Universidade de Brasília

INSTITUTO DE EXATAS - IE

DEPARTAMENTO DE CIÊNCIAS DA COMPUTAÇÃO - CIC

SEGURANÇA COMPUTACIONAL 1/2025

TRABALHO DE IMPLEMENTAÇÃO 3

Tema: Implementação de Um Firewall	**Marcelo Marques Rodrigues (221018960)**
	Arthur Delpino Barbabella (221002094)

1. INTRODUÇÃO

Este projeto tem como objetivo implementar e testar um *firewall* em uma rede segmentada em cinco sub-redes, aplicando regras de filtragem para restringir e controlar o tráfego entre diferentes zonas (*DMZ*, *Internet* Pública, Rede Interna e Servidores), através de regras definidas com o *iptables*. A configuração envolveu a criação de serviços de rede (como *DHCP* e *HTTP*) e o bloqueio de tráfego não autorizado. Os testes de funcionamento foram realizados com o auxílio do *Wireshark* e o ambiente foi simulado utilizando o *GNS3 (Graphical Network Simulator-3)* e o *VMWare*.

2. REDE: CONFIGURAÇÃO E TOPOLOGIA

Conforme mostrado na Tabela 1 a seguir, a rede foi organizada em cinco sub-redes distintas, cada uma responsável por funções específicas no ambiente.

Sub-rede	Função	Faixa de IP
Subnet 1	DMZ (Servidor WEB)	10.0.20.0/24
Subnet 2	Servidor DHCP	10.0.30.0/24
Subnet 3	Rede interna dos roteadores	192.168.0.0/30
Subnet 4	Internet Pública	172.16.0.0/24
Subnet 5	Estações de Trabalho Internas	10.0.40.0/24

Tabela 1 – Sub-redes da topologia implementada.

O comportamento esperado da rede é descrito a seguir:

- O *host webterm-workstation* (Sub-rede 5) deve obter *IP* via *DHCP*, com retransmissão feita pelo Router2 até o servidor na Sub-rede 2;

- O Router1, que implementa um *firewall* com *iptables*, deve permitir:
    - Tráfego *DHCP (Discover, Offer, Request, ACK)*;
    - Acesso *HTTP* da Sub-rede 5 e 4 ao Servidor *Web* (DMZ);
    - Pacotes de conexões estabelecidas;
- Todo o restante deve ser bloqueado, garantindo a vigência do controle de acesso exigido na descrição do projeto.

A Figura 1 apresenta a topologia da rede implementada no simulador *GNS3 (Graphical Network Simulator-3)*, contendo cinco sub-redes interligadas por dois roteadores *Debian*. Os servidores *(DHCP e Web)* foram emulados por máquinas virtuais no *VMware*. Cada segmento foi configurado com endereços *IP* estáticos e com rotas que forçam a passagem pelo roteador central (Router1), exceto o *webterm-workstation*, que recebe seu endereço *IP* dinamicamente via *DHCP*, após envio da solicitação inicial.

