Implementação de um Firewall

João Gilberto de Oliveira Teixeira - 211036070
Gabriel Pessoa Faustino – 231006121
Lucas Silva Nóbrega - 180035096

Universidade de Brasília

1 Introdução

Este relatório descreve o desenvolvimento e a configuração de uma topologia de rede simulada no GNS3, com o objetivo de implementar um firewall no Roteador 1 que aplique políticas de segurança entre diferentes sub-redes. A topologia utilizada é composta por cinco sub-redes distintas, incluindo uma rede externa (Internet Pública), uma zona desmilitarizada (DMZ), redes internas e uma rede com clientes DHCP. O uso de uma DMZ é uma prática comum na segurança de redes, pois permite a exposição controlada de serviços (como servidores web ou DHCP) a usuários externos sem comprometer a segurança da rede interna.

Para controlar o fluxo de pacotes entre essas redes, é essencial a utilização de um firewall, que atua como uma barreira de proteção entre diferentes domínios de confiança. Outro aspecto relevante é a utilização do DHCP Relay, que permite que clientes de uma sub-rede obtenham endereços IP de um servidor DHCP localizado em outra sub-rede. Essa abordagem reflete cenários reais em que centralizar os serviços de rede é preferível por questões de gerenciamento e segurança. Para isso, foi necessário configurar o Roteador 2 para encaminhar as solicitações DHCP da Sub-rede 5 até o servidor DHCP presente na DMZ.

A configuração da rede e a aplicação das pol´ıticas de firewall foram realizadas utilizando o GNS3 (Graphical Network Simulator-3), uma ferramenta amplamente utilizada para simulação de redes complexas. O GNS3 permite testar configurações reais de dispositivos de rede em um ambiente controlado, o que é ideal para fins educacionais e para validação de projetos antes de serem aplicados em produção.

2 Configuração dos Dispositivos

2.1 Roteadores

Roteador 1 (Firewall) foi configurado com interfaces para cada sub-rede, utilizando endereços IP estáticos. Também foi o ponto central de roteamento e

responsável pela aplicação das regras de firewall. Utilizamos o iptables para definir regras de entrada, saída e encaminhamento.

Roteador 2 teve a função principal de atuar como *DHCP Relay*. A configuração foi realizada para que pacotes DHCP recebidos na Sub-rede 5 fossem encaminhados ao Servidor DHCP na Sub-rede 2.

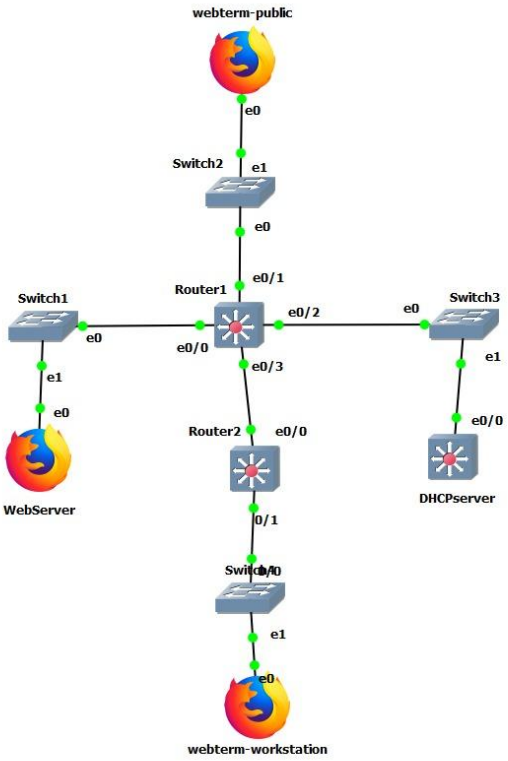
2.2 Servidores

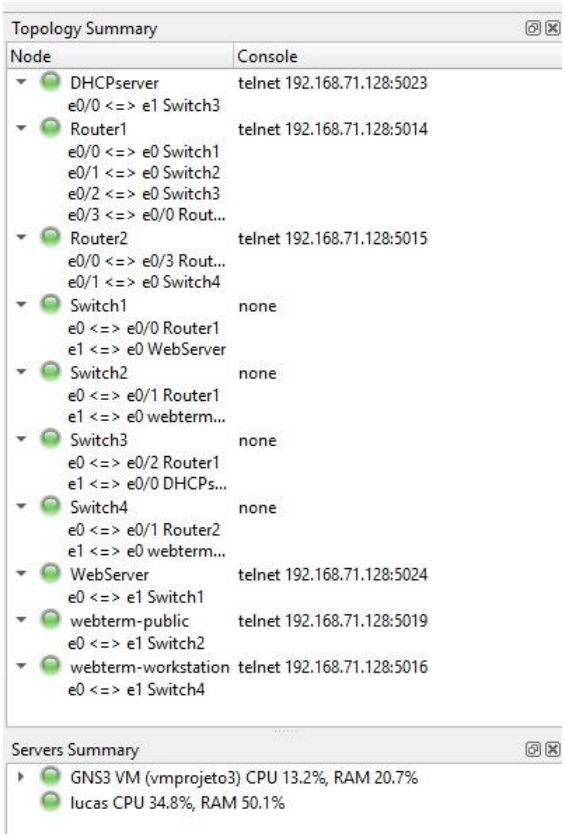
Servidor Web (WebServer) foi posicionado na DMZ (Sub-rede 2), com IP estático e serviço HTTP ativo, permitindo conexões públicas e internas controladas via firewall.

