Linux para Infraestrutura

Prof. André Nasserala

nasserala@gmail.com

Segurança da Informação

- Os atributos básicos, segundo os padrões internacionais, são os seguintes:

- **Confidencialidade;**

- **Integridade;**

- **Disponibilidade;**

Segurança da Informação

- O suporte para as recomendações de segurança pode ser encontrado em controles físicos e lógicos;
- Controles Físicos:

1. Portas;
2. Trancas;
3. Paredes;
4. Blindagens;
5. Guardas;

Segurança da Informação

- **<u>Controles Lógicos:</u>**

- Senhas;
- Sistemas Biométricos;
- Cartões Inteligentes;
- Firewall's.

Conceito de Firewall

- "...Um firewall é um dispositivo gerencia trafego entre redes distintas, e protege uma rede privada de uma rede pública (por exemplo, Internet)..."
- Como exemplo, o firewall deve acessar ambas redes (interna e a Internet) mas a rede interna não pode acessar diretamente a Internet e vice versa;
- São mecanismos de segurança que protegem os recursos de hardware e software da empresa dos perigos aos quais o sistema está exposto.

Tarefas de um Firewall

- Um firewall é um checkpoint, ou seja, ele é um foco para as decisões referentes à segurança, é o ponto de conexão com o mundo externo, tudo o que chega à rede interna passa pelo firewall;

- **São tarefas de um Firewall:**

1. Aplicar a política de segurança;
2. Logar eficientemente as atividades na Internet;
3. Limitar a exposição da empresa ao mundo externo.

Tarefas de um Firewall

- Não são tarefas de um Firewall:

1. Um firewall não pode proteger a empresa contra usuários internos mal intencionados;

"...se o inimigo mora dentro da própria casa, certamente não será esta uma morada segura..."

Tarefas de um Firewall

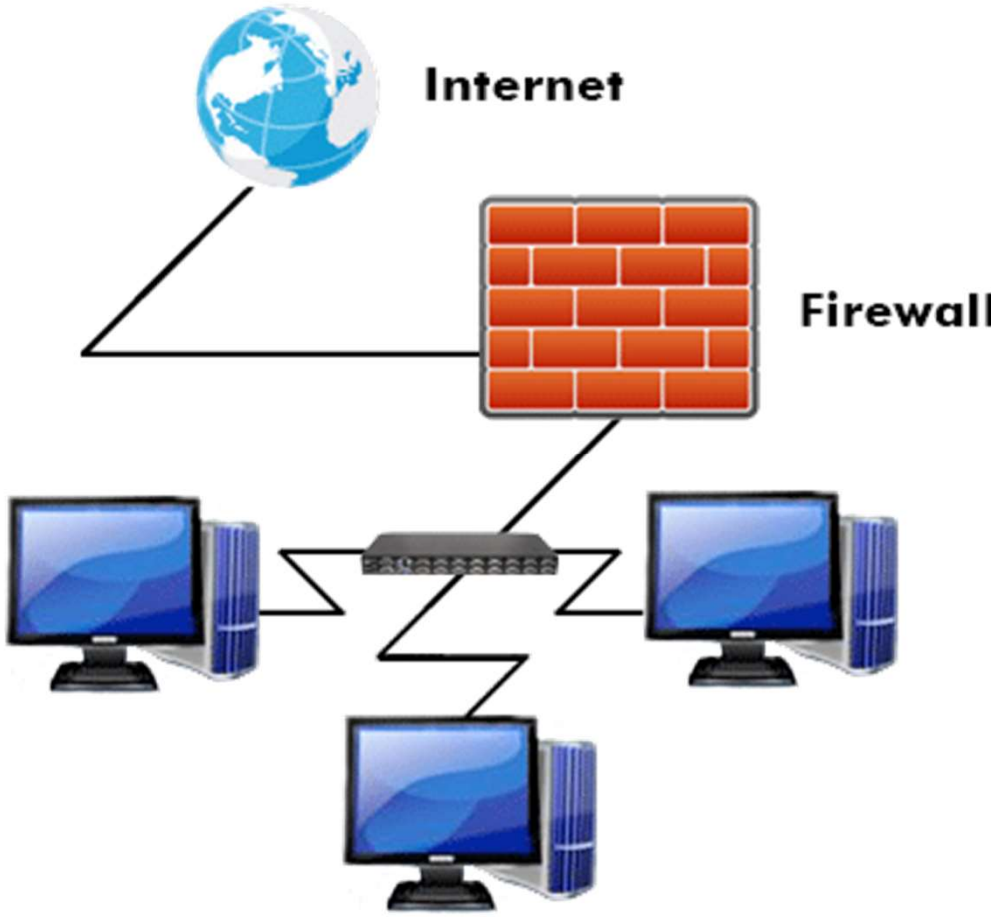
- Não são tarefas de um Firewall:

