

Gestão e Segurança de Redes LETI - 2015/16

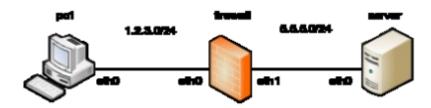
Guia de Laboratório 6

Objectivo

O objectivo do trabalho consiste em aprofundar os conhecimentos sobre *firewalls* usando o pacote *iptables*.

Exercício 1 - iptables

Implemente a topologia abaixo no Netkit com 3 máquinas virtuais.
 Configure a tabela de routing da firewall de modo a que os dois terminais consigam comunicar um com o outro. Teste com o comando ping.



- 2. Execute um servidor *apache2* no servidor e aceda-lhe a partir do PC usando um *browser*.
- 3. Se quiser bloquear o acesso do cliente ao servidor, quais são as *chain* e tabela do *iptables* que deve usar?
- 4. Crie uma regra *iptables* para bloquear o acesso ao porto TCP/80 do servidor. Tente novamente aceder ao servidor e observe como já não é possível.
- 5. Bloqueie as mensagens ICMP tipo 8 (Echo Request) do PC para o servidor. Observe como já não é possível fazer *ping* do PC para o servidor. Observe como ainda é possível fazer *ping* do servidor para o PC.
- 6. Liste as regras da firewall. Apague a segunda.

Exercício 2 - NAT com iptables

1. Realize o "official lab" do Netkit sobre NAT.

Referências

- Netkit, http://wiki.netkit.org/
- Netkit NAT lab, http://wiki.netkit.org/index.php/Labs-Official
- Oskar Andreasson, Iptables Tutorial, version 1.2.2, http://www.frozentux.net/iptables-tutorial/iptables-tutorial.html, 2006
- Frank Wiles, Quick-Tip: Linux NAT in Four Steps using iptables, http://www.revsys.com/writings/quicktips/nat.html
- Slides da cadeira sobre "Firewalls and intrusion detection", 2016.