TÉCNICO LISBOA

# Gestão e Segurança de Redes / Gestão de Redes e Serviços LETI / MEIC-T - 2014/15

Projeto 2

## Objetivo

Este projecto é a continuação do projecto anterior. Será usada a rede construída para o primeiro projecto.

O objectivo deste projecto é aumentar a segurança da rede da XPTO, limitando o seu acesso aos elementos autorizados e recorrendo a serviços seguros. Para tal a XPTO vai necessitar de configurar o serviço de firewall, utilizar SSH, usar HTTPS no acesso à sua página web, restringir o uso do DNS e disponibilizar um serviço de VPN. Também é necessário implementar o serviço de backups.

Para a realização deste projecto, o encaminhamento e o serviço DNS, configurados na entrega anterior, têm de funcionar a 100%. Recorram aos horários de dúvidas se necessário.

## SSH

A XPTO contratou um administrador de rede. Este trabalha remotamente, a partir da Internet. Utiliza o PC de testes ligado à Internet, já existente.

O administrador precisa de ter acesso de super utilizador aos servidores da XPTO. Para tal, criou um utilizador em cada um dos servidores (públicos e privados), ao qual acede com chaves assimétricas. Esse utilizador utiliza o comando *sudo* para executar comandos como root. O servidor SSH deverá impedir o login remoto como root.

## HTTPS

O site clientes.xpto.pt contém informação privadas dos clientes que é necessário salvaguardar de terceiros. Como tal, o primeiro trabalho que foi solicitado ao administrador de rede foi configurar o acesso por HTTPS a este site. Por uma questão de custos, será usado um certificado auto-assinado. O acesso a este site por HTTP deverá resultar no redireccionamento automático para o mesmo site por HTTPS.

## DNS

Os servidores DNS da XPTO servem dois propósitos: resolver nomes globais em nome das máquinas no interior da rede da XPTO; resolver os nomes do domínio xpto.pt para todas as máquinas que o solicitem, independentemente da sua origem.

Garanta que os servidores DNS da XPTO não resolvem pedidos DNS de domínios diferentes dos que servem para máquinas no exterior da XPTO.

## Firewall e NAT

O novo administrador de rede resolveu reduzir os riscos de ataque à rede da XPTO reduzindo os acessos do exterior ao mínimo necessário.

Todas as máquinas existentes no interior da rede da XPTO devem poder aceder à Internet sem restrições. Mesmo às máquinas que usam IPs privados deve ser dada essa possibilidade, recorrendo a NAT (com masquerade).

Do exterior não pode ser possível aceder a nenhuma das máquinas com endereçamento privado. Aos servidores públicos apenas deverá ser possível aceder aos serviço que estas disponibilizam como sua função primária (e.g. HTTP, HTTPS, SMTP, IMAP, DNS).

Também não é possível iniciar uma ligação do exterior para nenhum dos PCs com IP público, embora seja possível iniciar uma ligação destes para o exterior, como referido anteriormente.

## VPN

Com as novas regras de firewall, deixou de ser possível ao novo administrador aceder às máquinas que gere por SSH. Este decidiu assim implementar um serviço de VPN para que possa trabalhar remotamente como se estivesse no interior da XPTO.

As condições ao ligar à VPN devem ser as mesmas como se estivesse no interior da rede, nomeadamente devem ser usados os mesmos servidores de DNS, aceder a todas as máquinas e ter acesso restrito da Internet.

## Backups

O conteúdo do site clientes.xpto.pt é muito valioso. Para evitar a sua perda em caso de falha do servidor web, o administrador configurou um backup periódico

do site para o servidor de backups. Decidiu usar o rsync (para fazer uma cópia fiel, incluindo apagar os ficheiros que já não existem), que é corrido automaticamente de hora a hora, usando o crontab.

## Realização do projecto

Em informática e redes, o que não foi testado raramente funciona. Os grupos devem testar tudo o que fizeram e prepararem-se para mostrar esses testes durante a visualização do projecto.

As várias tarefas a realizar são independentes, podendo ser realizadas em paralelo. Recomenda-se o uso de um sistema de controlo de versões (tipo git).

O projecto deve ser realizado de modo a não ser necessário entregar as imagens dos sistemas de ficheiros das máquinas virtuais (ou seja, os ficheiros *.disk*), já que são ficheiros muito grandes. Para o efeito, as configurações devem ser feitas usando os ficheiros *.startup* e as directorias com os nomes das máquinas virtuais.

## Entrega e relatório

A entrega do projecto é realizada através do fenix até dia 22 de Maio às 17h00. A entrega é feita através do sistema Fénix e inclui um único ficheiro "**zip**" com: um relatório com 2 páginas (em **PDF**) a explicar as opções tomadas (ou seja, aquilo que for feito que não esteja explicitamente indicado neste enunciado, nomeadamente as escolhas efectudas); todos os ficheiros do projecto na pasta "proj" (o "laboratório Netkit" criado).

## Bibliografia


[Apache] Apache HTTP Server Documentation, http://httpd.apache.org/docs/

[GSR] Slides da cadeira

[Netkit] Netkit documentation, http://wiki.netkit.org

[OpenVPN] OpenVPN Howto, https://openvpn.net/index.php/open-source/documentation/howto.html