Universidade Tuiuti do Paraná
Faculdade de Ciências Exatas

http://www.netfilter.org/

André Luiz – andreluizsp@gmail.com

Conteúdo programático

- ✔ O que é netfilter/IPTables?
- ✔ Tabelas
- ✔ Chains
- ✔ Tagert
- ✔ Politica de segurança
- ✔ Criando e Removendo Regras
- ✔ NAT – Network Address Translator
- ✔ Redirecionamento de porta
- ✔ Criando um serviço de firewall
- ✔ Exemplos

O que é netfilter/IPTables?

O iptables é um programa de linha de comando usado para configurar o kernel Linux, permite formar um conjunto de regras para filtragem de pacotes IPv4. Ele é direcionado para administradores de sistema.

O pacote iptables também inclui ip6tables. ip6tables é usado para configurar o filtro de pacotes IPv6.

A filtragem de pacotes permite controle, segurança e vigilância.

Um firewall, ou filtro de pacotes, é utilizado para proteger máquinas ou rede através da filtragem dos pacotes de dados. No Linux esse recurso é implementado diretamente no kernel e recebe, nas versões de kernel > 2.4, o nome de netfilter.

O netfilter é capaz de manipular campos dos cabeçalhos de pacotes, fazer a tradução de endereços de rede (NAT), “marcar” pacotes e fazer o acompanhamento de conexões e filtragem.

Estes recursos fazem com o que o netfilter seja um firewall capaz de reconhecer o "estado" de uma conexão.

TABELA

Tabela é o local utilizado para armazenar regras de filtragem.

Existem três tabelas:

» Filter - utilizada para aceitar ou rejeitar pacotes;

» Mangle - manipular alguns campos do cabeçalho IP – TOS e TTL;

» Nat - utilizada para fazer Traduções de Endereços de Rede.

TABELA

Listando conteúdo das tabelas:

```
# iptables -L

# iptables -L -t nat

# iptables -L -t mangle
```

CHAIN

Chain conjunto de regras aplicadas sobre os pacotes.

Existem dois tipos:

✔ Chains do kernel

- PREROUTING, INPUT, FORWARD, OUPUT e POSTROUTING Estão ligadas a pontos especiais no caminho que os pacotes precorrem ao entrar e sair da máquina.

✔ Chains criadas pelo usuário

- Não estão ligadas a ponto algum, logo, é necessário que uma chain do kernel tenha como alvo uma chain de usuário para que os pacotes percorram essa chain.

CHAIN

- PREROUTING: chain consultada após a tomada de decisão de roteamento, usa a interface de entrada;
- INPUT: quando o pacotes entram na máquina;
- FORWARD: quando pacote é enviado a outra máquina;
- OUTPUT: quando o pacote está saindo da máquina;
- POSTROUTING: chain consultada após a tomada de decisão de roteamento, usa a interface de saída;
- A filtragem de pacotes é feita em basicamente 3 lugares:
  - Chains INPUT e OUTPUT para pacotes com origem e destino na máquina local
  - Chain FORWARD para pacotes que atravessam o roteador.

CHAIN

Quando um pacote "entra" numa chain, cada regra é avaliada, de maneira seqüencial, até que o pacote case com uma regra, ou o pacote atinja o final da chain. Quando um pacote atinge o final de uma chain sem que tenha casado com alguma regra, é aplicada então a política padrão da chain. Por padrão a política padrão da chain é "ACCEPT“, mas isso pode ser alterado pela política de acesso.

TAGERT

- ACCEPT: Aceita o pacote;
- DROP: Bloqueia um pacote sem resposta;
- REJECT: Bloqueia um pacote com resposta;
- LOG: Gera log de acordo com a regra definida;
- SNAT, DNAT, MASQUERADE: Realiza NAT sobre os pacotes.

