Linux - Dicas

FirewallD - Gerenciamento de Firewall

O **FirewallD** é uma ferramenta de gerenciamento de firewall padrão para sistemas operacionais Linux em distribuições como Fedora, Red Hat e CentoOS. Ele atua como um *front-end* para o *framework* de filtragem de pacotes do kernel Linux, conhecido como **netfilter**.

FirewallD - Conceito

Esse firewall possui algumas regras padrão e trabalha com o conceito de zonas onde a liberação de serviços é feito dentro delas.

A tabela abaixo demonstra como está configurado o firewall da rede após a instalação do sistema operacional:

Regra	**Comportamento**
INPUT	Liberado o acesso conexões do tipo RELATED,ESTABLISHED.
FORWARD	Aceita apenas conexões do tipo RELATED,ESTABLISHED.
OUTPUT	Não possui restrições.

Zonas

O firewalld gerencia um grupo de regras conhecido como zonas. As zonas definem o tipo de tráfego que será permitido baseado no nível de confiança da rede onde o seu servidor está conectado. Cada zona está atrelada a uma interface de rede existente no servidor.

O comando abaixo lista as zonas existentes:

```
firewall-cmd --get-zones
```

Abaixo são mostradas as zonas existentes no firewalld em ordem de nível de confiança:

Zona	**Descrição**
drop	Todos os pacotes são descartados.

block	Todos os pacotes são rejeitados.
public	Rede que você não conhece, pública.
external	Rede externa onde o servidor com o firewalld funciona como um
gateway	para a rede interna. É configurada com mascaramento para manter a privacidade da rede interna.
internal	É a parte interna da rede. Equipamentos nessa rede possuem um nível maior de confiança e serviços adicionais estão disponíveis.
dmz	São equipamentos isolados, ou seja, que não devem possuir acesso a sua rede. Apenas algumas conexões de entrada para esses equipamentos são permitidas.
work	Equipamentos de trabalho com liberação de serviços adicionais.
home	Equipamentos de casa. São dispositivos mais conhecidos e confiáveis e que possuem liberação para um pouco mais de serviços que a zona work.
trusted	Equipamentos de confiança. Praticamente todos os serviços estão disponíveis para os equipamentos nesta zona.

Listar as regras existentes

O comando abaixo lista todas as regras existentes no serviço firewalld:

```
firewall-cmd --list-all
```

Se desejar listar apenas as regras de uma determinada zona utilize a opção –zone:

```
firewall-cmd –zone=public --list-all
```

Liberar portas de entrada

Para modificar as regras de entrada do firewall do Fedora, utilizamos o comando firewall-cmd.

No exemplo abaixo é demonstrado como liberar as portas 80(TCP) e 443(TCP) para acesso da rede pública, de forma permanente, para um servidor HTTP através da linha de comando:

```
firewall-cmd --permanent --zone=public --add-port=80/tcp
firewall-cmd --permanent --zone=public --add-port=443/tcp
firewall-cmd --set-default-zone=public
firewall-cmd --reload
```

onde:

--permanent	Adiciona a regra de forma permanente, ou seja, após reiniciar o filtro as regras permanecerão. Se for omitida esta opção as regras são válidas até o firewalld ser reiniciado.
--zone=public	É a zona pública não confiável. São endereços que você não conhece mas podem ser autorizados caso a caso.
--add-port=80/tcp	Informação da porta e protocolo que serão adicionados na zona public.
--reload	Recarrega as regras mantendo o estado das conexões.
--set-default-zone=public	Define a zona public como a padrão a ser utilizada.

O exemplo abaixo demonstra como liberar a porta SSH para o servidor Linux:

```
firewall-cmd --permanent --zone=public --add-port=22/tcp
firewall-cmd --set-default-zone=public
firewall-cmd --reload
```

Liberando um host ou uma rede

Abaixo é demonstrado como liberar o acesso total ao servidor para a rede cuja origem é 192.168.1.0/24:

```
firewall-cmd --permanent --zone=public --add-source=127.0.0.1/8
firewall-cmd --reload
```

--permanent	Adiciona a regra de forma permanente, ou seja, após reiniciar o filtro as regras permanecerão. Se for omitida esta opção as regras são válidas até o firewalld ser reiniciado.
--zone=public	É a zona pública não confiável. São endereços que você não conhece mas podem ser autorizados caso a caso.
--add-source=192.168.1.0/24	Informação da rede ou host que serão adicionados na zona public.
--reload	Recarrega as regras mantendo o estado das conexões.

