Fatec
Araras

Servidores e seus sistemas operacionais

Prof. Orlando Saraiva Júnior
orlando.saraiva@unesp.br

Firewall

Prof. Me. Orlando Saraiva Júnior

Camadas de protocolos

Fatec Araras

Modelo OSI

Aplicação
Apresentação
Sessão
Transporte
Rede
Link de Dados (Enlace)
Física

Modelo TCP/IP

Aplicação
Transporte
Internet
Interface com a Rede

Firewall

Em teoria, um firewall simplesmente bloqueia qualquer comunicação não autorizada entre os computadores da organização e computadores fora dela.

Na prática, os detalhes dependem da tecnologia de rede, da capacidade da conexão, da carga do tráfego e da política da organização.

Assim, nenhuma solução simplesmente funciona para todas as organizações, montar um firewall padronizado e eficaz pode ser difícil.

Firewall

Uma das dificuldades da montagem de firewalls surge da potência de processamento necessária. Um firewall precisa de potência de computação suficiente para examinar todas as mensagem que entram e saem. Se o firewall retarda a transmissão de um pacote em um buffer enquanto decide se permite a transferência, o firewall ficará lotado de retransmissões e o buffer ficará sobrecarregado.

Tipos de Firewall

Nível de aplicação - Este tipo de firewall analisam o conteúdo do pacote para tomar suas decisões de filtragem. Firewalls deste tipo são mais intrusivos e permitem um controle relacionado com o conteúdo do tráfego. Alguns firewalls em nível de aplicação combinam recursos básicos existentes em firewalls em nível de pacotes combinando as funcionalidade de controle de tráfego/controle de acesso em uma só ferramenta. Servidores proxy, são um exemplo deste tipo de firewall.

Tipos de Firewall

Nível de pacotes - Este tipo de firewall toma as decisões baseadas nos parâmetros do pacote, como porta/endereço de origem/destino, estado da conexão, e outros parâmetros do pacote. O firewall então pode negar o pacote (DROP) ou deixar o pacote passar (ACCEPT).

Fatec
Araras

IPTABLES

Prof. Me. Orlando Saraiva Júnior

iptables

Fatec Araras

- Especificação de portas/endereço de origem/destino
- Suporte a protocolos TCP/UDP/ICMP (incluindo tipos de mensagens icmp)
- Suporte a interfaces de origem/destino de pacotes
- Manipula serviços de proxy na rede
- Tratamento de tráfego dividido em chains (para melhor controle do tráfego que entra/sai da máquina e tráfego redirecionado.
- Permite um número ilimitado de regras por chain.
- Possui mecanismos internos para rejeitar automaticamente pacotes duvidosos ou mal formados.

