha que consiste em 3 partes:

- nome de utilizador (username)
- domínio (realm)
- password

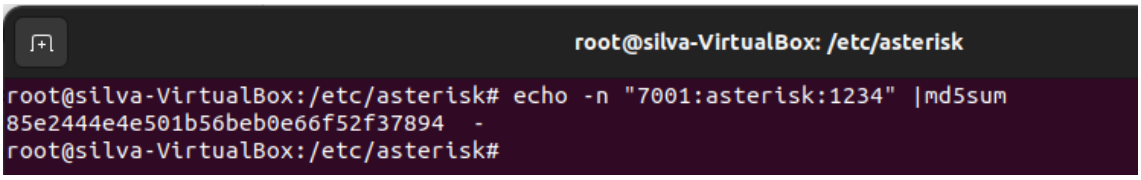
Como já temos o utilizador 7001 e o domínio asterisk (que vem por defeito), vamos criar a senha com a seguinte estrutura:

- **echo -n** para escrever o resultado da instrução
- dentro dos **"…"** colocam o **método de construção da senha** como descrito mais acima
- utilizar a barra ao alto "|" para separar o método da construção da senha (com associação ao utilizar) e escreva que quer usar o algoritmo **md5sum**

Exemplo:

echo -n "username:realm:secret" | md5sum

Exemplo: echo -n "7001:asterisk:1234" | md5sum



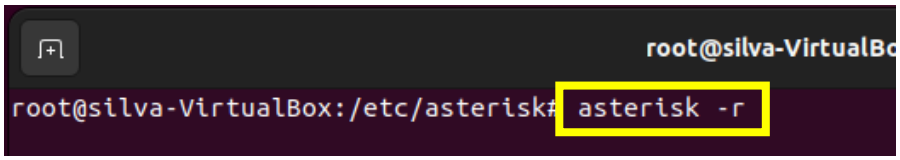
2 – Alterar password no ficheiro sip.conf

Como já temos o utilizador 7001 e o domínio asterisk (que vem por defeito), vamos colocar a senha anterior, com a seguinte estrutura → campo md5secret : password

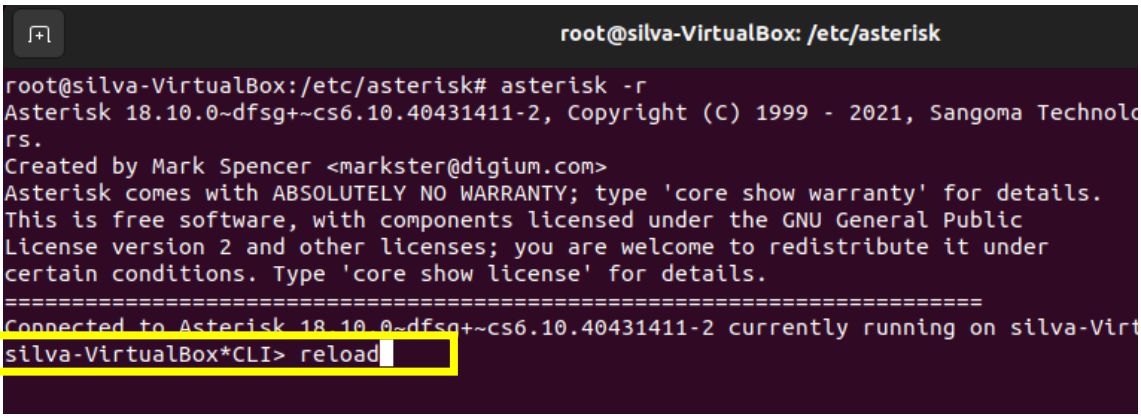
MUITO IMPORTANTE: No final, não deve esquecer de gravar as novas alterações!!!!!