2. Um firewall não pode proteger a empresa de conexões que não passam por ele;

"do que adianta colocar uma porta da frente em aço maciço e uma dúzia de fechaduras se alguém deixou a porta da cozinha aberta?"

Tarefas de um Firewall

- **<u>Não são tarefas de um Firewall:</u>**
- Um firewall não pode proteger contra ameaças completamente novas;
- Um firewall não pode proteger contra vírus.



Porque usar Firewall?

- Dentre vários motivos que podemos citar para uso de Firewalls, destacamos quatro:

- Alto índice de ataques a redes;
- Necessidade de controle de trafego;
- Garantir integridade aos serviços;
- Alta demanda dos serviços da Internet;

Princípios Básicos

- Sobre Firewalls existem 3 princípios básicos:

- Toda solicitação chega ao Firewall;
- Somente tráfego autorizado passa pelo Firewall;
- O próprio Firewall deve ser imune a penetração;

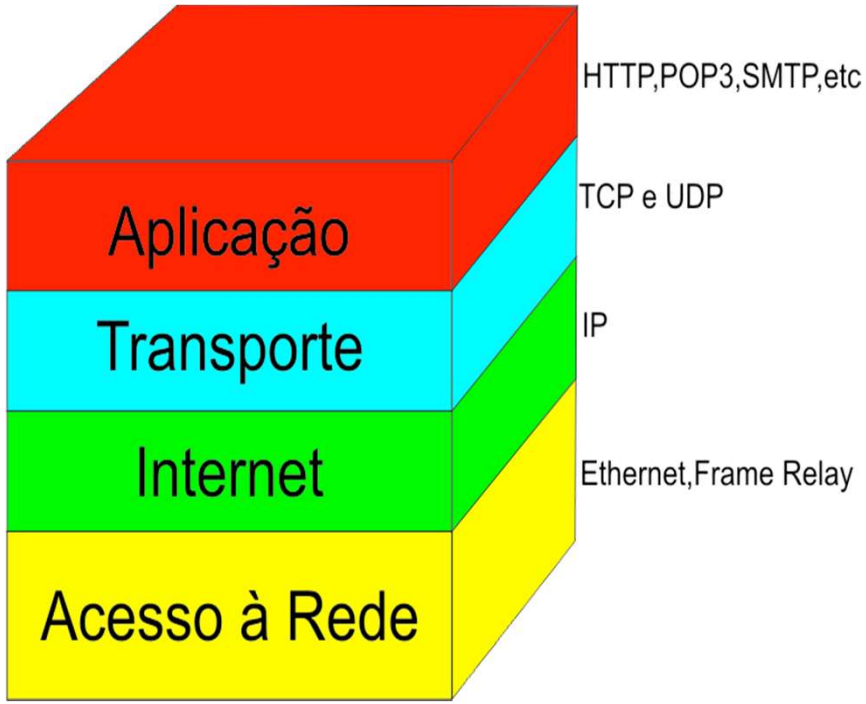
Tipos de Firewall(Níveis)

- Existem 2 tipos clássicos de Firewalls:
- Firewall Nível de Pacotes:
  - Opera nas camadas baixas do modelo OSI(Física, Enlace, Rede e Transporte);
  - Possibilidade de filtragem por protocolos das camadas baixas: UDP, TCP e ICMP;
  - Toma as decisões baseadas nos parâmetros do pacote, como porta/endereços de origem/destino;
  - Exemplo de firewall nível de pacote: Netfilter/Iptables(Forma Nativa);

Tipos de Firewall(Níveis)

- Firewall Nível de Pacotes(opções de filtragem:

- Endereço IP de origem;
- Endereço IP de destino;
- Protocolos TCP , UDP e ICMP;
- Portas TCP ou UDP origem;
- Portas TCP ou UDP destino;
- Tipo de mensagem ICMP.



