



**Ciências
ULisboa**

Faculdade
de Ciências
da Universidade
de Lisboa

Segurança e Confiabilidade

2016/2017

iptables

Grupo 005

Autores

Francisco João Guimarães Coimbra de Almeida Araújo, n.º 45701

João Marques de Barros Mendes Leal, n.º 46394

Joana Correia Magalhães Sousa, n.º 47084

Comandos iptables:

```
sudo /sbin/iptables -A INPUT -p icmp --icmp-type 8 -s 10.101.149.0/23 -j ACCEPT
sudo /sbin/iptables -A INPUT -p tcp -d 10.101.149.55 --dport 23456 -j ACCEPT
```

```
sudo /sbin/iptables -A OUTPUT -p icmp --icmp-type 8 -d gcc -j ACCEPT
```

```
sudo /sbin/iptables -A INPUT -p tcp -s 10.101.149.0/23 --sport 22 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
sudo /sbin/iptables -A INPUT -s 10.101.253.11 -p icmp -j ACCEPT
sudo /sbin/iptables -A INPUT -s 10.101.253.12 -p icmp -j ACCEPT
sudo /sbin/iptables -A INPUT -s 10.101.253.13 -p icmp -j ACCEPT
sudo /sbin/iptables -A INPUT -s 10.101.253.14 -p icmp -j ACCEPT
sudo /sbin/iptables -A INPUT -s 10.101.253.15 -p icmp -j ACCEPT
sudo /sbin/iptables -A INPUT -s 10.101.253.16 -p icmp -j ACCEPT
sudo /sbin/iptables -A INPUT -s 10.101.249.63 -p icmp -j ACCEPT
sudo /sbin/iptables -A INPUT -s 10.101.85.6 -p icmp -j ACCEPT
sudo /sbin/iptables -A INPUT -s 10.101.85.138 -p icmp -j ACCEPT
sudo /sbin/iptables -A INPUT -s 10.101.85.18 -p icmp -j ACCEPT
sudo /sbin/iptables -A INPUT -s 10.101.148.1 -p icmp -j ACCEPT
sudo /sbin/iptables -A INPUT -s 10.101.85.134 -p icmp -j ACCEPT
```

```
sudo /sbin/iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
sudo /sbin/iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
sudo /sbin/iptables -P INPUT DROP
sudo /sbin/iptables -P OUTPUT DROP
```

Método de teste e observações

Para testar os comandos iptables utilizámos como máquina servidora a máquina do laboratório 1.3.12 com ip 10.101.149.55.

Em primeiro lugar fizemos ping para o porto 23456 da máquina servidora utilizando a mesma máquina do laboratório que utilizámos para testar o snort e observámos que os ping eram aceites, como devia ser. Também testámos tentando fazer ping através do gcc utilizando o mesmo porto e, tal como previsto, era feito drop desses ping, ou seja, a máquina do gcc não obtinha resposta.

Para testar o ssh fizemos ssh da máquina utilizada para testes anteriormente para a máquina servidora e observámos que tudo funcionou bem.

Depois fizemos testes utilizando o myGit e o myGitServer, sendo o servidor a máquina servidora anteriormente referida, o observámos que todos os pedidos eram aceites, tal como previsto.