Firewall – IPTABLES

Fernando Resende Coelho
frcoelho@pop-mg.rnp.br

Sumário

- Conceitos
- Diagrama de fluxo
- Sintaxe
- Passo a passo
- Referências

O que é um Firewall?

- Um firewall é uma barreira inteligente entre duas redes, através do qual só passa tráfego autorizado. Este tráfego é examinado pelo firewall em tempo real e a seleção é feita de acordo com a política de segurança estabelecida.

Stateful Firewall

- Sempre que um pacote chega ao firewall, este inspeciona a sua lista de conexões e faz *state matching* conforme a lista de políticas.

Iptables

- É composto por 3 tabelas:
  - filter
    - tabela de filtros de pacotes.
  - NAT (network address translation)
    - Conexão de várias máquinas com endereço falso á internet através de poucos endereços IP´s válidos.
  - mangle
    - altera o conteúdo dos pacotes.

Iptables – Filter Table

- Quando um pacote chega a uma table é verificado se alguma regra se aplica a ele. Caso não haja, é aplicada a política defaut.
- Constituído por 3 chains:
  - INPUT – Pacote destinado a maquina de firewall.
  - OUTPUT – Pacote originado da maquina de firewall.
  - FORWARD – Pacote com destino e origem separados pela maquina de firewall.