Configurando o firewalld para agir como NAT

Para essa função faz-se necessário ter pelo menos 2 interfaces de rede no servidor, uma que faça a conexão com a rede pública e outra a rede interna.

No exemplo abaixo, a interface eth0 está conectada na rede pública e a eth1 na rede interna:

```
firewall-cmd --permanent –zone=internal –add-interface=eth1
firewall-cmd –permanent –zone=public -add-masquerade
firewall-cmd --reload
```

--permanent	Adiciona a regra de forma permanente, ou seja, após reiniciar o filtro as regras permanecerão. Se for omitida esta opção as regras são válidas até o firewalld ser reiniciado.
--zone=public --zone=internal	Selecionamos a zona public para fazer o mascaramento e a internal para informar a rede interna.
--add-masquerade	Adiciona o mascaramento na zona selecionada.
--reload	Recarrega as regras mantendo o estado das conexões.

Configurando o firewalld para Port Forward

Para redirecionar portas da rede externa para um endereço da rede interna, utilize os comandos abaixo:

```
firewall-cmd --permanent --zone=public –add-forward-
port=port=443: proto=tcp: toport=443: toaddr=192. 168. 1. 11
firewall-cmd --reload
```

--permanent	Adiciona a regra de forma permanente, ou seja, após reiniciar o filtro as regras permanecerão. Se for omitida esta opção as regras são válidas até o firewalld ser reiniciado.
--zone=public	É a zona pública não confiável. São endereços que você não conhece mas podem ser autorizados caso a caso.
--add-forward-port=	Ativa a regra para o port forward.
port=443	Porta de origem.
proto=tcp	Protocolo de origem.
toport=443	Porta de destino.
toaddr=192.168.1.11	IP de destino na rede interna.
--reload	Recarrega as regras mantendo o estado das conexões.

Contato

Monsta Tecnologia Ltda

Site: http://www.monsta.com.br

Downloads: http://www.monsta.com.br/download.html

E-mail: contato@monsta.com.br

Alterar o endereço IP em um servidor Fedora

Este tutorial passo a passo irá guiá-lo no processo de alteração do endereço IP em um servidor Linux Fedora. Aprenda a configurar um endereço IP estático ou dinâmico para garantir a conectividade de rede ideal para o seu servidor.

Configurar o IP do servidor

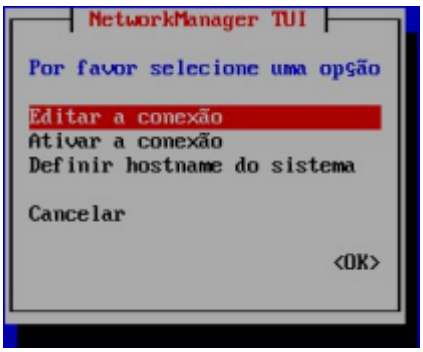
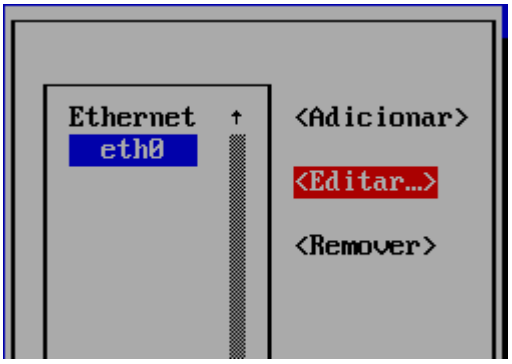
Entre com as credenciais de root em seu servidor. Uma vez logado, instale o programa para gerenciar interfaces de rede:

