Analisis *Throughput* dan *High Availability Firewall* sebagai *Virtualized Network Function* pada VMware ESXI

Ahmad Thoriq Azzam [1)], Rendy Munadi [2)], Ratna Mayasari [3)]

[1),2),3)]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
Jl. Telekomunikasi no. 1 Bandung
Email: azzamthoriq@gmail.com

Abstrak. *Seiring dengan berkembangnya dunia industri IT, teknologi virtualisasi perlahan-lahan mulai digunakan untuk membangun infrastruktur jaringan yang disebut dengan Network Function Virtualization (NFV). Teknologi ini berjalan diatas suatu hypervisor yang digunakan untuk mengatur manajemen dari hardware. Berbagai macam perangkat jaringan seperti firewall dan router dapat di implementasikan sebagai software tervirtualisasi yang berjalan diatas server. Software tervirtualisasi ini disebut VNF (Virtualized Network Function). Namun, NFV memiliki kelemahan salah satunya pada segi keamanan. Secara khusus, masalah tersebut dapat ditemukan pada VNF yang merupakan bagian penting dalam arsitektur NFV. VNF sangat rentan untuk diserang dari dalam atau luar lingkungan NFV. Karena itu, diperlukan firewall untuk melindungi komponen VNF lain dari serangan tersebut. Pada penelitian ini, akan dilakukan pengujian firewall Pfsense dan Fortigate pada hypervisor VMware EXSi dalam menghadapi serangan DoS SYN dengan menganalisa hasil parameter pengujian throughput dan High availability. Penelitian ini bertujuan untuk mengetahui kinerja dari kedua firewall tersebut ketika dijalankan dalam bentuk virtual pada NFV. Dari hasil pengujian dan analisis didapatkan bahwa Fortigate memiliki nilai throughput terbaik yaitu 66,49 MB/s dalam kondisi dibawah serangan sedangkan dalam kondisi normal pfsense memiliki nilai throughput terbaik yaitu 177,65 MB/s. sedangkan untuk parameter High availability Fortigate memiliki kinerja terbaik dengan delay sebesar 1,68 seconds.*

***Kata kunci**: Network Function Virtualization, Virtualized Network Function, firewall, hypervisor*

1. Pendahuluan

NFV (*Network Function Virtualization)* merupakan suatu konsep jaringan yang menawarkan cara baru untuk mendesain, menyebarkan serta mengatur layanan jaringan dengan mengambil fungsi perangkat jaringan yang berbentuk hardware menjadi software. Berbagai macam perangkat jaringan seperti firewall, load balancer dan router dapat di implementasikan sebagai software tervirtualisasi yang berjalan diatas *server* berspesifikasi tinggi. Software tervirtualisasi ini disebut VNF. Software ini dapat berjalan dalam satu CPU dengan menggunakan teknologi virtualisasi [1]. Virtualisasi berjalan diatas *hypervisor*, yang merupakan sebuah *software* yang digunakan untuk menciptakan serta mengatur *virtual machines*.

Kehadiran teknologi NFV memungkinkan untuk mempermudah ancaman untuk masuk ke jaringan telekomunikasi memungkinkan serangan DoS (*Denial of Service*) untuk menyerang ke sumber daya jaringan. Firewall dalam bentuk *Virtualized Network Function* (VNF) atau biasa disebut dengan *virtual firewall* (vFW) dapat digunakan sebagai solusi berupa firewall tervirtualisasi yang dapat melakukan packet filtering dan monitoring paket data yang hendak masuk ke jaringan. Beberapa *firewall* terkemuka seperti pfsense dan Fortigate yang merupakan *top* 10 *rated firewall* menurut survey yang dilakukan oleh IT Central Solution tahun 2018 dapat digunakan sebagai salah satu solusi untuk mengatasi permasalahan yang terdapat pada NFV [2].

