11ª Jornada Científica e Tecnológica do IFSULDEMINAS & 8º Simpósio de Pós-Graduação

FIREWALL IPV6: comparação entre Mikrotik e OPNsense

Renan T. de LIMA[1]; Silmara C. P. NUNES[2]; Vinícius F. de SOUZA[3]

RESUMO

A evolução da Internet e a crescente demanda por endereços IP, ocasionaram uma escassez de endereços IPv4 e motivaram o surgimento de uma nova geração do protocolo IP, denominada IPv6. No entanto, a transição do IPv4 para o IPv6 impõe muitos desafios para o administrador da rede, e uma das principais preocupações diz respeito à segurança e à implementação de firewalls. Este trabalho apresenta um estudo de caso sobre firewalls IPv6 por meio da comparação entre duas ferramentas com recursos para tal finalidade, Mikrotik e OPNsense, que visa investigar qual delas é mais flexível e adequada para uso em redes IPv6. Através de testes realizados em um ambiente inspirado em uma rede real, foi possível constatar algumas vantagens e desvantagens no uso de cada um dos softwares analisados. Os resultados apontaram o Mikrotik como uma solução mais adequada para a configuração de firewalls em redes IPv6.

Palavras-chave:
Filtro; Pacote; ICMPv6.

1. INTRODUÇÃO

É impossível pensar em uma rede de computadores sem um dispositivo de *firewall*, dado o alto nível de vulnerabilidade que a mesma estaria sem ele. Stallings (2012) afirma que um *firewall* forma uma barreira através da qual o tráfego indo a cada direção precisa passar. Uma política de segurança de *firewall* dita qual tráfego tem autorização para passar em cada direção. O *firewall* é um ponto entre duas ou mais redes, que pode ser um componente ou um conjunto de componentes, por onde passa todo o tráfego, permitindo que o controle, a autenticação e os registros de todo o tráfego sejam realizados. Desse modo, esse ponto constrói um mecanismo utilizado para proteger, geralmente, uma rede segura de uma rede pública não segura (NAKAMURA, 2007).

O aumento do uso da Internet para a realização de transações entre empresas e consumidores, por exemplo, fez com que um nível maior de segurança passasse a ser exigido, como a identificação de usuários e a criptografia dos dados, tornando necessário anexar novos mecanismos ao protocolo original, que garantisse tais serviços. O IPsec foi criado para suprir essa

1 Estudante, IFSULDEMINAS – *Campus* Inconfidentes. E-mail: renanmakise@gmail.com
2 Estudante, IFSULDEMINAS – *Campus* Inconfidentes. E-mail: silpomon@gmail.com
3 Orientador, IFSULDEMINAS – *Campus* Machado. E-mail: vinicius.souza@ifsuldeminas.edu.br

deficiência. Ele é uma suíte de protocolos que atua como uma extensão do protocolo IP e oferece serviços de segurança para prover autenticidade, integridade e confidencialidade aos pacotes IP (MOREIRAS, 2015).

Segundo a IANA (*Internet Assigned Numbers Authority*), o IPv4, que está em uso na Internet desde 1983, tem capacidade para endereçar aproximadamente 4,3 bilhões de dispositivos. Desde a década de 90 era esperado que a rede teria problemas de capacidade de endereçamento. O IPv4 está cada vez mais escasso e, como consequência, num futuro breve não haverá nenhuma rede disponível em IPv4 e a migração para o IPv6 se tornará inevitável.

O propósito deste trabalho é identificar algumas vantagens e desvantagens no uso de cada software analisado e verificar qual deles é mais flexível e seguro para a configuração de firewalls em redes IPv6. Os resultados dos testes realizados indicaram o *Mikrotik* como a solução mais adequada para tal finalidade.

2. MATERIAIS E MÉTODOS

O *Mikrotik* tem como principal produto um sistema operacional chamado *Mikrotik RouterOS*. Este sistema é o que possibilita ao roteador adquirir a função de *firewall* com diversos filtros. Através do software *Winbox*, pode-se administrar todo o ambiente, incluindo as regras de firewall, através de uma interface gráfica. O *OPNsense* é um software de código aberto que permite gerenciar as funcionalidades de um *firewall* através de uma interface gráfica com formulários, além de ser capaz de efetuar roteamento.

Foi empregada também a técnica de simulação de redes, por meio da criação de máquinas virtuais no programa *Citrix XenServer* para testes de conectividade, e o *sniffer* de pacotes *Wireshark* foi usado para a captura dos resultados. A topologia configurada consiste em dois *hosts* idênticos com *Windows 7*, conectados aos respectivos *firewalls*, que também executam a função de *gateway* local e, por sua vez, estão ligados a um roteador de borda responsável pela conexão à Internet.

