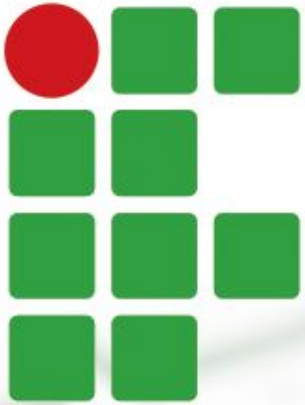


INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

# Admin. Serviços de Redes

## *- Firewall IPTables -*

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

# Firewall

- ***Firewall*** é uma ferramenta, sob forma de *software* ou equipamento dedicado, que tem como objetivo **aplicar uma política de segurança** para máquina ou rede através do **monitoramento do tráfego da rede**.

# 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**
  - **nunca** 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**
  - Analisa todo o **conteúdo** do pacote 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**.

# 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.
  - Mascaramento (*Masquerading*).

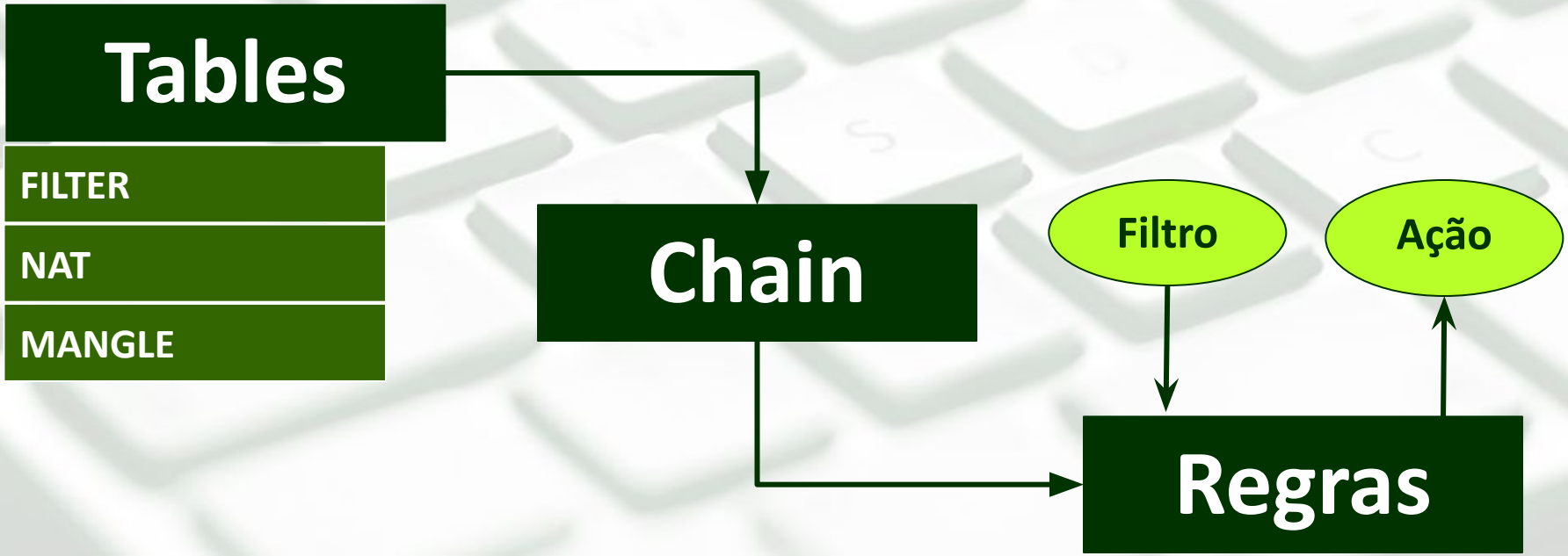
# IPTABLES

- **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 as respectivas **CHAINs** (cadeias ou *listas*).
  - Existem três **TABELAS** disponíveis no IPTABLES:
    - **FILTER** (tabela padrão => filtragem de pacotes)
    - **NAT** (tradução de endereços e portas)
    - **MANGLE** (tratamento especial de pacotes)

# Chains

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

*Sempre letras maiúsculas*

- ***IPTables*** também permite que um usuário possa criar sua própria CHAIN.