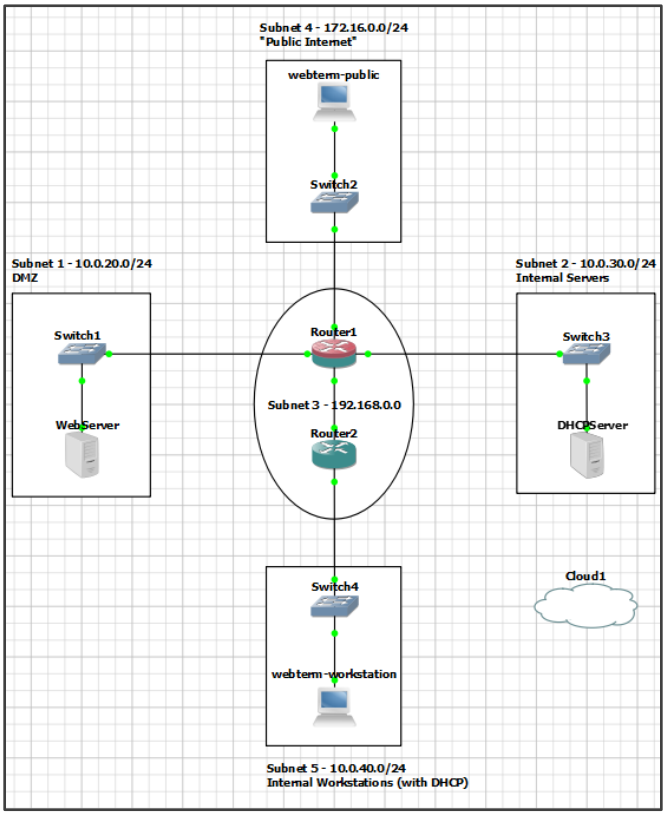

Figura 1 – Topologia da rede no GNS3.

3. CONFIGURAÇÃO DO FIREWALL

Os dispositivos de rede *WebServer*, *DHCPServer*, Router1, Router2, *webterm-workstation* e *webterm-public* são todos máquinas virtuais Debian 11.10, personalizados e configurados para que emulem o comportamento esperado de cada um deles. No caso do *firewall*, foi implementado em cima do Router1 (um Debian 11.10) e configurado com

a ferramenta *iptables*, responsável por filtrar o tráfego entre as sub-redes por meio da cadeia FORWARD. A política adotada foi restritiva, permitindo apenas os fluxos necessários ao funcionamento dos serviços exigidos.

A figura 2 é a saída do comando *sudo iptables -L -v –n, m*ostrando as políticas de bloqueio por padrão (DROP) nas cadeias de entrada (INPUT) e encaminhamento (FORWARD).

```
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

    0     0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0

    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0


Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

    0     0 ACCEPT     udp  --  *      *       10.0.30.1            10.0.40.253
          udp spt:67 dpt:67
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
          ctstate RELATED,ESTABLISHED
    0     0 ACCEPT     udp  --  *      *       192.168.0.2          10.0.30.1
          udp dpt:67
    0     0 ACCEPT     udp  --  *      *       10.0.30.1            192.168.0.2
          udp dpt:67
    0     0 ACCEPT     udp  --  *      *       10.0.30.1            10.0.40.0/24
          udp dpt:68
    0     0 ACCEPT     tcp  --  *      *       172.16.0.0/24        10.0.20.100
          tcp dpt:80
    0     0 ACCEPT     tcp  --  *      *       10.0.20.0/24         10.0.20.100
          tcp dpt:80
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0

    0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0
          LOG flags 0 level 4 prefix "[FIREWALL DROP] "
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0
```

Figura 2 – Regras de firewall.

As regras listadas permitem:

- Pacotes *DHCP* (portas *UDP* 67/68) entre o *DHCP Relay* e o Servidor *DHCP* (Sub-redes 3, 2 e 5);
- Conexões *HTTP* (porta *TCP* 80) advindas da Sub-rede 4 (172.16.0.0/24) e da Sub-rede 5 (10.0.20.0/24) com destino ao servidor *web* na DMZ (10.0.20.100);
- Pacotes de conexões estabelecidas;
- Requisições *ICMP* locais e *loopback*.

4. TESTES E VALIDAÇÃO

O funcionamento pleno da rede emulada no projeto pode ser verificado através da satisfação das seguintes exigências:

(1) “O host webterm-public e outros hosts nesta subrede conseguem acessar a página web no Servidor Web”.
(2) “O host webterm-public e outros hosts na subrede 5 conseguem acessar a página web no Servidor DHCP”.

(3) “O host webterm-public consegue acessar a página web no Roteador”.
(4) “Respostas DHCP de saída do Servidor DHCP para a Sub-rede 5 devem ser permitidas”.

4.1 . SUBNET 4 ACESSA PÁGINA WEB NO SERVIDOR WEB

Na sequência de pacotes capturados da Figura 3, observa-se o estabelecimento de uma conexão TCP entre o host webterm-public, localizado na Sub-rede 4 (172.16.0.100), e o Servidor Web na Sub-rede 1 (10.0.20.100). A troca inicial de pacotes (SYN, SYN-ACK, ACK) estabelece a sessão, seguida por uma requisição HTTP (GET /) e a resposta com o status HTTP 200 OK, mostrando o funcionamento do serviço e a liberação do tráfego pela regra de firewall correspondente.

