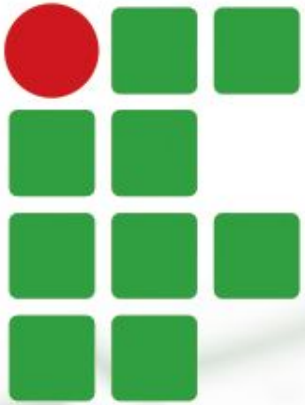


INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Admin. Serviços de Redes

- Firewall IPTables -

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Firewall

- ***Firewall*** é uma ferramenta, em forma de ***Software*** ou equipamento dedicado (***Appliance***), que tem por objetivo **aplicar políticas de segurança** para acesso a máquinas ou redes através do **monitoramento do tráfego**.

Firewall

- A palavra chave é **SEGURANÇA**!
  - Quais serviços da rede estão **liberados**?
  - Quais serviços da rede estão **bloqueados**?
  - Que tipo de tráfego poderá **entrar** na rede?
  - Que tipo de tráfego poderá **sair** da rede?
  - Quais **máquinas** terão acesso e a quais recursos?
  - Quais máquinas **nunca** deverão ter acesso?
  - Qual **conteúdo** pode atravessar uma rede?
  - *etc...*

Firewall

- A palavra chave é **SEGURANÇA**!
  - Quais serviços da rede estão **libera**
  - **[illegible]** deverão ter acesso?
  - Qual **conteúdo** pode atravessar uma rede?
  - *etc...*

Um Firewall pode especificar **que tipos de protocolos e serviços da rede serão disponibilizados**, tanto externa quanto internamente.

Firewall

- Existem basicamente dois tipos de Firewall:

- **Firewall de Aplicação / Content-Proxy**
  - Analisa o **conteúdo** dos pacotes para tomar as decisões de filtragem.
  - Vantagem: Permite controle mais refinado, levando em consideração o tipo de conteúdo do tráfego.
  - Desvantagem: Mais intrusivo.
  - Ex.: **Squid, Privoxy, TinyProxy…**

Firewall

- Existem basicamente dois tipos de Firewall:

- **Firewall de Pacotes**
  - Analisa parâmetros dos pacotes (p.e. endereços de origem/destino) para tomar as decisões de filtragem.
  - Vantagem: Facilidade para definição de regras, flexibilidade e rapidez no processamento.
  - Ex.: **IPtables**, **UFW**, ...

IPTABLES

- **IPTABLES**
  - Firewall nativo a partir do Kernel Linux 2.4.
  - Suporta filtragem por:
    - Interfaces de origem e destino.
    - Endereços de IP ou Portas origem e destino.
    - Protocolos TCP, UDP e ICMP.
  - NAT (*Source Nat e Destination NAT*).
  - Redirecionamento de Portas.
  - Marcação/Rotulação de Pacotes.

