14º SIEPE SALÃO INTERNACIONAL DE ENSINO, PESQUISA E EXTENSÃO
#EDUCAÇÃO + CIÊNCIA INDEPENDÊNCIA
30 nov. a 02 dez. 2022
REALIZAÇÃO: unipampa Universidade Federal do Pampa
APOIO: CNPq CAPES FAPERGS

Desenvolvimento de uma função de rede NAT por meio do uso de eBPF/XDP

Rodrigo Siveris Klein, discente de graduação, Universidade Federal do Pampa, Campus Alegrete
Marcelo Caggiani Luizelli, docente, Universidade Federal do Pampa

e-mail primeiro autor - rodrigoklein.aluno@unipampa.edu.br

Atualmente, diante da ascensão do acesso à Internet no mundo, estão presentes em todo lugar dispositivos eletrônicos interconectados que compartilham dados entre si. Cada aparelho, por estar devidamente conectado em uma rede de Internet, possui o seu próprio endereço IP (Internet Protocol) exclusivo, responsável pela sua identificação. Dentro de uma rede local existem vários dispositivos conectados, onde cada um possui o seu endereço IP privado que precisa passar por um processo de tradução para ser transformado em um único IP público que abrange todos esses dispositivos. Essa conversão é feita por uma técnica chamada NAT (Network Address Translation), que funciona como um mecanismo que realiza a conversão desse endereço privado para um endereço público, para que dispositivos consigam acesso a outros servidores, fora da rede interna. Esse processo é necessário porque a existência de endereços públicos se esgotaria rapidamente se cada aparelho tivesse o seu próprio IP público exclusivo ao redor do mundo. Através dessa tecnologia de tradução de endereços, os mesmos endereços privados podem ser reusados dentro de cada rede pública. Diante de um Centro de Processamento de Dados (CPD), o NAT é executado dentro do núcleo (Kernel) do sistema dos servidores, onde todos os pacotes são processados. O objetivo deste trabalho é otimizar o processamento de pacotes de um NAT através das tecnologias eBPF (Extended Berkeley Packet Filter) e XDP (eXpress Data Path), as quais viabilizam a programação de dispositivos de rede, permitindo funções como o monitoramento de rede, tratamento antecipado de pacotes e manipulação do tráfego de rede. O sistema eBPF é um recurso do Kernel do Linux que permite o processamento rápido de pacotes através de uma Máquina Virtual (VM) responsável pela compilação e execução de programas no espaço do Kernel. Quando um programa eBPF é carregado, acontece uma verificação para garantir que o mesmo possa ser executado sem levantar riscos em torno do sistema. Já o XDP atua como um framework que executa programas eBPF de forma imediata, fornecendo um caminho de dados de rede programável de alto desempenho. A metodologia do projeto consiste no desenvolvimento de um programa eBPF que simula a função de um NAT, onde recebe pacotes provindos de um servidor externo e realiza a troca do endereço IP local do pacote para um endereço IP público. Esse processo é realizado através de duas placas de Interface de rede configuradas no sistema Linux. Para avaliar os programas eBPF, gera-se tráfego de rede sintético em uma vazão de 10Gbit/s utilizando pacotes de 1500 bytes. O tráfego é então encaminhado para o programa eBPF e/ou para o processamento tradicional do Kernel do Linux para realizar a função de NAT. Quando o tráfego é processado pelo programa eBPF,

atinge-se uma vazão máxima de até 8Gbit/s. Em contrapartida, quando o tráfego é encaminhado para o Kernel do Linux, o processamento de pacotes é de apenas 1Gbit/s. Isto se dá principalmente pela cópia excessiva das estruturas de memória interna do sistema operacional. Diante do exposto, é visível o grande potencial que as ferramentas eBPF e XDP exercem sobre a área de processamento de pacotes de rede de forma a permitir novas funcionalidades e aumentar a vazão no processamento de pacotes. Mesmo sendo tecnologias recentes e que ainda vêm sendo pesquisadas, já são alvo de projetos nas maiores empresas multinacionais da era, como Google e Microsoft. Como trabalhos futuros, espera-se avaliar de maneira mais extensiva o desempenho de aplicações eBPF, assim como desenvolver mecanismos mais eficientes de processamento de pacotes.

Agradecimentos: agradeço aqui as instituições que fomentaram a iniciativa do trabalho: FAPERGS, UNIPAMPA.
Palavras-chave: Extended Berkeley Packet Filter; eXpress Data Path; Processamento de pacotes de rede; Network Address Translation; Redes de Computadores.