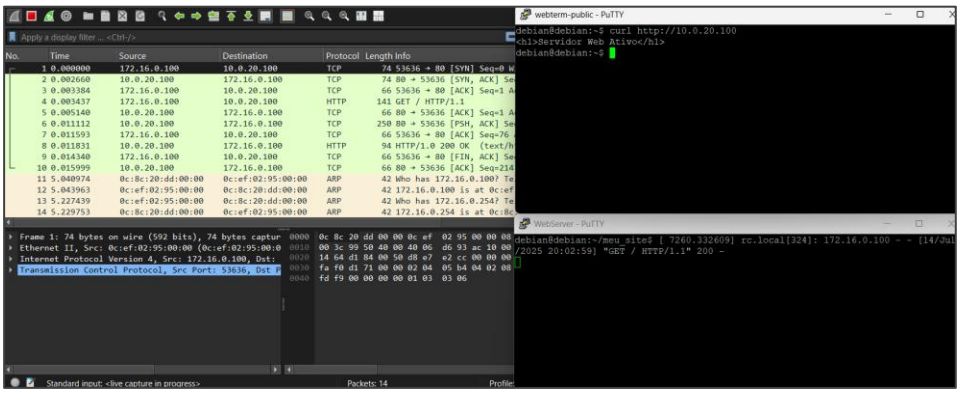

Figura 3 – Pacotes capturados na comunicação entre o webterm-public e o WebServer.

Para a captura, utilizou-se o recurso de “*Start capture*” do GNS3, com o *Wireshark* integrado. A escuta foi configurada diretamente no enlace entre a interface ens4 do *webterm-public* e o Switch2, possibilitando a interceptação precisa do tráfego gerado pela requisição *HTTP*.

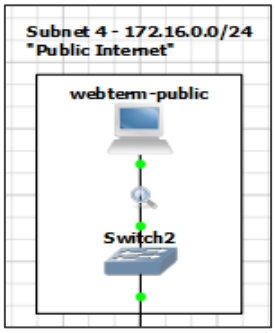

Figura 4 – *Feature* “*Start Capture*” ativada.

Como mostra a Figura 5, apenas a Sub-rede 5 possui permissão de acesso *HTTP* ao Servidor *Web*. Apesar do *ping* do *webterm-public* (Sub-rede 4) funcionar, a tentativa de conexão *TCP* (porta 80) é bloqueada pelo *firewall* no Router1. Isso resulta em retransmissões dos pacotes *SYN*, sem resposta, comportamento típico de pacotes descartados conforme a política de acesso definida no *iptables*.

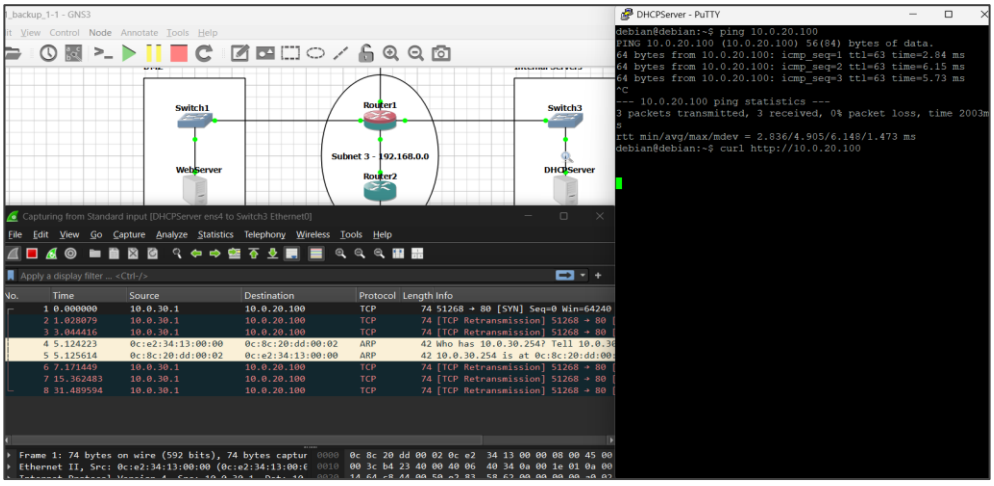

Figura 5 – Falha de conexão (bloqueio do firewall).