3 – Atualizar as novas alterações no servidor Asterisk

Correr o servidor asterisk em modo de consola:

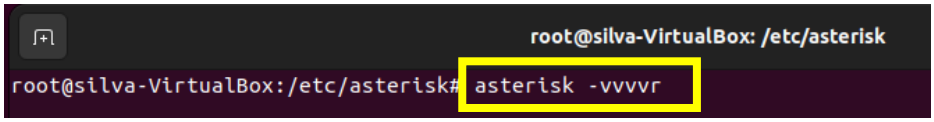


Pedir para recarregar todas as alterações efetuadas com o comando “reload”:



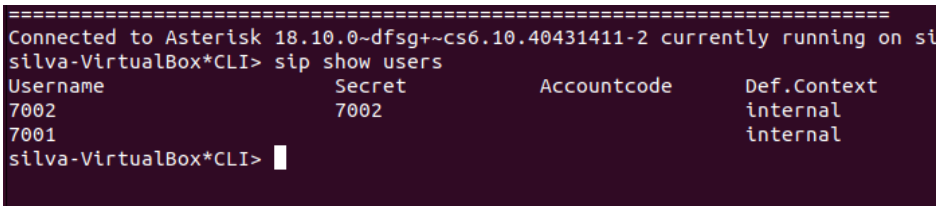
No final, vamos sair do modo de consola com o comando ***exit*** e de seguida, executar em modo de depuração (para ter os detalhes da aplicação ao nosso dispor).

Escreva o comando: ***sudo asterisk -vvvvvr***

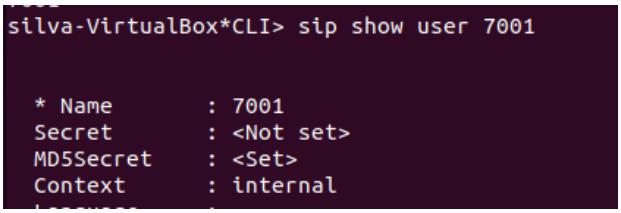


4 – Ver os utilizadores registados no ficheiro sip.conf

Use o comando "**sip show peers**" para exibir os dados dos utilizadores registados na plataforma (que estão no ficheiro sip.conf) e **repare que a password do utilizador 7001 desapareceu**:



Use o comando para obter informações de um utilizador detalhamento, com o comando "sip show peer xxxx" e repare que já aparece definido o campo md5secret como implementado:



5 – Testar os novos dados de acesso

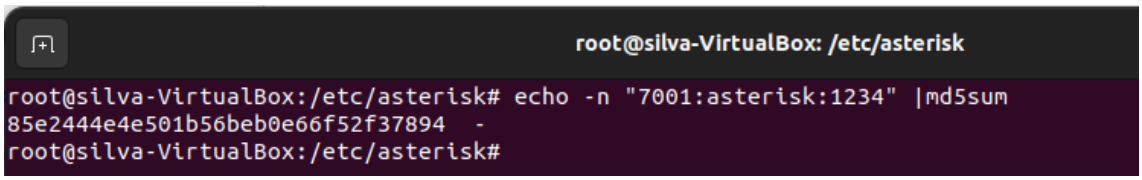
No software de chamada (Microsip ou MizuDroid), altere a senha antiga para a nova password que definiu nos passos anteriores (basta apenas o campo da password) e teste a aplicação.

Nota importante: a password a ser colocada tem de coincidir com a que foi aplicada no último campo

echo -n "username:realm:**secret**" | md5sum

Exemplo: echo -n "7001:asterisk:**1234**" | md5sum

É esta a senha que devem colocar no software Voip



Passo 10: Protocolo Transport Layer Security (TLS) em asterisk

Se tiver um servidor Asterisk conectado diretamente à internet, ou que está exposto através de uma porta padrão SIP (tipicamente a porta 5060), muito provavelmente podem deparar com alguém a tentar realizar chamadas internacionais utilizando as vossas linhas, ou então, tentar fazer autenticação as nossas contas de utilizador para utilizá-los de forma maliciosa.

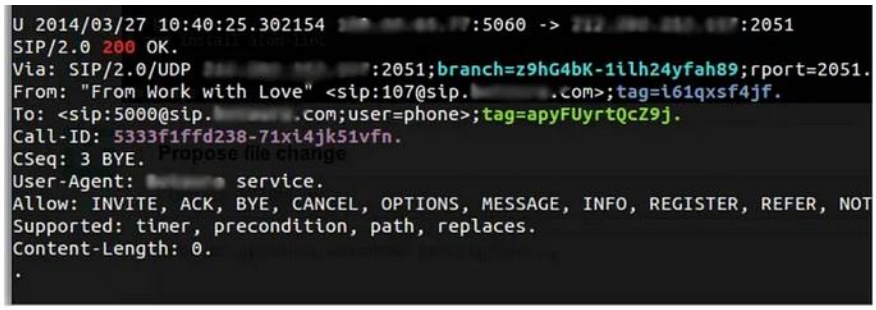
Alguns exemplos de ataques sem encriptação de dados:

- Os ataques por sniffing consistem na captura e descodificação dos pacotes IP, sendo bastante fáceis de executar em redes locais de meio físico partilhado. De notar que as populares redes sem fios são redes de meio partilhado e, portanto, são particularmente sensíveis a este tipo de ataques. Já a vulgarização das tecnologias de rede comutadas torna menos frequentes e menos abrangente este tipo de ataques em redes cabladas. Os objetivos dos ataques por sniffing são, normalmente, a captura de passwords, o acesso à informação confidencial ou a captura de informação que permita outros ataques, como por exemplo, informação sobre procedimentos de autenticação. Para além da facilidade com que estes ataques podem ser realizados, há ainda que ter em atenção que a presença de sniffers numa rede é por vezes difícil de detetar. Essa deteção é feita através de indicadores indiretos da presença de sniffer na rede, como por exemplo, medições de latência e interfaces o via scanning de endereços IP's ou endereços MAC's inválidos. A deteção da existência de sniffers numa dada máquina local pode ser feita por monitorização dos processos ativos, ou por análise dos ficheiros de log (registos internos).
- Uma outra categoria de ataques engloba os ataques por DoS (Denial of Service), que consiste no ataque à disponibilidade dos servidores e dos equipamentos de comunicação com o objetivo de causar a quebra de serviços. Esta categoria abrange ataques por disseminação de vírus, e-mail bombing, ataques a equipamento de rede, ataques a servidores e ataques de DoS distribuídos (DDoS).
- No caso do e-mail bombing, é enviado um grande volume de mensagens para a caixa de entrada ou listas de distribuição alvo, com o objetivo de congestionar os servidores de correio, as caixas de correio dos utilizadores ou os circuitos de acesso, fazendo com que isto leve a subcarregar as partições de e-mail. Possíveis soluções para este tipo de problema passam pela utilização de filtros de e-mail, utilização de mecanismos anti-spam, sistemas de exclusão de endereços de listas, implementação de sistemas de cotas em disco e controlo dos tempos de resposta do servidor e-mail.
- Os ataques por spoofing são relativamente vulgares e consiste na falsificação da identidade de uma máquina, que se faz passar por uma outra, a tentativa de ganhar acesso a recursos, ganhar

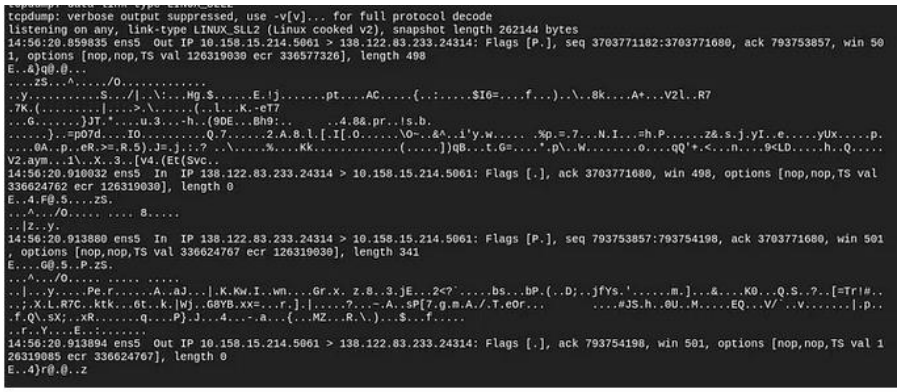
acesso à informação ou provocar DoS. Estes ataques podem dar-se a vários níveis, sendo frequentes ataques de ARP spoofing, IP spoofing, entre outros.

Uma solução bastante interessante é a utilização do SIP TLS, ou seja, ter as informações que vão dentro do protocolo de forma criptografadas!

