Relatório do 3º trabalho de Segurança Computacional

- Mateus Elias de Macedo - 222011561
- Andrey Calaça Resende - 180062433

1. Introdução

Esse relatório objetiva descrever a implementação de uma rede segmentada com regras de segurança aplicadas por meio de um firewall. A atividade consistiu em montar uma topologia composta por diferentes sub-redes, incluindo uma zona desmilitarizada, servidores internos, estações de trabalho e uma rede pública simulada, com o controle de acesso sendo realizado por um roteador com firewall configurado manualmente.

A rede foi simulada utilizando o GNS3, com roteadores MikroTik 6.47.1. Além disso, foi implementado um servidor DHCP em uma sub-rede separada, com o uso de DHCP relay para atender dispositivos em outra sub-rede. O funcionamento da rede foi verificado por meio da captura de pacotes utilizando Wireshark.

2. Topologia da Rede

A topologia da rede foi construída de acordo com os requisitos do projeto, com a divisão em múltiplas sub-redes, cada uma com um propósito específico. A estrutura geral possui os seguintes elementos:

- Internet Pública (Sub-rede 4 - 172.16.0.0/24)
- DMZ (Sub-rede 1 - 10.0.20.0/24)
- Servidores Internos (Sub-rede 2 - 10.0.30.0/24)
- Estações de Trabalho Internas (Sub-rede 5 - 10.0.40.0/24)
- Infraestrutura de Interligação (Sub-rede 3 - 192.168.0.0/30)

Os roteadores foram configurados com endereços IP em todas as interfaces, sendo o roteamento implementado de forma dinâmico com RIP, e a comunicação

foi controlada por regras do firewall. O Webserver e DHCPServer foram implementados como roteadores por conveniência;

