Elaboração de Script de Firewall de Fácil administração

Marcos Monteiro

http://www.marcosmonteiro.com.br
contato@marcosmonteiro.com.br

IPTables

- O iptables é um firewall em NÍVEL DE PACOTES e funciona baseado no endereço/porta de origem/destino do pacote, prioridade, etc. Ele funciona através da COMPARAÇÃO DE REGRAS para saber se um pacote tem ou não permissão para passar.
- Kernel do Linux 2.4 - firewall iptables (também chamado de netfilter)
- Tem a vantagem de ser modularizável, funções podem ser adicionadas ao firewall ampliando as possibilidades oferecidas.

Marcos Monteiro

IPTables

Também pode ser usado para:

- Modificar e monitorar o tráfego da rede,
- Fazer NAT (masquerading, source nat, destination nat),
- Redirecionamento de pacotes,
- Marcação de pacotes,
- Modificar a prioridade de pacotes que chegam/saem do sistema,
- Contagem de bytes,
- Dividir tráfego entre máquinas,
- Criar proteções anti-spoofing, contra syn flood, DoS, etc.
- O tráfego vindo de máquinas desconhecidas da rede pode também ser bloqueado/registrado através do uso de simples regras.

IPTables - Características

- Especificação de portas/endereço de origem/destino
- Suporte a protocolos TCP/UDP/ICMP (incluindo tipos de mensagens icmp)
- Suporte a interfaces de origem/destino de pacotes
- Manipula serviços de proxy na rede
- Tratamento de tráfego dividido em chains (para melhor controle do tráfego que entra/sai da máquina e tráfego redirecionado.
- Permite um número ilimitado de regras por chain
- Possui mecanismos internos para rejeitar automaticamente pacotes duvidosos ou mal formados.
- Suporte a módulos externos para expansão das funcionalidades padrões oferecidas pelo código de firewall
- Suporte a especificação de tipo de serviço para priorizar o tráfego de determinados tipos de pacotes.

IPTables – Ficha Técnica

- Pacote: iptables
- iptables - Sistema de controle principal para protocolos IPv4
- ip6tables - Sistema de controle principal para protocolos IPv6
- iptables-save - Salva as regras atuais em um arquivo especificado como argumento. Este utilitário pode ser dispensado por um shell script contendo as regras executado na inicialização da máquina.
- iptables-restore - Restaura regras salvas pelo utilitário iptables-save.

Firewall

O IPTables como firewall em nível de pacote toma as decisões baseadas nos parâmetros do pacote, como porta/endereço de origem/destino, estado da conexão, e outros parâmetros do pacote. O firewall então pode negar o pacote (DROP) ou deixar o pacote passar (ACCEPT).

O que são REGRAS?

As regras são como comandos passados ao iptables para que ele realize uma determinada ação (como bloquear ou deixar passar um pacote) de acordo com o endereço/porta de origem/destino, interface de origem/destino, etc.

As regras são armazenadas dentro dos CHAINS e processadas na ordem que são inseridas.

As regras são armazenadas no kernel, o que significa que quando o computador for reiniciado tudo o que fez será perdido. Por este motivo elas deverão ser gravadas em um arquivo para serem carregadas a cada inicialização.

iptables -A INPUT -s 123.123.123.1 -j DROP

O que são CHAINS?

Os CHAINS são locais onde as regras do firewall definidas pelo usuário são armazenadas.

Existem dois tipos de chains: os embutidos (como os chains INPUT, OUTPUT e FORWARD) e os criados pelo usuário.

Os nomes dos chains embutidos devem ser especificados sempre em maiúsculas (note que os nomes dos chains são case-sensitive, ou seja, o chain input é completamente diferente de INPUT).

O que são TABELAS?

Tabelas são os locais usados para armazenar os chains e as regras que cada um possui. As tabelas podem ser referenciadas com a opção -t tabela.