iptables

Fatec Araras

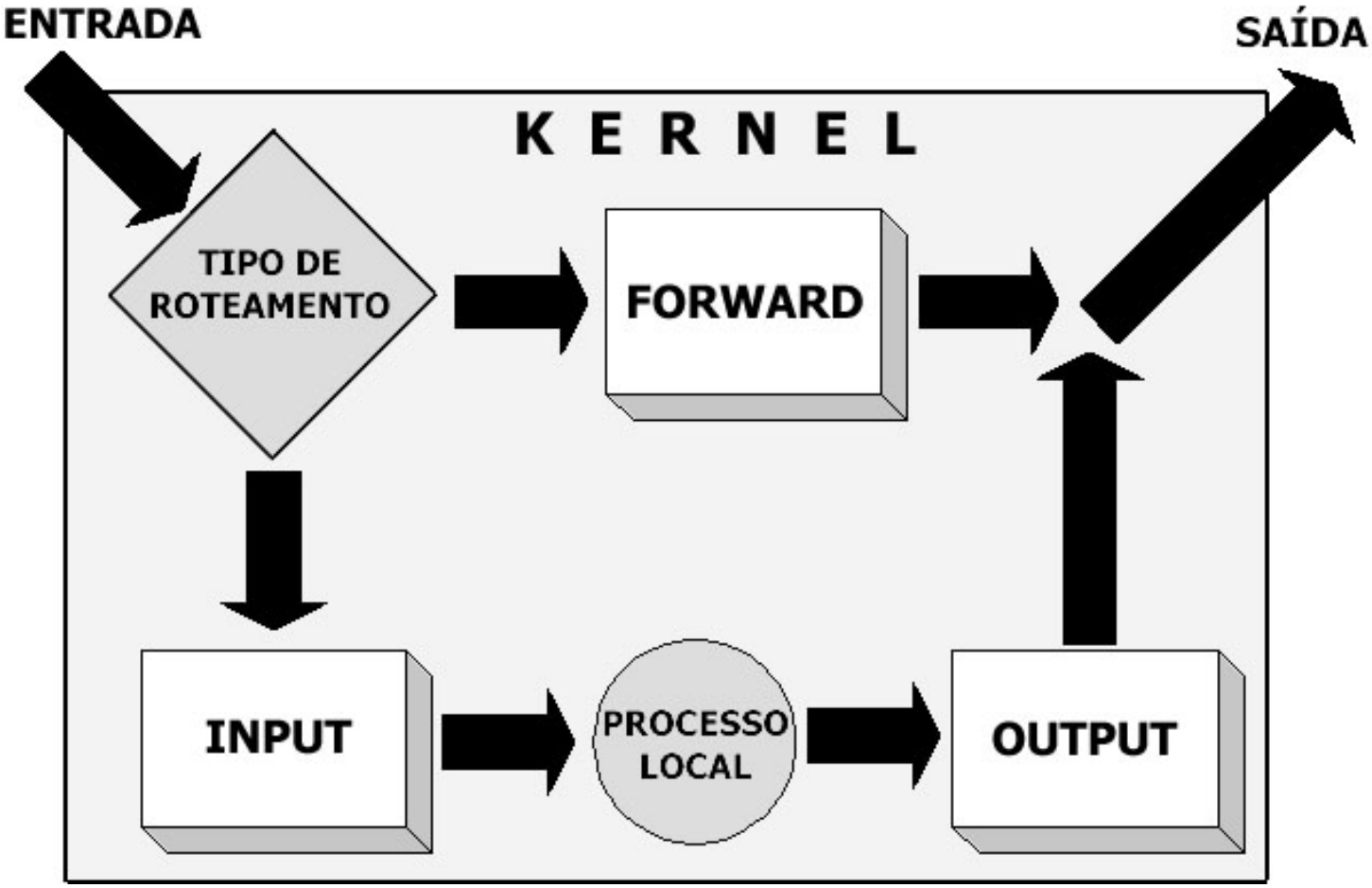
- Possui mecanismos internos para rejeitar automaticamente pacotes duvidosos ou mal formados.
- Suporte a módulos externos para expansão das funcionalidades padrões oferecidas pelo código de firewall.
- Suporte completo a roteamento de pacotes, tratadas em uma área diferente de tráfegos padrões.
- Suporte a especificação de tipo de serviço para priorizar o tráfego de determinados tipos de pacotes.
- Permite especificar exceções para as regras ou parte das regras.

iptables

Fatec Araras

- Suporte a detecção de fragmentos
- Permite enviar alertas personalizados ao syslog sobre o tráfego aceito/bloqueado.
- Redirecionamento de portas
- Masquerading
- Suporte a SNAT /DNAT (modificação do endereço de origem /destino das máquinas para um único IP ou faixa de IP's).
- Contagem de pacotes que atravessaram uma interface/regra.
- Limitação de passagem de pacotes/conferência de regra (muito útil para criar proteções contra, syn flood, ping flood, DoS, etc.

iptables


ENTRADA
SAÍDA
K E R N E L
TIPO DE ROTEAMENTO
FORWARD
INPUT
PROCESSO LOCAL
OUTPUT

iptables

Fatec Araras

Sintaxe básica:

iptables (-t <tabela>) <opção> <chain> <regra> -j <ação>

iptables

Fatec Araras

tabelas:
- filter (padrão)
- nat
- mangle

opções:
- -A (adiciona uma regra ao fim da lista)
- -I (inclui uma regra no início da lista)
- -D (deleta uma regra)
- -L (<--line-numbers>) (lista todas as regras)
- -F (limpa a lista)

iptables

Fatec Araras

chains (da tabela filter):
•INPUT (pacotes que chegam com destino ao host)
•OUTPUT (pacotes que saem do host)
•FORWARD (pacotes que passam pela máquina, a qual não é o destinatário)

ações:
•ACCEPT (aceita o pacote)
•REJECT (rejeita o pacote e fecha conexão)
•DROP (descarta o pacote e não retorna nada ao emissor)
•LOG (registra a incidência no arquivo padrão de log)

iptables

Fatec Araras

Opções básicas de regras:

- -p <protocolo (tcp, udp ou icmp)>
- --sport <porta de origem>
- --dport <porta de destino>
- -i <interface de entrada>
- -o <interface de saída>
- -s <endereço IP de origem>
- -d <endereço IP de destino>

iptables

O operador “!” indica a negação e inverte a regra.

iptables -A INPUT -p tcp –dport 22 -s ! 200.145.39.170 -j DROP

A regra acima diz os pacotes de entrada com destino ao serviço SSH (22 TCP) que não forem originários da máquina 200.145.39.170 serão descartados.