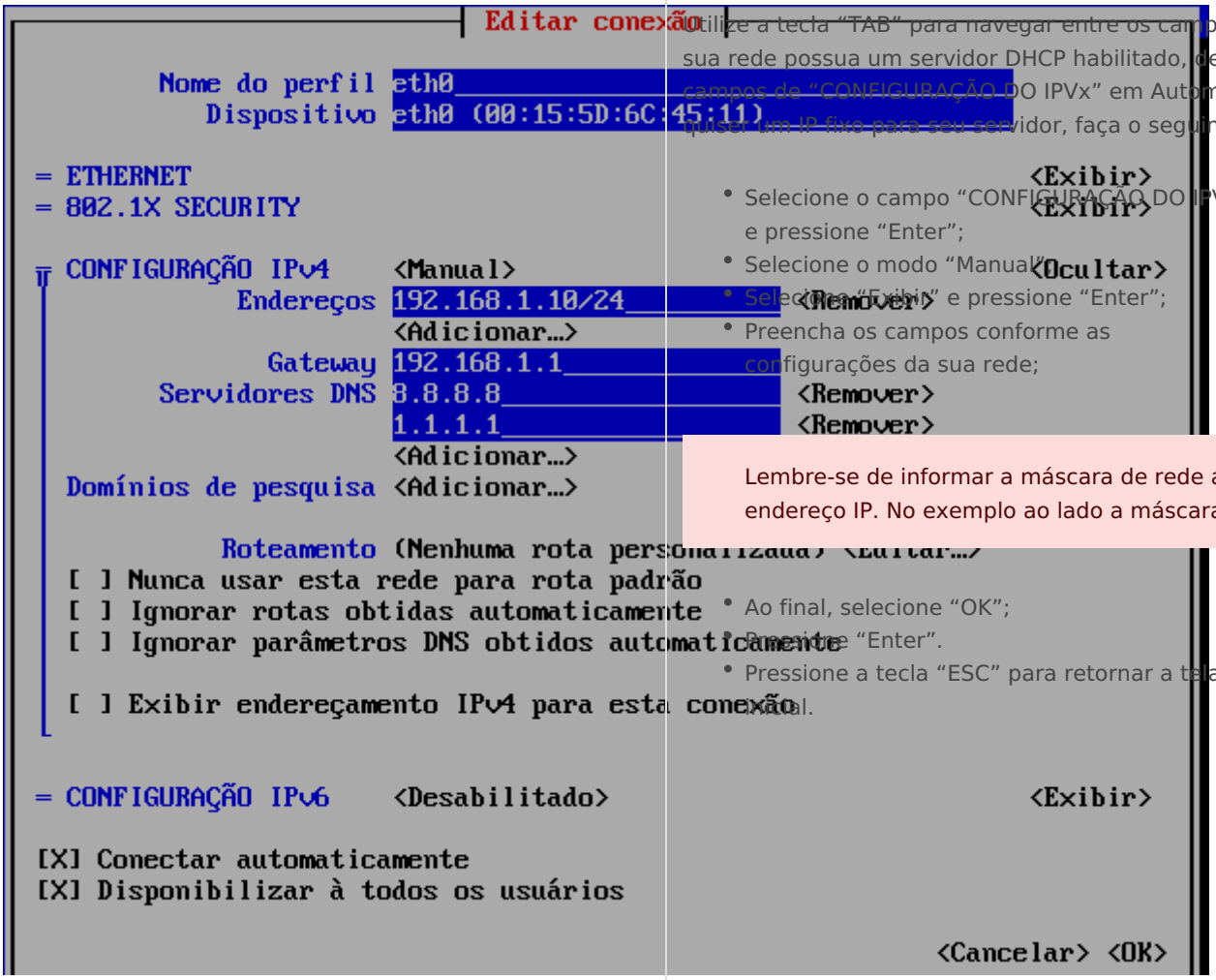
```
dnf install -y NetworkManager-tui
```

Depois de instalado, execute o gerenciador:

```
nmtui
```

Siga a sequência abaixo para editar as configurações de rede:

	• Selecione “Editar a conexão”; • Pressione “Enter”.
	• Selecione sua conexão de rede; • Selecione “Editar”.

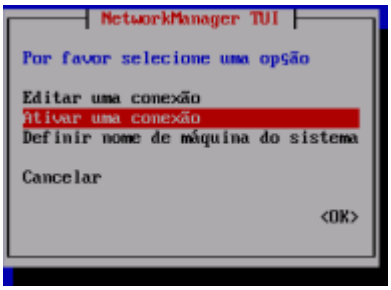


Utilize a tecla “TAB” para navegar entre os campos. Caso sua rede possua um servidor DHCP habilitado, deixe os campos de “CONFIGURAÇÃO DO IPVx” em Automático. Se quiser um IP fixo para seu servidor, faça o seguinte:

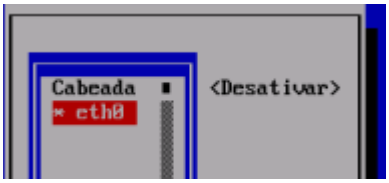
- Selecione o campo “CONFIGURAÇÃO DO IPVx” e pressione “Enter”;
- Selecione o modo “Manual”;
- Selecione “Exibir” e pressione “Enter”;
- Preencha os campos conforme as configurações da sua rede;

Lembre-se de informar a máscara de rede após o endereço IP. No exemplo ao lado a máscara é /24.

