Tecnologias Avançadas de Redes

Área departamental de Engenharia Electrónica e Telecomunicações e de Computadores (ADEETC)
Instituto Superior de Engenharia de Lisboa (ISEL)

1º Trabalho prático - Listas de Acesso (ACLs) e Network Address Translation (NAT)

Contexto

Pretende-se com este trabalho que os alunos obtenham prática na utilização de listas de acesso (ACLs), concretizadas na utilização da componente Netfilter (incluída no núcleo de sistemas operativos Linux), mas traduzidas para a nomenclatura presente no RouterOS (sistema operativo de equipamentos Mikrotic).

Em simultâneo será explorada a aplicação de ACLs na filtragem de tráfego, aplicação condicional de mecanismos de NAT e de manipulação genética (*mangle*) de campos de datagramas.

Cenário de testes

O cenário de testes deve ser baseado no ambiente de virtualização VirtualBox, neste pretende-se simular a topologia em que uma das máquinas virtuais desempenha o papel de *router* e as restantes (uma ou mais conforme conveniente para os testes) o de clientes numa rede interna.

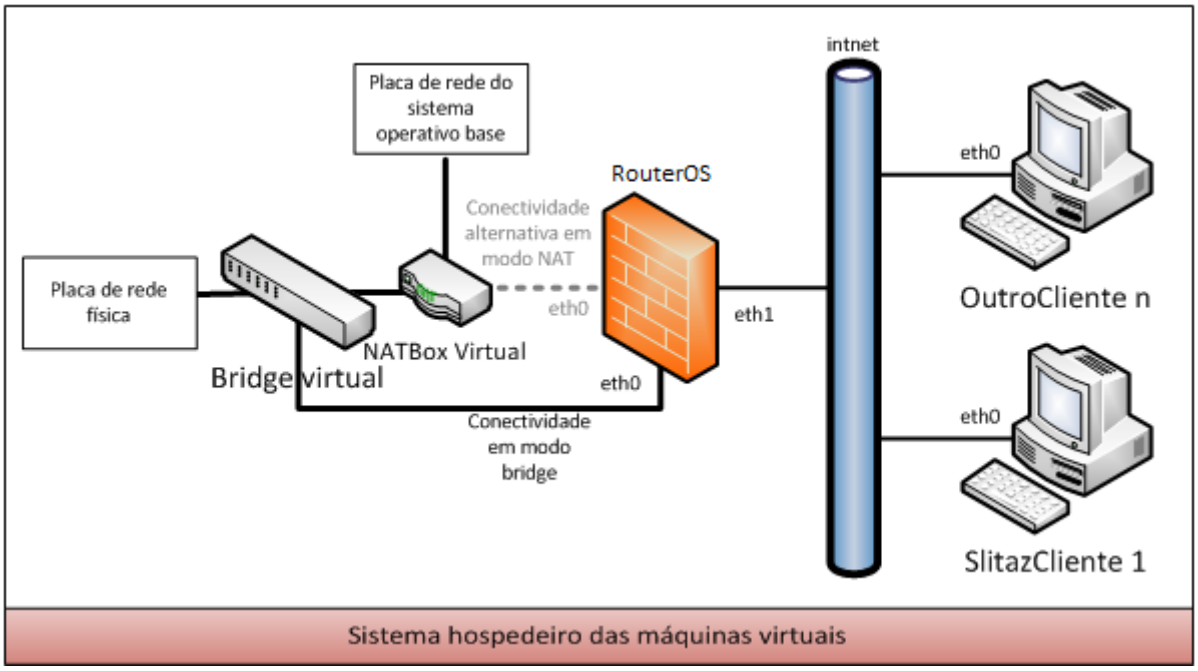
A construção do cenário de testes será baseada em duas máquinas virtuais (VM´s) onde será necessário instalar uma imagem do RouterOS na VM a realizar o papel de *router*. Encontra-se presente na secção de recursos toda a informação necessária para a sua instalação, bem como a sua parametrização. É dada total liberdade aos alunos para escolherem os sistemas operativos a utilizar como máquinas virtuais internas.

