INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Segurança de Rede
Aula 07: Utilizando o Firewal

Muitas empresas têm grandes quantidades de informações confidenciais, segredos comerciais, planos de desenvolvimento de produtos, estratégias de marketing, análises financeiras e etc. A revelação dessas informações para um concorrente poderia ter terríveis consequências. No entanto, estas empresas precisam ter acesso a Internet. E agora?

Em consequência disso, foi criado um dispositivo que centraliza a entrada e a saída de dados da empresa, ou seja, quando o tráfego que entra/sai de uma rede é registrado, descartado e/ou retransmitido. A entidade que faz isso é conhecida como *firewall*.

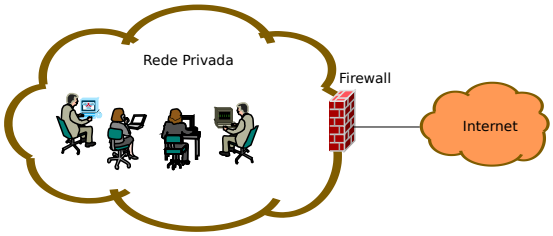

Figura 1: Localização de um *firewall* entre a rede administrada e o mundo exterior

O *firewall* é uma combinação de *hardware* e *software* que isola a rede interna de uma organização da Internet, permitindo que alguns pacotes passem e bloqueando outros.

Netfilter

O netfilter é um módulo que fornece ao sistema operacional Linux as funções de *firewall*, NAT e log de utilização de rede de computadores. Para administrar e inspecionar as regras do netfilter é utilizado uma ferramenta chamada iptables. Esta ferramenta esta presente em todas as distribuições Linux atuais.

As principais funções do iptables são:

- Listar as regras de filtragem dos pacotes;
- Adicionar, remover ou modificar as regras de filtragem dos pacotes;
- Listar, apagar por regras os contadores das regras de filtragem dos pacotes.

Há muitas ferramentas disponíveis para ajudá-lo a construir um *firewall* com GUI (Interfaces Gráficas), por exemplo, o Firestarter e o fwbuilder. Na aula de hoje utilizaremos apenas o iptables.

O *firewall* funciona mediante tabelas e regras pré-estabelecidas. São definidas tabelas. Cada tabela contém um número de *chains*. As *chains* são as situações possíveis (por exemplo, entrada, saída, retransmissão). Cada *chain* contém uma lista de regras que irão determinar como um pacote deverá ser tratado (por exemplo, aceito e rejeitado).

No Linux as tabelas são:

- *Filter*: tabela padrão. Nesta tabela estarão as regras de filtragem e controle dos pacotes. As *chains* da tabela *Filter* são:
  - *INPUT*: regras responsáveis pelo controle das conexão que chegam com destino à rede interna;
  - *OUTPUT*: regras responsáveis pelo controle das conexões que saem (são gerados) da rede interna;
  - *FORWARD*: regras responsáveis pelo controle das conexões que são redirecionadas pela rede interna (pacote que atravessa o *firewall*, oriundo de uma máquina e direcionado a outra);
- NAT: tabela que contém regras que irão modificar conexões. Regras que gerarão outras conexões através de *masquerading*, *source* nat, *destination* nat, *port forwarding*. As regras contidas nesta tabela serão verificadas antes da tabela *filter*.
  - *PREROUTING*: consulta os dados que deverão ser modificados antes de serem enviados para a *chain*.
  - *OUTPUT*: consulta os dados gerados localmente e que necessitam ser modificados antes de serem roteados. Este *chain* somente é consultado por conexões que se originam pela interfaces da máquina *firewall*;
  - *POSTROUTING*: verificando os dados que precisam ser modificados após as verificações das regras.
- *Mangle*: esta tabela é utilizada para modificações especiais no cabeçalho dos pacotes. As regras contidas nas *chains* desta tabela serão verificadas antes das regras de outras tabelas. Como exemplo de utilização de uma regra na tabela mangle seria a alteração a alteração do TOS (*Type of Service*) do pacote.

- Raw: utilizado para implementação de rastreamento de conexões;
- Security: utilizada para controle de segurança de acesso.

Regras são comando passados ao iptables para configurá-lo para o tratamento dos pacotes. Por exemplo, Liberá-los, bloqueá-los ou registrar log da sua passagem. O iptables nos permite criar regras complexas, com várias condicionais para tratamento dos pacotes.

As regras do iptables, geralmente, são compostas assim:

```
sudo iptables [tabela] [chain] [opção]
-j [ação]
```

As opções divididas em:

-P : define uma regra padrão;

-A : acrescenta uma nova regra às existentes;

-D : apaga uma regra;

-L : lista as regras existentes;

-F : apaga todas as regras;

-I : insere uma nova regra;

-h : mostra a ajuda;

-R : substitui uma regra;

-C : chega as regras existentes;

-Z : zera uma regra especifica;

-N : cria uma nova regra com um nome;

-X : exclui uma regra específica pelo seu nome.

