Iptables
Introdução e Gateway

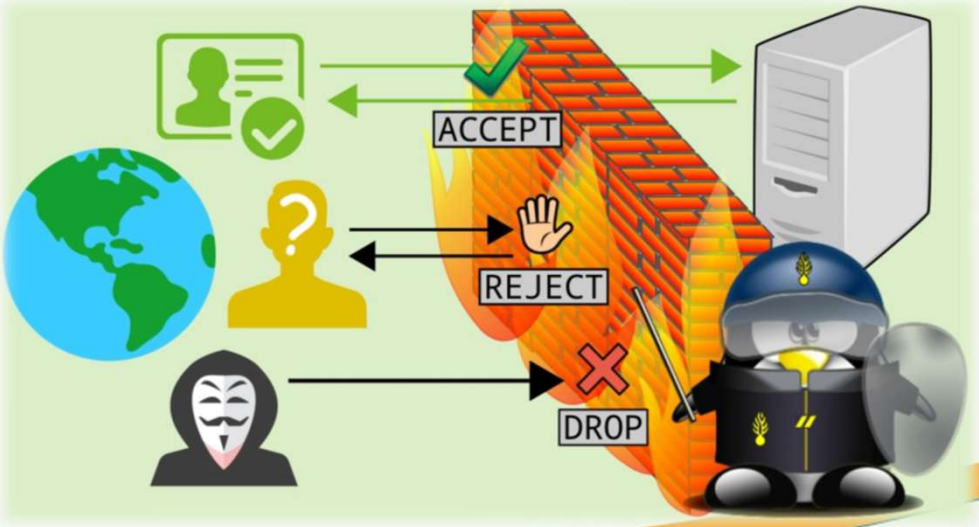
Prof. Marcos C. da Fonseca

Firewall no Linux

- O ***netfilter*** é um módulo que fornece ao sistema operacional Linux as funções de firewall de pacotes, NAT e log dos dados que trafegam por rede de computadores. https://www.netfilter.org/

- O ***iptables*** é a ferramenta que permite a criação de regras de firewall e NAT.