Tipos de Firewall(Níveis)

- **Firewall Nível de Aplicação:**
- Este tipo de firewall analisam o conteúdo do pacote para tomar suas decisões de filtragem;
- Firewalls deste tipo precisam de “mais hardware”, pois analisam o conteúdo de tudo que passa por ele, 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, como o Squid, são um exemplo deste tipo de firewall.

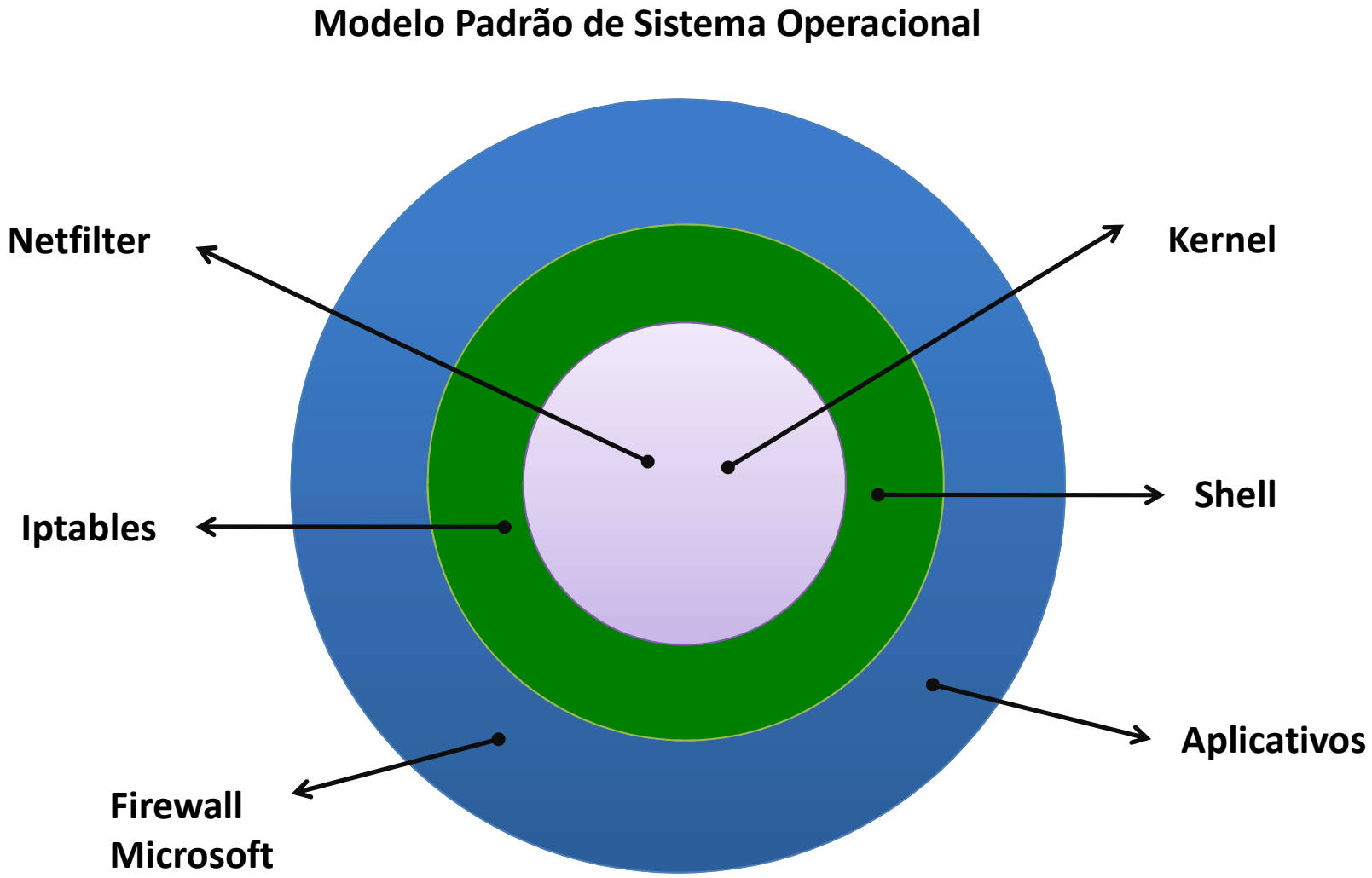
Tipos de Firewall(Níveis)