Política de Segurança

Política de segurança é configurada através do parâmetro "-P":

```
# iptables -P INPUT DROP

# iptables -P FORWARD DROP

# iptables -P OUTPUT ACCEPT
```

Criando e Removendo Regras

A sintaxe geral para se criar ou remover uma regra é a seguinte:

iptables -[AID] CHAIN [N] [-t TABLE] MATCH -j TARGET

-A é usada para se fazer o "append" de uma regra à uma chain

-I é usada para se inserir uma regra

-D é usada para se deletar uma regra.

iptables -F

iptables -t nat -F

iptables -t mangle -F

NAT – Network Address Translator

O tráfico originado em sua rede privada é assim "mascarado" como tendo originado de seu gateway:

```
# modprobe iptable_nat
# sysctl net.ipv4.ip_forward=1
# iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

Redirecionamento de porta

```
# modprobe ipt_REDIRECT
# iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j
REDIRECT --to-port 3128
```

Criando um serviço de firewall

```
# vim /etc/init.d/firewall
    #!/bin/bash
    case $1 in
      start)
            iptables -F
            iptables -t nat -F
            iptables -t mangle -F
            iptables -P INPUT DROP
            iptables -P FORWARD DROP
            iptables -P OUTPUT ACCEPT
            modprobe  modprobe iptable_nat ipt_REDIRECT xxx
             sysctl net.ipv4.ip_forward=1
             < regras >
             ;;
      stop)
            iptables -F
            iptables -t nat -F
            iptables -t mangle -F
            iptables -P INPUT ACCEPT
            iptables -P FORWARD ACCEPT
            iptables -P OUTPUT ACCEPT
            ;;
      *)  echo “Use: service firewall  [ start | stop ]”
            exit 1
           ;;
      esac
      exit 0
```

Exemplos

Dropa tudo que chegue ao roteador com destino ao host 192.168.0.3:

```
# iptables -A FORWARD -d 192.168.0.3/32 -j DROP
```

Bloqueia o acesso a porta 23 da máquina local de acessos vindos pela interface eth0:

```
# iptables -A INPUT -i eth0 -p tcp --dport 23 -j REJECT
```

Exemplos

Faz NAT para a rede interna:

```
# iptables -A POSTROUTING -t nat -s 192.168.0.0/24 -o eth1 -j
    SNAT --to-source 200.X.X.36
```

Utilizando proxy “transparente”:

```
# iptables -A PREROUTING -p tcp --dport 80 -s 192.168.0.0/24 -j
    REDIRECT --to-ports 3128
```

Utilizando dois servidores em uma Intranet e queremos balancear as conexões:

```
# iptables -A PREROUTING -p tcp  --dport 80 -i eth0 -j DNAT
    --to-source 192.168.1.5,192.168.1.6
```

creative commons

Atribuição-Compartilhamento pela mesma licença 2.5
(http://creativecommons.org/licenses/by-sa/2.5/deed.pt)

Você pode:

- copiar, distribuir, exibir e executar a obra
- criar obras derivadas
- fazer uso comercial da obra

Sob as seguintes condições:

Atribuição. Você deve dar crédito ao autor original, da forma especificada pelo autor ou licenciante.

Compartilhamento pela mesma Licença. Se você alterar, transformar, ou criar outra obra com base nesta, você somente poderá distribuir a obra resultante sob uma licença idêntica a esta.

- Para cada novo uso ou distribuição, você deve deixar claro para outros os termos da licença desta obra.
- Qualquer uma destas condições podem ser renunciadas, desde que Você obtenha permissão do autor.

Qualquer direito de uso legítimo (ou "fair use") concedido por lei, ou qualquer outro direito protegido pela legislação local, não são em hipótese alguma afetados pelo disposto acima.

Este é um sumário para leigos da Licença Jurídica
(na íntegra: http://creativecommons.org/licenses/by-sa/2.5/br/legalcode).
Termo de exoneração de responsabilidade:
http://creativecommons.org/licenses/disclaimer-popup?lang=pt