# Regras

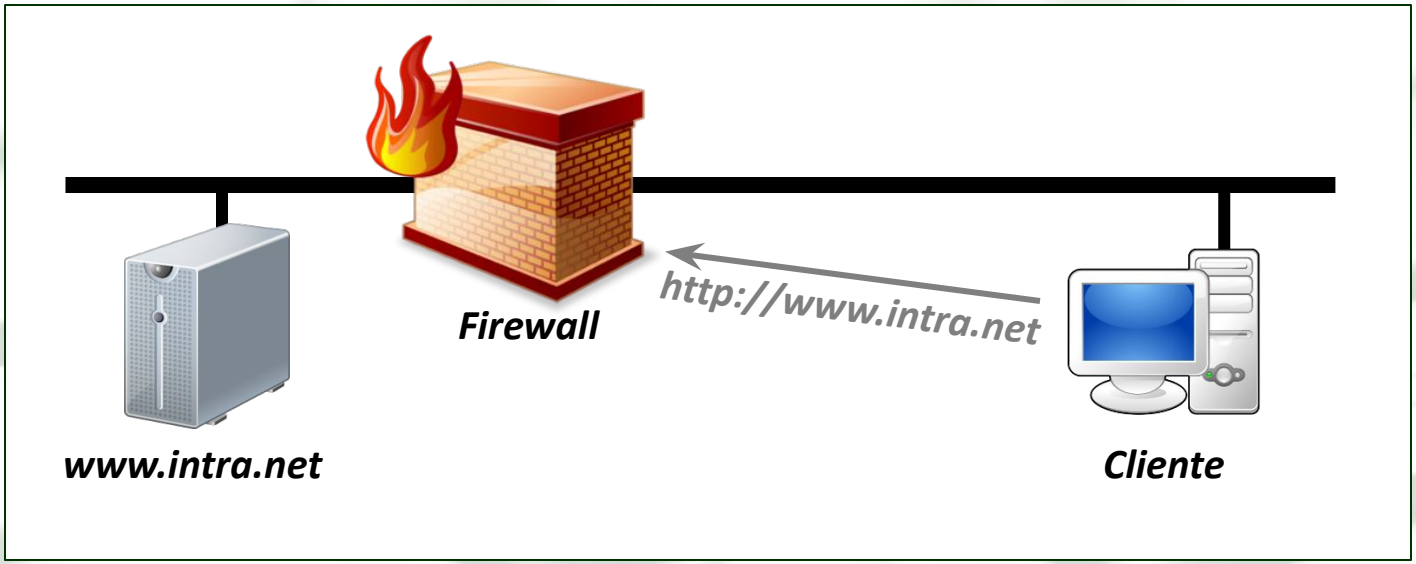
- **REGRA**
  - Indica uma **ação** a ser realizada para uma **seleção** de pacotes.
  - *Exemplos:*
    - **Aceitar** pacotes **provenientes da rede X**.
    - **Rejeitar** pacotes cujo **destino é uma porta Y**.

**ATENÇÃO**

As regras são processadas na ordem em que são inseridas.

