9ª Jornada Científica e Tecnológica do IFSULDEMINAS
6º Simpósio da Pós-Graduação

FIREWALL EM REDES IPV6: Comparação entre OPNsense e Iptables

Vinícius F. de SOUZA[1]; Leonardo P. ALVARENGA[2]; Renan A. MACIEL[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. Este trabalho apresenta uma análise comparativa entre duas ferramentas utilizadas para a configuração de um firewall em redes IPv6, com o objetivo de verificar qual delas é mais flexível e segura para esse propósito. Através da configuração de uma política de segurança e mediante a verificação de alguns recursos do protocolo IPv6, foi possível constatar algumas vantagens e desvantagens no uso de cada um dos softwares analisados: OPNsense e Iptables. Os resultados apontaram o Iptables como uma solução mais adequada para a configuração de firewalls em ambientes IPv6.

Palavras-chave: Filtro; Fragmento; ICMPv6; OPNsense; Iptables.

1. INTRODUÇÃO

O protocolo IPv6 foi concebido com a proposta de substituir totalmente, a longo prazo, o IPv4 como protocolo de endereçamento em redes de computadores. O IPv6 apresenta uma série de vantagens em relação ao seu antecessor e destaca-se, principalmente, por disponibilizar um maior espaço de endereçamento que permite atender toda a demanda atual da Internet, ao contrário do IPv4, sendo essa a maior motivação para o desenvolvimento do mesmo. Desde o seu lançamento oficial, em 6 de junho de 2012, vem sendo implantado gradativamente, funcionando junto com o IPv4 numa situação que pode ser denominada de pilha dupla ou *dual stack* (BRITO, 2013).

Com a popularização do IPv6, e a maior adesão por parte dos usuários da Internet em geral, tornou-se necessária uma maior atenção com a questão da segurança, tendo em vista que o novo protocolo traz grandes alterações em relação ao seu antecessor e, consequentemente, demanda novas medidas e conhecimento específico para garantir a segurança da rede (NIC.BR, 2016).

Quando o assunto é segurança, a presença de um *Firewall* para analisar o tráfego da rede torna-se imprescindível. Embora existam várias soluções *Open Source* baseadas em *FreeBSD* ou *Linux*, este não é o caso quando se requer suporte ao IPv6 (NIC.BR, 2016). Nesse contexto, foco

[1] IFSULDEMINAS – Campus Inconfidentes. Inconfidentes/MG. E-mail: vinicius.souza@ifsuldeminas.edu.br
[2] IFSULDEMINAS – Campus Inconfidentes. Inconfidentes/MG. E-mail: leonardokbj@gmail.com
[3] IFSULDEMINAS – Campus Inconfidentes. Inconfidentes/MG. E-mail: renan_alle@hotmail.com

deste trabalho, estão incluídos os softwares OPNsense, PfSense e Iptables. Também existem algumas soluções proprietárias com a mesma finalidade, tais como o Cisco PIX e o MikroTik.

Para esta análise comparativa foram selecionadas duas ferramentas *Open Source*, sendo uma baseada em *FreeBSD* (OPNsense) e a outra em *Linux* (Iptables). O OPNsense foi selecionado, em detrimento do PfSense que também é baseado em *FreeBSD*, por ser um projeto mais recente e que oferece várias atualizações de segurança. 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 Iptables como a solução mais adequada para tal finalidade.

2. MATERIAL E MÉTODOS

Para a realização da comparação proposta, foram utilizadas as seguintes versões de softwares: OPNsense 17.1.4 e Iptables 1.4.21 com o sistema operacional Debian 3.16.43-2. O OPNsense é uma plataforma que executa funções de roteamento e firewall, surgiu como um *fork* do PfSense e do *m0n0wall* em 2014, e foi lançado oficialmente em janeiro de 2015. A sua interface gráfica é amigável e intuitiva, e a integração com o código é muito fluida. Possui muitas das funções presentes em firewalls comerciais e oferece sistemas de monitoramento e controle de tráfego completos (OPNSENSE®, 2015).

O Iptables, nativo das distribuições *Linux* a partir do Kernel 2.4, proporciona flexibilidade ao permitir alterar, acrescentar ou retirar alguma regra a qualquer momento. Por outro lado, apresenta um certo grau de complexidade pelo fato de sua configuração ser realizada totalmente por linhas de comandos, sem o uso de qualquer tipo de interface gráfica. Existem alguns softwares que implementam uma interface gráfica para o Iptables, porém não são tão populares e na maioria dos casos acabam limitando a funcionalidade do mesmo (NETO, 2004).

A política *default* configurada é *deny all*, na qual somente o tráfego discriminado tem permissão para atravessar a máquina Firewall e todo o restante é negado por padrão. A política estabelecida permite traceroute, SSH (*Secure Shell*), HTTP (*HyperText Transfer Protocol*) e filtra os diferentes tipos de ICMPv6 (*Internet Control Message Protocol*), os cabeçalhos de extensão do IPv6 e pacotes IPv6 fragmentados, em conformidade com as respectivas RFCs (*Request for Comments*) e orientações do NIC.br (IETF 1998a, 1998b).

A Figura 1 apresenta a topologia empregada para a realização dos testes. Ambas as interfaces da máquina Firewall e os hosts 1 (Debian GNU/Linux) e 2 (Windows 7) foram configurados manualmente com os endereços IPv6 indicados na figura. O aplicativo Wireshark foi usado para analisar os pacotes marcados neste experimento.