Vejamos dois casos de servidor Asterisks a funcionar (sem e com encriptação):



Pacote SIP (sem encriptação - dados facilmente interpretados)



Pacote SIP criptografado

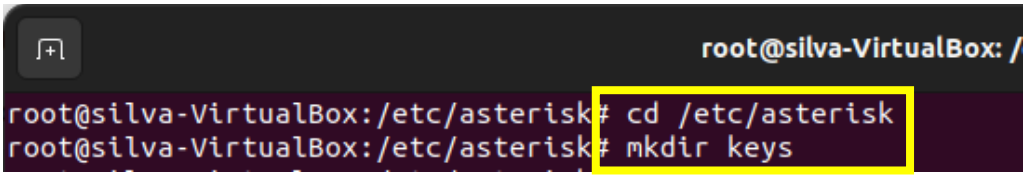
Transport Layer Security (TLS) fornece uma solução genérica para garantir segurança sobre as ligações com o uso de criptografia para as chamadas (mas é aplicado noutros contextos), suportando assim mecanismos de autenticação, integridade e encriptação de sessões de comunicação. É uma maneira prática de impedir que as pessoas que não são do domínio saibam quem estamos a ligar.

Assim sendo, o protocolo TLS assenta em 2 conceitos fundamentais:

- **o conceito de ligação**: é uma associação para par entre 2 entidades da camada de transporte de dados. A cada ligação existem vários parâmetros, como, por exemplo, chaves usadas para autenticação de mensagens e vetores de inicialização utilizados pelo servidor ou cliente para encriptação das mensagens;

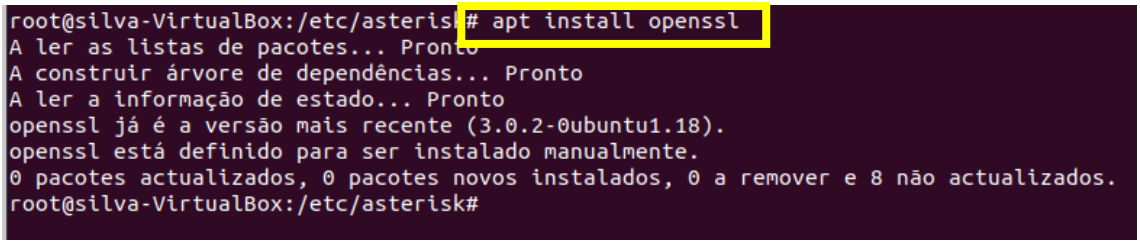
- **o conceito de sessão**: é uma associação entre o cliente e um servidor, que pode comportar múltiplas ligações, onde o conceito de sessão surge para evitar a necessidade de negociação e estabelecimento dos parâmetros de segurança por cada ligação estabelecida (a cada sessão estão associados parâmetros como o identificador de sessão, o certificado utilizado, o método de compressão de dados a utilizar, o algoritmo de autenticação, entre outros);

1 – Na pasta onde está a instalação do Asterisk, temos de criar uma pasta para deixar os certificados de segurança (neste caso os ficheiros que vamos gerar a seguir). Como tal, **aceda ao diretório da instalação** do asterisk (**/etc/asterisk**) e **crie a pasta** (comando **mkdir**), com o nome "**keys**":



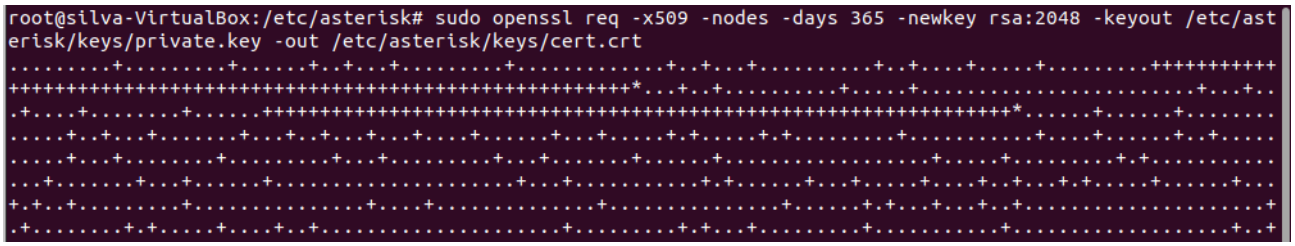
2 – Verificar se tem o pacote OpenSSL. Execute o comando:

apt install openssl



3 – Vamos gerar um novo certificado de segurança com o seguinte comando:

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/asterisk/keys/private.key -out /etc/asterisk/keys /cert.crt



Preencher as informações da geração dos dados do certificado:

```
.....+...+...........+.....+.........+......+.............+.........+..+......+...++++++++
++++++++++++++++++++++++++++++++++++++++
-----
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) [AU]:PT
State or Province Name (full name) [Some-State]:PT
Locality Name (eg, city) []:Viseu
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:teste@teste.pt
```