- **<u>Firewall Nível de Aplicação(Filtragem Exemplos):</u>**
- Filtragem por conteúdo de palavra não permitida em site WEB;
- Reconhecimento através da assinatura do pacote(conteúdo), de protocolos da camada de aplicação: P2P, DNS, SSH, HTTP, etc;
- Filtragem por usuário de acesso a sistemas ou Internet;
- Bloqueio de SPAM's;
- Criação de Listas de Acesso (ACL's).

Firewall em Linux

- O Netfilter é um módulo que fornece ao sistema operacional Linux as funções de firewall, NAT e log de utilização de rede de computadores;
- iptables é o nome da ferramenta do espaço do usuário que permite a criação de regras de firewall e NATs;
- Apesar de, tecnicamente, o iptables ser apenas uma ferramenta que controla o modulo netfilter, o nome "iptables" é frequentemente utilizado como referência ao conjunto completo de funcionalidades do netfilter;
- O iptables é parte de todas as distribuições modernas do Linux.

Firewall em Linux



Firewall em Linux Características

- Especificação de portas/endereço de origem/destino;
- Suporte a protocolos TCP/UDP/ICMP;
- Suporte a interfaces de origem/destino de pacotes;
- Manipula serviços de proxy na rede;
- Tratamento de tráfego dividido em chains/cadeias (para melhor controle do tráfego que entra/sai da máquina e tráfego redirecionado;
- Permite um número ilimitado de regras por chain;
- Muito rápido, estável e seguro;

Firewall em Linux Características

- 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;

Tabelas do Netfilter

- O nome iptables vem do fato de internamente o iptables funcionar manipulando tabelas do netfilter, cada uma especializada num tipo de tratamento de pacotes;

1. FILTER: nesta tabela cabem as regras responsáveis pela filtragem de pacotes;
2. NAT: mudanças nos cabeçalhos dos pacotes (incluindo NAT e IP Masquerade);
3. MANGLE: Especificação de tipo de serviço para priorizar o trafego;

- Portanto, dependendo do que se deseja fazer com um pacote em especifico, existe uma tabela adequada para tal.

Cadeias/Chains

- No iptables, existem diversas cadeias, a cada uma associado um certo tipo de tráfego. São elas:

- **PREROUTING**: tráfego ingressante na máquina(NAT e MANGLE);
- **INPUT** : tráfego ingressante na maquina(FILTER e MANGLE);
- **FORWARD**: tráfego passante pela máquina(FILTER e MANGLE);
- **OUTPUT**: tráfego de saída(NAT,MANGLE e FIL TER);
- **POSTROUTING**: tráfego que sai da máquina(NAT e MANGLE);

Trava de Segurança

- A cadeia FORWARD tem um tratamento especial no kernel do Linux, e vem com uma trava fora do firewall, que por padrão bloqueia tráfego por ela;
- Para permitir seu funcionamento, é necessário configurar o seguinte parâmetro da kernel do Linux:
- net.ipv4.ip_forward=1
- Ativando:
- echo "1" > /proc/sys/net/ipv4/ip_forward

