

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 DHCP Server foram implementados como roteadores por conveniência;

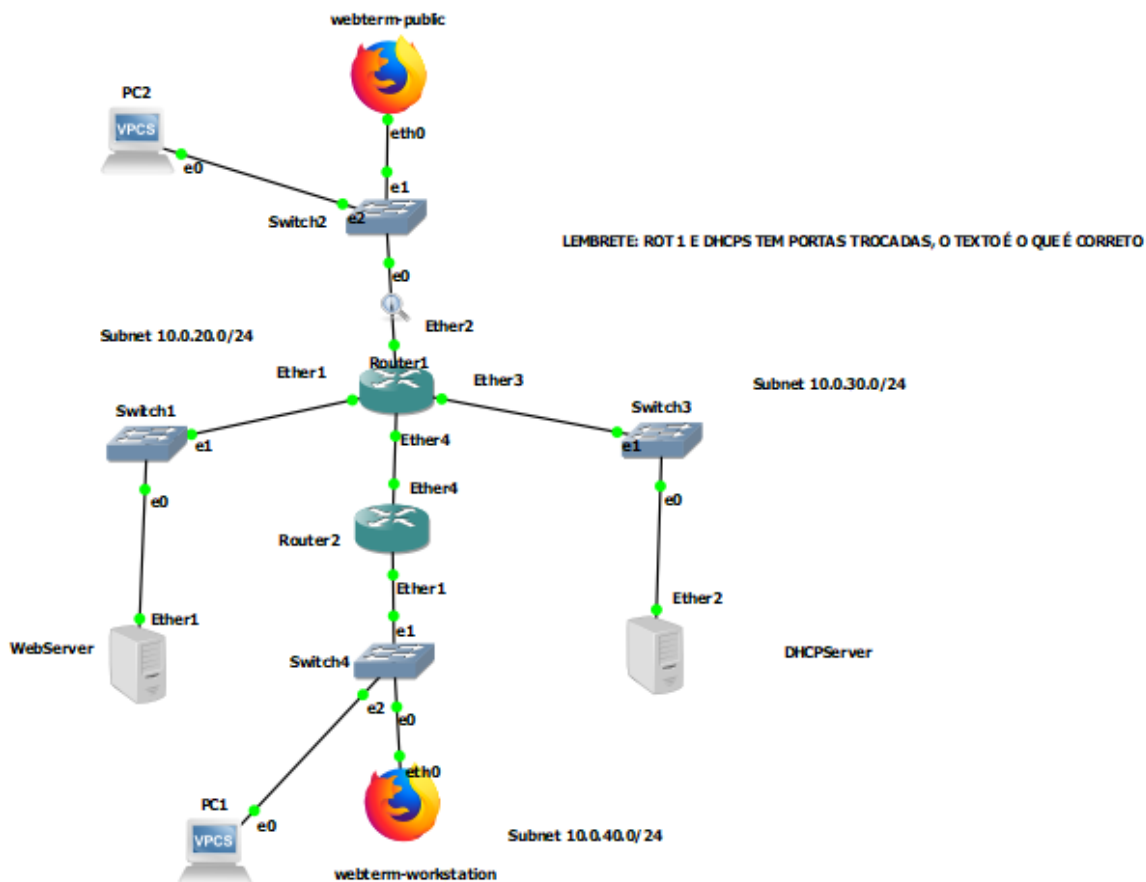


Figura 1 - Topologia da rede implementada.

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.

```
Flags: X - disabled, I - invalid, D - dynamic
0    ;; R1: Permitir conexoes TCP da SR4 com o servidor
    chain=forward action=accept connection-state=new protocol=tcp src-address=172.16.0.0/24 dst-address=10.0.20.1
    port=80

1    ;; R2: Permitir conexes estabelecidas ou relacionadas
    chain=forward action=accept connection-state=established,related

2    ;; R3: Permitir solicitacoes de entrada da SR3 para o servidor DHCP
    chain=forward action=accept connection-state=new protocol=udp src-address=192.168.0.0/30 dst-address=10.0.30.1
    port=67

3    ;; R4: Permitir respostas DHCP
    chain=forward action=accept connection-state=new protocol=udp src-address=10.0.30.1 dst-address=10.0.40.0/24
    port=67

4    ;; R5: Rejeicao padrao
    chain=forward action=drop
```

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).

```
[admin@router2] > ip dhcp-relay print
Flags: X - disabled, I - invalid
#  NAME                                INTERFACE    DHCP-SERVER    LOCAL-ADDRESS
0  relay1                              ether1       10.0.30.1      0.0.0.0
```

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

```
PC1> ip dhcp
DORA IP 10.0.40.253/24 GW 10.0.40.254
PC1> █
```

Figura 4 - IP atribuído automaticamente a um PC.

```
LXTerminal
File Edit Tabs Help
root@webterm-workstation:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.40.252 netmask 255.255.255.0 broadcast 0.0.0.0
    ether 02:42:27:02:71:00 txqueuelen 1000 (Ethernet)
    RX packets 1516 bytes 168825 (164.8 KiB)
    RX errors 0 dropped 180 overruns 0 frame 0
    TX packets 1134 bytes 93097 (90.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figura 5 - IP atribuído automaticamente a uma workstation.