4.2. SUBNET 4 E 5 ACESSAM PÁGINA WEB NO SERVIDOR DHCP

Na figura 6, verifica-se que o host webterm-public (Sub-rede 4) foi capaz de estabelecer conexão TCP receber a página web após fazer o comando curl http://10.0.30.1, endereço IP do servidor DHCP (Sub-rede 2). Isso confirma que o firewall no Router1 permite o tráfego HTTP proveniente da Sub-rede 4 para o servidor DHCP.

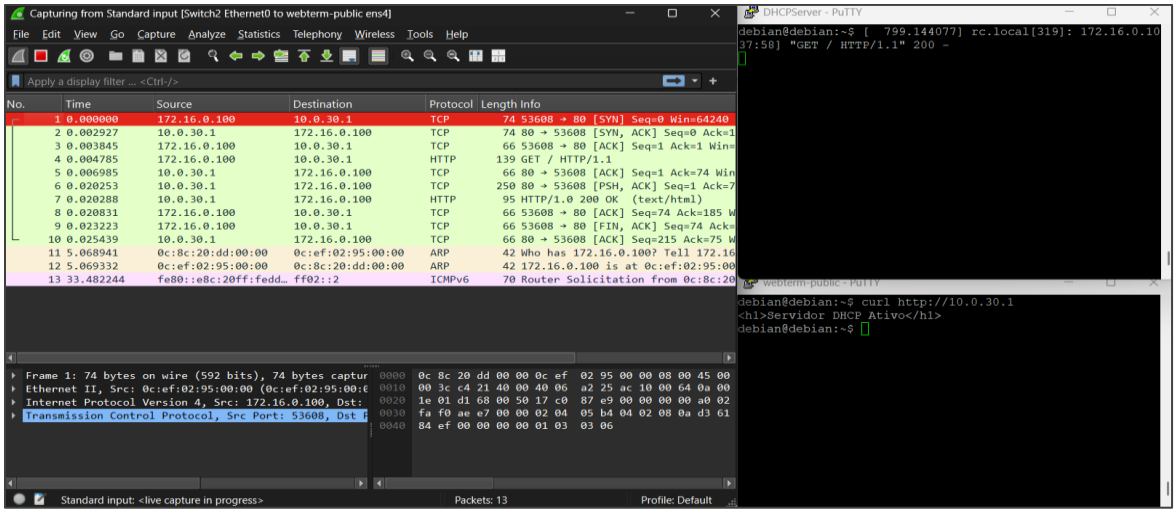

Figura 6 – Acesso bem-sucedido e conexão TCP.

O mesmo comportamento é verificado na Figura 7, com o *host webterm-workstation* (10.0.40.100, Sub-rede 5), confirmando que os sistemas finais de ambas as sub-redes estão autorizados a acessar o servidor *HTTP* do DHCPServer conforme as regras definidas no *firewall*.