- Ao final, selecione “OK”;
- Pressione “Enter”.
- Pressione a tecla “ESC” para retornar a tela inicial.



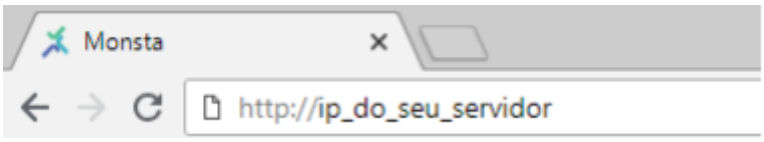
- Selecione “Ativar uma conexão” e pressione “Enter”.



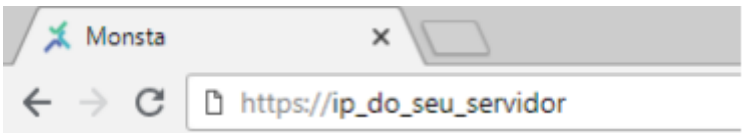
- Selecione a placa de rede que teve seu IP alterado e pressione “Enter” para desativá-la;
- Em seguida, pressione “Enter” novamente para ativá-la.
- Pressione “ESC” até sair do programa e retornar ao prompt de comando.

Acessar o Monsta

Após configurar o endereço IP do servidor, abra um navegador de internet e acesse:



ou



A tela de login do Monsta será apresentada. Para efetuar o login, utilize suas credencias.

Regras de Firewall (Opcional)

Se a sua rede possui um firewall que controla os acessos à internet, libere os seguintes hosts e portas:

> Host a.ntp.br e 2.fedora.pool.ntp.org
> Host mind.monsta.com.br na porta 443/TCP
> Host mind.monsta.com.br na porta 80/TCP

As portas acima para mind.monsta.com.br e www.monsta.com.br permitem:

-> Backup automático das configurações.
-> Restauração do backup em caso de alguma falha.
-> Envio de notificações por E-mail, SMS e Telegram.
-> Checagem do estado da comunicação entre o Monsta instalado em seu servidor e o a Nuvem do Monsta. Com isso é possível receber alertas em caso de paradas inesperadas do serviço de monitoramento, tal como o desligamento impróprio do servidor ou falha no link de internet.
-> Autenticação das Chaves de Licenciamento.
-> Verificar e atualizar a versão do sistema.

Dica

Utilize este tutorial para configurar regras do seu firewall caso sua instalação do Fedora tenha instalado o sistema FirewallD:

Firewalld - Utilização

Contato

Monsta Tecnologia Ltda

Site: http://www.monsta.com.br

Downloads: http://www.monsta.com.br/download.html

E-mail: contato@monsta.com.br

Linux perdendo pacotes por tabela nf_conntrack cheia

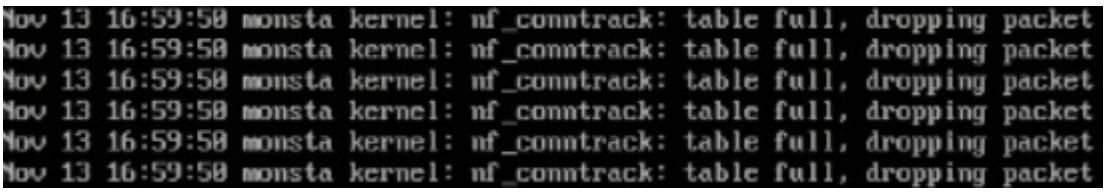
Este artigo demonstra como resolver o problema da perda intermitente de conexão ou pacotes que ocorre quando a tabela de rastreamento de conexões (*conntrack*) do kernel Linux está cheia.

1. Problema e Causas

O Linux usa o `nf_conntrack` (*Network Filter Connection Tracking*) para rastrear todas as conexões de rede ativas (TCP, UDP, ICMP etc.), necessário para o correto funcionamento do *firewall* (*iptables/nftables*) e do NAT (*Network Address Translation*).