# Regras

- *Exemplo do Processamento de Regras*

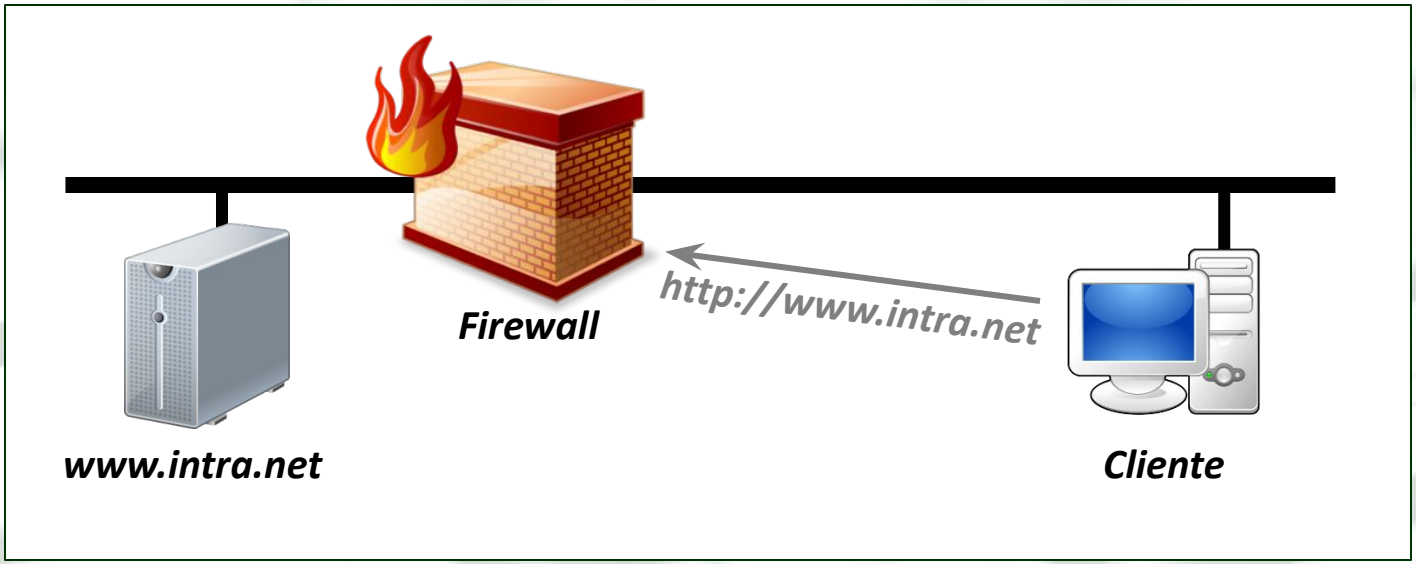



```
R1: Rejeite todos os pacotes destinados ao Web-Server.
R2: Aceite pacotes de conexão cujo destino é a porta 80.
```

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 as regras que **filtram pacotes** que se **originam**, **destinam** ou **atravessam** o host.

- Três CHAINs padrões:
  - **INPUT** => Pacotes que chegam à máquina.
  - **OUTPUT** => Pacotes que saem da máquina.
  - **FORWARD** => Pacotes que atravessam a máquina.

