

SERVIÇOS DE COMUNICAÇÕES

**RELATÓRIO LABORATORIAL
IMPLEMENTAÇÃO DE SOLUÇÃO IP PBX**

19 de Dezembro de 2014

Carlos Leocádio - ee09313@fe.up.pt

Tiago Ferreira - ee10085@fe.up.pt

Departamento de Engenharia Electrotécnica e de Computadores

Conteúdo

Introdução	2
Esquema da Implementação	3
Funcionalidades Implementadas	4
VM Asterisk A	4
VM Asterisk B	4
Interligação de 2 servidores PBX	5
Criação do túnel VPN	7
Comparativo: SIP vs IAX2	8
Conclusão	9
Referências	10

Introdução

Actualmente a utilização de serviços de voz sobre IP é cada vez mais comum. No entanto a sua utilização em grande escala no âmbito empresarial pode ser complexa, e acarretar custos elevados de aquisição de equipamento, operação e manutenção. Como tal devemos ter em consideração a existência de soluções baseadas em software open-source, que podem ser implementadas recorrendo a hardware comum. Este relatório apresenta a abordagem seguida na implementação de um serviço de VoIP e as suas funcionalidades mais comuns.

Esquema da Implementação

Procedeu-se à criação de duas máquinas virtuais A e B, que executavam a distribuição de AsteriskNow 6.12. Esta distribuição apresenta todos os pacotes necessários à criação de uma solução de comunicações de voz sobre IP (Asterisk, FreePBX GUI, CentoOS).

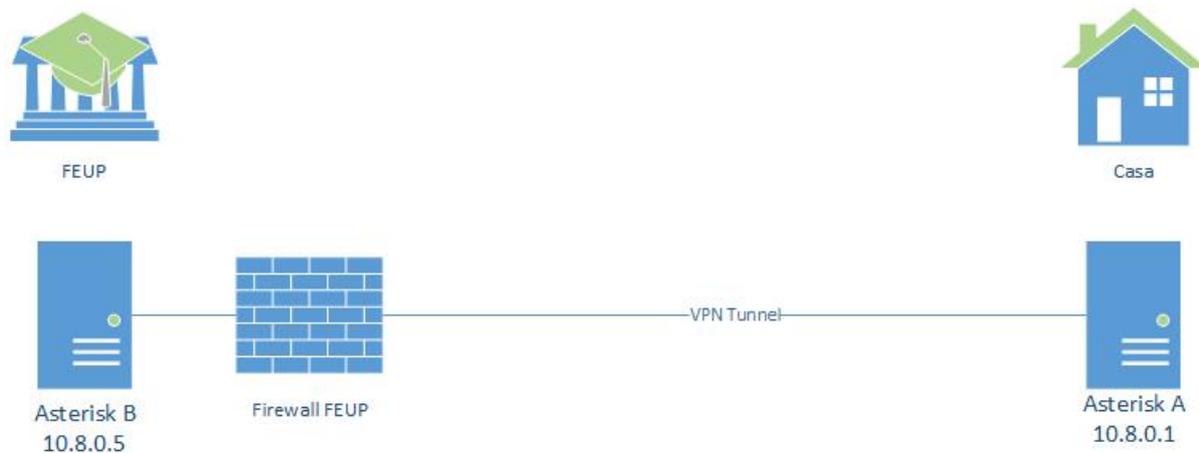


Figura 1: Esquema da implementação

O servidor Asterisk A foi colocado numa DMZ, para evitar problemas de comunicação com o exterior. Os endereços IP indicados são referentes à rede VPN criada, tal como explicado adiante.

Funcionalidades Implementadas

VM Asterisk A

Numa primeira fase procedeu-se à criação de 6 utilizadores com as extensões 100 a 105. Estes utilizadores foram criados recorrendo ao driver CHAN SIP.

A criação de extensões é efectuada através do menu Applications -> Extensions. Apesar de se ter optado por criar extensões do tipo CHAN SIP, é possível criar extensões de outros tipos de devices, por exemplo IAX2 ou PJSIP.

Procedeu-se à activação da funcionalidade de voice mail em todos os utilizadores. Esta funcionalidade fica acessível através da marcação dos números *97 ou *98. Desta forma um utilizador poderia deixar uma mensagem de voz na impossibilidade de estabelecer comunicação com o destinatário.

Efectuou-se também a configuração da funcionalidade de voicemail blasting disponível na extensão 500. Recorrendo a esta funcionalidade qualquer utilizador poderia gravar uma mensagem que seria enviada para o voicemail dos 6 utilizadores existentes.

Acedendo às configurações do SIP através do menu Settings -> Asterisk SIP Settings -> CHAN SIP, procedeu-se à activação do suporte de vídeo, activando todos os codecs disponíveis.

Finalizada esta etapa já era possível efectuar chamadas de voz e vídeo entre as 6 extensões criadas previamente.

Uma funcionalidade muito útil é a implementação de filas de espera para as chamadas. Na elaboração deste trabalho efectuou-se a criação de uma fila de espera disponível através da extensão 200, cujas chamadas seriam atendidas pelas extensões 102 e 103 numa política de “ringall”.

Por fim configurou-se a extensão 300 como extensão de conferência, acessível a todas as 6 extensões existentes.

VM Asterisk B

Neste servidor efectuou-se a criação de 2 utilizadores disponíveis nas extensões 400 e 401, com as mesmas funcionalidades utilizadas na configuração do servidor Asterisk A.