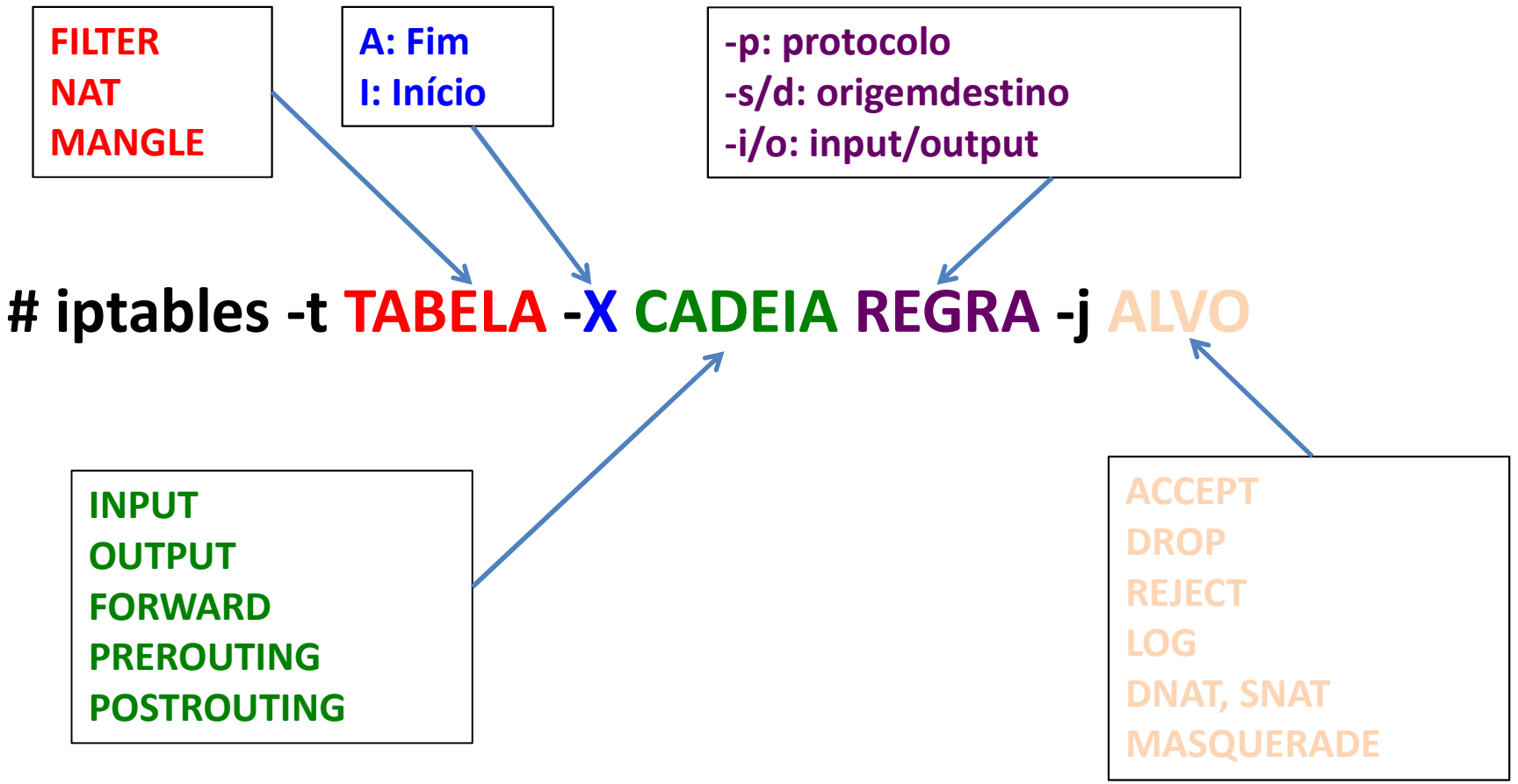
Regras

- Dada uma cadeia ou tabela em especifico, é necessário o uso de regras para selecionar em quais pacotes uma dita ação irá atuar;
- As regras gerais são:
- -p PROTOCOLO (tcp, udp, icmp,...);
- -s ENDEREÇO (192.168.0.23);
- -d ENDEREÇO (172.16.0.0/16);
- -i INTERFACE (eth1,ethx);
- -o INTERFACE (eth1,ethx);
- Obs: Nem todas as regras se aplicam a todas as cadeias.

Alvo

- Especifica a ação a ser tomada quando um pacote casar com uma dada regra de seleção. As ações padrões são:
- ACCEPT: aceita o pacote;
- DROP: ignorar completamente o pacote;
- REJECT: rejeita o pacote;
- LOG: Manda os dados do pacote para o syslog;
- DNAT: Altera o endereço de destino;
- SNAT: Altera o endereço de origem;
- MASQUERADE: Mascara o pacote.