Existem 3 tabelas disponíveis no iptables:

- filter
- nat
- mangle

filter

1- filter - Esta é a tabela padrão, contém 3 chains padrões:

- INPUT - Consultado para dados que chegam a máquina
- OUTPUT - Consultado para dados que saem da máquina
- FORWARD - Consultado para dados que são redirecionados para outra interface de rede ou outra máquina.

Os chains INPUT e OUTPUT somente são atravessados por conexões indo/se originando de localhost.

OBS: Para conexões locais, somente os chains INPUT e OUTPUT são consultados na tabela filter.

filter – Permitir porta 80

```
iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT
```


nat

Usada para dados que gera outra conexão (masquerading, source nat, destination nat, port forwarding, proxy transparente são alguns exemplos).

Possui 3 chains padrões:

- PREROUTING - Consultado quando os pacotes precisam ser modificados logo que chegam. É o chain ideal para realização de DNAT e redirecionamento de portas.
- OUTPUT - Consultado quando os pacotes gerados localmente precisam ser modificados antes de serem roteados. Este chain somente é consultado para conexões que se originam de IPs de interfaces locais.
- POSTROUTING - Consultado quando os pacotes precisam ser modificados após o tratamento de roteamento. É o chain ideal para realização de SNAT e IP Masquerading.

nat – compartilhamento de internet

```
iptables -t nat -A POSTROUTING -s 192.168.0.0/24
   -o eth0 -j MASQUERADE
```

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

mangle

Utilizada para alterações especiais de pacotes, como modificar o tipo de serviço (TOS) ou outros detalhes.

Possui 2 chains padrões:

PREROUTING - Consultado quando os pacotes precisam ser modificados logo que chegam.

OUTPUT - Consultado quando pacotes gerados localmente precisam ser modificados antes de serem roteados.

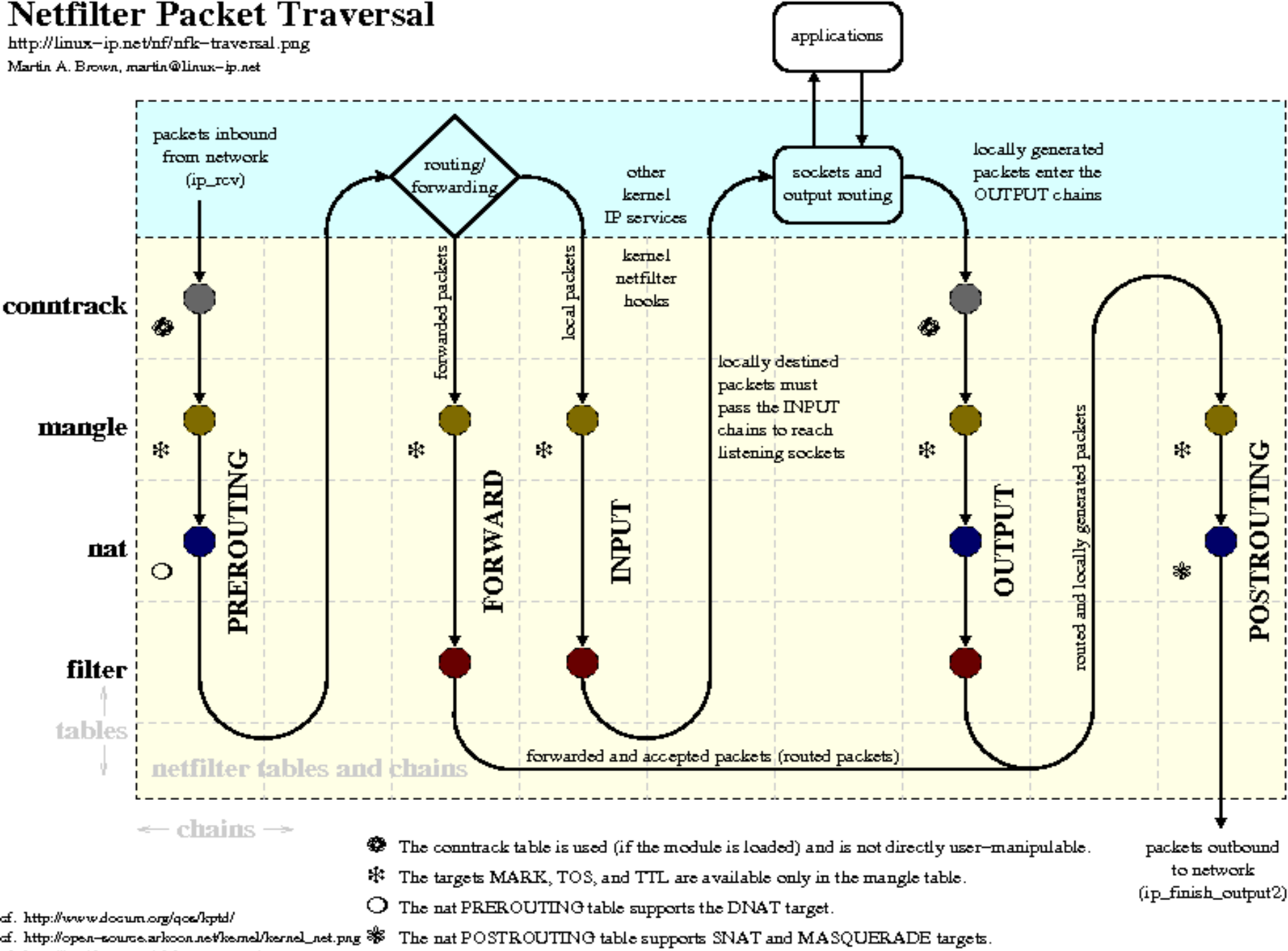
mangle - Priorizar o tráfego de http da rede:

```
iptables -t mangle -A OUTPUT -o eth0 -p tcp
  –dport 80 -j TOS --set-tos 16
```

