🔥 Servidor Firewall (nftables)

Este documento apresenta as etapas para **configuração do firewall** em servidores **Debian 13 (Trixie)** utilizando o **nftables**, responsável pelo controle e filtragem do tráfego entre as redes LAN, DMZ e WAN.

🎯 Objetivo

O **Firewall** tem como função **controlar o tráfego de entrada e saída de pacotes** entre redes, protegendo os servidores e usuários de acessos indevidos.
Com o **nftables**, é possível definir políticas de segurança, NAT (Network Address Translation) e regras de encaminhamento de pacotes de forma moderna e eficiente.

📋 Descrição do Serviço

Item	Detalhe
Software	nftables
Sistema operacional	Debian 13 (Trixie)
Função	Controle de tráfego e NAT entre redes (LAN ↔ DMZ ↔ WAN)
Arquivos principais	`/etc/nftables.conf` e `/etc/sysctl.d/99-custom-forwarding.conf`
Serviço	`nftables.service`

🛠 Instalação e Configuração do Firewall

1️⃣ Habilitar o encaminhamento de pacotes (IP Forwarding)

Crie o arquivo `/etc/sysctl.d/99-custom-forwarding.conf`:

```
sudo vim /etc/sysctl.d/99-custom-forwarding.conf
```

Adicione o conteúdo abaixo:

```
net.ipv4.ip_forward=1
```

Aplique a configuração:

```
sudo sysctl --system
```

> Essa etapa garante que o servidor possa encaminhar pacotes entre interfaces de rede distintas (função essencial de um firewall).

2️⃣ Configurar o nftables

Substitua o conteúdo do arquivo principal do firewall:

```
sudo vim /etc/nftables.conf
```

Copie o conteúdo do arquivo `nftables.conf` deste repositório e personalize conforme o ambiente (interfaces, sub-redes e regras de filtragem).

---

3 Aplicar e testar a configuração

Teste o arquivo de regras antes de ativar o serviço:

```
sudo nft -f /etc/nftables.conf
```

Visualize as regras aplicadas:

```
sudo nft list ruleset
```

---

4 Habilitar o serviço nftables

```
sudo systemctl enable nftables
sudo systemctl start nftables
sudo systemctl status nftables
```

Após reiniciar o servidor, o firewall será carregado automaticamente.

Testes de funcionamento

Após aplicar as regras, execute testes de conectividade entre as zonas:

```
# Verifique se tem conexão à Internet
ping google.com

# Verificar o IP público da sua rede
curl ifconfig.me
```

Para logs e diagnósticos:

```
sudo journalctl -u nftables
```
