IPTables

S. Danilo[1]

[1]Divisão de Serviços de Internet
Coordenadoria de Segurança e Serviços de Internet
Datacenter da UFPA

Belém, 2013

Agenda

Introdução à Firewall

IPTables

- Introdução
- Estrutura
  - Tabela Filter
  - Tabela Nat

Exemplos

- NetFilter
- Nat
- Outros exemplos

Definição

Um conjunto de aplicações que realiza controle de entrada e saída de uma determinada rede, sobre qualquer uma das camadas da pilha TCP/IP

- *NetFilter* - Pacotes
  - *Stateless*
    - Toma decisões baseado somente no pacote atual
    - Muito utilizado em roteadores simples
    - Baixo custo computacional
  - *Statefull*
    - Toma decisões baseado em informaões armazenadas
    - Mais utilizado em servidores
    - Alto custo computacional
- Squid (Proxy)
  - Filtro de aplicação
  - Bloqueio de url's e palavras chave

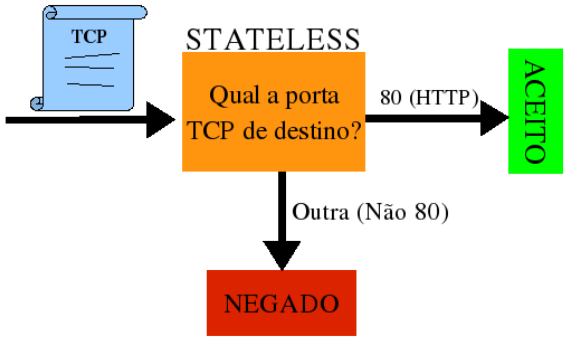
Importante

Um firewall mal configurado é pior do que não ter um firewall

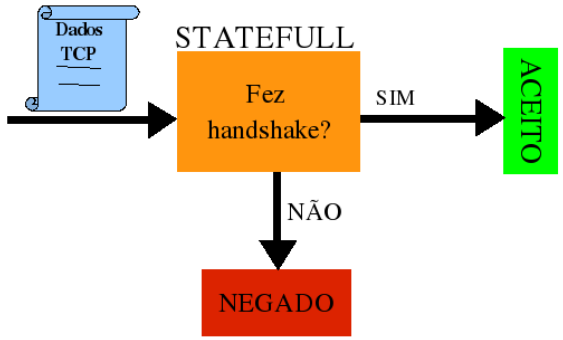
Proteção

- Firewall de *host*
  - Protege somente a máquina local
  - Regras mais robustas
- Firewall de rede
  - Protege a(s) rede(s) à qual pertence
  - Regras mais simples
  - Pode se tornar um gargalo

Proteção e Decisão



***Stateless ou estático**: para aceitar o pacote basta o firewall analisar o conteúdo do atual pacote, olhando se a porta de destino dele é ou não porta 80. Se for, aceita, se não for, nega.*



***Statefull ou dinâmico**: para aceitar o pacote é necessário que tenha ocorrido o handshake TCP. Se ocorreu, o firewall deve se lembrar, vendo em suas tabelas os pacotes anteriores. É chamado de dinâmico porque suas regras mudam de acordo com os pacotes que passam (fez handshake? Insere uma regra aceitando os dados)*

Figura 3: Filtro de pacotes estático e dinâmico

Exemplo de firewall de Host e de rede.
O firewall da máquina A está incorporado a própria máquina e deve proteger apenas ela. Já o firewall F tem como tarefa proteger toda a rede da Internet, incluindo as máquinas A, B, C, D e E. A tarefa do Firewall F é mais onerosa do que a do firewall da máquina A.