# Tabela NAT

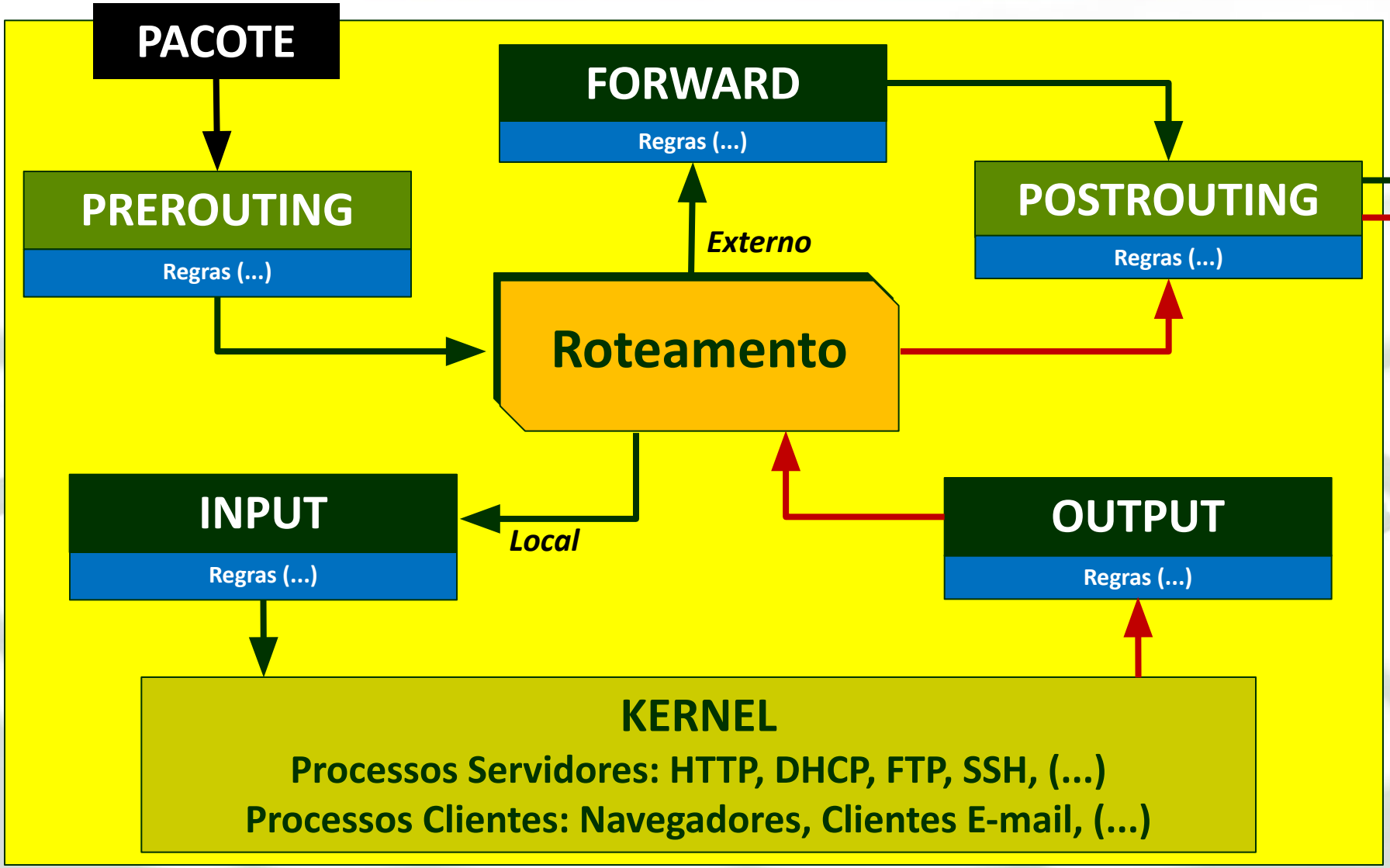
- **Tabela NAT (*Network Address Translation*)**
  - Tabela que armazena regras para **manipulação e tradução de endereços** públicos/privados.
  - P.ex.: Source NAT, Destination NAT, Redirecionamento de Portas, Proxy Transparente, etc.
- Três CHAINs padrões:
  - **PREROUTING** => Antes do processo de roteamento.
  - **POSTROUTING** => Após o processo de roteamento.
  - **OUTPUT** => Saída do pacote gerado localmente, antes do processo de roteamento.

# Tabela Mangle

- **Tabela Mangle**
  - Tabela que armazena regras para realizar alterações especiais em pacotes.
    - P.ex.: Modificar cabeçalhos dos pacotes, QoS, etc...
  - Esta tabela raramente é usada.
  - 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>
```

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>
```

- 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>
```

Comando para manipulação da CHAIN

**-A** : (ou **-I**) Adiciona uma regra na cadeia informada.
**-D** : Deleta uma regra da cadeia informada.
**-L** : Lista todas as regras da cadeia informada.
**-P** : Altera a política padrão da cadeia.
**-F** : Apaga todas as regras da cadeia.

# Configuração de Regras

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

```
# iptables -L
```

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

```
# iptables -F
```

# Alternando Políticas

- **Define a política padrão de uma Chain...**

- Política RESTRITIVA

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

- Política PERMISSIVA

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

# 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.

# Seleção de Pacotes

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

```
# iptables -A INPUT -s 192.168.100.0/24 -j REJECT
```

*O que faz a regra acima?*

# Seleção de Pacotes

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