Interligação de 2 servidores PBX

Frequentemente, uma empresa tem escritórios em pontos geográficos distintos. Como tal é necessário que os servidores PBX de cada local sejam interligados, por forma a que as extensões locais sejam contactáveis por utilizadores registados noutra servidor.

A interligação de dois servidores PBX é possível através da criação de um trunk entre eles. Esse trunk pode ser implementado como do tipo SIP, IAX2, DAHDi, entre outros. A criação de trunks está acessível através do menu Connectivity -> Trunks.

Os trunks do tipo SIP sofrem muitas vezes de problemas de mapeamento de portas, causado pelo atravessamento de firewall. Por seu lado, os trunks implementados com IAX2 conseguem evitar estes problemas de correspondência de portas, visto usarem apenas uma porta para toda a comunicação. No entanto apresentam piores características do ponto de vista da capacidade do canal.

Com o objectivo de tornar a implementação mais próxima do que seria uma implementação real, procedeu-se à interligação de dois servidores localizados em redes fisicamente separadas. Um servidor foi implementado na rede da FEUP e outro numa rede doméstica. Tipicamente as redes domésticas apresentam um IP dinâmico, tornado difícil a sua identificação. Para resolver este aspecto, utilizou-se um serviço de DNS dinâmico (no caso No-IP), ficando a rede doméstica disponível através do domínio kali2.ddns.net.

Com isto em mente tornou-se evidente que seria muito difícil contornar as restrições de inbound da firewall da faculdade, o que nos levou a procurar formas de contornar este problema.

A solução final passou pela criação de um túnel VPN entre os 2 servidores, e através do qual era encaminhado o tráfego do trunk IAX2.

A figura 2 apresenta a configuração do trunk no servidor Asterisk A.

O correcto funcionamento do trunk está dependente da configuração das rotas de outbound. A figura 3 apresenta a rota de outbound do servidor Asterisk A, que reencaminha todas as chamadas para a gama de extensões 4XX para o servidor Asterisk B através do trunk.

Outgoing Settings

Trunk Name [?]:

PEER Details [?]:

```
host=10.8.0.5|
username=user
secret=password
type=peer
```

Incoming Settings

USER Context [?]:

USER Details [?]:

```
secret=password
type=user
context=from-trunk
```

Figura 2: Configuração trunk no servidor Asterisk A

Dial Patterns that will use this Route [?]

() + || [/] [?]

() + || [/] [?]

[+ Add More Dial Pattern Fields](#)

Dial patterns wizards [?]:

Export Dialplans as CSV [?]:

Trunk Sequence for Matched Routes [?]

0

Figura 3: Configuração trunk no servidor Asterisk A

Criação do túnel VPN

Para implementar o túnel VPN recorreu-se ao pacote de software OpenVPN. No servidor Asterisk A foi feita a configuração de um servidor VPN, gerando os certificados necessários para o estabelecimento da comunicação. O servidor OpenVPN, quando em execução, cria uma interface de rede virtual, tal como se pode ver na seguinte figura.

```
[root@localhost ~]# ifconfig tun0
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
-00
          inet addr:10.8.0.1  P-t-P:10.8.0.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

Figura 4: Interface virtual de tunneling

A utilização de um túnel VPN para a interligação dos 2 servidores através da internet tem também a vantagem de assegurar a segurança da informação transmitida, resultante da encriptação do canal.

Comparativo: SIP vs IAX2

As principais diferenças entre SIP e IAX são as seguintes:

- **Largura de Banda** - A largura de banda usada pelo IAX é inferior à utilizada pelo SIP, dado que as mensagens em IAX são binárias ao passo que em SIP são mensagens de texto; por outro lado o IAX também procura reduzir o cabeçalho das mensagens, com consequentes diminuições na largura de banda utilizada
- **NAT** - Sinalização e dados em IAX são enviados em conjunto, evitando problemas de NAT, que normalmente ocorrem quando se utiliza SIP. No SIP, a sinalização e os dados são transferidos usando protocolos distintos, resultando muitas vezes em problemas provocados pela NAT/Firewall.
- **Portas utilizadas** - IAX utiliza apenas uma porta (4569) para transferir sinalização e dados, recorrendo para tal ao protocolo UDP. Por outro lado SIP usa uma porta para sinalização (5060) e duas portas RTP para cada conexão de áudio.
- **Fluxo dos dados** - No SIP as mensagens de sinalização atravessam sempre o servidor, mas a troca de mensagens de áudio/vídeo (fluxo RTP) é efectuada directamente entre os terminais, sem intervenção do servidor. Por outro lado, quando se utiliza IAX, todo o tráfego atravessa o servidor, implicando maior largura de banda.

Conclusão

A existência de soluções open-source para a implementação de soluções IP PBX permite que, virtualmente, qualquer empresa ou particular possa implementar o seu próprio servidor PBX.

A utilização destas soluções é vantajosa, pois permite uma escalabilidade futura consoante as necessidades, e possibilita a implementação de serviços para além dos comuns serviços de transferência de voz ou vídeo, sem os custos inerentes das soluções puramente comerciais.

Referências

<http://www.en.voipforo.com/IAX/IAXvsSIP.php>

<https://www.digitalocean.com/community/tutorials/how-to-setup-and-configure-an-openvpn-server-on-centos-6>