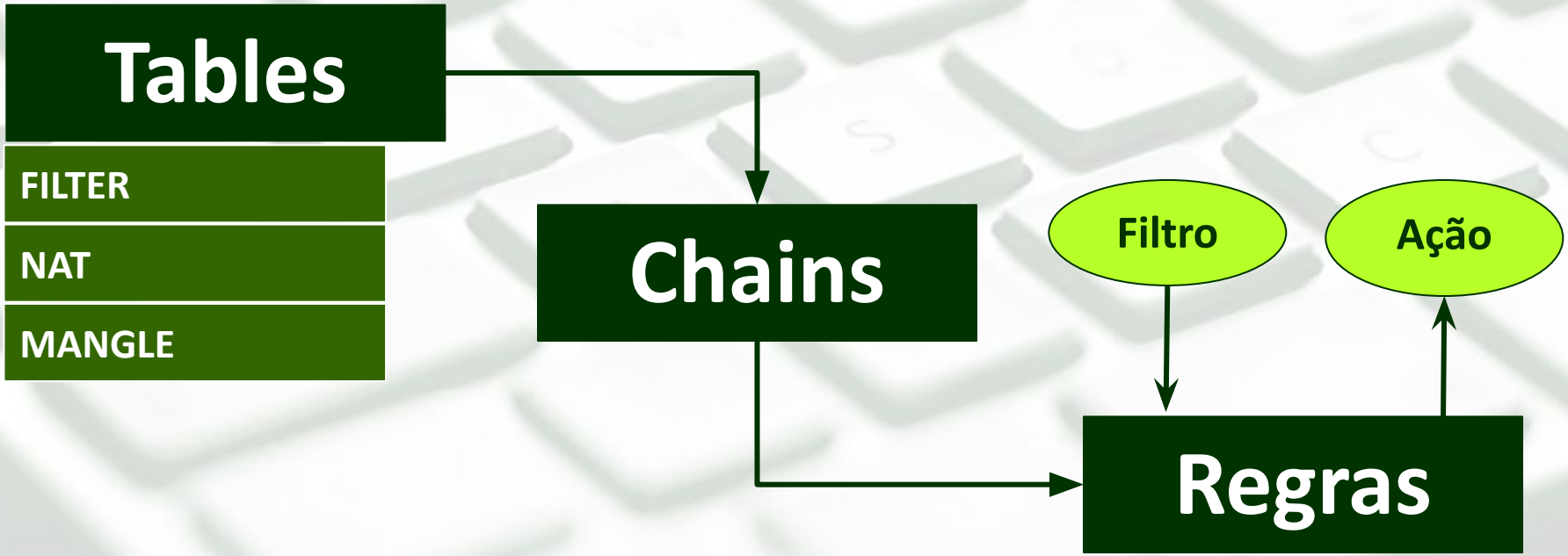
IPTABLES

- **IPTABLES**
  - Tratamento do tráfego dividido em **CHAINS.**
  - Número ilimitado de **REGRAS** por cada CHAIN.
  - Suporta módulos externos (FTP, IRC, ...).
  - Logs personalizáveis.
  - Suporte IPv6 (*IP6tables*).
  - Rápido, Estável e Seguro!

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

IPTABLES

- Três elementos básicos são fundamentais para que possamos compreender a organização lógica do IPTABLES: ***Tables, Chains e Regras***.



Tables

- **TABELAS**
  - As regras de monitoramento do IPtables são associadas a **TABELAS** e suas respectivas **CHAINs** (cadeias ou *listas*).
  - Existem três **TABELAS** disponíveis no IPTABLES:
    - **FILTER** (tabela padrão => filtragem de pacotes)
    - **NAT** (tradução de endereços IP e portas)
    - **MANGLE** (marcação de pacotes)

Chains

- **CHAIN** (Cadeia ou Lista)
  - As regras são organizadas em listas (**CHAINs**) que correspondem aos **possíveis fluxos de tráfego**.
  - *P.Ex… Existem três CHAINs na tabela **FILTER**:*
    - **INPUT**
    - **OUTPUT**
    - **FORWARD**

Sempre em letras maiúsculas

- ***IPTables*** também permite que o SysAdmin crie suas próprias CHAINs para organizar melhor as regras.

Regras

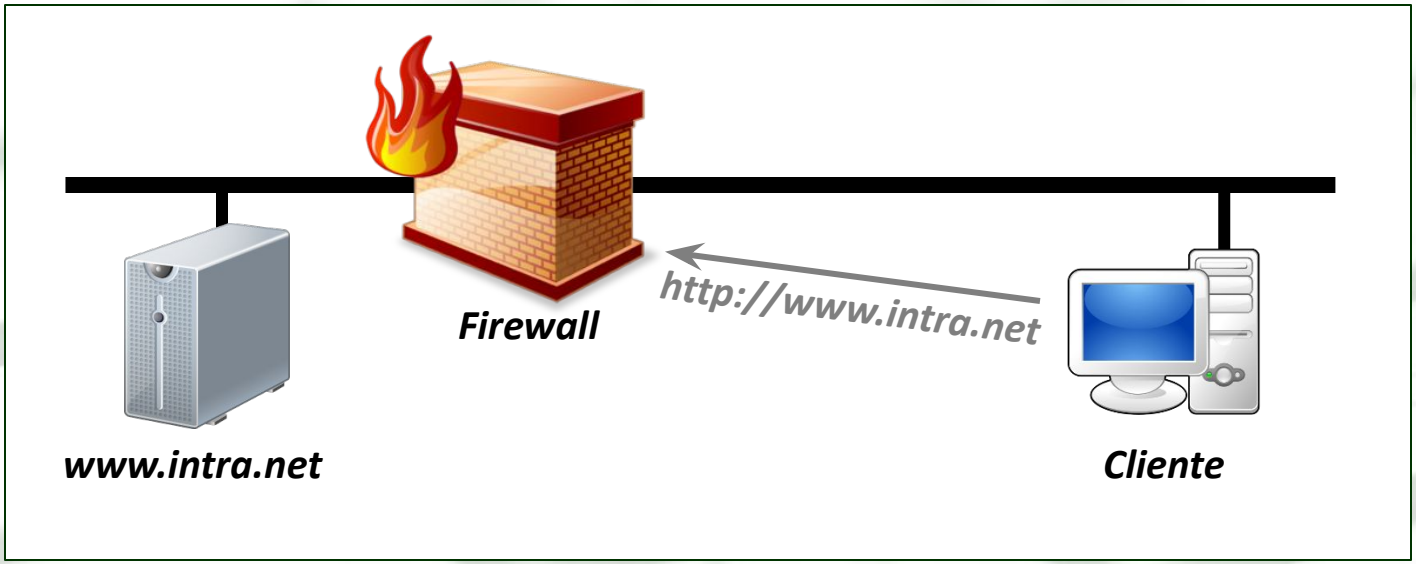
- **REGRA**
  - Indica uma **ação** a ser realizada para um **filtro** determinado de pacotes.
  - *Exemplos:*
    - **Aceitar** pacotes **provenientes da rede X**.
    - **Rejeitar** pacotes cujo **destino é a porta Y**.

ATENÇÃO

As regras são processadas na ordem em que são inseridas.