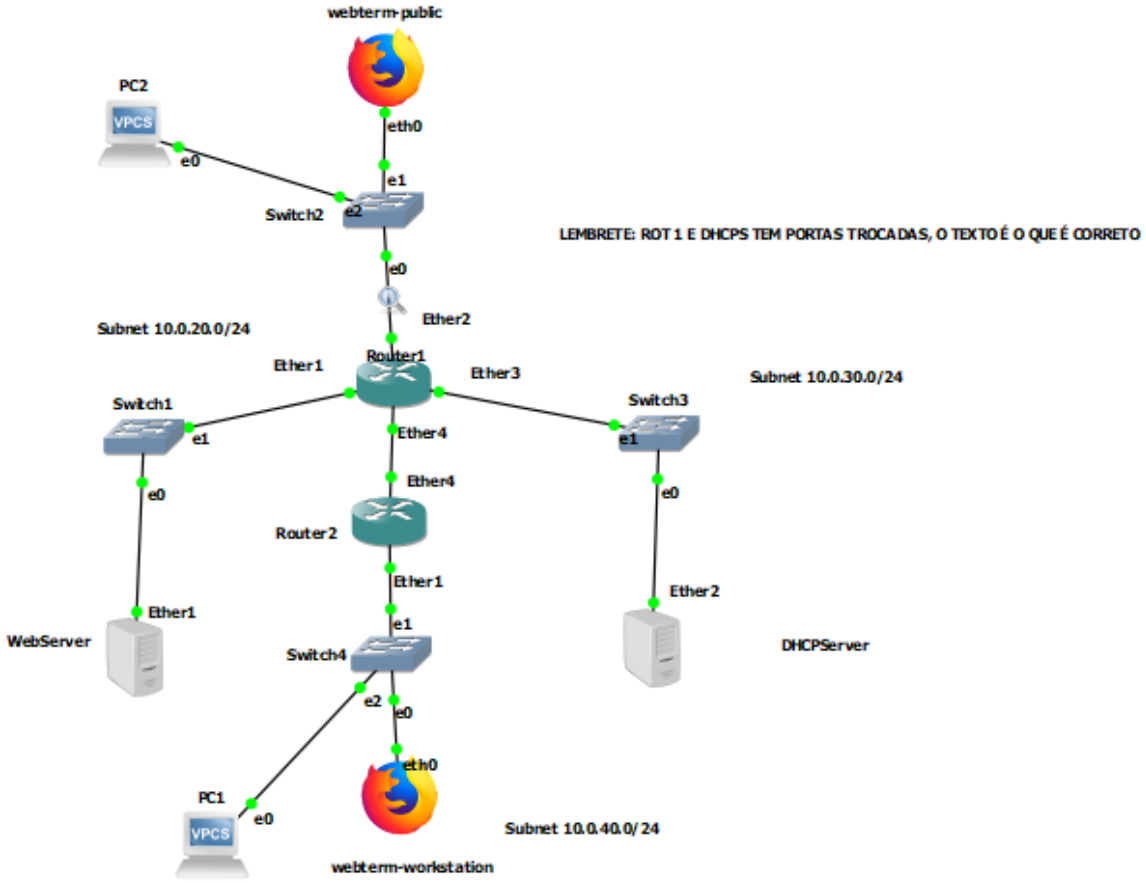

Figura 1 - Topologia da rede implementada.

3. Configuração do Firewall

O firewall foi configurado no Roteador 1 para controlar o tráfego entre as sub-redes, permitindo apenas os fluxos de dados explicitamente autorizados. Para isso foi adotada uma política de negação por padrão, na qual todo o tráfego é bloqueado, exceto aquele que atende às regras definidas manualmente.

A configuração foi realizada usando o MikroTik RouterOS, por meio da cadeia forward, responsável pelo tráfego que passa pelo roteador.

Como foi definido na especificação do projeto, 5 regras foram implementadas:

- 1 - Permissão de conexões HTTP, originadas na sub-rede 4 com destino ao Web Server na sub-rede 1, na porta TCP 80;

- 2 - Permissão de pacotes de conexões já estabelecidas ou relacionadas;
- 3 - Permissão de solicitações DHCP, originadas na sub-rede 3, na porta UDP 67;
- 4 - Permissão de respostas DHCP do Servidor (sub-rede 2) para o Cliente (Sub-rede 5);
- 5 - Bloqueio de todo o tráfego restante.

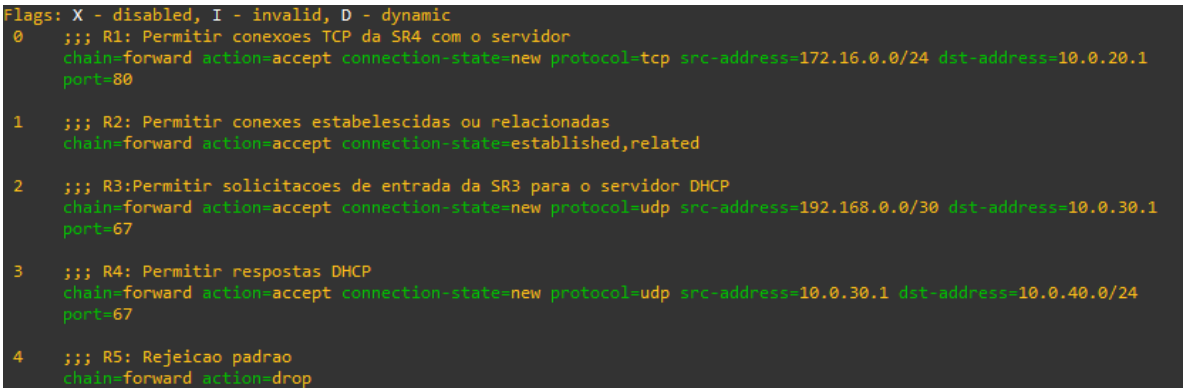

Figura 2 - Regras de firewall configuradas no roteador 1.