Netfilter Packet Traversal

http://linux-ip.net/nf/nfk-traversal.png

Martin A. Brown, martin@linux-ip.net



❁ The conntrack table is used (if the module is loaded) and is not directly user-manipulable.

❄ The targets MARK, TOS, and TTL are available only in the mangle table.

○ The nat PREROUTING table supports the DNAT target.

❃ The nat POSTROUTING table supports SNAT and MASQUERADE targets.

ef. http://www.docum.org/qos/kptd/

ef. http://open-source.arkoon.net/kernel/kernel_net.png

ef. http://iptables-tutorial.frozentux.net/

Módulos

O kernel precisa de módulos ativados para que o iptables funcione. O comando “modprobe” ativa cada um dos módulos listados a seguir.

- modprobe iptable_nat
- modprobe ip_tables
- modprobe ipt_state
- modprobe ip_conntrack
- modprobe ip_conntrack_ftp
- modprobe ipt_multiport
- modprobe ip_nat_ftp
- modprobe iptable_mangle
- modprobe ipt_tos
- modprobe ipt_limit

Limpar as Tabelas

Normalmente, antes de criar novas regras, o ideal é limpar todas as regras existentes. A opção “–F” é responsável pela limpeza (FLUSH) das regras. Veja que são 3 comandos para limpar as 3 tabelas padrões do IPTABLES.

- iptables -F
- iptables -F -t nat
- iptables –F –t mangle

Listar Tabelas

- iptables -L
- iptables -L -t nat
- iptables –L –t mangle

Liberar algumas portas

Para Liberar o HTTP, HTTPS, FTP, DNS, então fica:

```
iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 443 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 20 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 21 -j ACCEPT
iptables -t filter -A INPUT -p udp --dport 53 -j ACCEPT

iptables -A INPUT -p tcp --syn -j DROP
```

Brincando com o Shell

oi.txt

Congresso Estadual de Software Livre

cat oi.txt |cut -d” “ -f5

Livre

Marcos Monteiro

Brincando de Shell

```
for i in `cat oi.txt`; do
        echo $i;
done
```

Congresso
Estadual
de
Software
Livre

Então vamos Liberar algumas portas

Para Liberar o HTTP, HTTPS, FTP, DNS, então fica:

```
iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 443 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 20 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 21 -j ACCEPT
iptables -t filter -A INPUT -p udp --dport 53 -j ACCEPT

iptables -A INPUT -p tcp --syn -j DROP
```