Regras

- *Exemplo do Processamento de Regras*

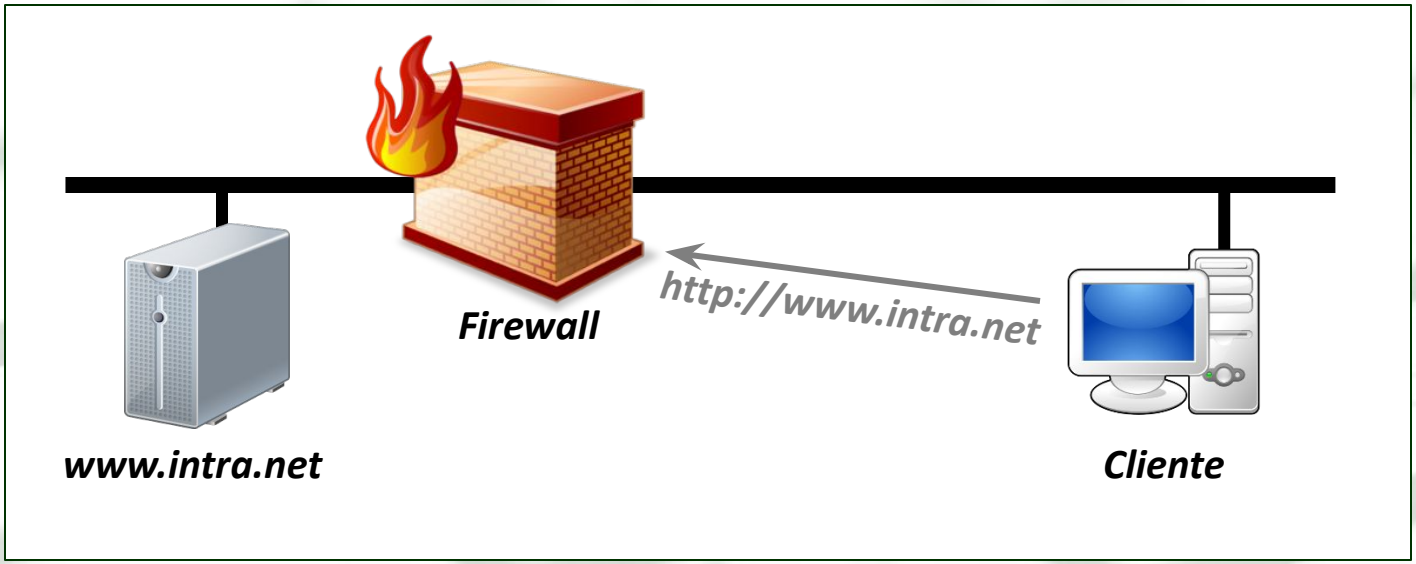



```
R1: Rejeite todos os pacotes destinados ao Web-Server.
R2: Aceite pacotes de conexão cujo destino é a porta 80.
```

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Regras

- *Exemplo do Processamento de Regras*



R1: Aceite pacotes de conexão cujo destino é a porta 80.
R2: Rejeite todos os pacotes destinados ao Web-Server.

Tabela Filter

- **Tabela FILTER**
  - **É a tabela padrão do IPTables.**
  - Armazena regras que **filtram pacotes** que se **originam**, **destinam** ou **atravessam** o host.

- Três CHAINs padrões:
  - **INPUT => Pacotes destinados ao *host*.**
  - **OUTPUT => Pacotes enviados pelo *host*.**
  - **FORWARD => Pacotes que atravessam o *host*.**