```
# iptables -A INPUT -s 192.168.100.0/24 -j REJECT
```

*O que faz a regra acima?*

*Insere uma regra (-A) que rejeita (REJECT) todo pacote de entrada (INPUT), cuja origem (**-s**ource) está na faixa de rede 192.168.100.0/24.*

# Seleção de Pacotes

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

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

*O que faz a regra acima?*

# Seleção de Pacotes

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

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

*O que faz a regra acima?*

*Esta regra descarta (DROP) todo pacote que atravessa o host (FORWARD) cujo destino está na rede 192.168.0.0/24.*

# Seleção de Pacotes

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

```
# iptables -A INPUT –i eth0 –j DROP
```

*Esta regra descarta (DROP) todo pacote que chega (**-i**n) pela interface eth0.*

- Filtrando pela Interface de Saída [**-o**]:

```
# iptables -A OUTPUT –o eth0 –tcp --dport 80 –j ACCEPT
```

*Esta regra aceita (ACCEPT) todo pacote (gerado localmente) que sai (**-o**ut) pela interface eth0, cujo protocolo (-p) é TCP e possui porta de destino (--dport) 80.*

# Seleção de Pacotes

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

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

```
# iptables -A OUTPUT –p tcp –j DROP
```

```
# iptables -A INPUT –p tcp --syn –j DROP
```

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

```
# iptables -A INPUT –p tcp --dport 80 –j DROP
```

```
# iptables -A OUTPUT –p tcp --sport 80 –j DROP
```

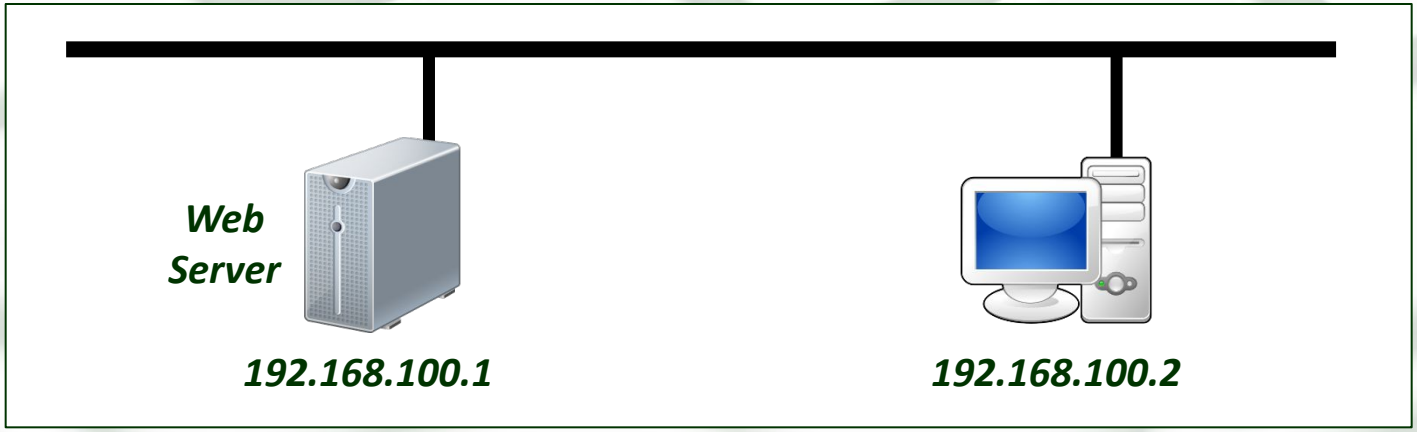
INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

# Seleção de Pacotes

- Especificando Serviços:

```
# iptables -A INPUT –p tcp --syn --dport 80 –j ACCEPT
# iptables -A INPUT –i eth0 -j REJECT
```

*Estas regras autorizam o Server aceitar apenas requisições de conexão para o serviço HTTP.*



INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

# Seleção de Pacotes

- Especificando Serviços:

```
# iptables -A INPUT -p tcp --syn --dport 80 -j ACCEPT
# iptables -A INPUT -i eth0 -j REJECT
```

***DICA***

**Utilize o aplicativo w3m para simular um Navegador WEB *text-based*.**

# Seleção de Pacotes

- Regras compostas...