Vamos verificar se dentro da pasta “keys”, gerou os ficheiros dos passos anteriores:

```
root@silva-VirtualB
root@silva-VirtualBox:/etc/asterisk# cd keys/
root@silva-VirtualBox:/etc/asterisk/keys# ls -l
total 8
-rw-r--r-- 1 root root 1350 out 26 12:13 cert.crt
-rw------- 1 root root 1704 out 26 12:12 private.key
```

No final, vamos dar permissões aos ficheiros (para não haver restrições na aplicação dos mesmos):

```
root@silva-VirtualBox:/etc/asterisk/keys# chmod 777 cert.crt
root@silva-VirtualBox:/etc/asterisk/keys# chmod 777 private.key
```

4 – Vamos adicionar as 4 linhas da ativação do protocolo TLS (ficheiro sip.conf)

Nas configurações iniciais do ficheiro **sip.conf**, deve colocar a implementação da encriptação de dados TLS:

tlsenable=yes

tlsbindaddr=0.0.0.0

tlscertfile=/etc/asterisk/keys/cert.crt

tlsprivatefile=/etc/asterisk/keys/private.key

```
Abrir   sip.co
        /etc/aste
 1 [general]
 2 context=dummy
 3 allowguests=yes
 4 disallow=all
 5 allow=ulaw
 6 callevent=yes
 7 notifyhold=yes
 8 callcounter=yes
 9 tlsenable=yes
10 tlsbindaddr=0.0.0.0
11 tlscertfile=/etc/asterisk/keys/cert.crt
12 tlsprivatekey=/etc/asterisk/keys/private.key
13
14 [7001]
```

Ainda no mesmo ficheiro, temos de **indicar nos utilizadores** a **utilização do tipo de transporte de dados via TLS**:

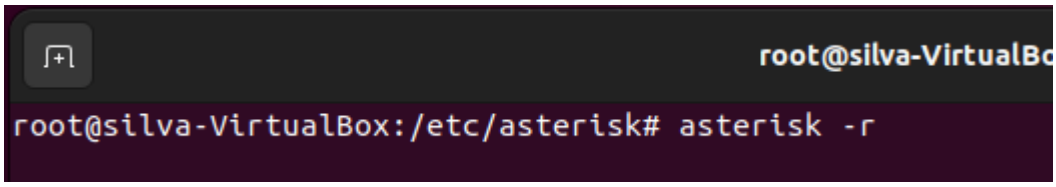
encryption=yes

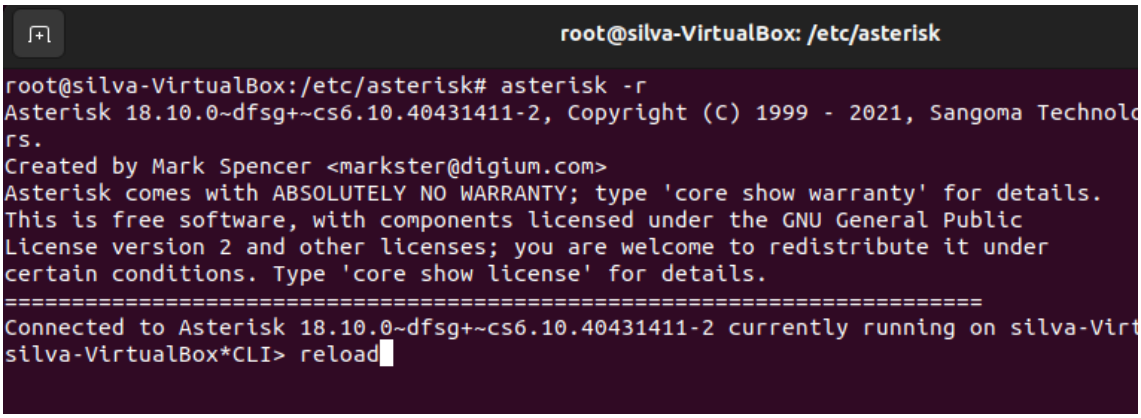
transport=tls

```
14 [7001]
15 type=friend
16 host=dynamic
17 md5secret=85e2444e4e501b56beb0e66f52f37894
18 context=internal
19 encryption=yes
20 transport=tls
```

