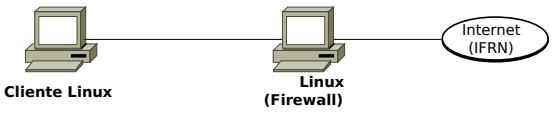
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Segurança de Rede
Prática 11: Firewall (Netfilter/Iptables)

Olá turma, todos nós temos grandes quantidades de informações confidenciais e não gostaríamos que estas informações fossem acessadas por outras pessoas não autorizadas. Agora imagine quantas informações confidenciais as empresas não teriam... e quanto as revelação dessas informações para um concorrente poderia ter terríveis consequências. Em consequência disso, foi criado um dispositivo, chamado de firewall. Iremos estudar ele hoje. Vamos lá??

Configurando o Ambiente

Para estudarmos estes conceitos e ferramenta iremos utilizar duas máquinas virtuais. Uma máquina Ubuntu Linux Firewall (com duas placas de rede, nas respectivas redes NAT e rede interna) e outra máquina com Ubuntu Linux Cliente (com uma placa de rede na rede interna) para testar e implementar o firewall, respectivamente.

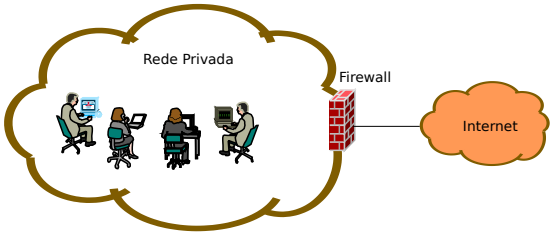


Faça as configurações de rede necessárias para ter conexão entre o Firewall e o cliente Linux.

O netfilter já vem instalado por padrão na distribuição Ubuntu Linux. Na sequência iremos aprender a utiliza-las.

Firewall

Um firewall consiste em uma técnica de segurança de redes bastante efetiva. O seu nome vem das portas corta-fogo (firewalls) utilizadas em edifícios para conter o fogo de um possível incêndio, de modo que ele não se espalhe para o resto do prédio. Pode ser definido como um componente ou conjunto de componentes que restringem acesso entre uma rede protegida e a internet.



Na prática, podemos pensar num firewall como uma forma de limitar a exposição da sua rede à internet, mantendo suas funcionalidades para os usuários. Em outras palavras o firewall tem a função de:

- Centralizar a entrada e a saída de dados da rede;
- Isolar a rede interna da rede externa (Internet), permitindo que alguns pacotes passem e bloqueando outros;
- Impedir que os atacantes consigam chegar em suas defesas mais internas.

As principais tipos de firewall são:

- Filtros de pacotes: é capaz de decidir sobre a passagem ou não de um pacote, de acordo com as informações encontradas no cabeçalho IP, TCP e UDP.
- Filtros de pacote dinâmicos: tem as funcionaliades do filtro de pacotes comum, porém mantém informações sobre o estado das conexões TCP e permite automaticamente todos os pacotes relacionados, de modo que o administrador necessita apenas especificar a regra do primeiro pacote e indicar que os pacotes relacionados serão automaticamente aceitos.
- Servidores proxy: tomam decisões de filtragem no nível de aplicação, onde para cada aplicação há um proxy diferente (ex.: proxy HTTP e proxy FTP).

Existem diversas soluções desenvolvidas sob o critério de licença de software livre que implementam o firewall em redes TCP-IP, por exemplo, Netfilter (Iptables), para Linux; Ipfilter (IPF) e IP Firewall (IPFW), para FreeBSD; Packet Filter (PF), para OpenBSD, e FreeBSD. Na aula de hoje iremos conhecer, implementar e testar o Netfilter.

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 características do iptables são:

- Permitem filtro de pacotes dinâmico.
- Realizam tradução de endereço e portas. O Netfilter denomina de NAT a tradução de endereço IP e de NAPT a tradução de portas TCP e UDP;
- Permite a manipulação de pacotes da pilha TCP/IP;
- Grande número de softwares adicionais (plugins) e módulos mantidos no repositório do Netfilter;
- Desenvolvido para ser flexível e extensível.

Uma virtude do Netfilter é suportar módulos, permitindo implementações das mais simples às mais sofisticadas.