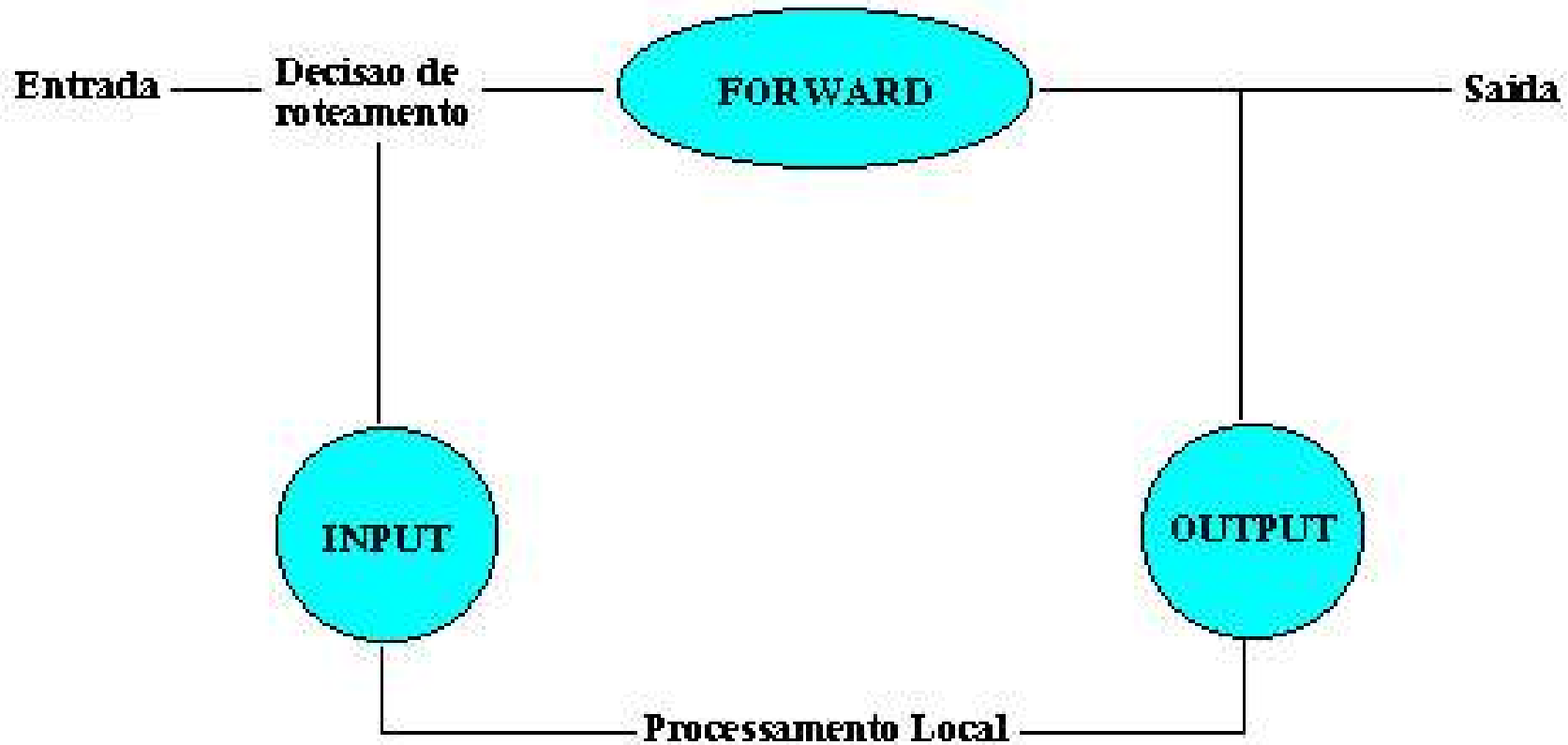
Política Default

- Política default do firewall consiste na regra que será utilizada caso algum pacote não se encaixe em nenhuma das regras estabelecidas.
- É altamente recomendado que a política default seja DROP, ou seja, tudo o que não for expressamente permitido será descartado (proibido).

Iptables – Filter Table

- Diagrama de Fluxo
  - Pacote entra num interface de rede
    - se o pacote é para a maquina é enviado para o chain **INPUT;**
    - se o destino não é esta maquina e o serviço de routing está activo, o pacote vai para o chain **FORWARD.**
  - um processo da maquina envia um pacote para a rede
    - pacote vai para o chain **OUTPUT.**

Iptables – Filter Table



Iptables – Filter Table

- Comandos para manipular chains
  - -N chain
    - cria uma user chain
  - -X [chain]
    - apaga uma user chain
  - -P chain target
    - muda a política default de uma chain
  - -L [chain]
    - lista as regras de uma chain
  - -F [chain]
    - apaga todas as regras de um chain
  - -Z [chain]
    - limpa todos os contadores de bytes e pacote de uma chain

Iptables – Filter Table

- Comandos para manipular regras de chains:
  - -A chain
    - acrescenta uma regra a uma chain
  - -I chain [rulenum]
    - insere regra numa posição da chain
  - -R chain rulenum
    - troca posição de regra na chain
  - -D chain
    - apaga regra de uma chain

Iptables – Filter Table

- Opções
  - -s [!] address[/mask]
    - especifica o endereço de origem
  - -d [!] address[/mask]
    - especifica o endereço de destino
  - -p [!] protocolo
    - especifica o protocolo (TCP , UDP , ICMP , ALL)
  - -i [!] input_name
    - especifica a interface de entrada dos pacotes
  - -o [!] output_name
    - especifica a interface de saída dos pacotes
  - [!] -f
    - indica que a regra se aplica só a fragmentos a partir do 2º pacote

IPTables - Filter Table - Extensão TCP

- Opções (-p tcp)
  - --tcp-flags [!] mask set
    - A mascara indica quais as flags a vigiar e o resultado esperado.
    - As flags podem ser: SYN,ACK,FIN,RST,URG,PSH,ALL,NONE.
  - [!] --syn
    - examina a flag TCP SYN.
  - --sport [!] port[:port]
    - indica a porta TCP da origem
  - --dport [!] port[:port]
    - indica a porta TCP de destino

IPTables - Filter Table - Extensão UDP

- Opções (-p udp)
  - --sport [!] port[:port]
    - indica a porta UDP de origem
  - --dport [!] port[:port]
    - indica a porta UDP de destino

IPTables - Filter Table - Extensão ICMP

- Opções (-p icmp)
  - --icmp-type [!] typename
    - examina os tipos icmp.