Berdasarkan penelitian terkait *firewall* sebelumnya [3], dilakukan pengujian *firewall* dengan menggunakan salah satu skenario simulasi penyerangan *flooding* (DOS) dengan berbagai macam metode. Pada penelitian berikutnya [4] dilakukan pengujian kinerja dari *virtual firewall* dalam memproses paket yang dilewatkan *virtual firewall* dalam linkungan *multitenant* dengan mengukur parameter throughput dan delay. Penelitian terakhir yang terkait [5] melakukan simulasi mengenai cara protocol CARP dalam menjaga agar *firewall* dapat berjalan dengan ketersediaan yang baik jika sewaktu-waktu *firewall* mengalami kegagalan dalam beroperasi. Berdasarkan latar belakang dari

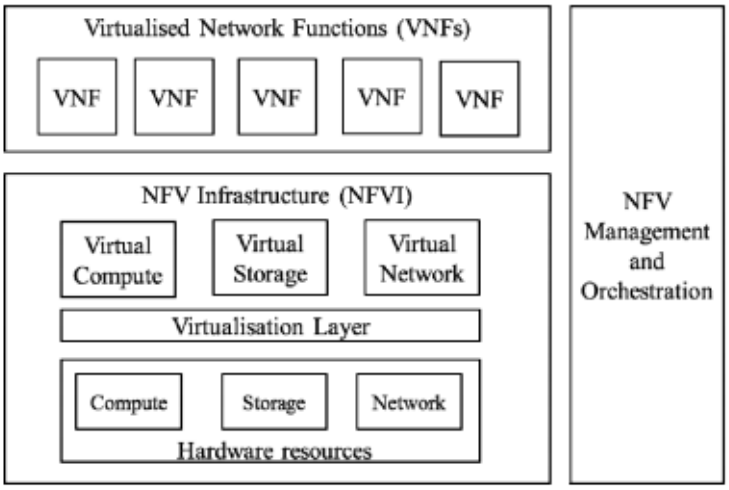
penelitian-penelitian sebelumnya maka penulis terdorong untuk melakukan penelitian untuk menguji kinerja dari *virtual firewall* pfsense dan fortigate dengan membandingkan kinerja *virtual firewall* pada VMware ESXi tersebut ketika dalam keadaan normal maupun dilakukan serangan DoS SYN dengan menganalisis hasil pengujian dari parameter *throughput* dan *high availability firewall*.

1.1. Virtualisasi

Virtualisasi merupakan teknologi yang menjadi dasar penting bagi perkembangan NFV. Teknologi ini membuat sebuah *hardware* seperti *server* dan komputer dapat menjalankan berbagai macam sistem operasi dalam bentuk sumber daya maya (*virtual)*. Namun dengan syarat, masing-masing sumber daya maya tersebut memiliki kinerja yang tidak terlalu berbeda dengan perangkat fisiknya. Tujuan dari teknologi virtualisasi ini adalah untuk memaksimalkan penggunaan sumber daya perangkat keras yang dimiliki sebagai contoh adalah *server* di *data center* yang mempunyai spesifikasi yang tinggi. Virtualisasi dapat meningkatkan penggunaan *hardware utilization rates* yang awalnya hanya sebesar 10 atau 15 persen menjadi 70 atau 80 persen [6]

1.2. Arsitektur *Network Function Virtualization*

Menurut ETSI, arsitektur NFV dibagi menjadi tiga bagian yaitu NFV *Infrastructure*, VNF dan NFV *Management and orchestration* seperti yang bisa dilihat pada gambar dibawah



Gambar 1. Arsitektur NFV menurut ETSI [1]

Berikut adalah penjelasan dari masing-masing bagian NFV diatas [1]:

- Network Function Virtualization Infrastucture (NFVI)

  NFVI merupakan bagian dari arsitektur NFV yang menjelaskan tentang komponen perangkat keras dan perangkat lunak di mana jaringan virtual dibangun. Bagian ini terdiri dari *hardware resources*, *virtualization layer* dan *virtual resources*. *Hardware resources* adalah komponen fisik dari NFVI terdiri dari computing, penyimpanan dan networking. *Virtual resource* merupakan abstraksi dari computing, penyimpanan dan networking resource. Abstraksi dicapai dengan menambahkan layer virtualisasi menggunakan *hypervisor*, yang memisahkan *virtual resource* dari *physical resource*

- Virtualized Network Function (VNF)

  VNF merupakan fungsi jaringan yang tervirtualisasi atau versi perangkat jaringan yang berbentuk software. Pemisahan software dari hardware memungkinkan mempermudah pengembangan dari setiap network function tersebut. Dan pengembangan tersebut

memungkinkan sebuah model dimana resource dari hardware infrastruktur dapat dibagikan melalui bermacam-macam software network function

- Network Function Virtualization Management and Orchestrator (MANO)