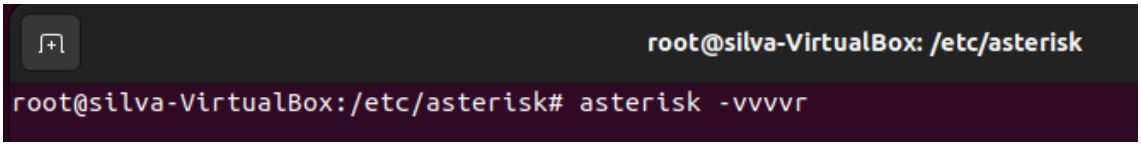
MUITO IMPORTANTE: Faça os mesmos passos para os outros utilizadores (apenas basta colocar as 2 linhas de ativação do serviço)

5 – Atualizar as novas alterações no servidor Asterisk





6 – Correr de novo o servidor Asterisk

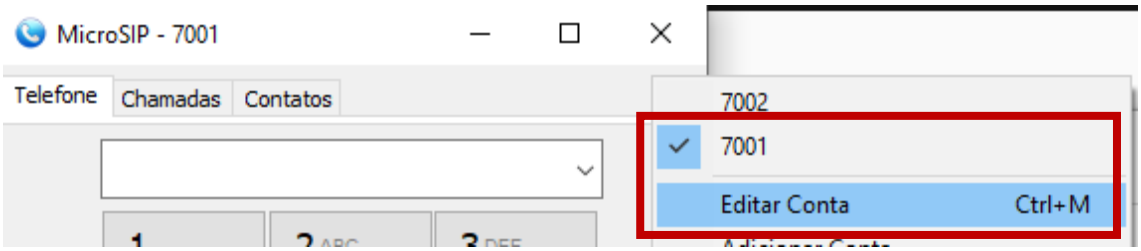


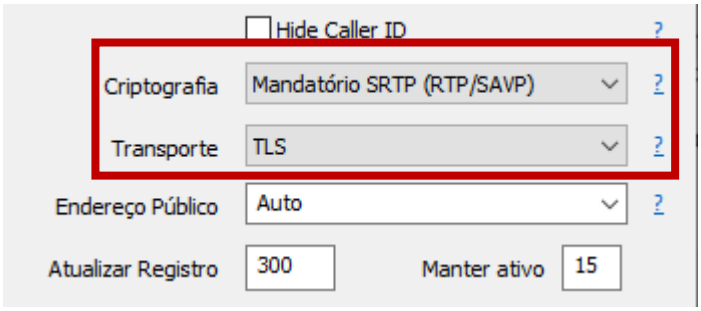
Se testar o seu cliente Voip, agora não consegue sincronizar a sua conta (pois adicionamos os certificados que foram gerados anteriormente) 😊

7 – Configurar os novos dados no software Voip (Cliente)

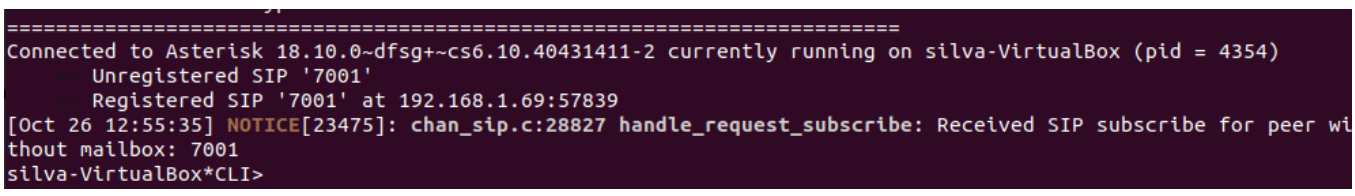
Como tal, temos de configurar os novos dados em causa. Abra o software MicroSip e edite a sua conta. Neste momento, terá de habilitar duas opções importantes para conseguir ligar ao servidor asterisk (pois agora utiliza encriptação e certificado TLS).

Como tal, edite os seguintes campos e coloque os valores:





Grave as novas alterações e veja o registo da ligação na máquina virtual onde está o asterisk:



Nota importante: se reparar no canto inferior da aplicação Voip, agora vai ver um cadeado em cima do telemóvel com a cor verde (pois agora usa certificados de segurança para encriptar a ligação):