Quando o número de conexões ativas atinge o limite máximo configurado, o *kernel* não consegue rastrear novas conexões e, por padrão, as descarta. Isso se manifesta como:

- Perda de conexão e pacotes no Linux.
- Falha intermitente para estabelecer novas conexões.
- Mensagens de erro no log do sistema (`/var/log/messages` ou `dmesg`), como:
  - `kernel: nf_conntrack: table full, dropping packet`
  - `nf_conntrack: table full`



Esse problema influencia no monitoramento do Monsta, causando falha de coleta em monitores de forma aleatória, pois o Monsta envia a solicitação e não recebe uma resposta.

Motivos que podem causar o esgotamento da tabela:

1. **Alto Tráfego de Conexões de Curta Duração:** Servidores que lidam com muitas conexões que são abertas e fechadas rapidamente podem encher a tabela rapidamente. Uma grande quantidade de monitores no Monsta pode contribuir.
2. **Ataques de Negação de Serviço (DDoS/DoS):** Um ataque de inundação de pacotes, especialmente *SYN floods* (que tentam abrir muitas conexões TCP incompletas), ou grandes volumes de tráfego UDP (que usa o *conntrack* para rastreamento básico) podem esgotar a tabela imediatamente.
3. **Timeouts Longos Demais:** Se o tempo que o kernel leva para "esquecer" uma conexão inativa (*timeout*) for muito longo, as entradas ficam presas na tabela, mesmo que a

conexão tenha sido encerrada. Isso é especialmente problemático para conexões TCP no estado `TIME_WAIT` (o *timeout* padrão de 60 segundos é frequentemente longo demais para ambientes de alto tráfego).

Como confirmar o problema

Você pode verificar o estado da tabela com os seguintes comandos:

```
# Limite máximo de conexões (nf_conntrack_max)
cat /proc/sys/net/netfilter/nf_conntrack_max

# Número atual de conexões ativas (nf_conntrack_count)
cat /proc/sys/net/netfilter/nf_conntrack_count
```

Se o `nf_conntrack_count` estiver muito próximo ou igual ao `nf_conntrack_max`, a tabela está cheia.

2. Solução: Aumentar e Otimizar os Limites

A solução é aumentar o limite máximo de conexões (`nf_conntrack_max`) e otimizar os parâmetros de desempenho da tabela. Para alterar de forma permanente (sem perder as configurações ao reiniciar o Linux), siga os passos:

2.1 Edite o arquivo configuração do sistema `/etc/sysctl.conf` com um editor de texto (`vi`, `nano`...)

```
vi /etc/sysctl.conf
```

2.2 Adicione as seguintes linhas ao final do arquivo

```
######################################################
# Otimização de Conntrack para alto tráfego
######################################################
net.netfilter.nf_conntrack_max = 262144
net.netfilter.nf_conntrack_buckets = 65536
net.netfilter.nf_conntrack_tcp_timeout_time_wait = 30
```

2.3 Salve e feche o arquivo

2.4 Aplique as novas configurações sem precisar reiniciar o sistema

```
sysctl -p
```

3. Verificação

Após aplicar as alterações, verifique o novo limite.

```
cat /proc/sys/net/netfilter/nf_conntrack_max
# O resultado deve ser 262144
```

Contato

Monsta Tecnologia Ltda

Site: http://www.monsta.com.br

Downloads: http://www.monsta.com.br/download.html

E-mail: contato@monsta.com.br

MONSTA

MONITORAMENTO DE REDES

Comando yum não funciona no CentOS 7

O CentOS 7 chegou ao seu fim de vida (*EOL - End Of Life*) em 30 Junho de 2024 e os `mirrors` utilizados para atualizações e instalação de programas não respondem mais. Porém, os arquivos foram movidos para um "arquivo histórico" (o *vault*). Este artigo demonstra como corrigir o repositório para consultar no `vault.centos.org` para acessar os pacotes arquivados e assim tornar possível utilizar o comando `yum` para instalar programas no CentOS 7.

1. Backup

Antes de realizar alterações, faça uma cópia do arquivo base do repositório do CentOS.

```
cp -avr /etc/yum.repos.d/CentOS-Base.repo /etc/yum.repos.d/CentOS-Base.repo.backup
```

2. Edite o arquivo CentOS-Base.repo para apontar para o Vault

Abra o arquivo com um editor de texto (`vi`, `nano`...)

```
vi /etc/yum.repos.d/CentOS-Base.repo
```

Dentro do arquivo, procure por linhas que começam com `mirrorlist=` e comente-as (adicione um `#` no início da linha). Em seguida, descomente (remova o `#`) as linhas que começam com `baseurl=` e altere o URL para `http://vault.centos.org/7.9.2009/`.