Tabela NAT

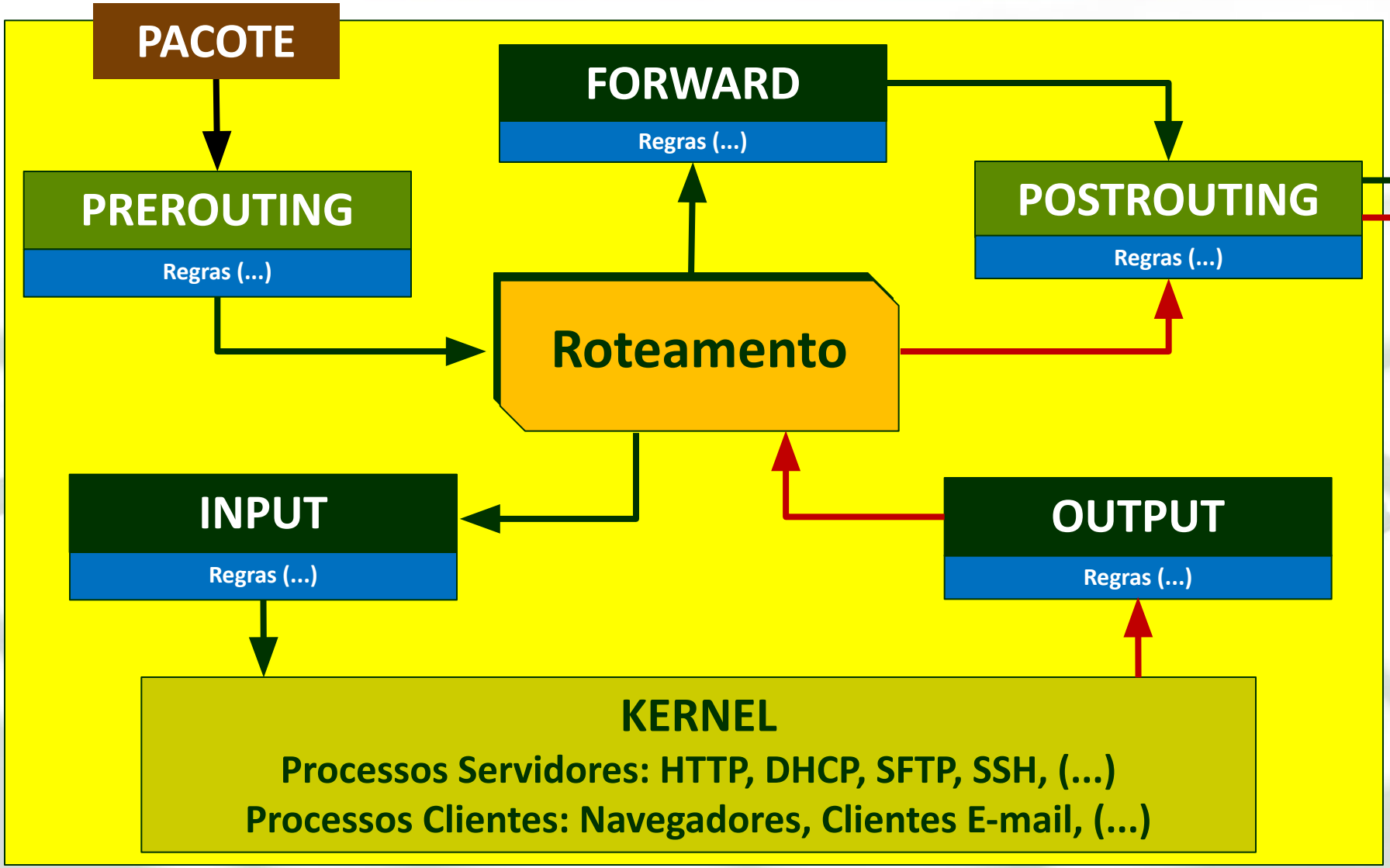
- **Tabela NAT (*Network Address Translation*)**
  - Armazena regras para **alteração de endereços IP ou portas de origem / destino**.
  - *P.ex.: Source NAT, Destination NAT, Redirecionamento de Portas, Proxy Transparente, etc…*
- Três CHAINs padrões:
  - **PREROUTING => Antes de realizar o roteamento.**
  - **POSTROUTING => Após realizar o roteamento.**
  - **OUTPUT => Pacotes enviados pelo host (e antes de realizar roteamento).**

Tabela Mangle

- **Tabela Mangle**
  - Armazena regras para realizar alterações (marcações) em cabeçalhos de pacotes.
    - *P.ex.: Definir políticas de prioridade, rotular pacotes para serem analisados por outro software, etc…*
  - CHAINs padrões:
    - **INPUT**
    - **OUTPUT**
    - **FORWARD**
    - **PREROUTING**
    - **POSTROUTING**

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Chains IPtables



Configuração de Regras

- Sintaxe padrão para configuração de regras no IPtables:

```
# iptables -t <tabela> -A <chain> [parametro] -j <ação>
```

Configuração de Regras

- Sintaxe padrão para configuração de regras no IPtables:

```
# iptables -t <tabela> -A <chain> [parametro] -j <ação>
```

- Informa em que tabela a regra será adicionada.
- Este parâmetro pode ser omitido caso se trate da tabela padrão "**filter**"
- Outras opções:
  `-t nat`
  `-t mangle`

Configuração de Regras

- Sintaxe padrão para configuração de regras no IPtables:

```
# iptables -t <tabela> -A <chain> [parametro] -j <ação>
```

Principais instruções para manipulação das CHAINs

-A Adiciona uma regra (ao final) da cadeia informada.
-I Insere uma regra (no início) da cadeia informada.
-D Deleta uma regra da cadeia informada.
-L Lista todas as regras da cadeia informada.
-F Apaga todas as regras da cadeia.

Configuração de Regras

- Comando para listar todas as regras da tabela **filter**:

```
# iptables -nL
```

- Comando para apagar todas as regras da tabela **filter**:

```
# iptables -F
```

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Configuração de Regras

- Sintaxe padrão para configuração de regras no IPtables:

```
# iptables -t <tabela> -A <chain> [parametro] -j <ação>
```

Possíveis filtros para seleção dos pacotes atingidos pela regra:

- Endereço IP ou Rede de Origem (**-s**)
- Endereço IP ou Rede de Destino (**-d**)
- Interface de Entrada (**-i**) ou Saída (**-o**)
- Protocolo de Comunicação (**-p [tcp/udp/icmp]**)
- Porta de Origem (**--sport**) ou Destino (**--dport**)

Configuração de Regras

- Sintaxe padrão para configuração de regras no IPtables:

```
# iptables -t <tabela> -A <chain> [parametro] -j <ação>
```

- Especificando uma ação para a regra:

ACCEPT => Aceita o pacote.
DROP => Descarta o pacote.
REJECT => Descarta o pacote, enviando um aviso.
LOG => Registra uma mensagem no log do sistema.

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Seleção de Pacotes

```
# iptables -A FORWARD -s 192.168.0.0/16 -j DROP
```

O que faz a regra acima?