Comandos do Iptables/Netfilter

Por exemplo, vamos imaginar que estamos querendo definir uma regra de filtragem que irá bloquear todos os pacotes provenientes da estação A (endereço IP 192.168.1.1) para o servidor B (endereço IP 192.168.1.2), na porta 110, utilizando o protocolo de transporte TCP. Relembrando os conceitos de TCP/IP, quando iniciamos uma conexão TCP, o remetente escolhe uma porta de origem que não esteja em uso, a partir da porta 1024.

Sendo assim, podemos definir a seguinte regra:

```
Descartar se IP_ORIGEM=192.168.1.1,
 IP_DESTINO=192.168.1.2,
 PORTA_ORIGEM >= 1024 e
 PORTA_DESTINO = 143.
```

Agora iremos aprender como realizar estes filtros no Netfilter. Para compreender a sintaxe do Netfilter, precisamos inicialmente conhecer o significado dos termos e expressões de **ação** sobre um pacote, são eles:

- Drop: o pacote é descartado e nenhuma outra ação é realizada; o pacote simplesmente desaparece.
- Reject: o pacote é descartado e uma mensagem é enviada para o host origem informando seu descarte.
- Accept: o pacote é aceito e encaminhado.
- LOG: registrar em registro a passagem da informação pelo firewall;
- MASQUERADE: utilizado para realização do NAT, significa que o firewall deverá mapeamr o endereço IP de origem do pacote para o endereço IP da interface da qual o pacote está saindo.

Com relação ao fluxo do pacote (chamado de ***chain***) no firewall, o mesmo é classificado em:

- INPUT: utilizada quando os pacotes têm como endereço IP de destino o próprio endereço do firewall.
- OUTPUT: utilizada quando o pacote é originado pelo firewall e sai por alguma interface de rede.
- FORWARD: utilizada quando um pacote atravessa o firewall, não tendo como destino o próprio firewall.
- PREROUTING: o pacote deverá ser tratado no momento em que chega à máquina.
- POSTROUTING: o pacote deverá ser analisado na saida do firewall e não sofrerão nenhum outro tipo de processamento pelo host.

Normalmente utilizamos INPUT e OUTPUT para proteger o próprio firewall, o FORWARD para proteger quem estiver na rede protegida pelo firewall, e PREROUTING e POSTROUTING utilizamos para fazermos manipulação e trocar campos em cabeçalhos de pacotes que passam pelo firewall.

As principais **tabelas** do Iptables são:

- Nat: utilizada para manipulação de tradução de endereços IP. Os pacotes podem ter os endereços de origem, destino, porta de origem e de destino alterados de acordo com o especificado na regra.
- Filter: utilizada exclusivamente para filtros de pacotes.

Agora entendido alguns conceitos, iremos cnhecer as regras do iptables, que são da seguinte forma:

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

Por exemplo, para listar as regras existentes utiliza-se a opção -L:

```
iptables -L
```

Para especificar uma tabela usada pelo Iptables utiliza-se a opção -t. Se não for especificada, o padrão é filter. Por exemplo:

```
iptables -t nat -L
```

Para apagar todas as regras aplicadas em uma tabela utilizamos a opção -F. Podemos utilizar apagando a tabela nat, com o comando:

```
iptables -t nat -F
```

O conjunto completo de comandos pode ser visto na *man page* do Iptables, acessível através do comando:

```
man iptables
```

Mas na aula de hoje iremos utilizar alguns comandos mais utilizados.

Compartilhamento de Internet

Compartilhamento de Conexão de Internet permite que um computador (chamado de Gateway) compartilhe sua conexão com os demais computadores da rede interna. O computador gateway é conectado a Internet utilizando duas placas de rede, uma para a rede externa (Internet) e outra para a rede interna. No nosso caso será o Ubuntu Linux Firewall.

Para realizar o compartilhamento de conexão no Linux é realizado pelo iptables. Para ativar o compartilhamento, precisamos carregar o módulo, ativar o roteamento de pacotes e inserir a regra de NAT no firewall usando os seguintes comandos (como usuário root):

```
echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -t nat -A POSTROUTING
 -o enp0s3 -j MASQUERADE
```

O "enp0s3" indica a placa de rede do Gateway que está a conexão com a Internet. Na sequência, os clientes da rede precisarão ser configurados para usar o endereço IP do servidor Linux como *gateway*.

Através do NAT Dinâmico é possível determinarmos que, de forma automática, ocorrá a tradução dos endereços IP de uma rede para um único endereço IP (do servidor) tanto na saída da rede quando no retorno a rede. Desta forma, todos os pacotes que saem da minha interface enp0s3 deverão receber o endereço IP do firewall e as respostas receberem o IP original e serem encaminhadas.