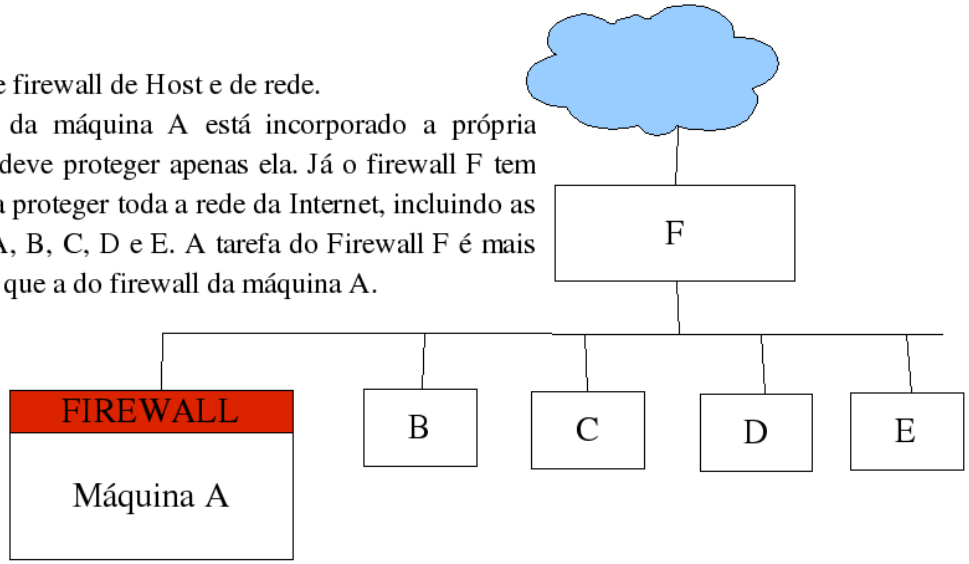


Figura 2: Exemplo firewall de rede e de Host

Ciclo de Vida e Ganchos

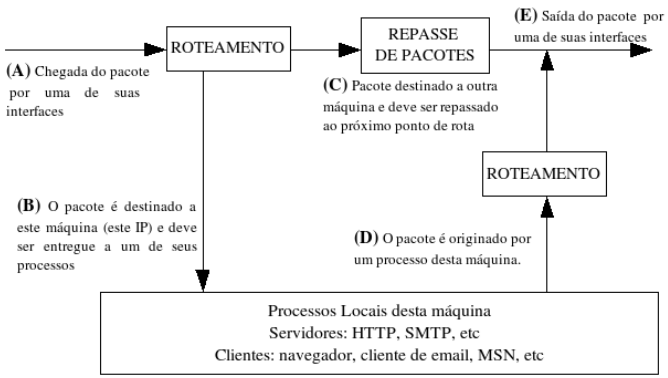


FIGURA 1: Ciclo de vida de um pacote IP dentro do kernel Linux > 2.4

./pictures/iptablesGan

Introdução

- A partir do kernel 2.4
- Manipula o *netfilter* (usuário)
- Está implementado diretamente no kernel
- Firewall *Statefull*
- Firewall de *host*/rede

Atua sobre ganchos do *netfilter*

Possui 3 tabelas

- *Filter* - Filtros simples
- Nat - Alterações nos cabeçalhos dos pacotes
- Mangle - Alterações mais específicas (TTL, TOS)

Cada tabela possui regras

Cada regra realiza uma ação

- Regras
  - INPUT - Avalia pacotes destinados ao IP local.
  - FORWARD - Avalia os pacotes repassados pela máquina.
  - OUTPUT - Avalia os pacotes gerados localmente.
  - REDIRECT - Realiza o redirecionamento de portas.
- Ações
  - REJECT - Rejeita um pacote e informa ao remetente
  - DROP - Rejeita um pacote e não informa ao remetente
  - ACCEPT - Aceita um pacote
  - LOG - Realizar o log de um pacote (/var/log/syslog ou messages)

- Listas
  - PREROUTING - Modifica o pacote antes do roteamento
  - POSTROUTING - Modifica o pacote depois do roteamento
  - OUTPUT - Modifica o pacote originado localmente antes do roteamento
- Ações
  - SNAT - Altera o endereço de origem do pacote POSTROUTING
  - DNAT - Altera o endereço de destino do pacote PREROUTING

Opções

Regras

Tabela + Opção + Regra + Dados + Ação

- Ações
  1. -P = Define uma regra padrão.
  2. -A = Adiciona uma nova regra as existentes. Esta tem prioridade sobre a -P.
  3. -I = Insere uma nova regra.
  4. -D = Apaga uma regra.
  5. -C = Faz a checagem das regras existentes.
  6. -X = Exclui uma regra específica pelo seu nome.
- Dados
  1. -i = Define a interface de entrada
  2. -o = Define a interface de saída
  3. -p = Define o protocolo
  4. -sport = Define a porta de origem
  5. -dport = Define a porta de saída

Exemplos - Netfilter

- iptables -t filter -A INPUT -p tcp -d 192.168.0.0/24 -j ACCEPT
- iptables -t filter -A OUTPUT -p tcp - s 192.168.0.0/24 -j ACCEPT
- iptables -t filter -A FORWARD -p udp -s 192.168.0.0/24 -s 192.168.1.0/24 -j ACCEPT
- iptables -t filter -A INPUT -p udp -s!192.168.1.1 -j ACCEPT

Exemplos - Nat

- iptables -t nat -A PREROUTING -i eth0 -p tcp ?dport 80 -j REDIRECT ?to- port 3128
- iptables -t nat -A PREROUTING -s 200.200.100.100 -i eth0 -j DNAT?to 192.168.0.50
- ptables -t nat -A POSTROUTING -s 192.168.0.50 -o eth0 -j SNAT ?to 200.200.100.100

Outros exemplos

Limpando regras

```
iptables -F
iptables -t nat -F
iptables -X
iptables -t nat -X
```

Monitorando trojan 's

```
TROJAN_PORTS=“12345 31336 31337 31338 3024
4092 5714 5742 2583 8787 5556 5557”
iptables -t filter -N trojans-in
for PORTA in $TROJAN_PORTS;do
iptables -A trojans-in -p tcp –sport=1024:
–dport=$PORTA -j LOG
–log-prefix “FIREWALL: Trojan $PORTA”
iptables -A trojans-in -p tcp –sport=1024: –dport=
$PORTA -j DROP
done
iptables -t filter -A INPUT -i ppp0 -j trojans-in
```