- Instalação do Iptables
- # apt install iptables



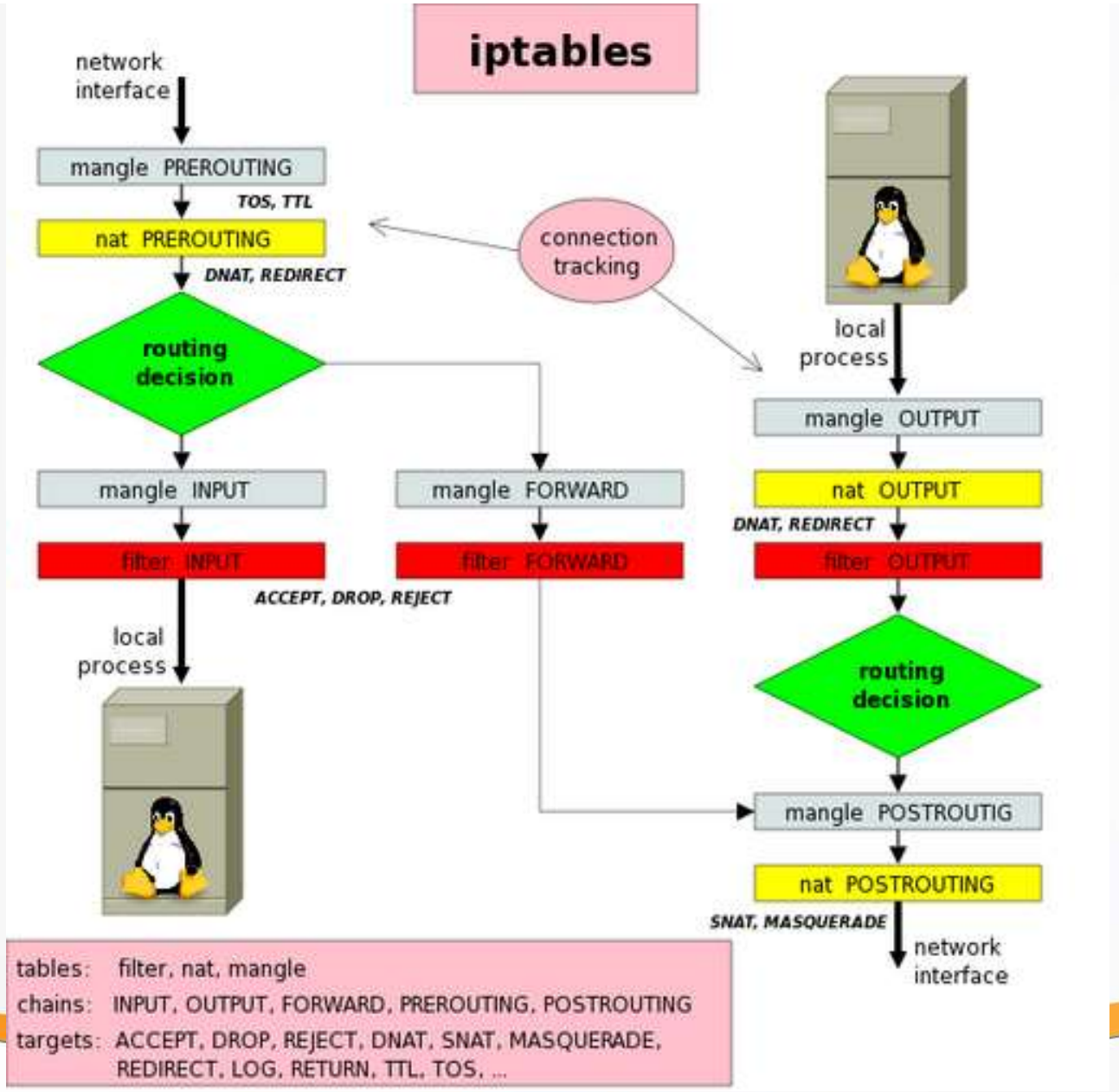
Comando SUDO ao usuário

- Algumas opções do ***iptables*** roda apenas se o usuário estiver usando *sudo*, mesmo na conta privilegiada *root* alguns comandos não são permitidos.
- Adicionando o usuário ao grupo sudo
- # usermod -aG sudo <nomeusuario>
- OU
- Permitindo usuários com sudo. Alterando o arquivo *SUDOERS* adicionar o usuário:
- # /usr/sbin/visudo
- <nomeusuario> ALL=(ALL:ALL) ALL

```
# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
aluno   ALL=(ALL:ALL) ALL
```