  NFV MANO adalah bagian dari NFV *architecture* yang fungsinya untuk mengatur VNF. Sedangkan, menurut ETSI kegunaan dari MANO adalah untuk mengatur perangkat jaringan yang tervirtualisasi serta sumber daya yang dibutuhkan oleh VNF seperti *compute, storage* dan *network.*

1.3. *Hypervisor*

Hypervisor merupakan suatu Teknik bagi teknologi virtualisasi yang membuat berbagai macam sistem operasi dapat berjalan secara simultan pada suatu komputer. Menurut jenisnya *Hypervisor* dibagi menjadi dua jenis yaitu:

- *Hypervisor* tipe 1 (*Bare-Metal Architecture*), berjalan secara langsung pada *hardware* yang digunakan. *Hypervisor* dapat diinstal langsung pada disk dan tidak memerlukan sistem operasi seperti Windows, Linux, Unix, MacOS. Contoh *hypervisor* jenis ini adalah Citrix Xen*Server*, VMWare ESX/ESXi dan Microsoft Hyper-V.

- *Hypervisor* tipe 2 (*Hosted Architecture*), merupakan sebuah aplikasi yang diinstal diatas sistem operasi seperti Windows, Linux dan macOS. Kita harus menginstal sistem operasi terlebih dahulu kemudian menginstal *hypervisor* diatas sistem operasi tersebut. Contoh *hypervisor* tipe ini adalah VMware Workstation, VirtualBox, VritualPC, KVM.

1.4. VMware ESXi

VMware ESXi merupakan *hypervisor* tipe 1 (bare-metal *hypervisor*) yang tidak memerlukan OS host agar dapat berjalan pada *hardware*. VMware ESXi dapat langsung diinstal diatas *hardware* seperti *server*. VMware ESXi memiliki arsitektur yang dapat beroperasi secara bebas terhadap berbagai macam sistem operasi. ini menimbulkan peningkatan dibidang keamanan, *reliability* serta manajemen. Selain itu, VMware ESXi didesain untuk pengintegrasian *hypervisor* secara langsung kepada *server* sehingga dapat mempercepat proses instalasi, konfigurasi dan *deployment*.

1.5. *Virtual Firewall*

Virtual firewall adalah *firewall* berbentuk virtual yang mempunyai fungsi untuk memonitor dan mengatur paket yang masuk atau keluar jaringan. *Virtual firewall* dapat berjalan diatas *Hypervisor* atau cloud. *virtual firewall* merupakan salah satu solusi yang dapat digunakan untuk melindungi jaringan *virtual. Firewall* jenis ini memiliki kemampuan serta fitur-fitur yang serupa dengan *firewall* berbentuk *hardware* pada umumnya.

a. Fortigate merupakan *firewall* yang dapat melindungi jaringan yang terdiri dari berbagai macam komponen dan fitur untuk menjaga keamanan jaringan. *Firewall* ini dibuat dan dikembangkan oleh Fortinet. Fortigate *virtual appliances* memungkinkan untuk mengurangi kelemahan pada sisi keamanan pada lingkungan virtual dengan menerapkan kontrol keamanan penting dalam infrastruktur virtual.

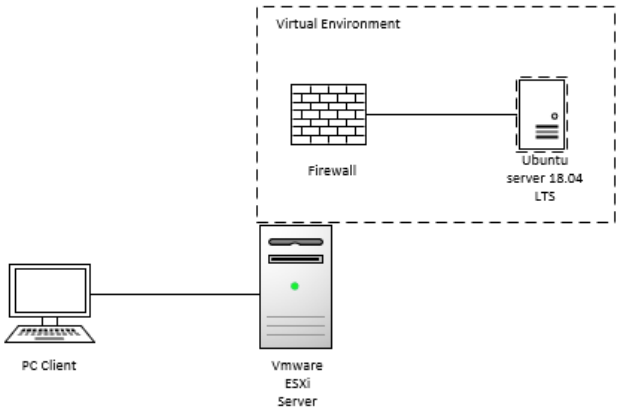
b. Pfsense adalah *firewall* dan router jaringan *open source* yang berbasis sistem operasi FreeBSD. Pfsense dilengkapi dengan sebuah *custom kernel* dan *third party software* sebagai fungsi tambahan. Pfsense dilengkapi oleh *web interface* untuk mengkonfigurasikan *firewall*.