4. Configuração do DHCP

A distribuição de endereços IP dinâmicos foi realizada por um servidor DHCP na sub-rede 2. Esse servidor foi configurado para atender a dispositivos na sub-rede 5, onde estão conectadas as estações de trabalho internas.

Como o servidor DHCP está em uma sub-rede diferente dos clientes, foi necessário configurar o roteador 2 como retransmissor DHCP (DHCP relay).

Figura 3 – DHCP relay no roteador 2.

Além da ativação do serviço, foi criado um pool de endereços válidos para a sub-rede 5, com exclusão dos IPs utilizados por dispositivos configurados estaticamente, como o roteador.

Durante os testes, dois dispositivos na sub-rede 5 receberam endereços IP automaticamente:

- Um PC recebeu o IP 10.0.40.253/24

- Uma workstation recebeu o IP 10.0.40.252/24

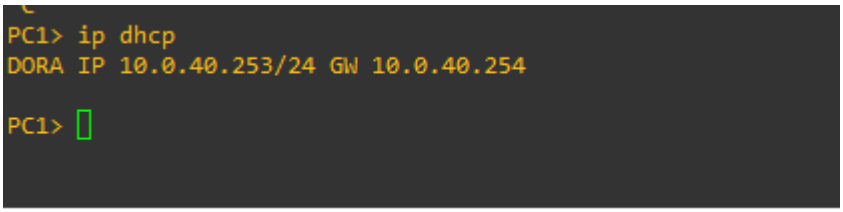

Figura 4 - IP atribuído automaticamente a um PC.

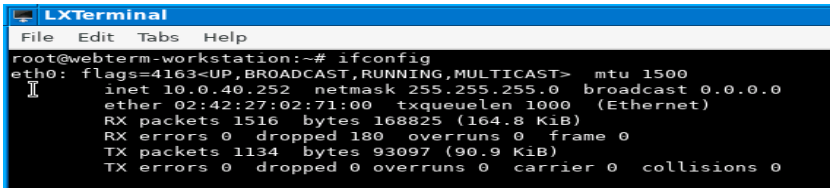

Figura 5 - IP atribuído automaticamente a uma workstation.

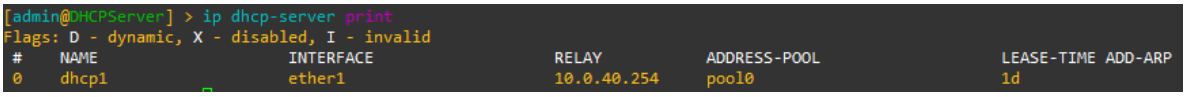

Figura 6 – Print do servidor DHCP no DHCPServer.

5. Testes e Resultados

Para validar a configuração da rede e o funcionamento das regras, foram realizados testes, sendo esses os principais:

- Atribuição IP via DHCP, como demonstrado na seção anterior
- Acesso HTTP ao Web Server

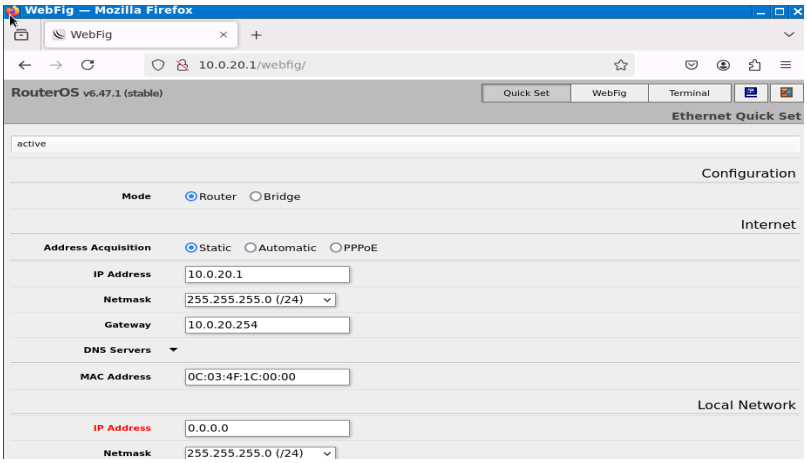

Figura 7 - Página carregada no navegador.