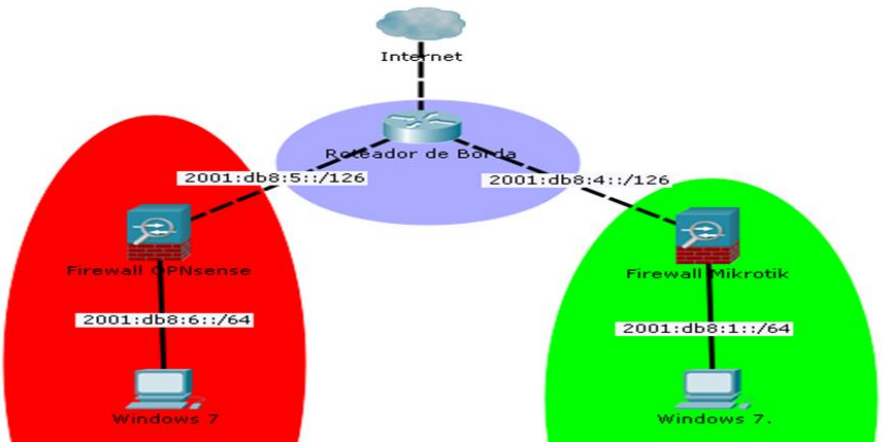

Figura 1 – Topologia de rede configurada. Fonte: Autor.

As regras de *firewall* configuradas consistem em: bloquear um único IP de acessar à Internet, bloquear o acesso remoto por meio do *Remote Desktop* do *Windows* para um único IP de destino, bloquear um tipo específico de pacote ICMPv6 e bloquear o acesso ao *Facebook*.

3. RESULTADOS E DISCUSSÕES

As duas ferramentas executaram com êxito o bloqueio do acesso à Internet baseado no endereço IP de origem e também o bloqueio ao protocolo RDP, usado pelo *Remote Desktop*, com a regra baseada em endereço IP de destino. Foi testada também a regra de bloqueio para o *Facebook*. A Figura 2 mostra uma tela do *Mikrotik*, onde ao digitar "*facebook.com*" no campo *Content* da aba *Advanced*, o *firewall* irá bloquear todos os pacotes que contenham esse termo.

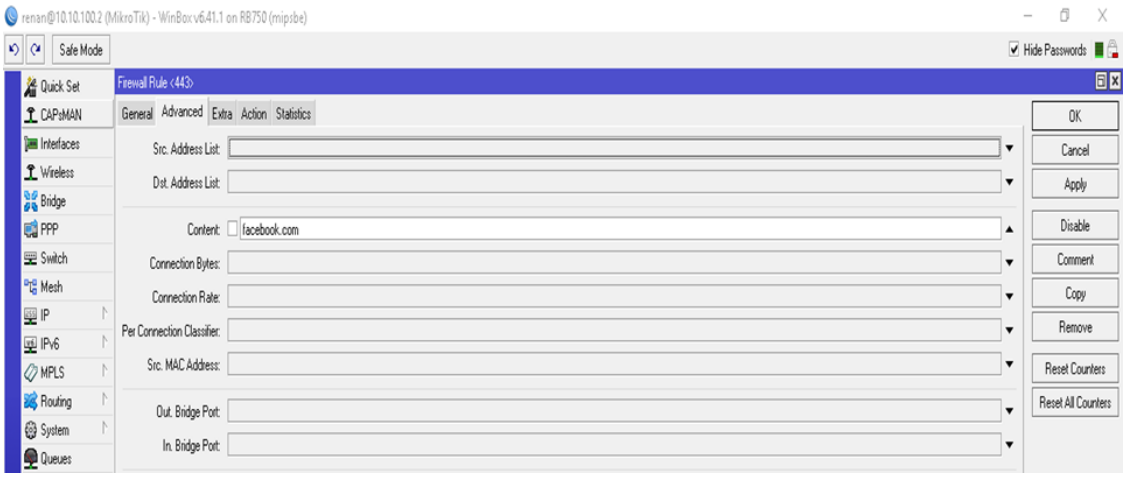

Figura 2 – Bloqueio do facebook.com no Mikrotik. Fonte: Autor.

Por sua vez, o *OPNsense* necessita de um *alias* associado ao *Facebook*, na aba *Aliases* para tal bloqueio (Figura 3). Isso abre precedentes para que o bloqueio não seja efetivo, pois o usuário pode conhecer outras URLs para acessar a mesma página, por exemplo, utilizando outros idiomas.