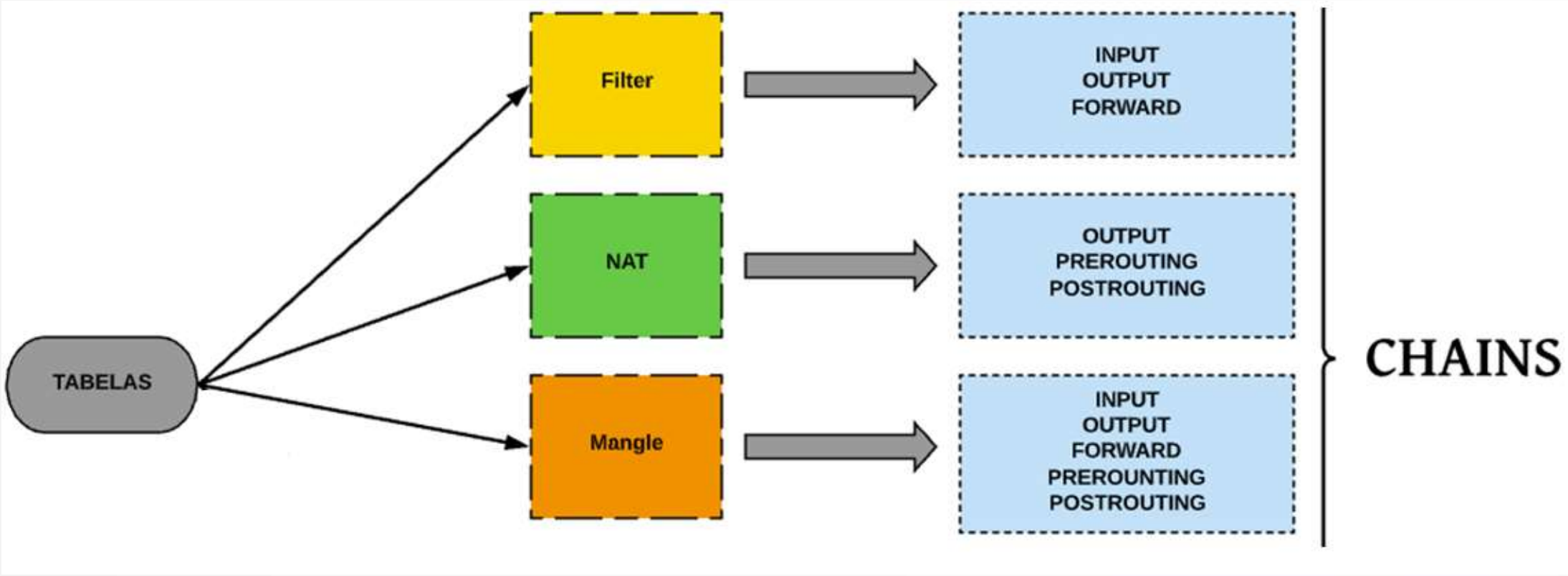
Exemplo básico de funcionamento



Iptables – Conceitos básicos

- **Tabelas**: são os locais usados para armazenar os ***chains*** e conjunto de regras.
- 3 principais tabelas:
  - **Filter:** tabela padrão.
  - **Nat:** usada para dados de outra conexão.
  - **Mangle:** Utilizada para alterações especiais de pacotes, como modificar o tipo de serviço.
- **Chains:** listas de regras que podem ser aplicadas as tabelas.
  - **INPUT:** chegada de pacotes.
  - **OUTPUT:** sápida de pacotes.
  - **FOWARD:** redirecionamento de pacotes.
  - **PREROUTING:** modifica o pacote quando chega.
  - **POSTROUTING:** modifica o pacote quando saí.

Iptables – Conceitos básicos



Iptables - Funcionamento básico

- Após criada uma lista definido regras, o pacote tratado pelo sistema, o firewall percorre a lista de regras, aplicando a regra que cabe a cada pacote.

1ª regra ✓
2ª regra ✓
3ª regra ✗
4ª regra
5ª regra

```
# Bloqueia qualquer tentativa de acesso ao programa Kazaa
iptables -A INPUT -m string --string "X-Kazaa" -j DROP

# Não permite que dados confidenciais sejam enviados para fora da empresa
# e registra o ocorrido.
iptables -A OUTPUT -m string --string "conta" -j LOG --log-prefix "ALERTA: dados confidencial "
iptables -A OUTPUT -m string --string "conta" -j DROP

# Somente permite a passagem de pacotes que não contém ".exe" em seu conteúdo
iptables -A INPUT -m string --string ! ".exe" -j ACCEPT
```

Iptables – Comandos básicos

- **iptables** habilita o gerenciador de regras.
- **-L** exibe as regas em uso (se não especificar a tabela, mostrará a tabela filter)
- **-t** *table* (escolhe qual tabela usar)
- **-A** *chain* (adiciona um regra)
- **-D** *delete* (deleta regra de número específico)
- **-F** *flush* (apaga todas as regras)
- **-I** *chain num* (insere uma regra de número na *chain* escolhida. Se num=2 é inserida a segunda regra)
- **!** (exceção a regra que vier depois do sinal !)