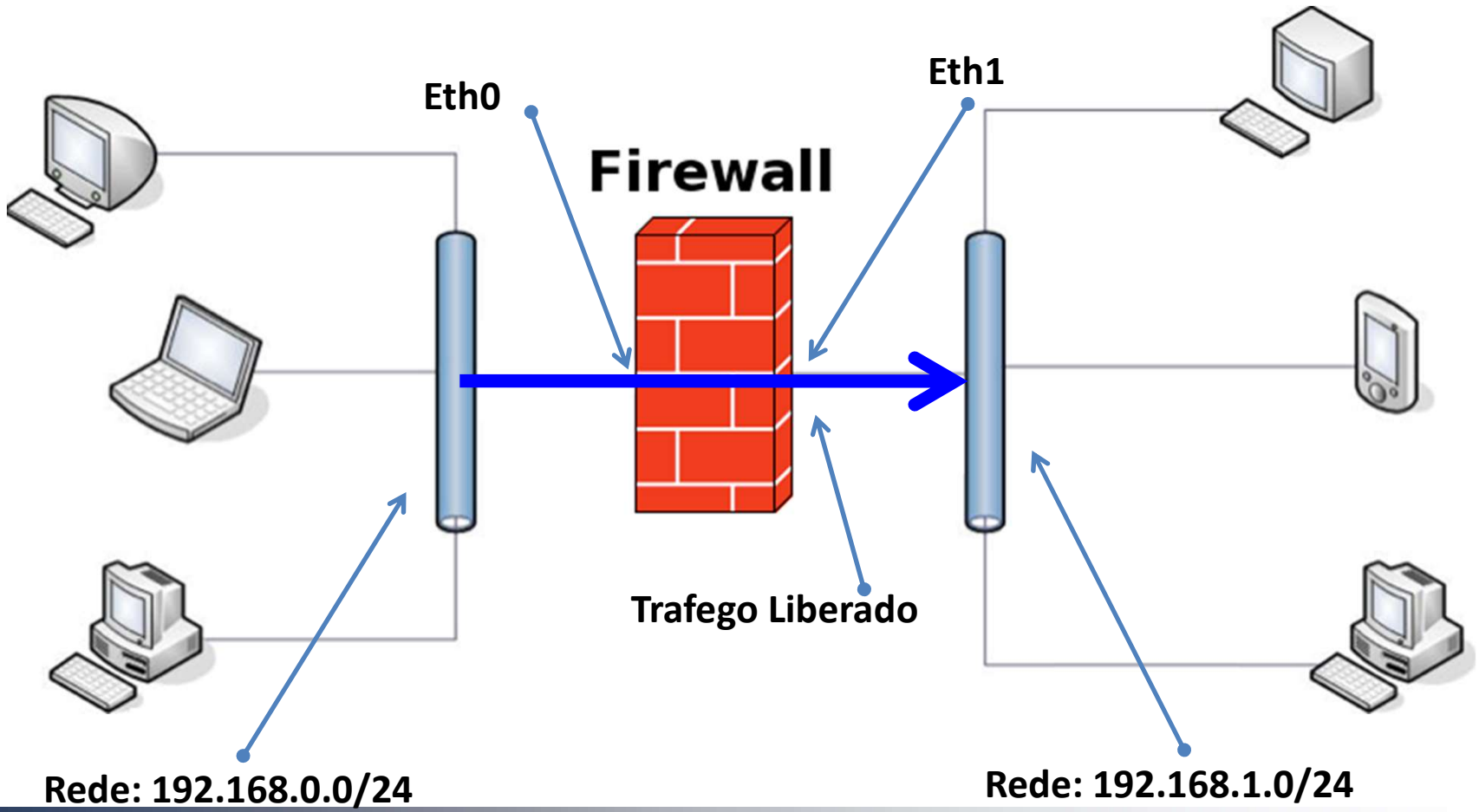
Escrevendo Regra



Escrevendo Regra

- Por exemplo, para permitirmos que a rede 192.168.0.0/24 ligada a interface de rede eth0 possa enviar trafego a rede 192.168.1.0/24 conectada a interface de rede eth1, devemos escrever a seguinte regra:
- **# iptables -t filter -A FORWARD -s 192.168.0.0/24 -d 192.168.1.0/24 -i eth0 -o eth1 -j ACCEPT**
- Ou:
- **# iptables -A FORWARD -s 192.168.0.0/24 -d 192.168.1.0/24 -i eth0 -o eth1 -j ACCEPT**
- A tabela Filter é a única que pode ser omitida na regra.