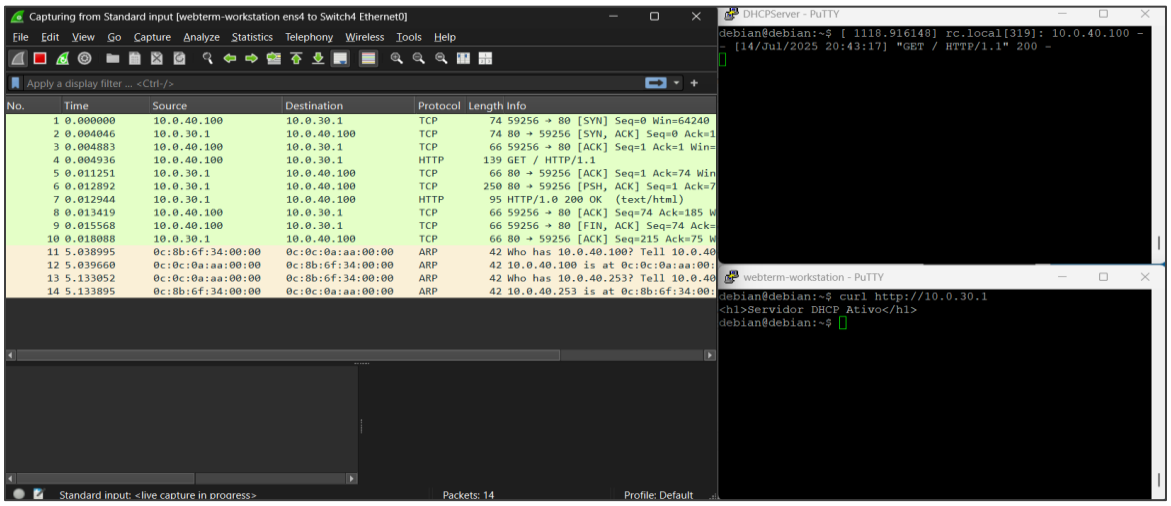

Figura 7 – Acesso bem-sucedido e conexão TCP.

4.3. SUBNET 4 ACESSA PÁGINA WEB NO ROTEADOR 1

O *host webterm-public* (Sub-rede 4) foi capaz de acessar com sucesso a página *web* disponibilizada pelo Router1, como evidencia a Figura 8. A partir do comando *curl http://172.16.0.254* correspondente ao endereço *IP* da interface do Router1 na Sub-rede 4, observou-se o recebimento do documento *HTML* no terminal. No *Wireshark*, é possível identificar o estabelecimento da conexão *TCP (SYN, SYN-ACK, ACK)*, seguido da requisição *HTTP* e da respectiva resposta enviada pelo Router1.

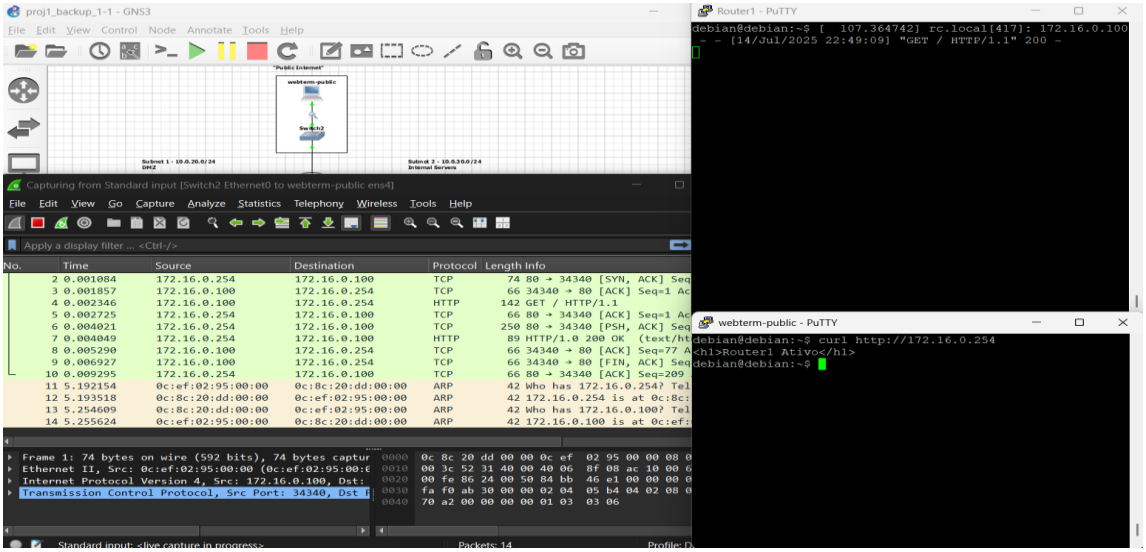

Figura 8 – Acesso bem-sucedido e conexão TCP.

