Linux Firewall

Roberto Sadao Yokoyama

UTFPR-CP

Setembro, 2016

Prática de hoje:[1]

[1] Baseado no exemplo:
http://www.planetaunix.com.br/2014/12/firewall-iptables-parte-01.htm

iptables

iptables: é o firewall padrão na maioria das distribuições Linux (netfilter.org)

- iptables verifica cada pacote que atravessa as interfaces de rede e comparando-os com um conjunto de regras pré-definidas para descobrir o que fazer com esses pacotes
- Algumas aplicações do iptables:
  - Construir firewalls de Internet baseados em filtragem de pacotes "stateless"e "stateful"
  - Usar NAT e masquerading para compartilhamento de Internet com uma rede local
  - Usar NAT para implementar proxies transparentes
  - Realizar manipulação de pacotes adicional (mangling), como alterar bits no cabeçalho IP
  - Realizar Encaminhamento de Portas (que é um tipo de DNAT)

iptables

Funcionamento do iptables

- iptables trabalha comparando o tráfego de rede que a máquina recebe/envia com um conjunto de regras pré-especificadas
- Regras verificam a correspondência com o pacote
  - protocolo
  - portas de origem ou destino
  - endereços IP de origem ou destino
  - interfaces em uso
- Após a correspondência entre um pacote e uma regra, uma ação será tomada, e a essa ação dá-se o nome de target
  - aceito ou descartado
  - movido para outra cadeia para processamento

iptables

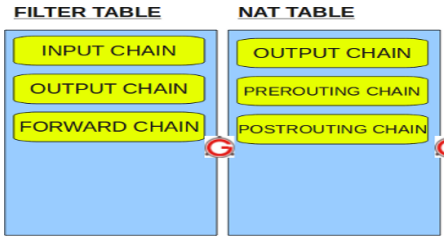
Funcionamento do iptables

- A arquitetura do iptables agrupa o processamento dos pacotes de rede em tabelas:
  - **filter** - Tabela padrão para manipular pacotes de rede, usada para configurar políticas para o tráfego que entra, atravessa ou sai do computador.
  - **nat** - Usada para alterar pacotes que criam uma nova conexão, e para redirecionar conexões para NAT..
  - **mangle** - Usada para tipos específicos de alteração de pacotes, como a modificação de opções do cabeçalho IP de um pacote.
- Cada qual possui cadeias (chains) de regras de processamento

iptables

Funcionamento do iptables

Tabela 1



iptables

Funcionamento do iptables

- **Cadeias**: As regras são organizadas em grupos denominados cadeias (chains), que por sua vez ficam contidas nas tabelas. Uma cadeia é então um conjunto de regras usadas para verificar a correspondência com um pacote - de forma sequencial.
- As tabelas possuem as cadeias a seguir:
  - Tabela Filter: Cadeias INPUT, OUTPUT e FORWARD
  - Tabela NAT: Cadeias PREROUTING, OUTPUT, POSTROUTING
  - Tabela Mangle: Cadeias PREROUTING, OUTPUT, POSTROUTING, INPUT e FORWARD
- Quando um pacote corresponde a uma regra na cadeia, a ação associada a essa regra é executada e as regras restantes não são verificadas contra esse pacote.
- Caso nenhuma regra corresponda ao pacote, a regra padrão será aplicada

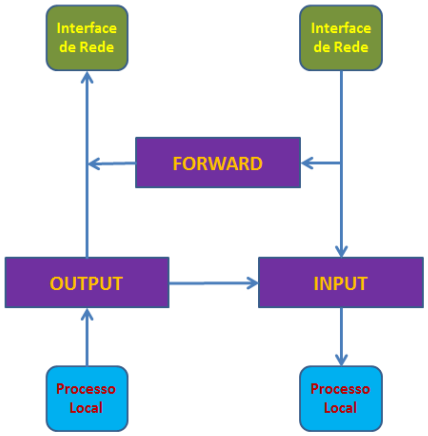
iptables

Cadeias

- **INPUT** - aplica regras aos pacotes de rede que chegam ao host
- **OUTPUT** - aplica regras aos pacotes originados do host antes de ser enviados a rede
- **FORWARD** - aplica regras aos pacotes de rede roteados através do servidor (para outro servidor ou outra interface de rede no mesmo servidor)
- **PREROUTING** - altera pacotes de rede quando eles chegam e antes do roteamento. Usado para DNAT (Destination NAT)
- **POSTROUTING** - altera pacotes de rede após o roteamento. Usado para SNAT (Source NAT)