OBS: os comandos diferenciam de letras maiúscula e minúsculas

Iptables – Comandos básicos

- **-d** *destino* (adiciona um destino)
- **-s** *origem* (adiciona uma origem)
- **-p** *protocolo* (aplica regra sobre o protocolo: TCP, UDP, ICMP)
- **-o** *interface* (interface de saída de dados)
- **-i** *interface* (interface de entrada de dados)
- **--sport** *porta* (define a porta de origem, deve ser usado com a opção -p)
- **--dport** *porta* (define a porta de origem, deve ser usado com a opção -p)
- **-j** ação (define qual ação será aplicada) Principais ações:
  - **DROP** – Descarta o pacote (nenhuma resposta ao remetente)
  - **REJECT** – Rejeita o pacote (retorna uma resposta ao remetente)
  - **ACCEPT** – Aceita o pacote

Iptables - Sintaxe dos comandos

iptables	[-t tabela]	[opção]	[chain]	[dados]	-j [ação]
	filter	-A	INPUT	-p TCP	ACCEPT
	nat	-I	OUTPUT	-d 192.168.0.1	DROP
	mangle	-D	FOWARD	--dport 80	REJECT

https://explainshell.com/

- Prática bloqueando o ping
- #iptables -A INPUT -p ICMP -j DROP
- #iptables -L (lista as regras)
- #iptables -F (apaga todas as regras)

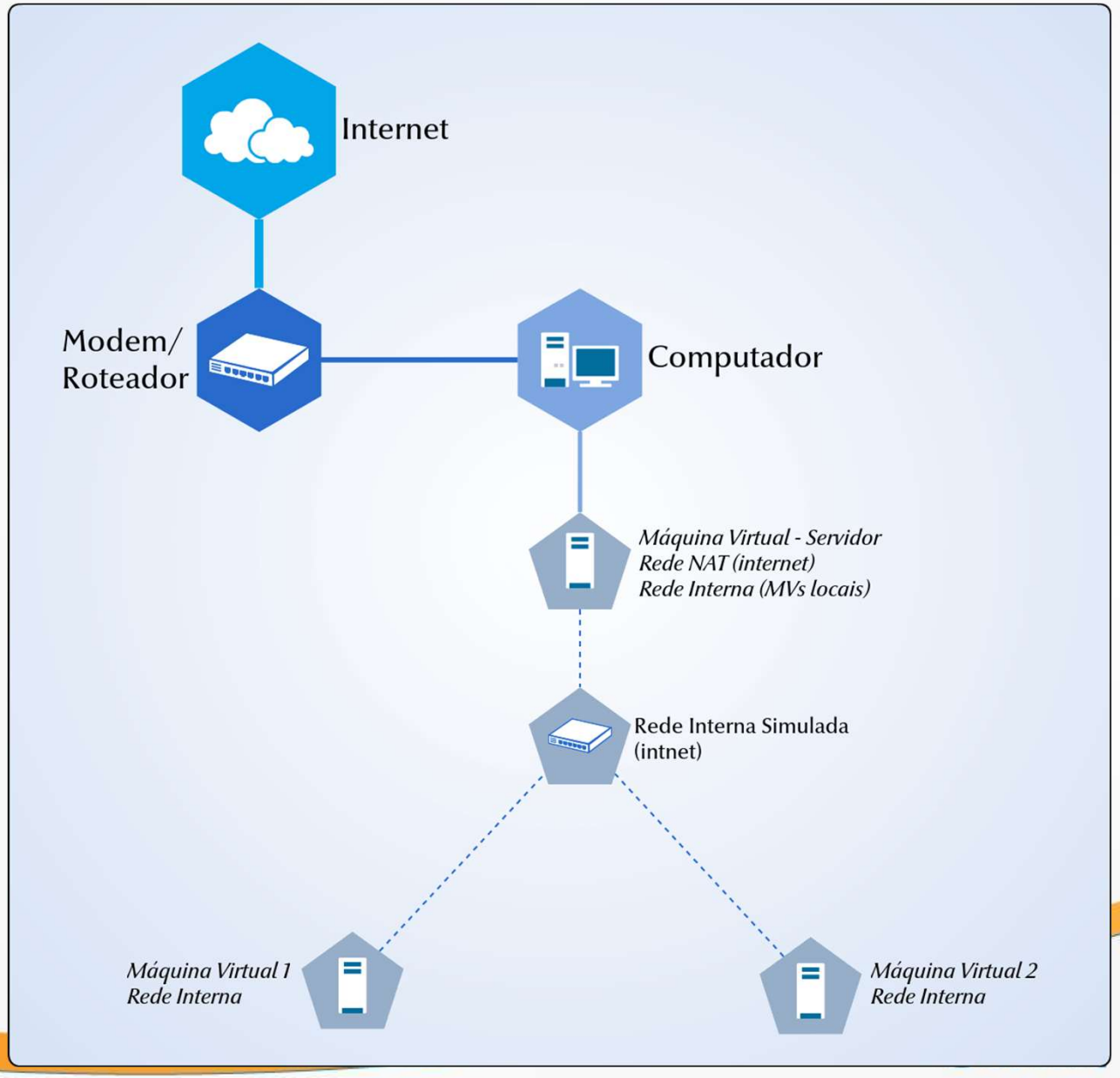
- Repita o comando e troque para REJECT
- Qual a diferença?