IPTables - Filter Table - Extensão Mac

- Opções (-m mac)
  - --mac-source [!] address
    - examina o Ethernet MAC address do pacote

IPTables - Filter Table – Extensão Owner

- Este módulo é usado para restringir o criador do pacote. Usado apenas na chain OUTPUT.
- Opções (-m owner)
  - --uid-owner userid
    - aceita pacote que tenha sido criado pelo user uid
  - --gid-owner groupid
    - aceita pacote que tenha sido criado pelo grupo de users gid
  - --pid-owner processid
    - aceita pacote que tenha sido criado pelo processo pid

IPTables - Filter Table - Extensão State

- Este módulo é usado para interpretar o output do módulo ip_conntrack (connection-tracking analysis)
- Opções (-m state)
  - --state state[,state]
    - Os estados possíveis são:
      - NEW : indica pacote que cria uma nova conexão
      - ESTABLISHED : indica um pacote que pertence a uma conexão já existente
      - RELATED : indica um pacote relacionado com uma conexão já existente
      - INVALID : pacote que não foi identificado

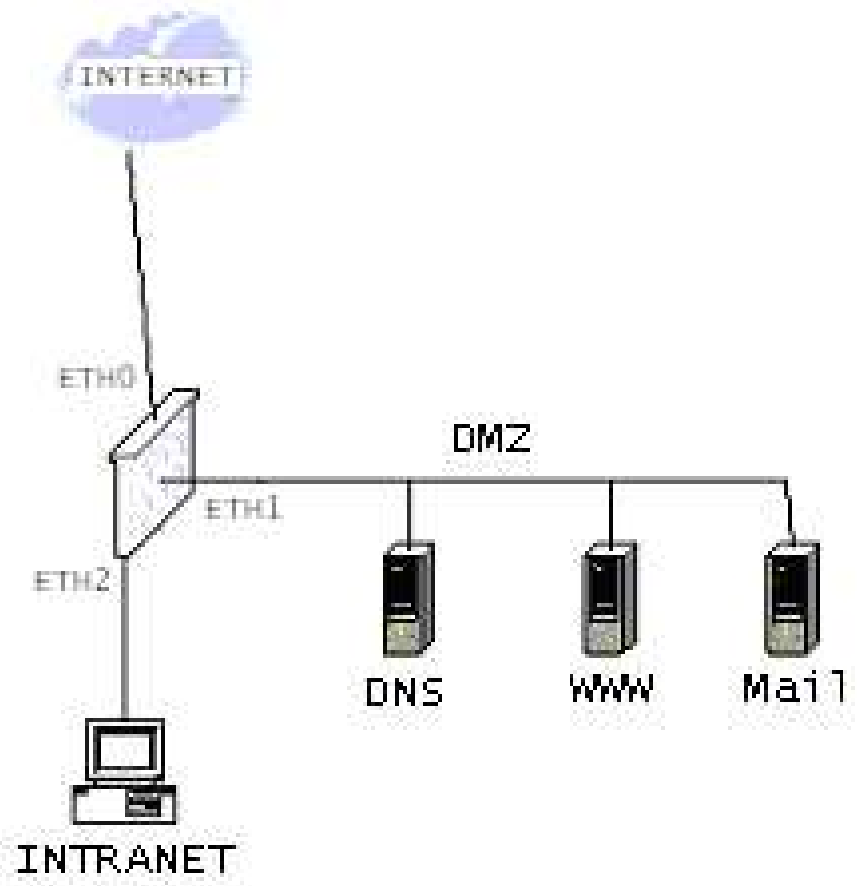
IPTables - Filter Table - Targets

- Toda regra tem um target, que é o que ocorrerá com o pacote cajo haja um *match* com a regra. Os target´s possíveis são:
- Opções (-j)
  - ACCEPT
    - o pacote será aceito.
  - DROP
    - o pacote será destruído.
  - REJECT
    - O pacote será rejeitado e uma mensagem icmp será enviada à origem.
  - USER_CHAIN
    - O pacote será enviado para uma outra chain.

IPTables - Filter Table - Log

- Este módulo fornece logging de pacotes.
- Opções
  - -j LOG
    - target
  - --log-level lvl
    - loga o pacote para o nível escolhido conforme o syslog.conf
    - Os níveis (lvl) podem ser: debug,info,notice,warning,err,crit,alert,emerg

Exemplo



Exemplo

- Passo a passo:
  - Definir variáveis;
  - Carregar módulos;
  - Apagar e restaurar as chains;
  - Definir políticas default;
  - Aplicar regras contra spoofings;
  - Aplicar regras contra flags;
  - Aplicar regras de conexões estabelecidas;
  - Adicionar regras desejadas.