Para Liberar o HTTP, HTTPS, FTP, DNS, então fica:

iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT

iptables -A INPUT -p tcp --syn -j DROP

Criar arquivo /root/fw/libportas
80
443
20
21

Criar arquivo /root/fw/libportasudp
53

```
for i in `cat /root/fw/libportas |cut -d" " -f1`; do
        iptables -A INPUT -p tcp --dport $i -j ACCEPT
     echo $i
done

for i in `cat /root/fw/libportasudp |cut -d" " -f1`; do
        iptables -A INPUT -p udp --dport $i -j ACCEPT
     echo $i
done


iptables -A INPUT -p tcp --syn -j DROP
```

DNAT e SNAT

```
iptables -t nat -A POSTROUTING -s 192.168.0.14  -j SNAT –to 200.253.18.44
iptables -t nat -A PREROUTING -s 200.253.18.44 -j DNAT --to 192.168.0.14
```

Marcos Monteiro

DNAT e SNAT

Criar o Arqvuivo /root/fw/NATsVIP

192.168.0.14 200.253.18.44 Computador do Financeiro
192.168.1.32 200.253.18.15 Computador do Adm Redes :)

Marcos Monteiro

Fazendo DNAT e SNAT

```
    c=1
for i in `cat /root/fw/NATsVIP |cut -d" " -f1`; do
    iy=`cat /root/fw/NATsVIP |cut -d" " -f2`
     y=`echo $iy |cut -d" " -f$c`
     c=$(($c+1))
     iptables -t nat -A POSTROUTING -s $i -j SNAT --to $y
     iptables -t nat -A PREROUTING -s $y -j DNAT --to $i
     echo "De $i para $y"
done
```

Redirecionamento de Porta

```
iptables -t nat -A PREROUTING -d 200.253.0.14 -p tcp --
    dport 21 -j DNAT --to 192.168.0.10
```

```
iptables -t nat -A PREROUTING -d 200.253.0.14 -p tcp --
    dport 20 -j DNAT --to 192.168.0.10
```


Arquivo /root/fw/redirectip

20 192.168.0.253 ftp File Server

21 192.168.0.253 ftp File Server

```
    c=1
for i in `cat /root/fw/redirectip |cut -d" " -f1`; do
     iy=`cat /root/fw/redirectip |cut -d" " -f2`
     y=`echo $iy |cut -d" " -f$c`
     c=$(($c+1))
iptables -t nat -A PREROUTING -d $IPNET -p tcp --dport $i -j DNAT --to $y
done
```

Exemplos

```
echo "Fazendo NAT"
for i in `cat /root/fw/NATs |cut -d" " -f1`; do
    iptables -t nat -A POSTROUTING -s $i -o $ETHNPD -j
    MASQUERADE
    echo "$i"
done

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

Exemplos

```
echo "Liberando acesso destes da LAN para outras
   redes"
for i in `cat /root/fw/printers |cut -d" " -f1`; do
        iptables -A FORWARD -s $WLAN -d $i -j ACCEPT
echo "liberando $i"
done
```


Exemplos

```
# Liberar MAC da rede sem fio para rede interna

for i in `cat /root/fw/libmacs |cut -d" " -f1`; do
        iptables -A FORWARD -m mac --mac-source $i -d
    $REDEINTERNA -j ACCEPT
done
```

Exemplos

Bloquear Computador para Internet por MAC

```
for i in `cat /root/fw/bloqnetformac |cut -d" " -f1`; do
    iptables -A FORWARD -m mac --mac-source $i  -p tcp
   -m tcp --dport 0:65534 -j DROP
done
```

fw.sh

Marcos Monteiro

Um muito Obrigado :)

Marcos Monteiro

http://www.marcosmonteiro.com.br
contato@marcosmonteiro.com.br