- OBS: Após a ação é possível acrescentar um comentário:
- -m comment --comment “seu comentário”

Senac

Gateway

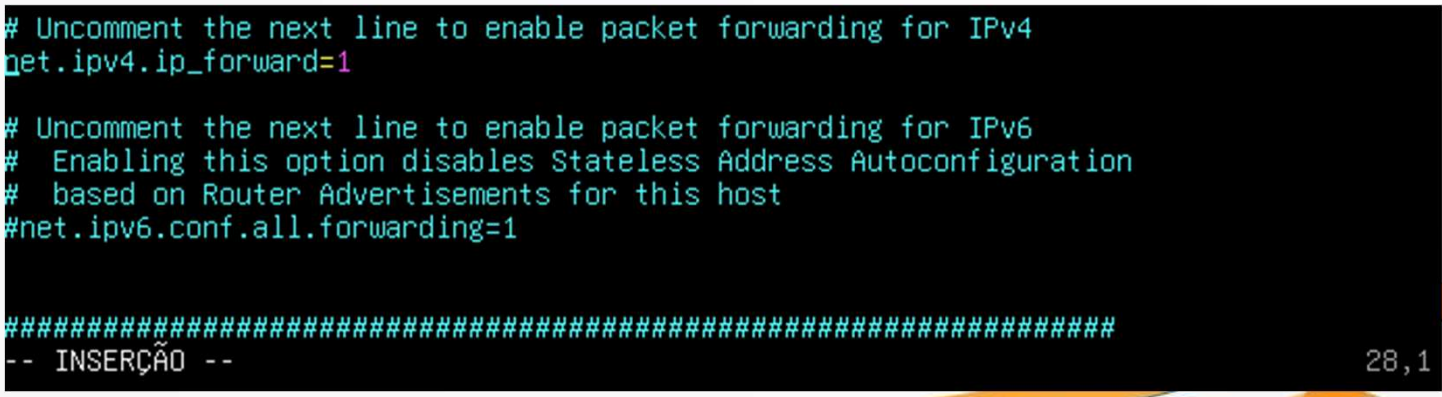
- É o dispositivo que dá acesso a redes externas normalmente a internet.
- Encaminha todo o fluxo de uma rede para outra.
- Exemplo do nosso cenário.
- Mas é possível executar em ambientes de produção.



Configurando o Servidor Gateway

- Isso irá possibilitar o Linux Debian ser o servidor *Gateway*, ou seja permite conexão com redes externa no caso a Internet.

