Relatório Acadêmico — Configuração de Firewall no Ubuntu 22.04 LTS

# 1. Introdução

Este relatório tem como objetivo apresentar de forma detalhada a configuração básica de firewall no sistema operacional Ubuntu 22.04 LTS, utilizando as ferramentas nativas UFW (Uncomplicated Firewall) e iptables. Os firewalls são considerados a primeira linha de defesa contra ataques cibernéticos, pois controlam o tráfego de entrada e saída em uma rede. No contexto acadêmico e corporativo, entender e dominar essas ferramentas é essencial para garantir segurança e estabilidade.  
  
O UFW foi desenvolvido para simplificar o uso do iptables, tornando a configuração mais acessível para usuários iniciantes e intermediários. Já o iptables oferece maior flexibilidade e granularidade, sendo amplamente utilizado em servidores e ambientes críticos. A comparação entre ambas as ferramentas permite compreender as vantagens e limitações de cada uma, contextualizando-as em cenários reais de uso.

# 2. Metodologia

O sistema operacional utilizado foi o Ubuntu 22.04 LTS (Jammy Jellyfish). O experimento consistiu em configurar regras de firewall utilizando tanto o UFW quanto o iptables, registrando os comandos e analisando seus efeitos.  
  
Procedimentos realizados:  
- Atualização do sistema e instalação do UFW.  
- Ativação do UFW e verificação de status.  
- Criação de regras para permitir portas de serviços essenciais (SSH, HTTP).  
- Bloqueio de portas inseguras (FTP, Telnet).  
- Testes de conectividade com ping, SSH e acesso a servidor web.  
- Aplicação de regras no iptables para reforçar segurança e comparação com UFW.  
  
Cada comando foi analisado de forma a compreender sua função e impacto prático no tráfego de rede.

# 3. Análise dos Comandos e Configurações

A seguir, detalhamos os principais comandos utilizados, com explicações do que cada um realiza na prática:

UFW — Principais comandos utilizados:

sudo apt update → Atualiza a lista de pacotes.

sudo apt install ufw -y → Instala o firewall UFW.

sudo ufw enable → Ativa o firewall.

sudo ufw status verbose → Mostra as regras atuais e status do firewall.

sudo ufw allow 22/tcp → Libera a porta 22 (SSH).

sudo ufw allow 80/tcp → Libera a porta 80 (HTTP).

sudo ufw deny 21/tcp → Bloqueia a porta 21 (FTP).

sudo ufw delete allow 80/tcp → Remove a regra que libera a porta 80.

ipTABLES — Principais comandos utilizados:

sudo iptables -L -v → Lista as regras aplicadas, com detalhes de pacotes.

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT → Libera conexões SSH.

sudo iptables -A INPUT -p tcp --dport 21 -j DROP → Bloqueia conexões FTP.

sudo iptables-save > /etc/iptables/rules.v4 → Salva regras para persistirem após reinicialização.

Na prática, o UFW simplificou a execução de regras básicas, enquanto o iptables demonstrou ser mais flexível e poderoso, mas exigiu maior atenção e cuidado com a sintaxe. Erros comuns, como esquecer de salvar regras no iptables, podem comprometer a configuração após reinicialização.

# 4. Comparação e Análise Crítica

Para avaliar as duas ferramentas, o grupo construiu uma análise comparativa considerando diferentes critérios:

• Facilidade de uso: O UFW é simples e intuitivo, ideal para iniciantes. Já o iptables requer conhecimento técnico avançado.  
• Nível de controle: O UFW atende necessidades básicas; o iptables permite criar regras extremamente específicas.  
• Sintaxe: O UFW usa comandos curtos e fáceis de memorizar; o iptables exige uma sintaxe detalhada.  
• Indicado para: UFW é recomendado para usuários domésticos e pequenas empresas; o iptables é mais adequado para administradores de sistemas e servidores corporativos.  
• Consumo de recursos: Ambos consomem poucos recursos, mas em servidores de alta disponibilidade o iptables oferece maior robustez.  
  
Discussão: O grupo concluiu que o UFW é útil para aprendizado inicial e para configurações rápidas, mas o iptables é indispensável em ambientes críticos. Portanto, ambos se complementam dentro do Ubuntu.

# 5. Conclusão

O trabalho alcançou seu objetivo principal, permitindo compreender como configurar um firewall no Ubuntu 22.04 LTS utilizando UFW e iptables. A prática evidenciou que o UFW é eficiente para tarefas simples e rápidas, enquanto o iptables se mostra essencial para configurações avançadas e ambientes de missão crítica.  
  
O estudo reforçou a importância de dominar ambas as ferramentas, pois cada uma atende a diferentes necessidades. Além disso, destacou a relevância do firewall como camada fundamental de proteção contra ataques cibernéticos. Futuramente, recomenda-se explorar também o uso de nftables, que vem sendo adotado como sucessor do iptables.

# 6. Autoavaliação e Referências

O trabalho foi desenvolvido de forma colaborativa pelo grupo. Cada integrante contribuiu em etapas distintas: alguns focaram na pesquisa teórica, outros na execução prática e nos testes, enquanto houve dedicação especial na revisão e organização do relatório.  
  
As principais dificuldades estiveram relacionadas à sintaxe do iptables, que exige precisão. Houve momentos em que regras foram aplicadas incorretamente, exigindo correção e aprendizado na prática. Essa experiência demonstrou a importância de testar e revisar constantemente as configurações de firewall. No entanto, o grupo avaliou positivamente o resultado final, pois todos adquiriram maior compreensão sobre segurança de redes e configuração de firewalls no Linux.

Referências:

Documentação oficial do Ubuntu: https://help.ubuntu.com/community/UFW

Documentação iptables: https://linux.die.net/man/8/iptables

Vídeo: https://www.youtube.com/watch?v=wwaf0yJuv04

Vídeo: https://www.youtube.com/watch?v=BZ4yuTQmxdo