BAB 1
PENDAHULUAN

1.1 Latar Belakang

Network Function Virtualization atau biasa yang disebut NFV merupakan sebuah konsep baru dalam mendesain, menyebarkan, dan mengelola sebuah layanan jaringan dengan cara pembuatan virtual sebuah perangkat jaringan dari yang sebelumnya berbentuk fisik atau perangkat keras sehingga dapat dipakai dan dipindahkan di berbagai lokasi jaringan yang diperlukan tanpa harus melakukan pemasangan alat baru. NFV memungkinkan beberapa perangkat jaringan dapat berjalan pada satu komputer. Perangkat – perangkat jaringan yang divirtualkan pada NFV disebut sebagai VNF (Virtual Network Function).

Untuk menjalankan VNF dibutuhkan sebuah *hypervisor* yang mengatur manajemen *hardware* yang digunakan. *Hypervisor* atau yang dikenal sebagai *virtual machine management* dibagi menjadi 2 tipe, yaitu *bare-metal hypervisor* dan *hosted hypervisor*. B*are-metal hypevisor* dapat berjalan langsung pada perangkat keras komputer sedangkan *hosted hypervisor* memerlukan *operating system environment* (OSE) untuk menjalankannya [1]. Salah satu contoh *bare-metal hypervisor* adalah XEN. Xen ProjectTM adalah *platform* virtualisasi *open source* yang mendukung beberapa *cloud* terbesar dalam produksi saat ini. Amazon Web *Services*, Aliyun, Rackspace *Cloud* Umum, Verizon *Cloud* dan banyak layanan *hosting* menggunakan software Xen [2].

Salah satu contoh VNF adalah *virtual firewall*. Kelebihan *virtual firewall* dibandingkan *firewall* fisik adalah mudah dikelola, dapat dipakai sesuai kebutuhan, dan efektivitas biaya [3]. Pada tugas akhir ini *virtual firewall* yang digunakan adalah OPNsense, pfSense, dan IPFire karena ketiga *firewall* tersebut bisa didapatkan secara gratis dan bersifat *open source* serta ketiga *firewall* tersebut dapat dikonfigurasi melalui *web*. pfSense merupakan *firewall* berbasis FreeBSD yang sangat populer untuk solusi keamanan serta *user* dapat melakukan modifikasi dan mudah dalam instalasi [4]. IPFire adalah sebuah distribusi Linux yang berfokus pada *setup* yang mudah, penanganan yang yang baik, dan tingkat keamanan yang tinggi [5]. Sedangkan OPNsense bermula sebagai turunan dari pfSense dan

m0n0wall pada tahun 2014 dan dirilis resmi pada Januari 2015. OPNsense merupakan *open source virtual firewall* yang mudah digunakan dan mudah dalam membuat *firewall* dan *routing platform* berbasis FreeBSD [6].

Berdasarkan penelitian yang telah dilakukan oleh Hasan Fayyad dan teman – temannya pada "*Benchmarking the Performance of Microsoft Hyper-V server, VMWare ESXi and Xen Hypervisors*" [7] didapatkan bahwa *hypervisor* XEN dapat digunakan sebagai *soft real-time* OSs karena XEN memungkinkan pengguna untuk melakukan kontrol penuh terhadap seluruh sistem. Pada penelitian yang dilakukan oleh Revan Faredha A. dikatakan bahwa XEN memiliki performansi yang terbaik secara keseluruahn dibanding KVM dan Vmware ESXi dengan nilai performansi 88.2% [2]. Sedangkan pada *white paper* Telco System [8], dengan adanya NFV memungkinkan untuk mempermudah ancaman untuk masuk ke jaringan telco selain itu dapat membuat *malware* dapat berjalan di perangkat manapun dan memungkinkan DDoS (*Distributed Denial of Service*) untuk menyerang ke sumber daya jaringan. Menurut penelitian yang dilakukan oleh Amit Thakur [4] pada tiga *firewall* (Untangle, pfSense, dan Zeroshell) yang dijalankan pada VMware EXSi, pfSense merupakan *firewall* yang paling baik digunakan dalam penelitian tersebut dibanding *firewall* lain karena sebagian besar fitur pfSense didukung dengan spesifikasi *hardware* yang rendah. Dan pada penelitian yang dilakukan oleh Fredrik Jakobsson [5], IPFire dianggap terbaik dibandingkan dengan ClearOS dan Untangle NG Firewall karena unggul dalam hal *throughput* dan *latency*.