Você precisará fazer isso para as seções `[base]`, `[updates]`, e `[extras]` (podes fazer também para o `[centosplus]`, se desejar).

Aqui está um exemplo de como deve ficar:

```
[base]
name=CentOS-$releasever - Base
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=os&infra=$in
fra
baseurl=http://vault.centos.org/7.9.2009/os/$basearch/
gpgcheck=1
```

```
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#released updates
[updates]
name=CentOS-$releasever - Updates
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=updates&infra=$infra
baseurl=http://vault.centos.org/7.9.2009/updates/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#additional packages that may be useful
[extras]
name=CentOS-$releasever - Extras
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=extras&infra=$infra
baseurl=http://vault.centos.org/7.9.2009/extras/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#additional packages that extend functionality of existing packages
[centosplus]
name=CentOS-$releasever - Plus
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=centosplus&infra=$infra
baseurl=http://vault.centos.org/7.9.2009/centosplus/$basearch/
gpgcheck=1
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
```

Salve e feche o arquivo.

Limpe o cache do `yum`.

```
yum clean all
```

Agora é possível instalar os programas desejados utilizando o comando `yum`.

Contato

Monsta Tecnologia Ltda

Site: http://www.monsta.com.br

Downloads: http://www.monsta.com.br/download.html

E-mail: contato@monsta.com.br

UFW - Gerenciamento de Firewall

UFW significa **Uncomplicated Firewall** (Firewall Descomplicado).

Ele é uma interface para gerenciar o firewall Netfilter no Linux, que é o sistema de filtragem de pacotes do sistema. O UFW foi desenvolvido com o objetivo de simplificar o processo de configuração de regras de firewall através do utilitário `iptables`.

O UFW é o método mais popular e recomendado para gerenciar o firewall em distribuições baseadas em Debian e Ubuntu.

Exemplos de Comandos UFW (Guia Prático)

A maioria dos comandos UFW exige privilégios de superusuário (`sudo`).

1. Verificação de Status

Verifique se o UFW está ativo e veja as regras atuais:

Ação	Comando	Saída de Exemplo
Verificar Status	`ufw status`	`Status: inactive` (ou `active`)
Verificar Detalhes	`ufw status verbose`	Lista todas as regras de forma detalhada.

2. Ativação e Desativação

É crucial definir as regras antes de ativar, para não se trancar para fora do servidor.

Ação	Comando	Observação
Ativar UFW	`ufw enable`	**Atenção:** Se não tiver uma regra `allow ssh`, você perderá o acesso remoto.
Desativar UFW	`ufw disable`	Remove o firewall (não recomendado).

Ação	Comando	Observação
Resetar Regras	`ufw reset`	Remove todas as regras definidas pelo usuário.

3. Políticas Padrão (Default)

Configure o que acontece com o tráfego que não corresponde a nenhuma regra específica.

Ação	Comando	Resultado
Bloquear Entrada (Recomendado)	`ufw default deny incoming`	Nenhuma conexão externa é permitida, a menos que especificada.
Permitir Saída	`ufw default allow outgoing`	Seu servidor pode iniciar conexões com o mundo exterior.

4. Adicionar Regras (Permissões)

Objetivo	Comando	Observação
Permitir SSH (Porta 22)	`ufw allow ssh`	Usa o nome do serviço para liberar a porta 22/TCP.
Permitir HTTP (Porta 80)	`ufw allow http`	Libera a porta 80/TCP.
Permitir HTTPS (Porta 443)	`ufw allow 443/tcp`	Libera pelo número da porta e protocolo.
Porta Específica	`ufw allow 5432/udp`	Libera a porta 5432 apenas para o protocolo UDP.
Tráfego de IP Específico	`ufw allow from 192.168.1.100 to any port 3306`	Permite que apenas o IP `192.168.1.100` acesse a porta 3306 (MySQL).

5. Remover Regras

A remoção pode ser feita pelo número da regra ou pelo texto da regra.

Ação	Comando	Observação
Remover por Texto	`ufw delete allow http`	Remove a regra de acesso a porta http (80/TCP).
Remover por Número	`ufw status numbered` `ufw status delete [número]`	O primeiro comando retorna uma lista com as regras existentes e sua posição, o segundo remove a regra na posição selecionada.