```
# iptables -A OUTPUT –o eth0 –d 192.168.100.0/24 –p icmp
–j DROP
```

```
# iptables -A INPUT –s 192.168.100.0/24 –p tcp --syn
--dport 22 –j LOG --log-prefix “Acesso SSH”
```

```
# iptables -A INPUT –i eth1 -p icmp --icmp-type
echo-request -j REJECT
```

```
# iptables -A FORWARD –s 192.168.100.0/24 –d
www.facebook.com.br –j DROP
```

# Exceções

- Muitos parâmetros de seleção podem ser precedidos do sinal **"!"**
- **Esse sinal representa uma exceção à regra.**

```
# iptables -A INPUT ! -s 200.200.200.10 -j DROP
# Exclua todos os pacotes, EXCETO os de origem 200.200.200.10
```

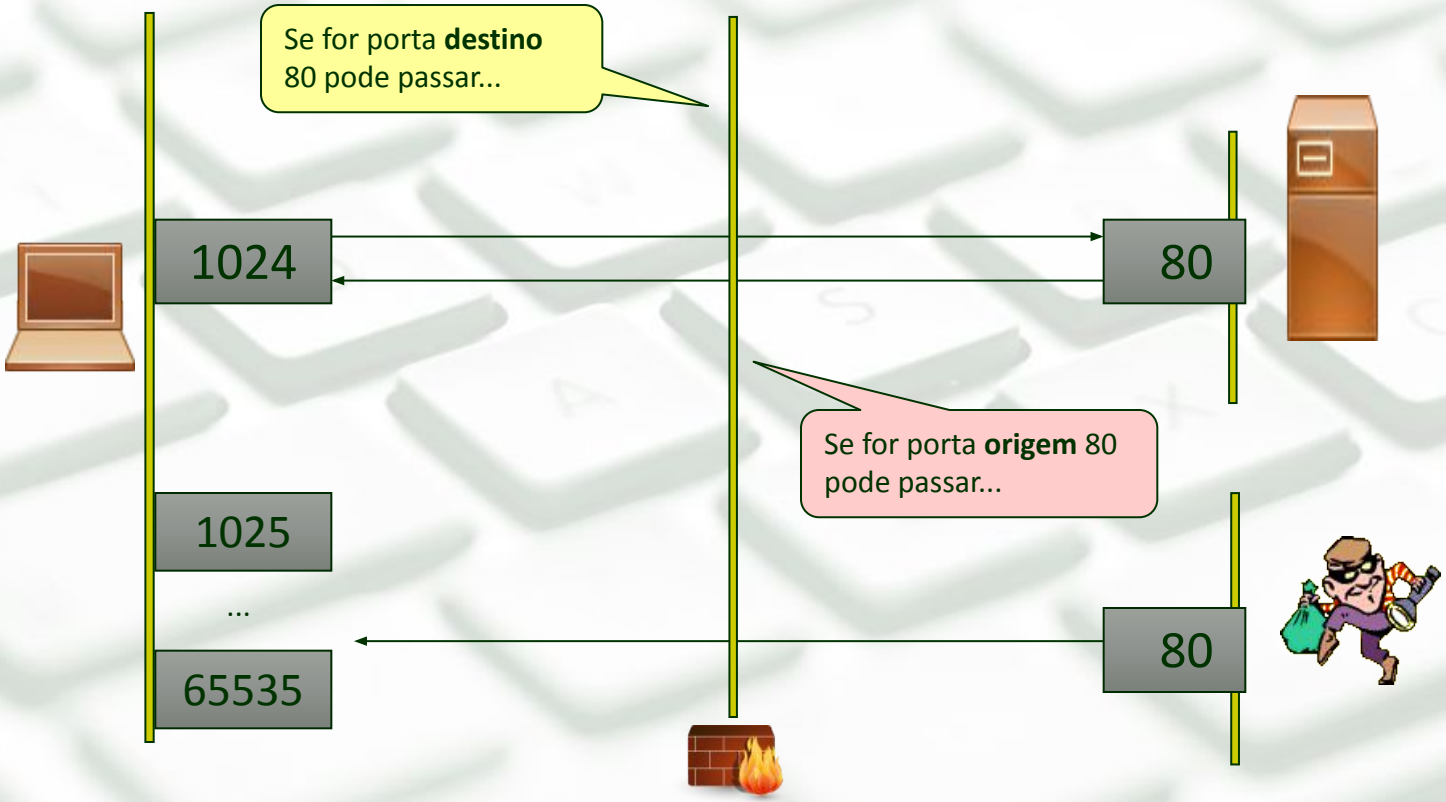
```
# iptables -A INPUT -s 200.200.200.10 ! -p tcp -j DROP
# Exclua todos os pacotes vindos de 200.200.200.10, EXCETO os
pacotes do protocolo TCP.
```

