Gestão e Segurança de Redes

Relatório da 2ª Parte

Grupo 19:

Heydi Marques 79062

Veniamin Craciun 82028

Teodor Atroshenko 82058

**Opções tomadas**

**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**

Para o que o acesso a *clientes.contatudo.gsr* seja por **HTTPS** foi gerado um certificado auto-assinado com *openssl*, adicionada nova configuração para reencaminhar trafico **HTTP** (Port:80) para **HTTPS** (Port:443)e a activação do acesso por **SSL** com o comando *a2enmod ssl.*

**HTTP**

Restringir o acesso ao intranet.contatudo.gsr foi efectuado através das directivas *order, allow* e *deny* que foram adicionadas a configuração do site *intranet* restringindo o acesso ao website com base no **IP**.

**DNS**

Para restringir a resolução de nomes para maquinas fora da rede **ContaTudo**, usamos o *statement allow-recursion*  e uma *acl* apenas para gamas de **IP** presentes dentro da rede.

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

Para o administrador de rede conseguir ver os nome da maquina em vez dos seu **IPs**, foi configurado no router do **ISP** reverse DNS como também indicado quem é reponsável pelas sub-redes e onde se fez a tradução de IP para nome de maquina.

**FIREWALL**

Foram adicionadas regras para evitar o acesso a maquinas do interior a partir do exterior, evitar ataques de spoofing, foi fornecido acesso a internet para maquinas com **IP** publico/visitantes e limitaram-se as portas abertas existentes e deixando apenas abertas as estritamente necessárias para acesso aos serviços oferecidos na organização.

**VPN**

Para a configuração do VPN, foi necessário criar certificado da *Certificate 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 a usar 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**