iptables

Fatec Araras

Quanto aos parâmetros, a filosofia padrão para as regras é: para qualquer item que não for mencionado, será assumido como “qualquer um”.

iptables -A FORWARD -p udp -j DROP

Essa regra se aplica a todas as portas de origem e destino, interfaces de entrada e saída e endereços IP de origem e destino.

iptables

Outros exemplos:

#iptables -A FORWARD -p icmp --icmp-type echo-request -m limit --limit 1/s -j ACCEPT
#iptables -A FORWARD -p icmp --icmp-type echo-request -j DROP

Contra Ping da morte

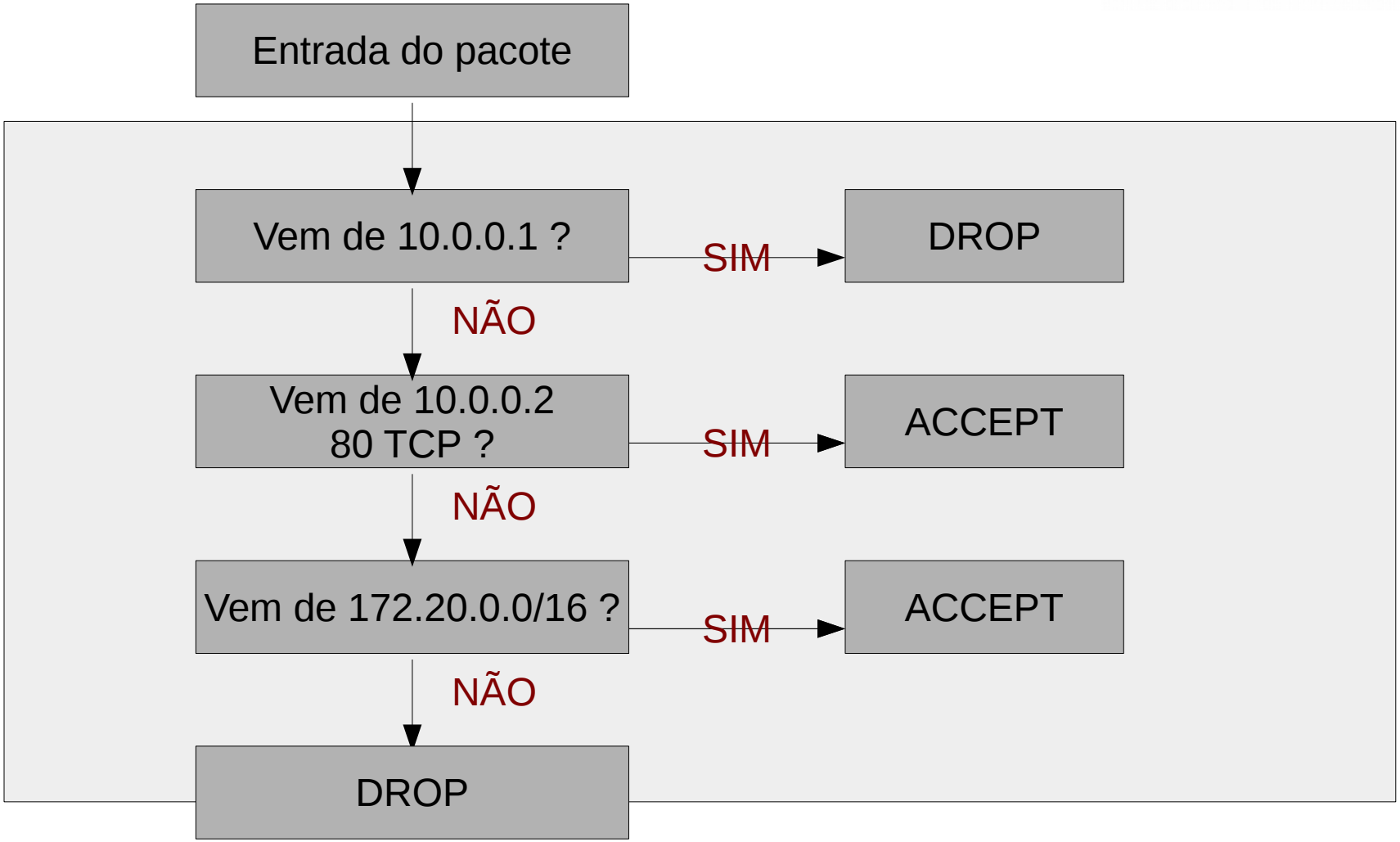
Política de segurança

Fatec Araras

Exemplo de uma política de segurança simples:

```
# iptables -P INPUT DROP
# iptables -A INPUT -s 10.0.0.1 -j DROP
# iptables -A INPUT -s 10.0.0.2 -p tcp --dport 80 -j ACCEPT
# iptables -A INPUT -s 172.20.0.0/16 -j ACCEPT
```

