

# Redes de Computadores 2 - Firewall

Gustavo Yudi Bientinezi Matsuzake

Universidade Tecnológica Federal do Paraná  
Profº Fabiano Scriptor de Carvalho

*yudi.matsuzake@gmail.com*

<https://github.com/yudi-matsuzake/firewall-apresentacao>

28 de Junho de 2015

# Sumário

## Introdução

O que é?

Onde posso encontrar firewalls?

Software

Hardware

Analogia do castelo

## História

## Tipos de firewall

Filtros de pacote (stateless)

Filtros de estado de conexão (stateful)

Camada de aplicação

## FIM

# Definição

- ▶ Em computação, um firewall é um sistema de segurança de redes de computadores;
- ▶ Note que é um SISTEMA (não apenas software, hardware ou um muro mesmo);
- ▶ SIM, os três podem ser um sistema de firewall em computação (até o muro)!

## É, onde eu posso encontrar esses firewall?

A pergunta que você deve fazer ao sistema que você desconfia ser um firewall é:

"Você faz alguma coisa pra proteger meu sistema de coisas externas?"

**Se a coisa responder "sim", então ele é um firewall!**

# Tudo que protege seu sistema de ameaças externas!

Você não acredita, né? Então toma uns exemplos:

- ▶ Dispositivos de firewall
- ▶ Software desses dispositivos de firewall
- ▶ Programas do seu sistema operacional
- ▶ Firmware ou Sistema operacional do seu roteador/switch
- ▶ O muro do local físico do servidor (por essa você não esperava, né?)
- ▶ O Zé, o segurança que cuida do prédio onde está localizado o seu servidor

## Software

```
R1(config)#
R1(config)#ip access-list resequence OutBoundAccess 10 10
R1(config)#do sh access-list OutBoundAccess
Extended IP access list OutBoundAccess
 10 permit ip 192.168.1.0 0.0.0.255 any
 20 deny tcp 192.168.2.0 0.0.0.127 any eq smtp
 30 deny tcp 192.168.2.0 0.0.0.127 any eq sunrpc
 40 deny tcp 192.168.2.0 0.0.0.127 any eq pop2
 50 deny tcp 192.168.2.0 0.0.0.127 any eq nntp
 60 deny tcp 192.168.2.0 0.0.0.127 any eq ftp
 70 deny tcp 192.168.2.0 0.0.0.127 any eq ftp-data
 80 deny tcp 192.168.2.0 0.0.0.127 any eq telnet
 90 deny tcp 192.168.2.0 0.0.0.127 any eq cmd
100 deny tcp 192.168.2.0 0.0.0.127 any eq irc
110 permit ip 192.168.2.0 0.0.0.255 any
120 permit ip 192.168.3.0 0.0.0.255 any
130 permit ip 192.168.4.0 0.0.0.255 any
140 permit ip 192.168.5.0 0.0.0.255 any
R1(config)#
R1(config)#
```

Figura : Access Control List

## Software

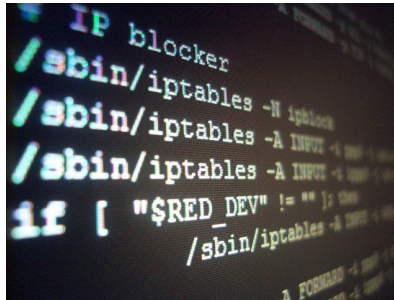


Figura : iptables

## Software

```
avp@ironman:~$ sudo ufw status
Status: active

To Action From
--
80/tcp ALLOW Anywhere
22 ALLOW Anywhere
21/tcp ALLOW Anywhere
3306 ALLOW Anywhere
2267 ALLOW Anywhere
80/tcp ALLOW Anywhere (v6)
22 ALLOW Anywhere (v6)
21/tcp ALLOW Anywhere (v6)
3306 ALLOW Anywhere (v6)
2267 ALLOW Anywhere (v6)

avp@ironman:~$ _
```

Figura : UFW - Uncomplicated Firewall



# Software



Figura : Firewall do Windows

# Hardware



Figura : Netgate

# Hardware



Figura : Dell

## Hardware



Figura : Barracuda

## Hardware



Figura : Asa

## Analogia do Castelo <sup>1</sup>

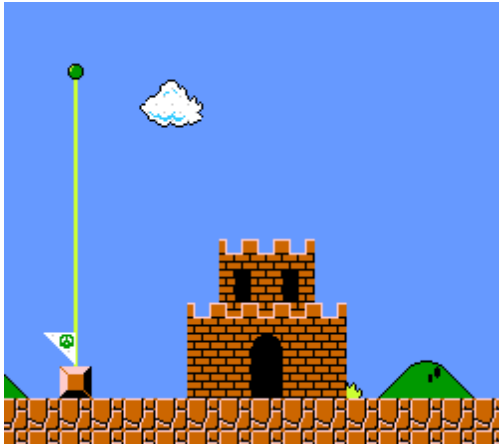


Figura : Castelo sem firewall

O firewall de borda protege a rede de ataques externos

O posso do castelo protege o castelo de ataques externos



Figura : O posso do castelo é o "firewall" do castelo

O firewall pode permitir a entrada/saída da rede e negar a entrada/saída da rede

A ponte do castelo pode ser abaixada para permitir a entrada, e levantada para negar a entrada

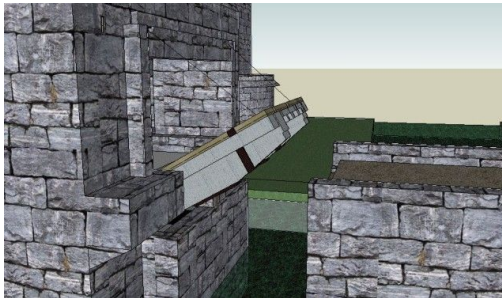


Figura : A ponte pode recusar sua entrada, Mário.



Os cidadãos do império tem suas casas com paredes para uma maior segurança

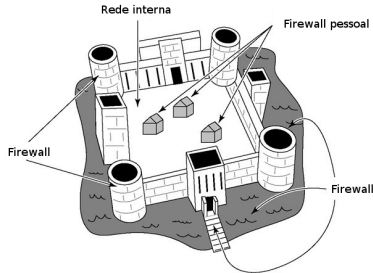


Figura : Analogia do castelo [1]

## References



Tcp/ip.



Talal Alkharobi.  
Firewall, 2007.

Acabou :(

Dúvidas?

## Redes de Computadores 2 - Firewall

Gustavo Yudi Bientinezi Matsuzake

Universidade Tecnológica Federal do Paraná  
Profº Fabiano Scriptor de Carvalho

*yudi.matsuzake@gmail.com*

<https://github.com/yudi-matsuzake/firewall-apresentacao>

28 de Junho de 2015