```
# iptables -A INPUT -m multiport -p tcp ! --dports
  22,9000 -j DROP
# Exclua todos os pacotes EXCETO para as portas 22 e 9000.
```

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

# Firewall *Stateful*

- **Problema**: Ataque *Port Spoofing*



# Firewall *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 Statefull

- Especificando o Estado da Conexão:

```
# iptables -A INPUT –m state --state ESTABLISHED -j ACCEPT
# iptables -A OUTPUT –m state --state ESTABLISHED -j ACCEPT
# iptables -A FORWARD –m state --state ESTABLISHED -j ACCEPT
```

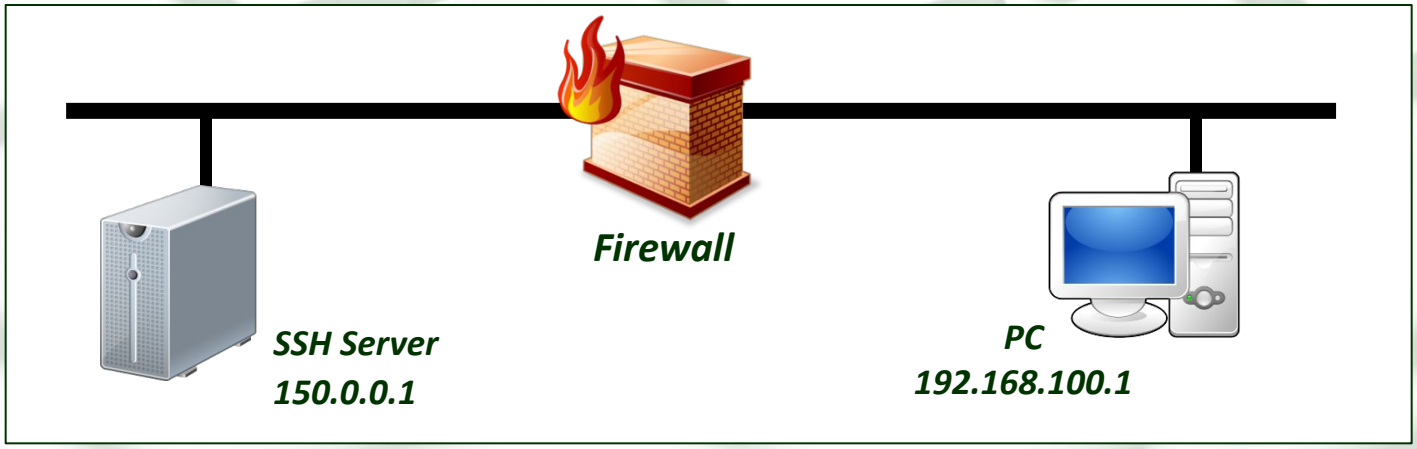
*Essas regras permitem que pacotes oriundos de conexões já estabelecidas (ESTABLISHED) possam ser aceitos no host.*

***Regra útil em ambientes que utilizam política RESTRITIVA.***

INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Januária

# Atividade Prática

- Configure o Firewall de forma que:
  - Adote política RESTRITIVA para todas as *chains* da tabela *Filter*.
  - Permita o estabelecimento de Conexão SSH entre o "PC" e o "SSH Server"



# 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
```