Exemplo

- Passo a passo:
  - Definir variáveis;
  - Carregar módulos;
  - Apagar e restaurar as chains;
  - Definir políticas default;
  - Aplicar regras contra spoofings;
  - Aplicar regras contra flags;
  - Aplicar regras de conexões estabelecidas;
  - Adicionar regras desejadas.

Exemplo

MY_IP=“xxx.xxx.xxx.xxx“ #IP externo da maquina de firewall

LOOPBACK="127.0.0.0/8“ #Endereço da interface de loopback

EXTERNAL_INT=“eth0“ #interface do firewall ligada a internet

DMZ_INT=“eth1” #interface do firewall ligada à DMZ

INTERNAL_INT=“eth2” #interface do firewall ligada à intranet

CLASS_A="10.0.0.0/8" #class A private network

CLASS_B="172.16.0.0/12" #class B private network

CLASS_C="192.168.0.0/16" #class C private network

CLASS_D_MULTICAST="224.0.0.0/4" #class D multicast address

CLASS_E_RESERVED_NET="240.0.0.0/5" #class E reserved address

INTERNAL_NET=“xxx.xxx.xxx.xxx/xx”

DMZ_NET=“xxx.xxx.xxx.xxx/xx”

Exemplo

- Passo a passo:
  - Definir variáveis;
  - Carregar módulos;
  - Apagar e restaurar as chains;
  - Definir políticas default;
  - Aplicar regras contra spoofings;
  - Aplicar regras contra flags;
  - Aplicar regras de conexões estabelecidas;
  - Adicionar regras desejadas.

Exemplo

```
#Loading appropriate modules
/sbin/modprobe ip_conntrack
/sbin/modprobe ipt_LOG

#Turning on IP forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward

#Enable broadcast echo Protection
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

#Enable TCP SYN Cookie Protection
echo 1 > /proc/sys/net/ipv4/tcp_syncookies
```

Exemplo

- Passo a passo:
  - Definir variáveis;
  - Carregar módulos;
  - Apagar e restaurar as chains;
  - Definir políticas default;
  - Aplicar regras contra spoofings;
  - Aplicar regras contra flags;
  - Aplicar regras de conexões estabelecidas;
  - Adicionar regras desejadas.

Exemplo

```
#Flush any existing rules from all chains
iptables -F
#Delete all chains
iptables -X
#Reset the packet and byte counters associated with all chains
iptables -Z
```

Exemplo

- Passo a passo:
  - Definir variáveis;
  - Carregar módulos;
  - Apagar e restaurar as chains;
  - Definir políticas default;
  - Aplicar regras contra spoofings;
  - Aplicar regras contra flags;
  - Aplicar regras de conexões estabelecidas;
  - Adicionar regras desejadas.

Exemplo

```
#Flush any existing rules from all chains
iptables -F
#Delete all chains
iptables -X
#Reset the packet and byte counters associated with all chains
iptables –Z

#Set up the default policy
iptables -P OUTPUT ACCEPT
iptables -P INPUT DROP
iptables -P FORWARD DROP

#Allowing unlimited traffic on the loopback interface
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

Exemplo

- Passo a passo:
  - Definir variáveis;
  - Carregar módulos;
  - Apagar e restaurar as chains;
  - Definir políticas default;
  - Aplicar regras contra spoofings;
  - Aplicar regras contra flags;
  - Aplicar regras de conexões estabelecidas;
  - Adicionar regras desejadas.

Exemplo

```
#Refuse packets claiming to be from you.
iptables -A INPUT –i $EXTERNAL_INT -s $MY_IP -j DROP
iptables –A INPUT –i $EXTERNAL_INT –s $DMZ_NET –j DROP
iptables –A INPUT –i $RXTERNAL_INT –s $INTERNAL_NET –j DROP