As principais ações são:

ACCEPT : aceitar, permite a passagem do pacote.

DROP : abandonar, não permite a passagem do pacote, descartando-o. Não avisa a origem sobre o ocorrido.

REJECT : igual ao *DROP*, mas avisa a origem sobre o ocorrido (envia pacote icmp *unreachable*).

LOG : cria um log referente à regra, em "/var/log/messages".

Exemplos de Regras

Vejamos alguns exemplos de regras:

- Para verificar as regras existentes, pode utilizar o comando:

```
sudo iptables -L
```

- Adicionar a tabela *filter*, na *chain INPUT* a informação que os dados que entrarem na rede na porta 80 (http) serão bloqueados.

```
  iptables -A INPUT -p tcp --dport 80
-j DROP
```

- Adicionar a tabela *filter*, na *chain INPUT* a informação para liberar acesso a porta 53 (DNS)

```
  iptables -A INPUT -p udp --dport 53
-j ACCEPT
```

- Liberando acesso acesso de uma determinada rede (192.168.5.0/24) ao servidor de email (pop3 e smtp).

```
  iptables -A INPUT -p tcp -m multiport
--dport 25,110 -s 192.168.5.0/24
-j ACCEPT
```

- Utilizando a tabela nat para realizar um redirecionamento da porta 80 (http) para a porta 3128.

```
  iptables -t nat -A PREROUTING -p tcp
--dport 80 -j REDIRECT --to-port 3128
```

- Definindo que a conexão que for proveniente do *host* 200.200.200.200 e que esteja sendo originada na porta 25 (smtp) seja aceita.

```
  iptables -A INPUTs 200.200.200.200
-p tcp --sport 25 -j ACCEPT
```

- Nesta regra definimos que todas as conexões com destino a portas altas (de 1024 até 65535) sejam bloqueadas. Caso não seja definido a porta de inicial (:1024) ele assumirá como porta inicial a 0, e caso não seja definido a porta final (1024:) será assumido como porta final a 65535.

```
  iptables -A INPUT -p tcp --dport
1024:65535 -j DROP
```

- Todos os pacotes oriundos de qualquer sub-rede e destinados a qualquer sub-rede deverão ser aceitos.

```
  iptables -A FORWARD -j ACCEPT
```

- Os pacotes oriundos da sub-rede 10.0.0.0/8 e destinados ao *host* `portal.ifrn.edu.br` deverão ser descartados. Deverá ser enviado um ICMP avisando à origem.

```
  iptables -A FORWARD -s 10.0.0.0/8 -d
portal.ifrn.edu.br -j REJECT
```

- Os pacotes destinados oriundo do *host* `portal.ifrn.edu.br` deverão ser descartados.

```
iptables -A FORWARD -s portal.ifrn.edu.br
-j DROP
```

- Caso tenha uma máquina suspeita com esta regra, todo o tráfego de pacotes TCP oriundos da porta 80 do *host* 10.0.0.5 e destinados a qualquer lugar deverá ser gravado em log. No caso, "/var/log/messages".

```
iptables -A FORWARD -s 10.0.0.5 -p tcp
--sport 80 -j LOG
```

- Regra para bloquear uma máquina de acordo com o seu endereço MAC.

```
iptables -A INPUT -m mac --mac-source
XX:XX:XX:XX:XX:XX -j DROP
```

- Regra para limpar as regras do firewal.

```
iptables -F
```

- Regra bloquear o site https://www.facebook.com.

```
iptables -A FORWARD -p tcp -d www.facebook.com
--dport 443 -j DROP
```

- Regra bloquear o site https://www.facebook.com pelo IP (157.240.12.35).

```
iptables -A FORWARD -p tcp -d 157.240.12.35
--dport 443 -j DROP
```

As regras são processadas na ordem em que aparecem. Deste modo, se houver conflito entre regras, sempre valerá a primeira. Assim, entre as regras:

```
iptables -A FORWARD -p icmp -j DROP
iptables -A FORWARD -p icmp -j ACCEPT
```

Valerá a primeira (DROP).

Exercício

1. Pesquisar e implemente um controle sobre os serviços P2P, impedindo o uso desse recurso na sua Intranet.

2. Mostre as regras necessárias para Configurar de modo a bloquear as conexões ICMP, TELNET e FTP de entrada.

3. Permitir as conexões ao serviço SSH de seu servidor e bloquear as demais conexões da sua rede interna.

4. Descreve uma regra que bloquei o site `www.4share.com` para um IP (192.168.0.134) da sua rede.

5. Qual a regra para um computador (192.168.0.12) da rede interna possa se comunicar via RDESKTOP (porta 3389).