```
[admin@DHCPserver] > ip dhcp-server print
Flags: D - dynamic, X - disabled, I - invalid
# NAME INTERFACE RELAY ADDRESS-POOL LEASE-TIME ADD-ARP
0 dhcp1 ether1 10.0.40.254 pool10 1d
```

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

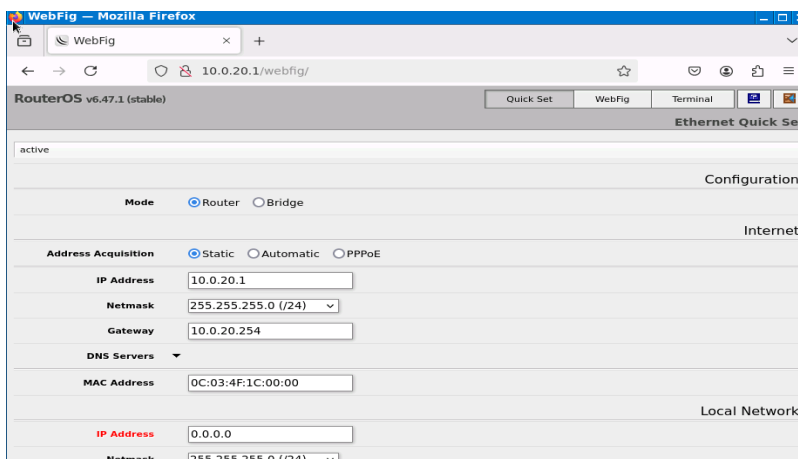


Figura 7 - Página carregada no navegador.

- Acesso ao roteador 1

Standard input [Router1 Ether4 to Switch2 Ethernet0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
121	6.438709	172.16.0.254	172.16.0.1	HTTP	504	HTTP/1.1 200 OK (msg)
122	6.453608	172.16.0.1	172.16.0.254	HTTP	432	POST /jsproxy HTTP/1.1 (msg)
123	6.454182	172.16.0.254	172.16.0.1	TCP	66	80 → 60034 [ACK] Seq=3886 Ack=3014 Win=23072 Len=0 TSval=1349409 TSecr=67389667
124	7.050539	172.16.0.1	10.0.20.1	ICMP	98	Echo (ping) request id=0x0006, seq=7607/46877, ttl=64 (reply in 125)
125	7.051374	10.0.20.1	172.16.0.1	ICMP	98	Echo (ping) reply id=0x0006, seq=7607/46877, ttl=63 (request in 124)
126	7.444875	172.16.0.254	172.16.0.1	HTTP	504	HTTP/1.1 200 OK (msg)
127	7.450806	172.16.0.1	172.16.0.254	HTTP	432	POST /jsproxy HTTP/1.1 (msg)
128	7.451317	172.16.0.254	172.16.0.1	TCP	66	80 → 60034 [ACK] Seq=4324 Ack=3380 Win=24128 Len=0 TSval=1349509 TSecr=67390665
129	8.051109	172.16.0.1	10.0.20.1	ICMP	98	Echo (ping) request id=0x0006, seq=7608/47133, ttl=64 (reply in 130)
130	8.052205	10.0.20.1	172.16.0.1	ICMP	98	Echo (ping) reply id=0x0006, seq=7608/47133, ttl=63 (request in 129)
131	8.438294	172.16.0.254	172.16.0.1	HTTP	504	HTTP/1.1 200 OK (msg)
132	8.444496	172.16.0.1	172.16.0.254	HTTP	432	POST /jsproxy HTTP/1.1 (msg)
133	8.444926	172.16.0.254	172.16.0.1	TCP	66	80 → 60034 [ACK] Seq=4762 Ack=3746 Win=25216 Len=0 TSval=1349600 TSecr=67391658
134	9.057011	172.16.0.1	10.0.20.1	ICMP	98	Echo (ping) request id=0x0006, seq=7609/47389, ttl=64 (reply in 135)
135	9.062163	10.0.20.1	172.16.0.1	ICMP	98	Echo (ping) reply id=0x0006, seq=7609/47389, ttl=63 (request in 134)

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

- Bloqueio de acesso à Sub-rede 2

Capturing from Standard input [DHCP Server Ether2 to Switch3 Ethernet0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.30.254	255.255.255.255	MNPD	151	5678 → 5678 Len=109
2	0.000859	0c:33:ed:81:00:00	CDP/VTP/DTP/PAGP/UD...	CDP	103	Device ID: Router1 Port ID: ether3
3	0.001323	0c:33:ed:81:00:00	LLDP_Multicast	LLDP	106	MA/0c:33:ed:81:00:00 IN/ether3 120 SysN=Rc
4	1.447308	10.0.30.1	255.255.255.255	MNPD	154	5678 → 5678 Len=112
5	1.450047	0c:6c:0b:12:00:01	CDP/VTP/DTP/PAGP/UD...	CDP	106	Device ID: DHCP Server Port ID: ether1
6	1.450630	0c:6c:0b:12:00:01	LLDP_Multicast	LLDP	109	MA/0c:6c:0b:12:00:01 IN/ether1 120 SysN=Df
7	59.997848	10.0.30.254	255.255.255.255	MNPD	151	5678 → 5678 Len=109
8	59.998595	0c:33:ed:81:00:00	CDP/VTP/DTP/PAGP/UD...	CDP	103	Device ID: Router1 Port ID: ether3
9	59.999151	0c:33:ed:81:00:00	LLDP_Multicast	LLDP	106	MA/0c:33:ed:81:00:00 IN/ether3 120 SysN=Rc
10	61.445458	10.0.30.1	255.255.255.255	MNPD	154	5678 → 5678 Len=112
11	61.445731	0c:6c:0b:12:00:01	CDP/VTP/DTP/PAGP/UD...	CDP	106	Device ID: DHCP Server Port ID: ether1
12	61.445862	0c:6c:0b:12:00:01	LLDP_Multicast	LLDP	109	MA/0c:6c:0b:12:00:01 IN/ether1 120 SysN=Df

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>