Escrevendo Regra



Política Padrão

- No caso de não existir alguma regra especifica para um determinado trafego, é possível configurar uma politica padrão para cada cadeia / tabela;
- Esta politica aponta um alvo a ser executado, caso nenhuma regra terminativa nesta mesma cadeia / tabela atue no pacote.
- Para definir uma politica padrão:
- **# iptables -t TABELA -P CADEIA –j ALVO**
- Por exemplo:
- **# iptables -t filter -P OUTPUT ACCEPT**
- Irá permitir tráfego livre por padrão na cadeia OUTPUT da tabela filter.

Pequeno Script de Firewall

```
#!/bin/bash
echo "1" > /proc/sys/net/ipv4/ip_forward
iptables –F
Iptables -t nat -F
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables –A INPUT -i localhost –j ACCEPT
iptables –A INPUT –p tcp --dport 22 –j ACCEPT
iptables -t nat -A PREROUTING -i eth0 -p tcp -- dport 80 -j
    REDIRECT --to-port 3128
iptables -t nat -A POSTROUTING -j MASQUERADE
```

```
#!/bin/bash
echo "1" > /proc/sys/net/ipv4/ip_forward
iptables -F
iptables -t nat -F
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -s 192.168.0.0/24 -d 192.168.1.0/24 -j ACCEPT
iptables -A FORWARD -s 192.168.1.0/24 -d 192.168.0.0/24 -j ACCEPT
iptables -t nat -A PREROUTING -p tcp --dport 21 -j DNAT --to 192.168.0.10:21
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 3128
iptables -t nat -A POSTROUTING -p tcp --dport 21 -j MASQUERADE
iptables -t nat -A POSTROUTING -p udp --dport 5060 -j MASQUERADE
iptables -t nat -A POSTROUTING -s 192.168.1.11 -p tcp --sport 80 -j SNAT --to 200.103.16.22:80
~
~
~
~
~
~
~
```

```
[root@localhost ~]# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:http

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  192.168.0.0/24       192.168.1.0/24
ACCEPT     all  --  192.168.1.0/24       192.168.0.0/24
[root@localhost ~]# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  anywhere             anywhere            tcp dpt:ftp to:192.168.0.10:21
REDIRECT   tcp  --  anywhere             anywhere            tcp dpt:http redir ports 3128

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  tcp  --  anywhere             anywhere            tcp dpt:ftp
MASQUERADE  udp  --  anywhere             anywhere            udp dpt:sip
SNAT       tcp  --  192.168.1.11         anywhere            tcp spt:http to:200.103.16.22:80
```

Atividade

1. Qual a diferença entre Firewall de pacotes e de aplicação?
2. Para que serve a “trava de segurança” do Linux?
3. Qual a diferença entre Netfilter e Iptables?
4. Quais são e para, e para que servem as tabelas do Netfilter?
5. Qual a diferença entre Cadeias e Tabelas? E o que é o alvo?
6. Escreva uma regra que bloqueie(DROP ou REJECT), todo trafego passante UDP na porta 500 para o destino 200.252.28.2.
7. Escreva um regra que aceite o o trafego SSH para o firewall vindo da origem 201.15.122.36 na interface eth1.
8. Escreva uma regra que bloqueie o ping para o destino www.uol.com.br de qualquer origem.
9. Escreva uma regra que impeça o firewall de utilizar a porta TCP 2222 para o destino 187.5.166.3 para estabelecer uma conexão.
10. Escreva um pequeno script de firewall adequado as necessidades de compartilhar internet, apenas com a cadeia INPUT restrita ao loopback e SSH.