Gestão e Segurança de Redes

Relatório da 2ª Parte

Grupo 19:

Heydi Marques 79062

Veniamin Craciun 82028

Teodor Atroshenko 82058

**SSH**

Para a configuração do **SSH** foi preciso gerar uma chave assimetrica no PC do administrador,sendo a sua chave publica partilhada com os servidor que necessita gerir. Foi impedido o acesso aos servidores por **SSH**com o user *root.* Foram também criados scripts a serem usados quando se trata do acesso a uma servidor privado da rede **ContaTudo**. Para aceder ao servidor **FTP** (fileServer)*,* é possível executando os scripts:  
 -**sh /root/scripts/fileServer.sh**

-**sh /root/scripts/adminFileServer.sh**

**HTTPS**

**HTTP**

**DNS**

Para restringir a resolução de nomes para maquinas fora da rede **ContaTudo**

Para garantir a tranferência de zonas de forma segura foi preciso criar uma chave secreta com o comando *dnssec-keygen*, que foi adicionada de seguida adicionada a configuração e indicado que a tranferência de zonas deve usar a secreta.

**FIREWALL e NAT**

**VPN**

Para a configuração do VPN, foi necessário criar certificado da C*ertificate Authority* (**CA**), como também a criação das chaves e certificados do server (dnsHttp) e do cliente (admin). Foi também realizada a configuração dos ficheiros server- e client.conf. Para a configuração do *server* indicou-se a gama endereços (**192.168.1.0/29**) que é disponibilizado pelo VPN, a rede que deve ser acedida por VPN e para *client* ter acesso ao servidor de nomes foi necessário indicar os servidores **DNS** disponíveis e responsáveis pela rede. A configuração do *client* foi mais simples foi só preciso indicar **IP** qual o servidor VPN a usar.

**PROXY WEB**