

## ABSTRAK

Teknologi virtualisasi telah mengubah arah revolusi industri komputer dengan cara penurunan biaya-biaya modal, biaya operasional, ketersediaan layanan yang lebih tinggi dan mekanisme perlindungan data. Begitupun di Balai Teknologi Polimer yang menerapkan server-servernya di dalam mesin virtualisasi, pada penelitian ini dilakukan analisa dan penerapan firewall dengan menggunakan nftables pada mesin virtualisasi. Nftables adalah firewall generasi baru di sistem operasi linux yang siap menggantikan iptables sebagai firewall. Implementasi firewall nftables diterapkan dalam mesin virtualisasi untuk melindungi layanan server-server yang ada dibelakang firewall. Penelitian ini menguji kinerja firewall nftables terhadap serangan DDoS (*Distributin Denial of Service*).

Pengambilan data pengujian DDoS dilakukan sebanyak 30 kali dengan tools yang ada di linux, yaitu hping3 dan wireshark. Skenario 1 tanpa gangguan DDoS diambil data sebanyak 10 kali, skenario 2 dengan DDoS gangguan ke server sebanyak 32000 byte dengan 3 komputer sebanyak 10 kali. Dan terakhir skenario 3 dengan gangguan DDoS sebanyak 65000 byte dengan 6 komputer sebanyak 10 kali juga. Hasil penelitian menunjukkan saat tidak ada serangan DDoS server berjalan baik dengan *throughput* yang besar dan pemakaian sumber daya CPU (%) yang kecil. Namun setelah dilakukan serangan DDoS terjadi penurunan nilai *throughput* dan pemakaian CPU yang besar. Semakin besar jumlah serangan maka semakin menurunkan nilai *throughput* dan makin membesarnya pemakaian sumber daya CPU dari server firewall.

Kata kunci : *firewall, virtual mesin, DDoS, Linux, nftables, throughput, CPU Usage.*

UNIVERSITAS  
MERCU BUANA

## ABSTRACT

Virtualization technology has changed the direction of the computer industry revolution by reducing capital costs, operational costs, higher service availability and data protection mechanisms. Likewise at the Polymer Technology Center that implements its servers in the virtualization engine, in this study an analysis and application of a firewall using nftables on a virtualization machine was carried out. Nftables is a new generation firewall in the Linux operating system that is ready to replace iptables as a firewall. Implementation of nftables firewalls is implemented in virtualization machines to protect the services of servers behind the firewall. This study tested the performance of the firewall nftables against DDoS (Distributin Denial of Service) attacks.

Retrieving DDoS test data is done 30 times with the tools in Linux, namely htping3 and wireshark. Scenario 1 without DDoS interference data is taken 10 times, scenario 2 with DDoS interference to 32000 bytes servers with 3 computers 10 times. And finally scenario 3 with DDoS interference of 65000 bytes with 6 computers 10 times as well. The results show that when there is no DDoS attack the server runs well with large throughput and small CPU usage (%). But after a DDoS attack there is a decrease in throughput and large CPU usage. The greater the number of attacks, the lower the throughput value and the greater the use of CPU resources from the firewall server.

Keywords: firewall, virtual machine, DDoS, Linux, nftables, throughput, CPU Usage



UNIVERSITAS  
MERCU BUANA