Máquina router

A máquina que desempenha o papel de *router* terá duas interfaces virtuais, a **ether1** como exterior que obtém a configuração através do protocolo DHCP sendo a sua conectividade obtida através do ambiente de virtualização por *bridging* (se possível) com a interface física da máquina hospedeira do ambiente virtual ou em alternativa em modo NAT sobre o endereço da própria máquina hospedeira. A interface interna **ether2** terá um endereço fixo da gama 172.16.0.0/24 (recomenda-se o primeiro útil).

Máquina(s) cliente

Nas máquinas que desempenham o papel de clientes internos apenas deve ser realizada a configuração mínima necessária para que esta obtenha conectividade IP, resolução de nomes DNS sob a interface **ether1**, e outros programas/serviços que se considerem convenientes para o teste das regras de firewall aplicadas na VM *router*. Como servidor de DNS deve ser referenciado o IP interno da máquina que desempenha o papel de *router*, posteriormente usando NAT encaminharemos esses pedidos para o servidor conveniente.
Ao nível do sistema de virtualização as interfaces ether2 do *router* e ether1 dos clientes deverão ser associadas à "Internal Network" designada de "intnet" que é um segmento de rede virtual disponibilizado para comunicação entre as máquinas virtuais.



Objetivos

São os seguintes, os objetivos da parametrização da componente firewall do RouterOS a aplicar á máquina virtual que desempenha o papel de *router*/NATBox: (**É obrigatória a apresentação no relatório de todas as regras na nomenclatura de netfilter**)

Internet->Router (destinado a este)

- Todo o tráfego considerado INVALID pelo *conntrack* é negado.
- Todo o tráfego associado a comunicações iniciadas do *router* para o exterior deve ser aceite.
- Todo o tráfego relacionado com comunicações iniciadas do *router* para o exterior deve ser aceite.
- Só é possível estabelecer ligações TCP para os portos 80 (HTTP) e 22 (SSH) do *router*.
- As tentativas de ligação ao porto TCP 25 (SMTP) devem ser registadas, rejeitadas e devolvida uma mensagem TCP/RST.
- Só são aceites 10 mensagens de ICMP Echo-Request por minuto, podendo ocorrer uma rajada inicial de 20 pedidos que também serão aceites.
- É aceite todo o tráfego mínimo necessário para o funcionamento do cliente de DHCP que o router executará para obter a configuração da interface externa (eth0).
- Todo o restante tráfego é negado sem qualquer resposta e gera log, podendo no entanto este log não ser realizado para tráfego que se verifique ocorrer frequentemente e que seja considerado inóculo.

Router->Internet (originado no router), RedeInterna->Router (destinado ao router) e Router->RedeInterna (originado do router)

- São aceites todas as comunicações sem restrições.

Internet->RedeInterna (através do router)

- Todo o tráfego considerado INVALID pelo *conntrack* é negado.
- Todo o tráfego associado a comunicações iniciadas na rede interna deve ser aceite.
- Todo o tráfego relacionado com comunicações iniciadas na rede interna deve ser aceite.
- Todo o tráfego que tenha sido sujeito a NAT após entrar na eth0 deve ser aceite.

- Todo o restante tráfego é negado sem qualquer resposta e gera log, podendo no entanto este log não ser realizado para tráfego que se verifique ocorrer frequentemente e que seja considerado inóculo.

RedeInterna->Internet (através do router)

- As tentativas de ligação ao porto TCP 25 (SMTP) devem ser registadas, rejeitadas e devolvida uma mensagem TCP/RST.
- Deve perder-se (DROP) 1% dos datagramas ICMP Echo-Request
- Todo o tráfego restante deve ser aceite sem restrições.

