IPTables

Aplicação NetFilter para Firewall

IPTables faz parte do Netfilter, opera na camada 3, embora também contenha comandos para camada 2. O IPTables se aplica ao ipv4, sendo IP6tables para o IPv6. Podemos além de filtrar pacotes, fazer NAT, alterar bits no cabeçalho IP, encaminhar portas, balancear a carga, entre outros.

TABELAS

FILTER - tabela padrão para manipulação de pacotes, aplicado em tráfego que entra, atravessa ou sai do firewall
NAT - tabela de alteração para pacotes que criam novas conexões ou são redirecionadas pra NAT
MANGLE - Alterações especiais como em cabeçalho IP
RAW - marcar pacotes para não serem manipulados pelo sistema de rastreamento de conexões

As regras ficam em /etc/iptables/rules.v4
A sintaxe de utilização é: **iptables COMANDO CADEIA PARAMETRO(S) VALOR(ES) AÇÃO**

COMANDOS

-A insere a regra no final da cadeia
-F apaga todas as regras da cadeia
-L lista todas as regras da cadeia (--line-numbers para mostrar o número da regra/linha)
-S lista as regras de forma simplificada (exibe o conteúdo do arquivo rules)
-N cria uma nova cadeia
-P configura a regra padrão da cadeia
-D apaga uma regra em uma posição da cadeia
-X exclui uma cadeia vazia
-I insere uma regra em uma posição específica na cadeia

CADEIAS

Cada tabela contém cadeias como um conjunto de regras sequenciais. Podemos também criar nossas próprias cadeias, mas normalmente utilizamos as que já existem. As cadeias de cada tabela são:
FILTER - INPUT, OUTPUT, FORWARD
NAT - PREROUTING, OUTPUT, POSTROUTING
MANGLE - PREROUTING, OUTPUT, POSTROUTING, INPUT FORWARD
RAW - PREROUTING E OUTPUT (tabela raramente utilizada)

INPUT - a regra é aplicada nos pacotes que entram no firewall, isto é, chegam no servidor
OUTPUT - a regra é aplicada nos pacotes que saem no firewall, isto é, originam-se no servidor
FORWARD - a regra é aplicada aos pacotes roteados para outro servidor ou outra interface de rede no mesmo servidor
PREROUTING - a regra é aplicada aos pacotes que chegam e antes do roteamento (como DNAT)
POSTROUTING - a regra é aplicada aos pacotes, após o roteamento (como SNAT)

PARÂMETROS/VALORES

Ao escrever uma regra, utilizamos os parâmetros para filtrar, estes podem ser:
-t tabela da regra (padrão é filter)
-j ação (desnecessário em política padrão)
-p protocolo da regra
-s IP de origem
-d IP de destino
-i interface de rede de entrada
-o interface de rede de saída

--sport porta de origem
--dport porta de destino
--syn nova conexão TCP
--icmp-type tipo de mensagem ICMP (echo reply, request, etc)
-m "match" para combinar com algumas opções dinâmicas

AÇÕES
ACCEPT - aceita o pacote
DROP - descarta o pacote silenciosamente
RETURN - aplica a regra padrão direto
REJECT - descarta o pacote e envia feedback ICMP ao remetente (apenas INPUT, OUTPUT, FORWARD)
DNAT - reescreve o endereço de destino (NAT)
SNAT - reescreve o endereço de origem (NAT)
MASQUERADE - mascara o IP privado com o IP público de saída
LOG - insere informações sobre o pacote no log do iptables

Cada cadeia pode possuir mais de uma regra e também um política padrão, caso as regras não sejam atendidas. A política padrão pode ser ACCEPT (deixa o pacote passar) ou DROP (descarta o pacote).

A ação REJECT pode ser complementada com:
--reject-with definir a mensagem do REJECT, podendo ser:
icmp-net-unreachable: rede inacessível
icmp-host-unreachable: host inacessível
icmp-proto-unreachable: protocolo inacessível
icmp-port-unreachable: porta inacessível (mensagem padrão)
icmp-net-prohibited: rede proibida
icmp-host-prohibited: host proibido
icmp-admin-prohibited
tcp-reset

EXEMPLOS:

iptables -L
iptables -t nat -L
iptables -A INPUT -s 0/0 -i eth0 -d 192.168.1.1 -p tcp -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j DROP
iptables -A INPUT -s 192.168.1.100 -j ACCEPT
iptables -A INPUT -s 192.168.1.100 -j REJECT
iptables -A INPUT -p imcp --imcp-type echo-request -j ACCEPT
iptables -F INPUT
iptables -P INPUT DROP
iptables -D INPUT 4
iptables -I INPUT 2 -m mac --mac-source 0A:20:BB:22:AC:FF

PARA SALVAR: iptables-save > arquivo
PARA RESTAURAR: iptables-restore > arquivo

Ou de forma mais fácil, instalamos o pacote iptables-persistent
service iptables-persistent save

Exercícios:

1 - Crie um regra para bloquear o PING e teste
2 - Apague todas as regras da tabela filter, na cadeia INPUT
3 - Altere a política padrão da cadeia INPUT para DROP e teste acesso via SSH
4 - Libere os pacotes para SSH
5 - Aceite pacotes de ping
6 - Explique o que as seguintes regras fazem:

a) iptables -t filter -A INPUT -s 192.168.0.0/255.255.255.0 -i eth1 -j ACCEPT
b) iptables -A INPUT -j LOG --log-prefix "FW INPUT"
c) iptables -I FORWARD -s 192.168.0.0/255.255.255.0 -d www.facebook.com -j DROP
d) iptables -A OUTPUT -o lo -j ACCEPT
e) iptables -D FORWARD -s 192.168.13.0/24 -d www.google.com -j REJECT
f) iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

7 - Criar regras para as seguintes funções:

a) Permitir todo o tráfego "de volta" na subtabela FORWARD da tabela filter
iptables -t filter -I FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT

b) Filtrar os acessos da rede interna (10.0.10.0/24) entrando pela interface eth0 utilizando o protocolo de camada de aplicação HTTP e saindo com destino à Internet.
iptables -t filter -A FORWARD -s 10.0.10.0/24 -i eth0 -p tcp --dport 80 -o eth1 -d 0.0.0.0/0.0.0.0 -j DROP

c) Mudar o endereço IP de origem de todos os pacotes originados da rede interna (10.0.10.0/24) para a Internet saindo pela interface eth12 para o endereço externo que pertence ao firewall 200.200.200.200
iptables -t nat -A POSTROUTING -s 10.0.10.0/24 -o eth12 -j SNAT --to-address 200.200.200.200

d) Rejeitar os pacotes que são destinados ao firewall na interface interna (eht0) que não são provenientes da rede 172.16.1.0/24.
iptables -t filter -A INPUT -s 172.16.1.0/24 -i eth0 -j ACCEPT
iptables -t filter -A INPUT -i eht0 -j DROP
ou
iptables -t filter -A INPUT -s ! 172.16.1.0/24 -i eth0 -j DROP