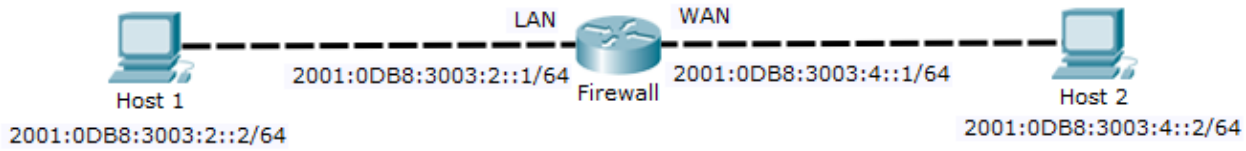

Figura 1- Topologia de rede IPv6 configurada. Fonte: Autor.

3. RESULTADOS E DISCUSSÕES

No OPNsense, a configuração da política padrão e das regras que liberam o tráfego para traceroute, SSH, HTTP e ICMPv6 é simples e facilitada pela presença da interface gráfica. É importante ressaltar que há uma opção no OPNsense que, se ativada, garante que o firewall fique acessível via HTTP na interface LAN (*Local Area Network*) sem restrição. Com essa opção desativada, o acesso HTTP ao firewall pode ser limitado com a criação de uma regra específica.

A ferramenta não permite filtrar os diferentes tipos de pacotes ICMPv6, somente admite bloquear ou liberar o tráfego ICMPv6 sem qualquer especificação. Tal condição caracteriza uma importante falha de segurança no OPNsense, pois existem diversos tipos de ataques que utilizam recursos dos pacotes ICMPv6 (ATLASIS, 2016). Por outro lado, há determinados tipos de pacotes ICMPv6 que precisam ser autorizados para a correta operação do protocolo IPv6 na rede.

O OPNsense oferece opções para filtrar diversos tipos de cabeçalhos de extensão e fragmentos do IPv6. Porém, nos testes realizados e disponíveis no link (https://drive.google.com/drive/folders/0B3otjpt6xiFQbDlHeHZPX2pjbGM), esses filtros não funcionaram e os pacotes, mesmo marcados para bloqueio no firewall, foram recebidos pelo Host 2, o que também indica uma falha de segurança dessa ferramenta.

Já no firewall usando Iptables, a configuração da política padrão e das regras descritas anteriormente não tem o auxílio de uma interface gráfica amigável e, somada a uma sintaxe de comandos complexa, torna-se uma tarefa dispendiosa e propensa a erros. Apesar disso, a ferramenta permite a criação de regras específicas para o tratamento de pacotes sob diversos parâmetros.

O Iptables oferece opções funcionais para filtrar cabeçalhos de extensão e fragmentos do IPv6, além dos diversos tipos de pacotes ICMPv6. Nos testes realizados, ao contrário do OPNsense, os pacotes não autorizados no firewall foram bloqueados e não chegaram ao destino.

4. CONCLUSÕES

Na configuração do firewall, a principal vantagem do OPNsense é a presença de uma interface gráfica amistosa e intuitiva, que facilita a criação e manipulação das regras definidas na política de segurança da rede. Entretanto, a ferramenta apresentou algumas limitações no tratamento dos recursos oferecidos pelo protocolo de endereçamento IPv6. Os filtros disponíveis no OPNsense para os fragmentos de pacotes IPv6 e os diferentes tipos de cabeçalhos de extensão do protocolo, mesmo habilitados, não funcionaram corretamente. Além disso, outra desvantagem da ferramenta, é o fato de não aceitar especificar os variados tipos de pacotes ICMPv6 para serem filtrados. Essas características sinalizam falhas de segurança importantes do OPNsense no trato do protocolo IPv6. Já o Iptables, apesar da sua configuração menos amistosa e mais onerosa por meio de linhas de comandos, mostrou-se uma solução mais flexível e segura ao admitir a implementação de filtros específicos para IPv6 e ICMPv6, sendo que todos os filtros testados funcionaram corretamente.

REFERÊNCIAS

ATLASIS, Antonios. **The Impact of Extension Headers on IPv6 Access Control Lists - Real Life Use Cases.** [2016]. Disponível em: <https://www.troopers.de/media/filer_public/77/ad/77ad71b5-daea-441c-afb1-e14625ed11d0/tr16_aatlasis_the_impact_of_extension_headers_on_ipv6_access_control_lists.pdf>. Acesso em: 02 ago. 2017.

BRITO, S. H. B. **IPv6:** O novo protocolo da internet. 1 Ed. São Paulo, Novatc Editora LTDA, 2013.

INTERNET ENGINEERING TASK FORCE (IETF). **RFC 2460**: Internet Protocol, Version 6 (IPv6) Specification. [s. I.]: Internet Engineering Task Force, 1998a. 39 p. Disponível em: <https://tools.ietf.org/html/rfc2460>. Acesso em: 02 ago. 2017.

INTERNET ENGINEERING TASK FORCE (IETF). **RFC 4443**: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification [s. I.]: Internet Engineering Task Force, 1998b. 39 p. Disponível em: < https://tools.ietf.org/html/rfc4443>. Acesso em: 02 ago. 2017.

NETO, U. **Dominando Linux Firewall Iptables**. 1. Ed. Rio de Janeiro, Ciência Moderna, 2004.

NIC.BR. Levantamento sobre a implantação do IPv6 ao redor do mundo. **IPv6.br**, São Paulo, 29 jun. 2016. Disponível em: < http://ipv6.br/post/levantamento-sobre-a-implantacao-do-ipv6-ao-redor-do-mundo/> Acesso em: 02 ago. 2017.

OPNSENSE® (Holanda). **ABOUT OPNsense®**. [2015]. Disponível em: <https://opnsense.org/about/about-opnsense/>. Acesso em: 02 ago. 2017.