2. Pembahasan

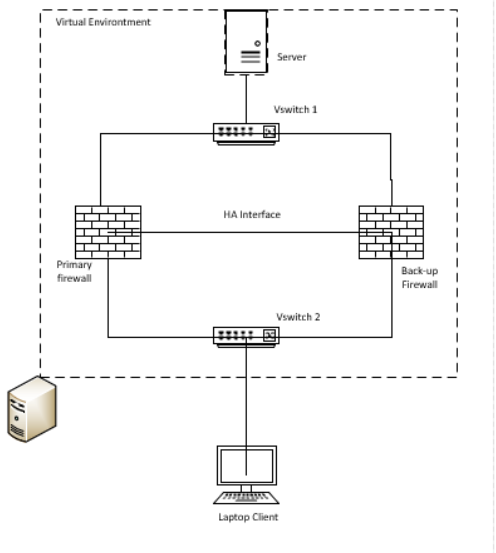
Penelitian ini terdiri dari dua skenario pengujian. Skenario pertama berupa pengujian *throughput* dengan melewatkan paket-paket data dari PC *client* terhadap *server* dalam kondisi normal tanpa serangan maupun, dalam serangan DoS SYN. Skenario kedua berupa pengujian *high availability* Pfsense dan Fortigate dengan cara mengalirkan paket-paket ICMP PING selama 30 detik dari PC *client* terhadap sebuah *cluster firewall* terdiri dari dua buah *firewall*. Di mana di detik ke 15 salah satu *firewall* dalam *cluster* akan dimatikan secara paksa. Pengujian skenario ini dilakukan sebanyak 20 kali untuk setiap jenis *firewall* secara bergantian.

2.1. Topologi Pengujian

Pada penelitian ini terdapat dua topologi yang berbeda untuk masing-masing skenario. penelitian ini akan dijalankan pada *server* yang telah diinstal *hypervisor* VMware ESXi. Kemudian, diatas *virtualization layer* atau *hypervisor* diinstal dua buah firewall yang berbeda berupa VNF serta akan diinstal ubuntu LTS *server* 18.04.



Gambar 2. Topologi pengujian skenario satu



Gambar 3. Topologi pengujian skenario dua

2.2. Skenario Pengujian

Pengujian dilakukan dengan mengambil nilai rata-rata dari masing-masing skenario. Berikut merupakan skenario pengujian:

a. Throughput

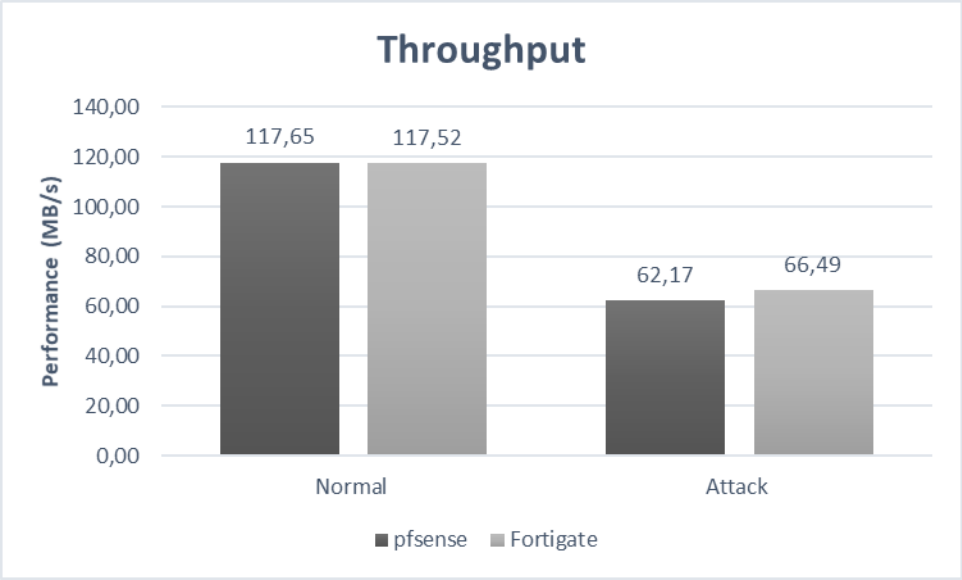
Throughput adalah rata – rata maksimum paket data yang berhasil dikirimkan tanpa adanya paket data yang hilang. Pada parameter pengujian ini akan ditampilkan trafik throughput yang dihasilkan dari *server* yang diakses oleh *client*. Parameter ini akan didapatkan dengan melakukan metode pengujian pertama menggunakan topologi pada gambar 2.