Seleção de Pacotes

- Filtrando pelo IP de Origem do Pacote [**-s**]:

```
# iptables -A FORWARD -s 192.168.0.0/16 -j DROP
```

O que faz a regra acima?

Adiciona uma regra (-A) que descarta (DROP) todo pacote que atravessa (FORWARD) o host e cuja origem é uma faixa de rede privada.

Seleção de Pacotes

- Filtrando pelo IP de Origem do Pacote [**-s**]:

```
# iptables -A FORWARD -s 192.168.0.0/16 -j DROP
```

O que faz a regra acima?

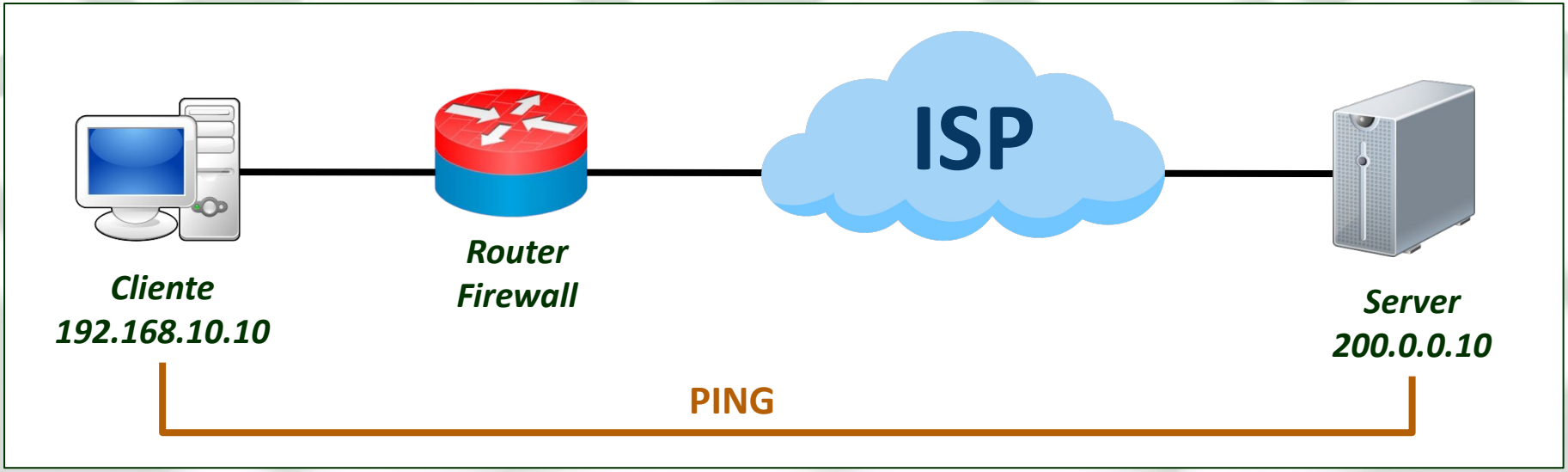
DROP OU REJECT, QUAL USAR???

Adiciona uma regra (-A) que descarta (DROP) todo pacote que atravessa (FORWARD) o host e cuja origem é uma faixa de rede privada.

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Laboratório 12-1

- Sabemos que no mundo real, um **IP Privado não é capaz de alcançar um IP Público**, isso porque **os roteadores da Internet não propagam pacotes cuja origem ou destino é privada**.
- Configure o "**ISP**" para agir como no mundo real.
- Compare a diferença entre as ações REJECT e DROP.



Seleção de Pacotes

```
# iptables -A OUTPUT -d ifnmg.edu.br -j REJECT
```

O que faz a regra acima?

Seleção de Pacotes

- Filtrando pelo Destino do Pacote [**-d**]:

```
# iptables -A OUTPUT -d ifnmg.edu.br -j REJECT
```

O que faz a regra acima?

*Insere uma regra (-A) que rejeita (REJEITA) saída de pacotes (OUTPUT), cujo destino (**-d**estination) seja o IP correspondente ao domínio ifnmg.edu.br.*

Seleção de Pacotes

```
# iptables -A INPUT -s 192.168.10.0/24 -j ACCEPT
```

O que faz a regra acima?

Seleção de Pacotes

- Filtrando pela Origem do Pacote [**-s**]:

```
# iptables -A INPUT -s 192.168.10.0/24 -j ACCEPT
```

O que faz a regra acima?

*Insere uma regra (-A) que aceita (ACCEPT) pacotes de entrada (INPUT), cuja origem (**-s**ource) está na faixa da rede local 192.168.10.0/24.*

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Seleção de Pacotes

```
# iptables -A INPUT -i eth1 -j DROP
```

```
# iptables -A FORWARD -o eth0 -p tcp --dport 80 -j ACCEPT
```

Seleção de Pacotes

- Filtrando pela Interface de Entrada [**-i**]:

```
# iptables -A INPUT -i eth1 -j REJECT
```

*Esta regra rejeita (REJECT) todo pacote que chega com destino ao host (INPUT) pela interface (**-i**n) eth1.*

- Filtrando pela Interface de Saída [**-o**], Protocolo e DPort.

```
# iptables -A FORWARD -o eth0 -p tcp --dport 80 -j ACCEPT
```

Esta regra aceita (ACCEPT) todo pacote que atravessa o host (FORWARD) e que sai (-out) pela interface eth0, e cujo protocolo (-p) é TCP e com porta de destino (--dport) 80.