Política de segurança



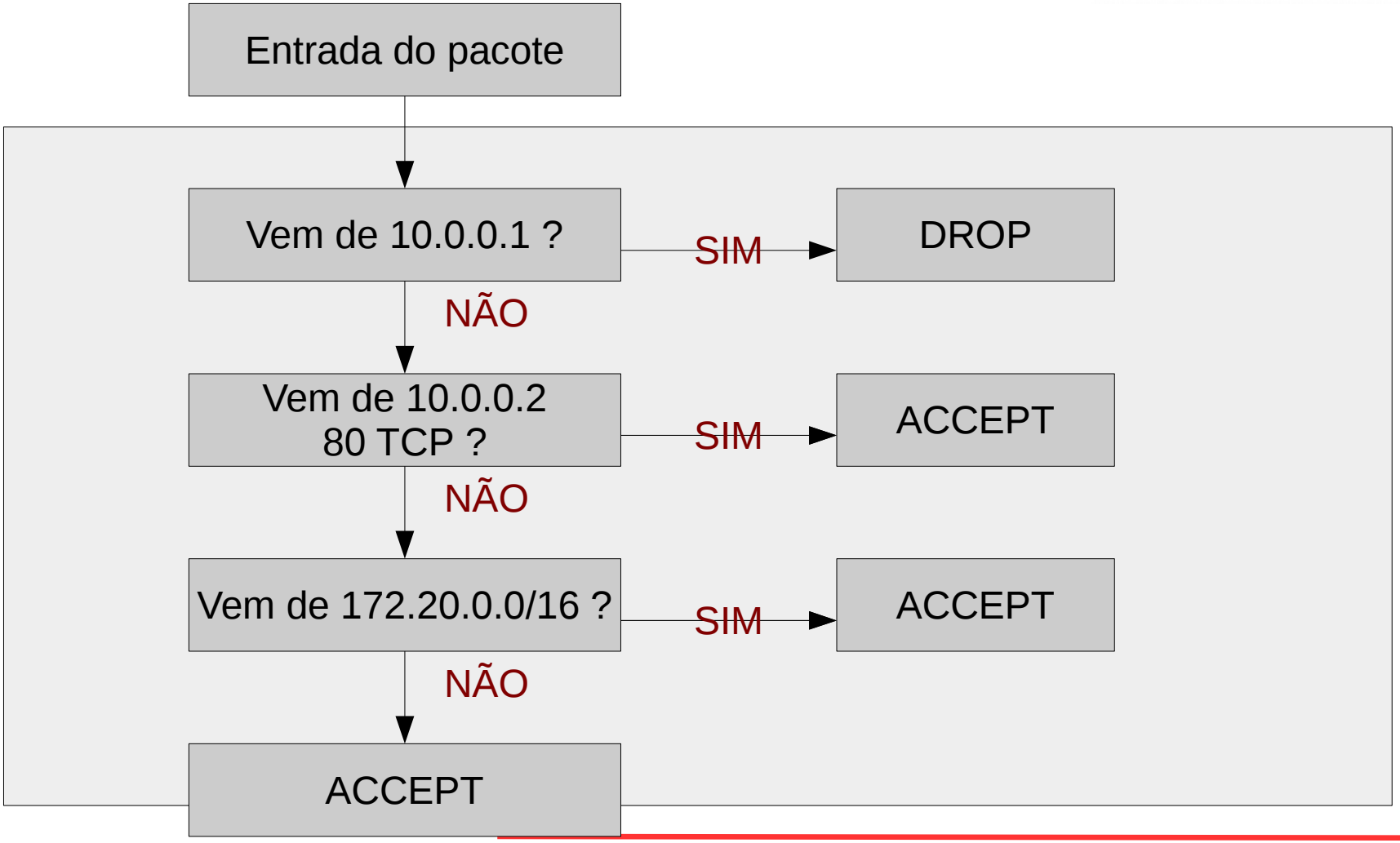
Política de segurança

Fatec Araras

Mudança na política de segurança:

```
# iptables -F
# iptables -P INPUT ACCEPT
# iptables -A INPUT -s 10.0.0.1 -j DROP
# iptables -A INPUT -s 10.0.0.2 -p tcp --dport 80 -j ACCEPT
# iptables -A INPUT -s 172.20.0.0/16 -j ACCEPT
```

Política de segurança



Fatec
Araras

Hora da prática

Prof. Orlando Saraiva Júnior
orlando.saraiva@unesp.br