b. *High Availability*

High availability merupakan sebuah mekanisme respons kegagalan untuk infrastruktur. Pengujian ini berfungsi untuk mengetahui kemampuan dari *firewall* dalam melakukan *failover*, merupakan mode operasional cadangan di mana fungsi komponen *firewall* utama diambil alih oleh *firewall* cadangan ketika *firewall* utama menjadi tidak tersedia karena kegagalan sistem. Pengujian ini dilakukan dengan mengirimkan paket ICMP PING dari *client* kepada *server* menggunakan topologi pada gambar 3. Parameter skenario ini adalah *delay.*

2.3. Hasil

Pada bab ini akan dibahas mengenai analisis dari hasil pengujian yang telah dilakukan sesuai dengan skenario dan parameter pengujian yang telah ditetapkan.



Gambar 4. Grafik pengujian *throughput*

Berdasarkan hasil pengujian pada gambar 4 bahwa Pada keadaan normal, throughput pfsense memiliki nilai sebesar 117,65 MB/s lebih besar dibandingkan dengan Fortigate dengan nilai sebesar 117,52 MB/s. Namun, Fortigate memiliki ketahanan terhadap serangan DoS SYN yang lebih baik dibanding pfsense dengan nilai penurunan performa menjadi 66,49 MB/s dibandingkan dengan pfsense menjadi sebesar 62,17 MB/s. Pada pengujian *throughput*, paket yang dialirkan dibiarkan dalam jumlah yang tidak terbatas sehingga dapat menyesuaikan dengan besarnya *bandwidth* yang dapat dilewati.

Tabel 1. Hasil pengujian *High availability*

High Availability		
NO	Firewall	Delay (seconds)
1	Pfsense	2,14
2	Fortigate	1,68

Berdasarkan pengujian *high availability* pada tabel 1. Pfsense memiliki *delay* yang lebih besar dengan nilai 2,14 *seconds* dibandingkan dengan Fortigate yang memiliki *delay* sebesar 1,68 *seconds*. Hal ini menandakan bahwa ketika proses *failover* terjadi, Pfsense membutukan waktu lebih lama dibandingkan dengan fortigate.

3. Kesimpulan

Berikut adalah beberapa kesimpulan dari penelitian ini.

1. Berdasarkan pengukuran parameter throughput Pfsense memilki kinerja yang lebih baik dari pada Fortigate baik dalam keadaan normal dengan nilai sebesar 177,65 MB/s sedangkan setelah simulasi serangan DoS SYN Fortigate memilki nilai throughput yang lebih baik sebesar 66,49 MB/s
2. Berdasarkan hasil pengujian *high availability*, Fortigate memiliki kinerja terbaik dari segi *delay* dengan nilai sebesar 1,68 *seconds* dibanding dengan pfsense dengan nilai 2,14 *seconds*

Ucapan Terima Kasih
Penulis mengucapkan terima kasih kepada rekan-rekan di Universitas Telkom dan kepada dosen yang telah membimbing penulis publikasi dari penelitian ini.

Daftar Pustaka

[1] ETSI, “Network Functions Virtualisation (NFV); Architectural Framework,” *ETSI GS NFV 002 v1.2.1*, vol. 1, pp. 1–21, 2014.
[2] IT Central Station, “Business Intelligence Tools Buyer ’ s Guide and Reviews February 2018,” no. February, 2018.
[3] M. Arunwan, T. Laong, and K. Atthayuwat, “Defensive performance comparison of firewall systems,” *2016 Manag. Innov. Technol. Int. Conf. MITiCON 2016*, pp. MIT221-MIT224, 2017.
[4] L. Zabala, R. Solozabal, A. Ferro, and B. Blanco, “Model of a Virtual Firewall Based on Stochastic Petri Nets,” *2018 IEEE 17th Int. Symp. Netw. Comput. Appl.*, pp. 1–4, 2018.
[5] G. Attebury and B. Ramamurthy, “Router and firewall redundancy with OpenBSD and CARP,” *IEEE Int. Conf. Commun.*, vol. 1, no. c, pp. 146–151, 2006.
[6] M. L. T. Cossio *et al.*, *Virtualization:A manager’s guide*, vol. XXXIII, no. 2. 2012.