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Seleção de Pacotes

- Especificando o Protocolo [**-p**] (TCP, UDP ou ICMP):

```
# iptables -A INPUT -p icmp -j DROP
```

```
# iptables -A INPUT -p tcp -j REJECT
```

- Especificando Portas de Origem [**--sport**] e Destino [**--dport**] e **multiportas** [**-m multiport**]:

```
# iptables -A INPUT -p tcp --dport 23 -j REJECT
```

```
# iptables -A FORWARD -p tcp --dport telnet -j DROP
```

```
# iptables -A INPUT -p tcp -m multiport --dports
  22,80,443 -j ACCEPT
```

Exceções

- Filtros podem ser precedidos do sinal “!”
- Esse sinal representa exceção da regra.

```
# iptables -A INPUT ! -s 192.168.10.0/24 -j DROP
# Exclua todos os pacotes, EXCETO os de origem 192.168.10.0/24
```

```
# iptables -A INPUT -i eth1 ! -p icmp -j DROP
# Exclua todos os pacotes vindos da iface eth1, EXCETO os
  pacotes ICMP.
```

```
# iptables -A FORWARD -m multiport -p tcp ! --dports
  22,80,443 -j DROP
# Exclua todos os pacotes EXCETO para as portas 22, 80 e 443.
```

Taxa de Bloqueio

- Regra para bloquear a inundação de um serviço.
- Prevenção de ataques DoS.

```
# iptables -A INPUT -p tcp --dport 443 -m limit --limit
  100/minute --limit-burst 200 -j ACCEPT
```

- A regra acima limita as conexões de entrada para uma taxa de 100 requisições por minuto, e define um limite de rajada (requisições simultâneas) para 200.

Alternando Políticas

- **Define a POLÍTICA PADRÃO de uma Chain...**
- Política RESTRITIVA

```
# iptables -P INPUT DROP
```

- Política PERMISSIVA

```
# iptables -P OUTPUT ACCEPT
```

*Obs.: Não há política **REJECT**.*

Alternando Políticas

- **Define a POLÍTICA PADRÃO de uma Chain...**

- Política RESTRITIVA

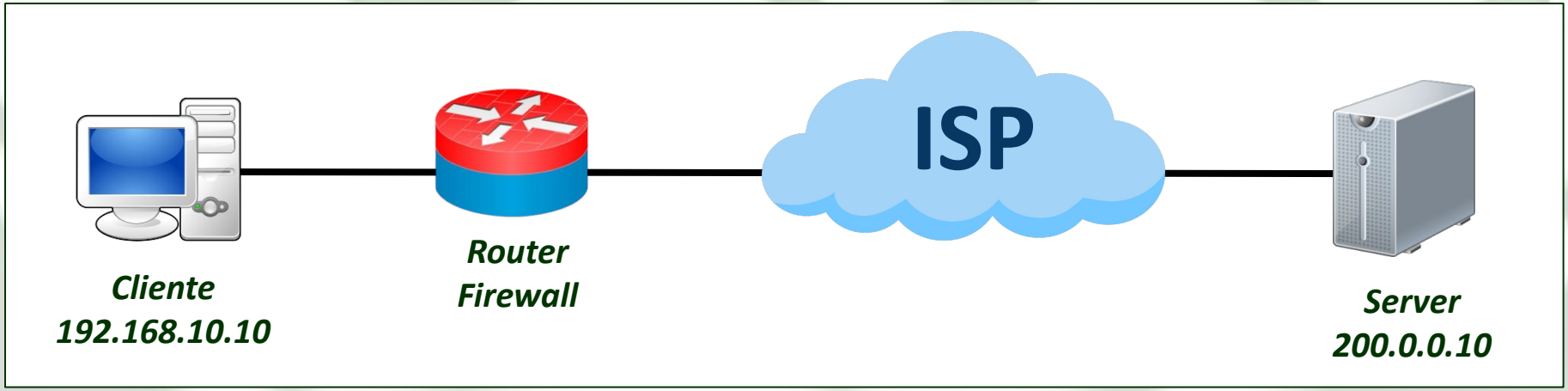
```
# iptables -P INPUT DROP
# iptables -P FORWARD DROP
```

POR **BOA PRÁTICA**, ROTEADORES/FIREWALLs DEVEM POSSUIR **POLÍTICA RESTRITIVA** PARA AS CHAINs **INPUT** E **FORWARD!!!**