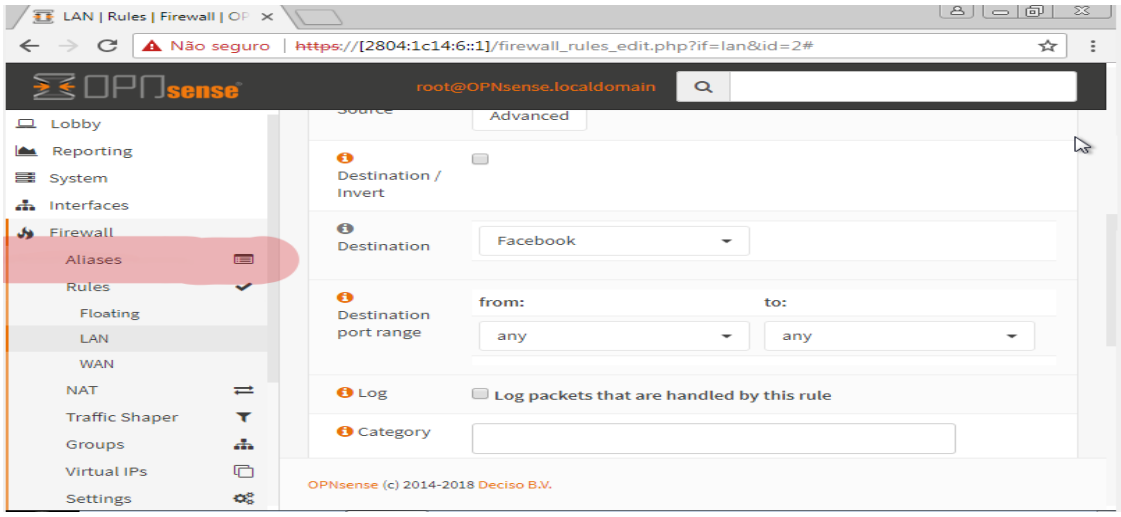

Figura 3 – Bloqueio do facebook.com no OPNsense. Fonte: Autor.

No teste sobre ICMPv6 (*Internet Control Message Protocol*), o *OPNsense* bloqueou além dos *pings* (mensagens *echo requests*), também pacotes de *neighbors solicitations* (solicitações de vizinhos), relativos ao protocolo NDP (*Neighbor Discovery Protocol*). Este protocolo utiliza mensagens ICMPv6 para descobrir vizinhos e associar o endereço IP com o endereço MAC do dispositivo, algo similar ao que o protocolo ARP (*Address Resolution Protocol*) faz com o endereçamento IPv4. Portanto, bloquear o protocolo ICMPv6 como um todo não é uma opção viável. As regras do *Mikrotik* permitiram bloquear tipos específicos de pacotes ICMPv6, como as mensagens *echo requests*, deixando que todas as mensagens do protocolo NDP fossem entregues com sucesso.

4. CONCLUSÕES

Ao comparar as duas ferramentas em operação sob todos os critérios previamente apontados, foi detectada uma possível brecha de segurança que, ao ser explorada, ao menos até a data da realização dos testes, inviabiliza o *OPNsense* como *firewall* IPv6, pois o mesmo não permite especificar os variados tipos de pacotes ICMPv6 para serem filtrados, o que compromete a atuação do *OPNsense* no trato do protocolo IPv6. Essa ferramenta está em evolução e conta com um fórum ativo, além de atualizações constantes. O *OPNsense* foi capaz de efetuar o bloqueio com base em IP de origem e destino com a mesma eficácia do *Mikrotik*, mas o *Mikrotik* mostrou-se uma opção mais eficiente e confiável para a segurança de uma rede IPv6, já que aplicou com êxito na rede todas as regras propostas, incluindo a implementação de filtros específicos para o protocolo IPv6.

REFERÊNCIAS

INTERNET ASSIGNED NUMBERS AUTHORITY (IANA). **Recursos numéricos.** Disponível em: <https://www.iana.org/numbers>. Acesso em: 01 ago. 2019.

MOREIRAS, Antonio Marcos et al. **Laboratório de IPv6:** aprenda na prática usando um emulador de redes. São Paulo: Novatec, 2015. 398 p.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de Redes em Ambientes Cooperativos.** São Paulo: Novatec, 2007. 488 p.

STALLINGS, William. **Criptografia e Segurança de Redes:** Princípios e Práticas. 4. ed. São Paulo: Pearson Education do Brasil Ltda, 2012. 492 p. Tradução de: Daniel Vieira.