4.4. CONFIGURAÇÃO DHCP

O DHCP no projeto é fornecido por um servidor localizado na Sub-rede 2, implementado em uma máquina virtual Debian configurada com o pacote isc-dhcp-server. Esse servidor oferece endereços IP na faixa de 10.0.40.100 a 10.0.40.200 para os hosts da Sub-rede 5. Como essa sub-rede não está diretamente conectada ao servidor, o Router2 foi configurado como um DHCP Relay, encaminhando as mensagens entre os clientes e o servidor. O funcionamento foi viabilizado por regras específicas no firewall do Router1, que permitem o tráfego DHCP entre as sub-redes envolvidas.

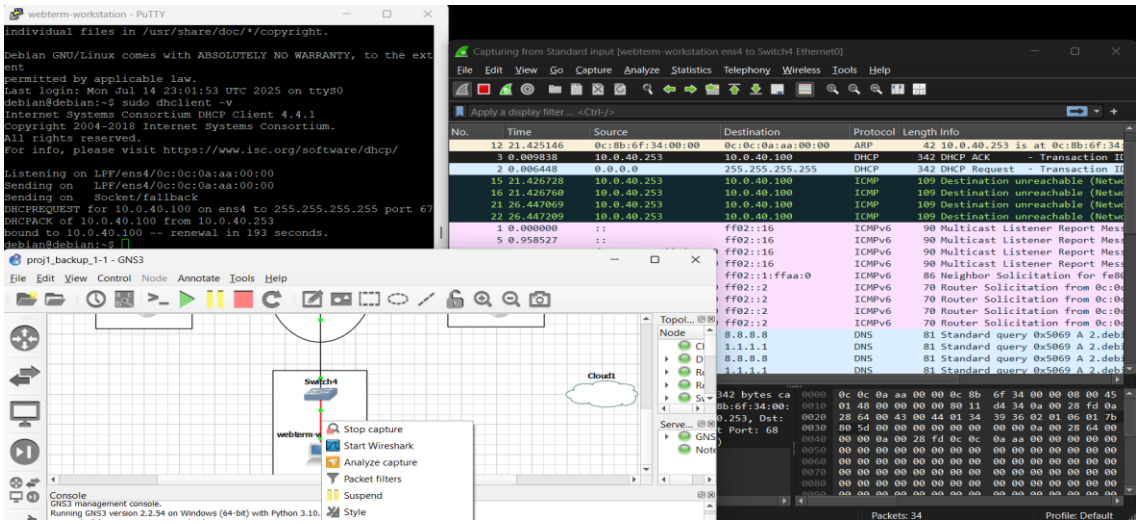

Figura 9 – Captura dos pacotes DHCP e atribuição de IP.

A Figura 9 comprova o funcionamento do DHCP. Ao executar *sudo dhclient -v* no *host webterm-workstation* (Sub-rede 5), foi atribuído o *IP* 10.0.40.100, conforme exibido no terminal. O *Wireshark* capturou os pacotes *DHCP (Request e ACK)*, demonstrando a interação entre o cliente, o Router2 (*relay*) e o servidor *DHCP* da Sub-rede 2.

5. COMENTÁRIOS ADICIONAIS

Como medida de automação, os *scripts* de configuração de rede e inicialização dos servidores *HTTP* foram inseridos no arquivo */etc/rc.local*, garantindo que os serviços necessários à simulação sejam executados automaticamente no *boot*. O uso do *rc.local* mostrou-se funcional e eficiente para o propósito do projeto, permitindo restaurar rapidamente o estado da rede em caso de reinicialização das máquinas virtuais no ambiente simulado.

6. CONCLUSÃO

A rede foi configurada com sucesso, cumprindo os requisitos propostos, como as regras específicas no *firewall*. Os testes demonstraram que os acessos foram devidamente permitidos ou bloqueados conforme o esperado, e os serviços (como o servidor *web*) funcionaram corretamente nas sub-redes designadas. No geral, o projeto mostrou a utilidade e o funcionamento de *firewalls* na aplicação de políticas de segurança e para garantir o controle e a comunicação entre os diferentes pontos da topologia.