iptables

Fluxo de pacotes de rede da tabela filter



iptables

Regras

- A estrutura geral de uma regra é a seguinte:
- *iptables subcomando chain parâmetro_1 valor_1 parâmetro_n valor_n ação*
- Os subcomandos principais que podem ser usados são os seguintes[2]:
  - -A anexa a regra no final da cadeia especificada
  - -F apaga todas as regras na cadeia especificada
  - -L lista todas as regras da cadeia
  - -P configura a regra padrão da cadeia
  - -D apaga uma regra em uma posição na cadeia
  - -X exclui uma cadeia vazia
  - -I insere uma regra em uma posição na cadeia

[2] https://access.redhat.com/documentation/pt-BR/Red_Hat_Enterprise_Linux/6/html/Security_Guide/sect-Security_Guide-IPTables-Command_Options_for_IPTables.html

iptables

Regras

- Já as ações (targets) possíveis estão listadas na tabela a seguir:
  - ACCEPT - pacote permitido
  - DROP - Descartar o pacote
  - REJECT - Descarta o pacote e envia feedback ao remetente.
  - DNAT - reescreve endereço de destino (NAT)
  - SNAT - reescreve endereço de origem (NAT)
  - LOG - coloca no log informações sobre o pacote

iptables

Regras

Parâmetro	Significado
-t tabela	Especificar a tabela (filter é a padrão)
-j ação	Realiza a ação especificada
-p protocolo	Especifica o protocolo (icmp, tcp, udp, all)
-s IP	IP de origem do pacote
-d IP	IP de destino do pacote
-i interface	Nome da interface de rede de entrada do pacote
-o interface	Nome da interface de rede de saída do pacote
--sport portas	Portas de origem
--dport portas	Portas de destino
--syn	Identifica nova requisição de conexão
--icmp-type	tipo de mensagem ICMP

iptables

Regras

- *iptables -A INPUT -s 0/0 -i eth0 -d 192.168.1.1 -p TCP -j ACCEPT*
- Destrinchando a regra acima, temos:
  - iptables - Comando iptables
  - -A INPUT - Anexar a regra no final da cadeia INPUT
  - -s 0/0 - Endereço IP de origem: qualquer um
  - -i eth0 - Interface de entrada a ser monitorada: eth0
  - -d 192.168.1.1 - Endereço IP de destino do pacote: 192.168.1.1
  - -p TCP - Protocolo a ser verificado: TCP
  - -j ACCEPT - Ação a ser aplicada no pacote: ACCEPT (permitir)

iptables

Limpando as regras de uma cadeia

- Podemos apagar todas as regras de uma cadeia (exceto a regra padrão) com a opção -F:
- *# iptables -F INPUT*
- Ou limpar todas as regras de todas as cadeias da tabela especificada:
- *# iptables -F*

Configurando a regra padrão de uma cadeia

- Usamos a opção -P para configurar a regra padrão de uma cadeia. Veja os exemplos:
- *# iptables -P INPUT DROP*
- *# iptables -P OUTPUT ACCEPT*
- *# iptables -L*

Listando os números das regras

- *# iptables -L –line-numbers*
- Ex: Liberar o acesso SSH por meio da porta 22 com a regra a seguir:
- *# iptables -A INPUT -p tcp –dport 22 -j ACCEPT*

Referências

Tutorial:
http://www.planetaunix.com.br/2014/12/firewall-iptables-parte-01.html
Vídeo:
https://www.youtube.com/watch?v=LJlJlLgkNxg&index=1&list=PL4i0dRYFvxd0fEJIkzTB_PNMcPCgUHLtQ