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

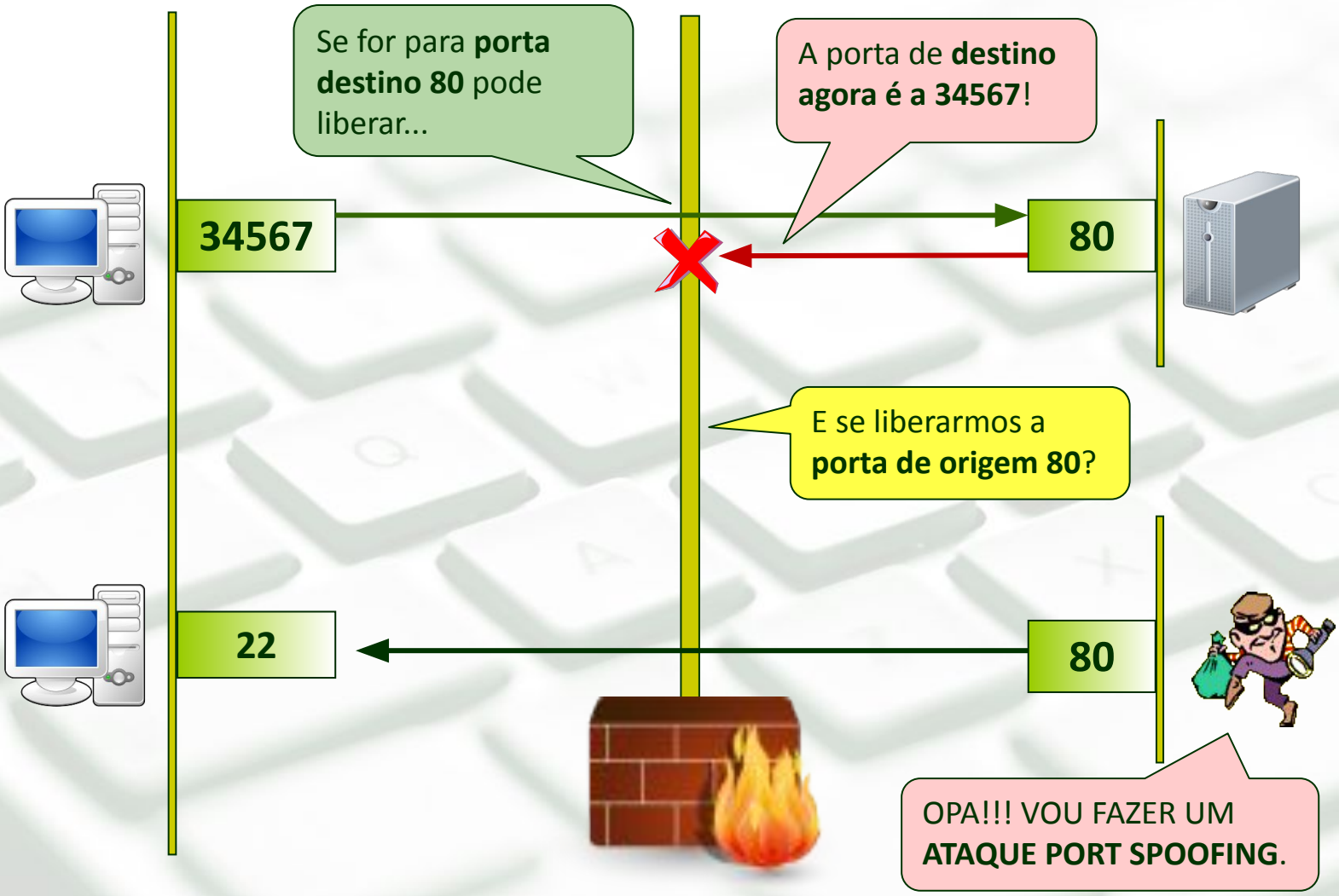
Laboratório 12-2

- "Router/Firewall" deve:
  - Seguir **BOAS PRÁTICAS** (veja slide anterior!).
  - Aceitar conexões SSH provenientes apenas da rede local (lembre de ligar o serviço SSH).
  - Aceitar pings provenientes da rede local normalmente.
  - Aceitar pings externos na taxa de 4/m e rajada de 1.
  - Permitir Clientes internos acessar **somente serviços HTTP e HTTPS da Internet** (use o netcat para testar as portas).



INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

O Problema da Política Restritiva



Firewall *Stateful*

- A forma segura de corrigir o problema anterior, é a configuração de um Firewall com regras *Stateful*.
- Regras que permitem ao *firewall* **verificar o estado dos pacotes em suas respectivas conexões**.
- Possíveis estados de um pacote em relação à conexão:
  - **NEW**: Refere-se a pacotes que iniciam uma conexão.
  - **ESTABLISHED**: Pacotes que já fazem parte de uma conexão estabelecida anteriormente.
  - **RELATED**: Pacotes que fazem parte de um fluxo, mas não necessariamente uma conexão: Ex.: ICMP, FTP.
  - **INVALID**: Pacotes sem reconhecimento em alguma conexão ou com opções inválidas.

Firewall *Stateful*

- Especificando o Estado da Conexão:

```
# (...) -m state --state ESTABLISHED, RELATED -j ACCEPT
```

Essas regras permitem que pacotes oriundos de conexões já estabelecidas (ESTABLISHED) possam ser aceitos no host.

Regra útil em ambientes que utilizam política RESTRITIVA.

- **Volte ao Laboratório 12-2 e finalize-o.**

Configuração de Regras

- Toda regra criada no **IPTables** fica armazenada temporariamente na memória RAM, sendo perdida quando a máquina é reiniciada.