#Refuse packets claiming to be from a Class A, B, C private network
#and Class D multicast and Class E reserved IP addresses
#or claiming to be from the loopback interface.
iptables -A INPUT -i eth1 -s $CLASS_A -j DROP
iptables -A INPUT -i eth1 -s $CLASS_B -j DROP
iptables -A INPUT -i eth1 -s $CLASS_C -j DROP
iptables -A INPUT -i eth1 -s $CLASS_D_MULTICAST -j DROP
iptables -A INPUT -i eth1 -s $CLASS_E_RESERVED_NET -j DROP
iptables -A INPUT -i eth1 -s $LOOPBACK -j DROP
```

Exemplo

- Passo a passo:
  - Definir variáveis;
  - Carregar módulos;
  - Apagar e restaurar as chains;
  - Definir políticas default;
  - Aplicar regras contra spoofings;
  - Aplicar regras contra flags;
  - Aplicar regras de conexões estabelecidas;
  - Adicionar regras desejadas.

Exemplo

 # Stealth Scans and TCP state flags

 # All of the bits are cleared

iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP

 # SYN and FIN are both set

iptables -A INPUT -p tcp --tcp-flags SYN,FIN SYN,FIN -j DROP

 # SYN and RST are both set

iptables -A INPUT -p tcp --tcp-flags SYN,RST SYN,RST -j DROP

 # FIN and RST are both set

iptables -A INPUT -p tcp --tcp-flags FIN,RST FIN,RST -j DROP

Exemplo

 # FIN is the only bit set, without the expected accompanying ACK

iptables -A INPUT -p tcp --tcp-flags ACK,FIN FIN -j DROP

 # PSH is the only bit set, without the expected accompanying ACK

iptables -A INPUT -p tcp --tcp-flags ACK,PSH PSH -j DROP

 # URG is the only bit set, without the expected accompanying ACK

iptables -A INPUT -p tcp --tcp-flags ACK,URG URG -j DROP

Exemplo

- Passo a passo:
  - Definir variáveis;
  - Carregar módulos;
  - Apagar e restaurar as chains;
  - Definir políticas default;
  - Aplicar regras contra spoofings;
  - Aplicar regras contra flags;
  - Aplicar regras de conexões estabelecidas;
  - Adicionar regras desejadas.

Exemplo

#Allows already stablished connections

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

Exemplo

- Passo a passo:
  - Definir variáveis;
  - Carregar módulos;
  - Apagar e restaurar as chains;
  - Definir políticas default;
  - Aplicar regras contra spoofings;
  - Aplicar regras contra flags;
  - Aplicar regras de conexões estabelecidas;
  - Adicionar regras desejadas.

Exemplo

#Allows already stablished connections

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

#liberar acesso ssh vindo da Intranet

iptables –A INPUT –s $INTERNAL_NET –p tcp –dport ssh –j ACCEPT

ou

iptables –A INPUT –i $INTERNAL_INT –p tcp –dport ssh –j ACCEPT

#liberar ping vindo da DMZ

iptables -A INPUT -s $DMZ_NET -p icmp --icmp-type ping -j ACCEPT

ou

iptables -A INPUT -i $DMZ_INT -p icmp --icmp-type ping -j ACCEPT

Exemplo

 # Libera tráfego de saída de toda a sua rede

iptables -A FORWARD -o $EXTERNAL_INT -j ACCEPT

#Liberar consulta ao servidor HTTP que esta na DMZ

iptables –A FORWARD –p tcp –d ip.do.servidor –dport http –j ACCEPT

#Bloquear tráfego da porta 445 para a intranet

Iptables –A FORWARD –d $INTERNAL_NET –dport 445 –j DROP

Iptables –A FORWARD –s $INTERNAL_NET –sport 445 –j DROP

Exemplo

 # Configurando a Chain LOG_DROP para logar e descartar os pacotes

iptables -N LOG_DROP

iptables -A LOG_DROP -j LOG --log-level notice --log-prefix "DROPPED_FIREWALL "

iptables -A LOG_DROP -j DROP

 # Logar e descartar a tentativas de acesso vindo do ip xxx.xxx.xxx.xxx

iptables –A FORWARD –p tcp –s xxx.xxx.xxx.xxx –j LOG_DROP

 # Liberar tráfego das portas altas que não sejam pedidos de conexão

iptables -A FORWARD -p tcp --dport 1024:5999 ! --syn -j ACCEPT

Referências

- http://www.netfilter.org/
- http://www.linuxguruz.com/iptables/
- http://www.dicas-l.unicamp.br/dicas-l/20030705.shtml
- Linix Firewalls – Second Edition
  - Robert L. Ziegler
  - Editora New Riders