- Acesso ao roteador 1

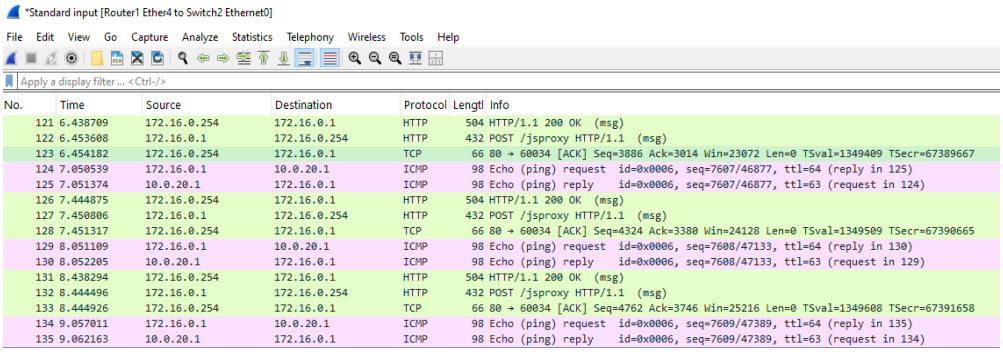

Figura 8 - Captura de pacotes mostrando troca bidirecional de dados.

- Bloqueio de acesso à Sub-rede 2

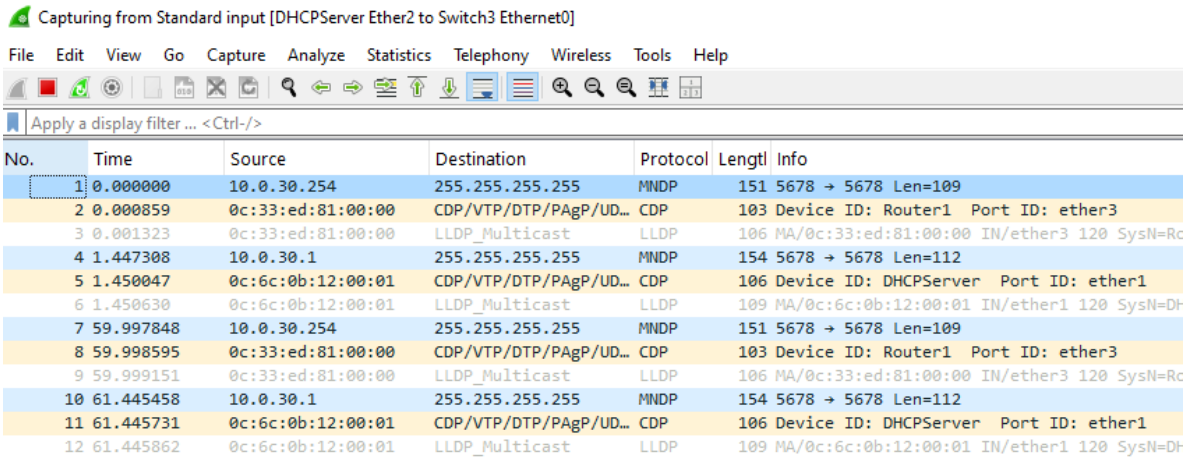

Figura 9 - Captura de pacotes mostrando bloqueios.

6. Conclusão

A implementação da rede segmentada com firewall atendeu aos requisitos do projeto, permitindo apenas o acesso devidamente autorizado a serviços como HTTP e DHCP, e bloqueando todo o restante.

Os testes comprovaram o funcionamento correto das regras do firewall, do servidor DHCP e da estrutura de roteamento.

O trabalho permitiu aplicar na prática conceitos fundamentais de segurança de redes e controle de tráfego.

Link do repositório: https://github.com/Mattelis/SG-P3