- Utilize o comando abaixo para salvar as regras criadas...

```
# iptables-save > nome_do_arquivo
```

- ... e o comando abaixo para recuperar as regras.

```
# iptables-restore < nome_do_arquivo
```

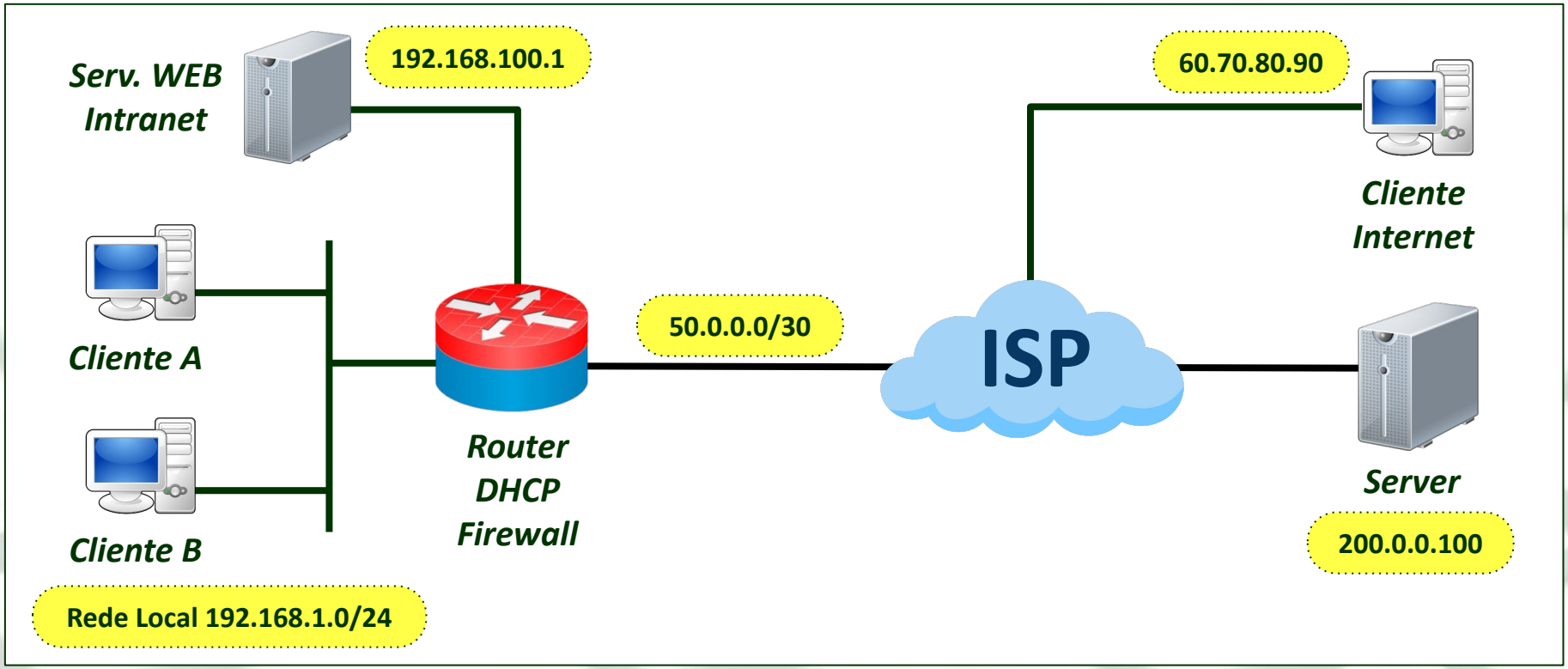
Configuração de Regras

- Na maioria dos casos, um script contendo diversas regras do **IPTables** é criado e executado na inicialização do sistema.
- Essas regras dependem muito do ambiente em questão, não existindo um “script padrão” para todas as redes.
- Certamente, boas práticas de segurança devem sempre ser lembradas durante a criação do script de configuração do firewall.

Pesquise na Internet exemplos de scripts de inicialização do firewall IPtables.

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Laboratório 12-3



Política Restritiva para o "Firewall" - use netcat para testar os serviços.

"Clientes" podem Acessar Serviços HTTP, HTTPS e SSH do "Server" no mundo.

"Cliente Internet" pode estabelecer VPN com Router (Serviço na Porta 1194).

SSH do "Router" disponível apenas para "Clientes da Rede Local".

HTTP e HTTPS do "Servidor Intranet" Liberados para Qualquer tipo de Acesso.

SSH e SFTP do "Servidor Intranet" Liberados apenas para Clientes da Rede Local.

Ah...e claro, o DHCP deve funcionar 😉

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Seminário Individual

NAT

Revisão NAT…

- ***O que é?***
- ***Funcionamento***
- ***Source NAT vs. Destination NAT***

NAT com IPtables

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Seminário Individual

- Assista ao vídeo abaixo, sobre a ferramenta **Fail2Ban**

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

Referências

- **Guia Foca GNU/Linux**.

Disponível em http://www.guiafoca.org/

- **Documentação NetFilter.**

Disponível em http://www.netfilter.org/documentation/

- **Prof. Ph.D. Edgard Jamhour**

Disponível em https://www.ppgia.pucpr.br/~jamhour/Pessoal/Graduacao/Ciencia/Teoria/

- MORIMOTO, Carlos E; **Servidores Linux - Guia Prático**.