Ferramentas de monitorização de tráfego

O objetivo deste trabalho é sensibilizar o estudante para as ferramentas de monitorização do tráfego de sistemas e serviços de uma rede, com particular relevância nas ferramentas baseadas na Web, de uso gratuito.

Para tal, propõe-se a utilização de duas ferramentas que disponibilizam numa interface HTML os dados de monitorização provenientes das variáveis de gestão nos equipamentos, no caso da ferramenta *"The Multi Router Traffic Grapher"* (MRTG), ou da análise do tráfego na rede, como no caso da *"Network TOP"* (**ntop**).

O trabalho consiste na utilização do MRTG e do **ntop** para fazer a monitorização de uma rede em produção e em particular dos routers e dos serviços nela disponibilizados. Este protótipo de rede será simulado na bancada de trabalho.

1. Consulte a documentação disponível no site oficial do MRTG e avalie as suas potencialidades. Instale-o num dos servidores da sua bancada, gerando-o a partir do código fonte ou instalando o pacote pré-configurado da distribuição Unix do servidor escolhido.
2. Configure nos servidores disponíveis na sua bancada o protótipo de rede em produção com o seguinte conjunto de serviços: um servidor Web, um servidor FTP/sFTP, um servidor NTP, um servidor de e-mail e um servidor de DNS *cache server*. Apresente o resultado de uma consulta a cada serviço, como demonstração do bom funcionamento.
3. Configure o MRTG para monitorizar o router da sua bancada e em particular a interface de acesso para a rede do laboratório (é recomendável que faça a inicialização da configuração do MRTG usando a ferramenta **cfgmaker**). Apresente os resultados de monitorização durante o maior intervalo de tempo possível.
4. Noutro servidor da bancada instale o **ntop** e configure-o para monitorar os mesmos equipamentos e serviços do ponto 2. Apresente os resultados de monitorização durante o maior intervalo de tempo possível, indicando os sistemas descobertos, os protocolos e a distribuição dos fluxos.
5. Descreva e apresente uma análise comparativa das funcionalidades das duas ferramentas.
6. Como conclusão do trabalho, elabore um relatório com as respostas às perguntas acima e envie-o por e-mail para <joao.neves_at_fe.up.pt>.

Anexos

- Credenciais de acesso ao router

```
Username: root
Password: 8nortel
```

- Comandos Cisco IOS para ativar o serviço SNMP

```
rtr-gnuX#config terminal
rtr-gnuX(config)#snmp-server community public ro
rtr-gnuX(config)#exit
rtr-gnuX#show running-config
```

- Instalação dos pacotes pré-compilados para o Ubuntu

```
#apt-get install ntp ntpdate
#apt-get install bind9 dnsutils
#apt-get install mrtg
#apt-get install ntop
```

Material de Consulta

- https://oss.oetiker.ch/mrtg/
- https://www.ntop.org
- https://www.cisco.com