

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>

1 de Julho de 2015

Sumário

Introdução

O que é?

Onde posso encontrar firewalls?

Software

Hardware

Analogia do castelo

História

Um pouco mais sobre firewalls

Tipos de firewall

Filtros de pacote (stateless)

Filtros de estado de conexão (stateful)

Camada de aplicação

Referências

FIM

Primeira vez que o termo foi usado

- ▶ Usamos a palavra parede (*Wall*) para indicar proteção contra intrusos;
- ▶ A primeira vez que o termo firewall foi utilizado para proteger a estrutura e os habitantes de uma construção do fogo;
- ▶ O maior firewall de todos os tempos;

Definição

- ▶ Em computação, um firewall é um sistema de segurança de redes de computadores;
- ▶ Note que é um SISTEMA (pode ser um 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



```
* IP blocker
/sbin/iptables -N ipblock
/sbin/iptables -A INPUT -i eth0 -j ipblock
/sbin/iptables -A INPUT -i eth1 -j ipblock
if [ "$RED_DEV" != "" ]; then
    /sbin/iptables -A INPUT -i eth0 -j ipblock
    /sbin/iptables -A FORWARD -i eth0 -j ipblock
```

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 ¹

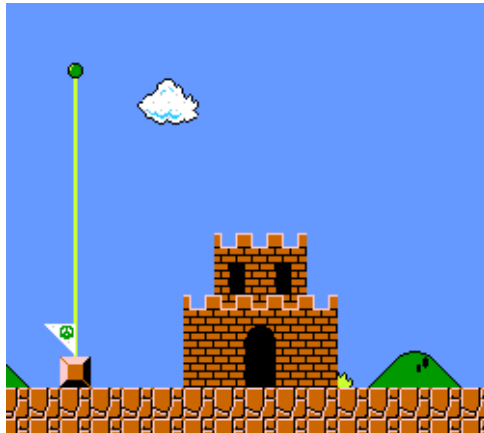


Figura: Castelo sem firewall

O firewall de borda protege a rede de ataques externos

O fosso do castelo protege o castelo de ataques externos



Figura: O fosso 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

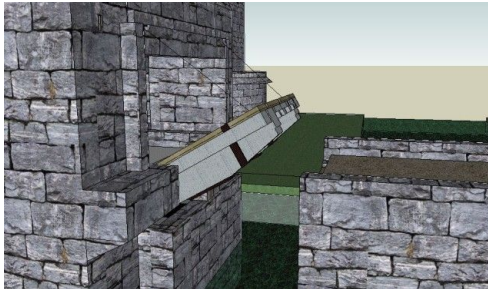


Figura: A ponte pode recusar sua entrada, Mário.

O começo [3]

- ▶ A internet era suportada por uma comunidade pequena;
- ▶ Era formada de usuários que valorizavam a liberdade de compartilhar e colaboração;
- ▶ Em 1988 Clifford Stoll descobriu espiões russos zoando com seu sistema [4];
 - ▶ Criaram uma "cadeia" para o hacker;
 - ▶ Deixaram ele pensar que ele tinha realmente invadido;
 - ▶ Estudaram seus ataques e seus métodos;
 - ▶ Daí tomaram medidas administrativas na rede.
- ▶ Uma curiosidade interessante da história dos firewalls é que seu desenvolvimento foi coincidindo em métodos cada vez mais "altos" nas camadas de protocolos da camada OSI.

O que são firewalls? Pra computero, por favor

- ▶ Firewalls são sistemas no qual reforçam as políticas de segurança uma organização;
- ▶ Utilizam métodos para filtrar o tráfego da rede através do modelo OSI, que é o mais comum;
- ▶ Existem algumas pesquisas para outros métodos;
- ▶ As regras de filtragem do tráfego são chamadas de *policy* (política) [3];

Tipos de firewall

- ▶ Primeira geração: Filtros de pacote (Filtros "*Stateless*");
- ▶ Segunda geração: Filtros "*Stateful*";
- ▶ Terceira geração: Camada de aplicação.

Funcionamento

- ▶ Seu funcionamento é baseado na filtragem de pacotes; (ah, vá!)
- ▶ Seu funcionamento é simples:
 - ▶ Se o pacote casar com as políticas do firewall:
 - ▶ O pacote entra na rede na maior tranquilidade;
 - ▶ Se o pacote não casar com as políticas do firewall:
 - ▶ O pacote é descartado;

Políticas

- ▶ Esse tipo de firewall só verifica a informação do pacote em si;
- ▶ i.e. o firewall não guarda a informação do status da conexão;
- ▶ Geralmente atributos verificados são:
 - ▶ IP de origem e IP de destino
 - ▶ O protocolo (UDP e TCP)
 - ▶ A porta

Modelo OSI

- ▶ O firewall stateless verifica informações das camadas física, enlace, rede e um pouquinho da camada de transporte;

Exemplos

- ▶ ACL - *Access Control List*
- ▶ iptables ²;

²O iptables por si só não é um firewall stateful. Mas o iptables se torna uma ferramenta muito fácil de se *scriptar* um firewall stateful

Funcionamento

- ▶ São chamados de Firewalls da Próxima Geração (NGFW⁴);
- ▶ Trabalham na camada de aplicação e "entendem" como os protocolos dessa camada funcionam (e.g FTP, DNS, HTTP);
- ▶ Inspecionam profundamente os pacotes e seções DPI⁵;

⁴Next-generation Firewall

⁵Tradução livre de *deep packet inspection*

Funcionalidades extendidas

As três funcionalidades que DEVEM ter em um NGFW por causa do DPI e não tem em um stateful firewall é:

- i Sistema de Prevenção de Intrusão (IPS⁶);
- ii Integração a Identificação do Usuário (UII⁷);
- iii Firewall de Aplicação Web (WAF⁸).

⁶Intrusion Prevention System

⁷User Identity Integration

⁸Web Application Firewall

Referências



Tcp/ip.

<http://what-when-how.com/>.



Talal Alkharobi.

Firewall, 2007.



Kenneth Ingham and Stephanie Forrest.

A history and survey of network firewalls.



Clifford Stoll.

Stalking the wily hacker.

Communication of the ACM, 1988.

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>

1 de Julho de 2015