Na vertente NAT

- As comunicações da rede interna para a Internet devem sofrer NAT reutilizando o endereço da interface externa do *router* de forma automática (MASQUERADE), no entanto os acessos a servidores WEB (80/TCP) e DNS (53/UDP) exteriores não devem ter o porto origem preservado durante o NAT inicial, sendo este sempre aleatório.
- Todos os pedidos DNS (53/UDP) dirigidos a partir da rede interna ao endereço da interface interna do router devem ser redirecionados para o servidor com IP 193.137.220.130 (quando estiver a usar esta regra fora da rede do IPL/ISEL deve usar em vez deste endereço o do servidor DNS do seu operador Internet).
- As tentativas de estabelecimento de ligações SSH para o porto 10022/TCP realizadas a partir da Internet para o IP externo do *router* devem ser mapeadas por NAT para o porto 22/TCP da máquina cliente interna que para teste deste requisito deve estar a correr um servidor SSH.
- As aplicações cliente de FTP a correrem nas máquinas da rede interna deve aceder sem quaisquer problemas no modo passivo e ativo a servidores localizados na Internet.
- As máquinas internas com endereços entre 172.16.0.101 e 172.16.0.254 não sofrem NAT ao tentarem comunicar para a Internet, o seu trafego passa o *router* sem que ocorra NAT.

Alteração genérica de cabeçalhos

De forma a atribuir ao tráfego diferentes filas de espera de transmissão, deve o valor de DSCP dos datagramas gerados no *router* e na rede interna serem alterados da seguinte forma:

- O tráfego destinado a servidores DNS (53/UDP) na Internet deve ter o DSCP = 0x10
- O tráfego destinado à Internet e que tenha como porto origem 53,67 ou 123 UDP deve ter o DSCP = 0x10
- O tráfego das ligações de dados de FTP de ambos os modos deve ter o DSCP = 0x08

As listas de acesso a realizar para o cumprimento dos requisitos acima devem ser o mais eficientes, sintetizadas e seguras possíveis.

Sugestões de algumas formas de verificar o comportamento das listas realizadas

- Por observação de datagramas capturados no Wireshark, quando possível.
- Pelo teste através da instalação de programas/aplicações/ferramentas que usem o protocolo/porto em causa.
- Pela observação da janela do connection tracking do RouterOS.

Sugestões para desenvolvimento

Segue um guia de inicialização rápida do trabalho, para agilizar o processo de instalação da plataforma de testes:

- Download Mikrotic CHR: https://mikrotik.com/download (make sure to download the .OVA).
- Download Virtualbox: https://www.virtualbox.org/wiki/Downloads
- In Virtualbox import the CHR.OVA file.
- Add a 2nd interface in the VM options. Make sure to add the interface to the intnet network.

- Start the VM/*router*. (User: admin Pass: Empty/None).
- Check if ether1 interface has an ip address: ip address print.
- Access the RouterOS with an Web browser – http://<router ip>.
- Give an static ip address to the ether2/Lan interface.
- Explore the available settings … – Give him a name in System->Identity.
- Explore the IP/Firewall settings.
- Download a OS of your choice for the client virtual machine.
- Place the network card in the intnet network.
- Configure a static ip on the network interface with the dns server pointing to ether2 interface ip of RouterOS.

Deve ser entregue até à data do 2º teste o relatório devidamente identificado em formato PDF, bem como a descrição justificada das configurações realizadas, a listagem completa dos ficheiros de configuração alterados, testes realizados, resultados obtidos e demais informação que considere conveniente para a valorização do trabalho efetuado.

Os trabalhos poderão ser realizados por grupos de 2 a 3 alunos.

Recursos para suporte do trabalho

Ambiente de virtualização VirtualBox

- https://www.virtualbox.org/wiki/Downloads

Wireshark

- http://www.wireshark.org/

Página base do projecto Netfilter/IPTables

- http://www.netfilter.org/

Página da Mikrotic e sistema operativo RouterOS

- https://mikrotik.com/download

Slides da UC de TAR e de apoio à instalação de RouterOS

- Na página do Thoth do docente respetivo

NOTA

Caso detete neste enunciado alguma aparente ambiguidade ou falha, se encontrar algo que julgue incorreto agradece-se que alerte o seu docente. Sugere-se a consulta com alguma frequência a página da unidade curricular para verificação da existência de revisões deste enunciado (versão indicada no rodapé).

Os docentes

Pedro Ribeiro – pribeiro@deetc.isel.ipl.pt

João Silva – jsilva@deetc.isel.ipl.pt