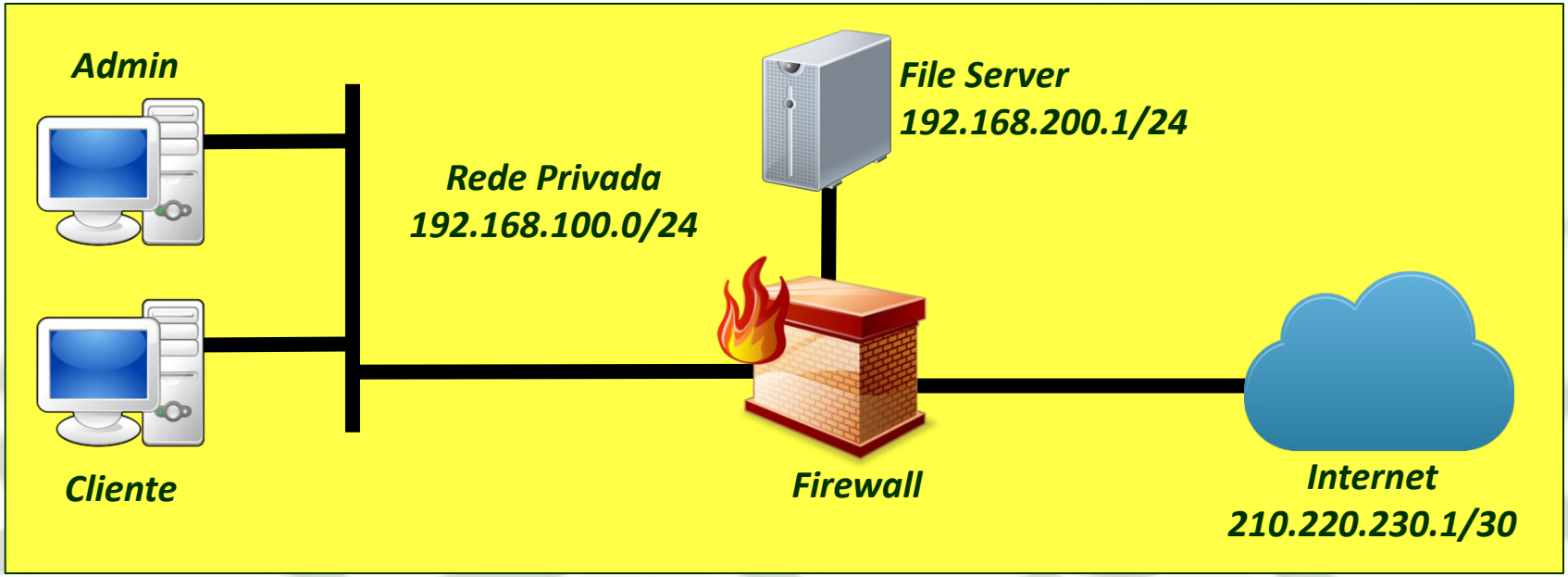
# Configuração de Regras

- 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

# Exercícios




**A Internet** não pode acessar PC's da **rede privada**.

**A Internet** só pode ter acesso ao serviço SFTP do **File Server.**

**As solicitações de ping** não podem ser encaminhadas ao **File Server.**

Somente o **PC Admin** pode usar o serviço SSH do **File Server**.

As tentativas de acesso ao SSH do **File Server** pela **Internet** devem ser Rejeitadas e Registradas no LOG do **Firewall** com o prefixo: "SSH: Tentativa Acesso Externo Recusada."

As tentativas de acesso ao SSH do **File Server** pela **Rede Privada** devem ser Rejeitadas e Registradas no LOG do **Firewall** com o prefixo: "SSH: Tentativa Acesso Interno Recusada."

# Exercícios

- Pesquise na Internet, como criar regras no **IPtables** para bloquear os seguintes ataques...
  - Bloquear ataques de **Força Bruta** (*Bruteforce*) a um determinado serviço de rede.
  - Bloquear ataques **DoS** (*Denial of Service*) a partir da recepção de pacotes mal formados**.**
  - Bloquear ataques **DoS** do tipo **SYN Flood**.
  - Bloquear ataques de **IP Spoofing**.

# 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**.