- Editor arquivo e habilitar o parâmetro *Forward*
- #vim /etc/sysctl.conf
- Desabilitar o comentário da linha (apagar o hashtag):
- #net.ipv4.ip_forward=1
- Reinicie o serviço
- #systemctl reboot



Editando script Gateway no Iptables

- Criando um arquivo script, esse arquivo será iniciado toda a vez que o servidor ligar.
- $ sudo vim /usr/local/sbin/gateway.sh

- Escreva as seguinte linhas:
- #!/bin/bash
- iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
- iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
- iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

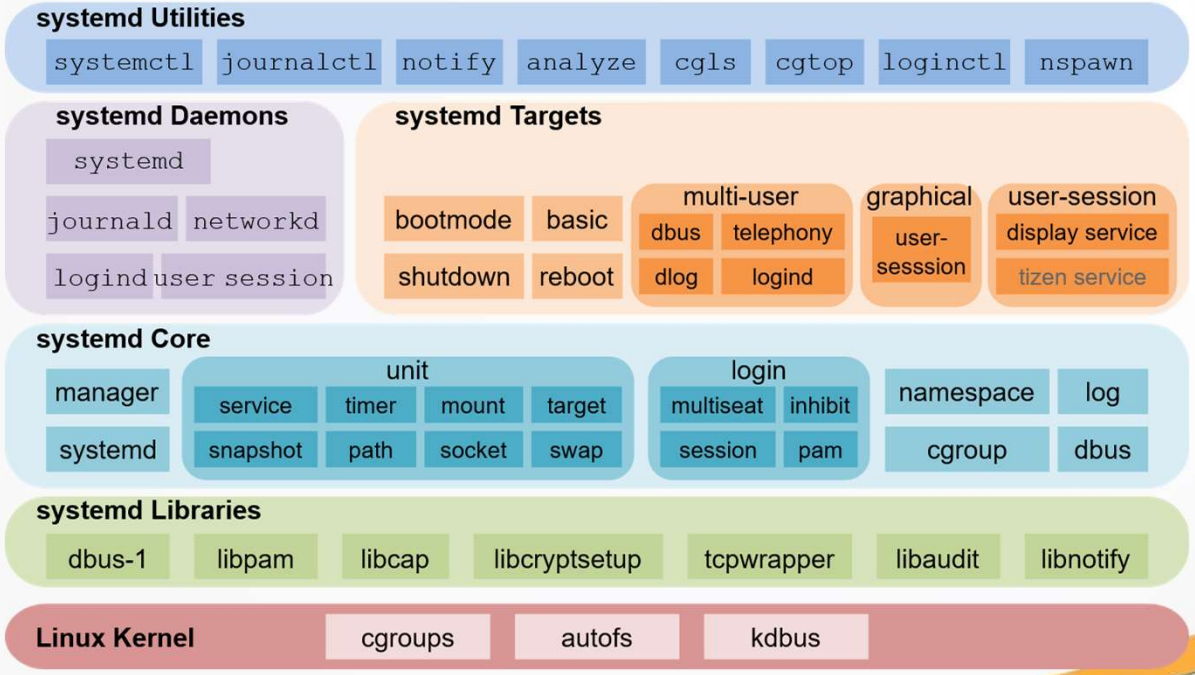
- Garantindo que o arquivo irá ser executado
- $ sudo chmod +x /usr/local/sbin/gateway.sh

- Testando o script Gateway
- $ sudo /usr/local/sbin/gateway.sh

Systemd

- É um sistema de inicialização (*init system*) composto por um conjunto de programas executado em segundo plano.

- Na prática, o *systemd* assume o controle assim que o kernel é ativado pelo gerenciador de *bootloader*, a partir daí, são carregados os processos que se iniciam com o sistema.



Habilitando para início do serviço

- Criando um arquivo que será usado pelo *Systemd* para inicialização automática, para isso crie o arquivo:
- #sudo nano /etc/systemd/system/gateway.service
- Editando o arquivo

```
[Unit]
Description=Gateway
After=network.target

[Service]
ExecStart=/usr/local/sbin/gateway.sh

[Install]
WantedBy=multi-user.target
~
```

Habilitando para início do serviço

- Habilitando o serviço de Gateway que acabamos de criar:
- #sudo systemctl enable gateway.service

- Reinicie o Servidor Gateway
- #reboot