Testando Regras

Utilizando a máquina Firewall e o cliente Linux iremos testar algumas regras de utilização do Iptables, além do compartilhamento de conexão já realizado.

Bloqueando ping

Faça um ping do seu Linux para o Firewall, depois adicione a seguinte regra:

```
iptables -A INPUT -p icmp -j DROP
```

a opção -A significa acrescentar no final da tabela INPUT uma regra para descartar (DROP) mensagem de ICMP (utilizada pelo ping). Deste modo, o servidor não responderá a requisições de ping.

Para testar, sem apagar o comando anterior, faça:

```
iptables -A INPUT -p icmp -j ACCEPT
```

Agora estamos pedindo para aceitar o protocolo ICMP, mas o que ocorreu? O servidor respondeu ao ping?

As regras são processadas na ordem em que aparecem. Deste modo, se houver conflito entre regras, sempre valerá a primeira. Assim, entre as regras acimas valerá a primeira (DROP) e sequer chega a encontrar a segunda regra.

Agora iremos apagar a regra e testar.

```
iptables -F
```

Observe agora que o ping voltará a responder. A regra padrão é para aceitar o protocolo ICMP.

Bloqueando porta

Utilizando o Netcat no Ubuntu Firewall abra a porta 8080 e no cliente Linux acesse (também com o Netcat) a respectiva porta do da máquina Firewall.

```
netcat -lvp 8080 (no servidor)

netcat 192.168.0.1 8080 (no cliente)
```

Agora adicione a regra ao final da tabela Filter para descartar segmentos TCP na porta de destino 8080, da seguinte forma:

```
iptables -A INPUT -p tcp --dport 8080
 -j DROP
```

Agora com o Netcat tente acessar a porta da máquina Firewall. O que ocorreu?

Redirecionamento de portas

Podemos utilizar a tabela nat para realizar um redirecionamento de portas TCP e UDP. Por exemplo, podemos trocar os segmentos TCP da porta 3128 para a porta 8080. Este recurso se faz necessário quando alguns serviços não utilizam portas padrões.

```
iptables -t nat -A PREROUTING -p tcp
--dport 3128 -j REDIRECT --to-port 8080
```

Para testarmos utilize o Netcat da seguinte forma:

```
netcat -lvp 8080 (no servidor)

netcat -lvp 3128 (no cliente)
```

Bloqueio de sites

No Linux cliente acesse o site `www.ifrn.edu.br`. O site deverá aparecer normalmente, caso ocorra algo diferente, observe as suas configurações de rede e o compartilhamento de internet.

Agora adicione uma regra na tabela FORWARD para não permitir que todos os pacotes oriundo do *host* `www.ifrn.edu.br` entrem na rede interna, através do comando:

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

Observe que agora o site para de responder. Neste caso, ocorrerá a solicitação que chegará até o site o IFRN. Entretanto a resposta que será bloqueada.

Podemos bloquear já na saida da rede através do comando:

```
iptables -F

iptables -A FORWARD
 -d portal.ifrn.edu.br
 -j REJECT
```

outra diferença é que agora estamos descartando e enviando um pacote ICMP avisando o descarte à origem do pacote (com a ação REJECT).

Gravando registros

Podemos utilizar o firewall para registrar em logs a passagem de determinados pacotes. Por exemplo podemos criar uma regra na tabela FORWARD para gravado em log todos os segmentos TCP na porta encaminhados para o site www.instagram.com. Esta regra é utilizada quando existe uma máquina suspeita e queremos armazenar as suas informações.

```
iptables -A FORWARD
 -d www.instagram.com
 -j LOG
```

Agora utilizando o navegador acesse a página do instagram. Depois observe o registro no log. No ubuntu o arquivo de log está localizado em /var/log/syslog.

Atividade

1. Pesquise e escreva os comandos iptables que realizam as seguintes requisições:

- Permitir conexões TCP (ida e volta) para envio de correio eletrônico para um servidor SMTP (porta 25).
- Bloquear conexões UDP para o servidor DNS (porta 53).
- Permitir que um computador na rede interna possa se comunicar via RDESKTOP com o servidor (porta 3389).

2. Crie o ambiente descrito na aula e compartilhe a conexão com a Internet do seu servidor/firewall. Depois teste os comandos que você respondeu na questão anterior usando o Netcat (visto na aula prática passada) para abrir as portas e testar as conexões.