Tugas akhir ini akan membandingkan beberapa performa dari ketiga *virtual firewall* (pfSense, OPNsense, dan IPFire) dan sebuah *virtual router* (VyOS) yang dijalankan pada *hypervisor* XEN. Perbandingan performa dari keempat VNF tersebut akan didasarkan pada RFC 2544 yang ada pada IETF (*Internet Engineering Task Force*) yaitu *throughput*, *latency*, *packet loss*, *Denial of Service* (DoS) *handling* yang berdasarkan pada RFC 3511 dan dengan tambahan parameter *jitter* dan CPU *usage*.

1.2 Rumusan Masalah

Berdasarkan deskripsi dari latar belakang yang telah dipaparkan sebelumnya, maka masalah dalam tugas akhir ini dapat dirumuskan sebagai berikut :

1. Bagaimana cara konfigurasi *virtual firewall* agar jenis paket yang dilewatkan hanya paket ingin dianalisa saja?
2. Bagaimana cara menguji *throughput*, *packet loss*, *latency*, *jitter*, *denial of service handling*, dan CPU *usage* pada VNF yang dijalankan?
3. Apakah terdapat perbedaan perfomansi pada keempat VNF yang dijalankan?
4. VNF manakah yang memiliki hasil lebih bagus pada parameter yang diujikan saat menghadapi serangan *denial of service*?

1.3 Batasan Masalah

Batasan masalah yang ada pada tugas akhir ini adalah *Virtual Network Function* (VNF) yang digunkan dalam tugas akhir ini adalah OPNsense, pfSense, IPFire, dan VyOS yang dijalankan pada *hypervisor* XEN dengan tidak melibatkan optimasi dari *server* yang digunakan. Layanan yang digunakan untuk mengukur performansi dari VNF yang digunakan adalah *video streaming*. Parameter yang diujikan berupa *throughput*, *latency*, *packet loss*, *jitter*, *denial of service handling* dan CPU *usage*.

1.4 Tujuan

Tujuan pada tugas akhir ini adalah menganalisis perbedaan performa dari *virtual firewall* (pfSense, OPNsense, dan IPFire) dan virtual router (VyOS) yang digunakan berdasarkan RFC 2544 yaitu *throughput*, latency, packet loss dan RFC 3511 yaitu *Denial of Service* (DoS) *handling* serta dengan tambahan parameter *jitter* dan CPU *usage*. Keempat VNF tersebut akan dijalankan diatas *bare-metal hypervisor* (XEN) sehingga dapat menghasilkan suatu kesimpulan *virtual firewall* terbaik dalam melakukan beberapa pengujian pada performa *virtual firewall* dan perbedaan perfoma antara *virtual router* dengan *virtual firewall* yang digunakan sesuai RFC 2544 dan RFC 3511 pada IETF.

1.5 Metodologi Penelitian

Adapun metode yang digunakan dalam proses penyelesaian tugas akhir ini adalah sebagai berikut :

1. Studi Literatur

   Studi literatur ini bertujuan untuk mempelajari teori - teori dasar mengenai virtual firewall yang akan digunakan dalam tugas akhir ini.

2. Perancangan

   Melakukan perancangan algoritma dan pembuatan kode program.

3. Simulasi

   Melakukan simulasi dan optimasi sehingga sesuai dengan spesifikasi yang diinginkan.

4. Pengujian dan Analisis

   Melakukan pengukuran dan analisis terhadap parameter – parameter yang dipakai untuk membandingkan performa dari virtual firewall. Adapaun parameter tersebut adalah *throughput, packet loss, latency, jitter, Denial of Service* (DoS) *handling*, dan CPU *usage*.

5. Pembuatan laporan

   Segala proses yang dilakukan dalam penelitian ini akan dibukukan.