Servidor DHCP também foi posicionado na Sub-rede 2. Criamos um escopo de endereçamento para a Sub-rede 5, excluindo os endereços já utilizados. Configuramos o gateway padrão, o tempo de concessão e o DNS.

2.3 Estações de Trabalho

A Sub-rede 5 representa clientes que recebem endereços IP via DHCP. As configurações foram validadas atrav´es do recebimento automático de IP e acesso à rede.





3 Regras de Firewall

As regras foram implementadas no Roteador 1 com o uso do iptables, respeitando os seguintes critérios:

1. Permitir conexões HTTP (porta 80) da Sub-rede 4 para o Servidor Web.
2. Permitir pacotes de conexões estabelecidas ou relacionadas.
3. Permitir solicitações DHCP (UDP 67) da Sub-rede 5 (encaminhadas via Roteador 2) para o Servidor DHCP.
4. Permitir respostas DHCP (UDP 68) do Servidor DHCP para clientes da Sub-rede 5.
5. Negar todo o restante (regra padrão de DROP).

As regras foram organizadas nas cadeias INPUT, OUTPUT e FORWARD, com prioridade para as pol´ıticas de encaminhamento.

4 Testes Realizados

Para validar a implementação da topologia e as regras de firewall configuradas no Roteador 1, foram planejados e executados os seguintes testes:

4.1 Teste de Conectividade entre as Sub-redes

- Ping entre sub-redes autorizadas:
Realizamos testes de conectividade utilizando o comando ping entre as estações das sub-redes internas e o servidor Web na DMZ. Esse teste tinha como objetivo confirmar que o firewall permitia o tráfego legítimo conforme as regras estabelecidas.

- Bloqueio de tráfego não autorizado:
Testamos o bloqueio de conexões originadas de redes que não deveriam acessar diretamente a DMZ ou a Internet. As tentativas de conexão foram corretamente bloqueadas, evidenciando o funcionamento da política de DROP por padrão no firewall.

4.2 Teste de Acesso ao Servidor Web

Tentamos acessar a página hospedada no servidor Web da DMZ através de navegadores nas estações da Sub-rede 4, via requisição HTTP na porta 80. No entanto, durante esse teste, foi identificado um problema na camada de aplicação: as requisições não retornavam o conteúdo da página esperada**.**

Esse problema inviabilizou a realização de capturas no Wireshark referentes ao tráfego HTTP, pois o handshake e a resposta do servidor não foram completados com sucesso. Após análise, constatou-se que o erro estava relacionado à configuração do serviço HTTP no servidor Web ou a uma falha na publicação da página, e não às regras do firewall, visto que o tráfego na porta 80 estava sendo corretamente liberado.

4.3 Teste de DHCP Relay

Na Sub-rede 5, configurada com clientes DHCP, foi realizado o teste de requisição de endereço IP. O Roteador 2 operou como DHCP Relay, encaminhando as solicitações ao servidor DHCP localizado na DMZ (Sub-rede 2).
Os testes confirmaram que, os clientes da Sub-rede 5 receberam endereços IP corretamente, o gateway padrão e o servidor DNS foram atribuídos conforme esperado, e pôr fim, a comunicação entre o DHCP Relay e o servidor DHCP funcionou de forma transparente, validando a configuração do encaminhamento de pacotes UDP nas portas 67 e 68.

5 Conclusão

A implementação da topologia no GNS3 permitiu simular de forma prática um ambiente corporativo com diferentes zonas de segurança e serviços essenciais de rede. A configuração do firewall no Roteador 1, utilizando iptables, foi eficaz para controlar o tráfego entre as sub-redes, aplicando políticas específicas para cada cenário.

A utilização de uma DMZ demonstrou-se adequada para a exposição controlada de serviços públicos, como o servidor Web e o servidor DHCP, sem comprometer a segurança da rede interna. Além disso, a configuração do DHCP Relay no Roteador 2 permitiu centralizar a distribuição de endereços IP, refletindo práticas reais de gerenciamento de redes.

O projeto proporcionou uma valiosa oportunidade de integrar conhecimentos teóricos sobre segurança, roteamento, firewall e serviços de rede em um ambiente simulado, promovendo uma compreensão mais sólida dos desafios e soluções presentes em redes reais.

Link para o Github: https://github.com/Gabe-Faus/Implementa-o-de-Firewall/tree/main