UNIVERSITAS INDONESIA

IMPLEMENTASI DAN ANALISA KINERJA XEN VIRTUAL SERVER DENGAN METODE IP FORWARD DAN PORT FORWARD PADA INFRASTRUKTUR JARINGAN BERBASIS VIRTUALISASI

SKRIPSI

ACHMAD FARISY
0806338992

FAKULTAS TEKNIK UNIVERSITAS INDONESIA
DEPARTEMEN TEKNIK ELEKTRO
TEKNIK KOMPUTER
DEPOK
JULI 2012

UNIVERSITAS INDONESIA

IMPLEMENTASI DAN ANALISA KINERJA XEN VIRTUAL SERVER DENGAN METODE IP FORWARD DAN PORT FORWARD PADA INFRASTRUKTUR JARINGAN BERBASIS VIRTUALISASI

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik

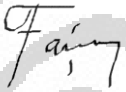
ACHMAD FARISY
0806338992

FAKULTAS TEKNIK UNIVERSITAS INDONESIA
DEPARTEMEN TEKNIK ELEKTRO
TEKNIK KOMPUTER
DEPOK

JULI 2012

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama	**:**	**Achmad Farisy**
NPM	**:**	**0806338992**
Tanda Tangan	**:**	
Tanggal	**:**	**Juli 2012**

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh :

Nama	:	Achmad Farisy
NPM	:	0806338992
Program Studi	:	Teknik Komputer
Judul Skripsi	:	Implementasi dan Analisa Kinerja Xen Virtual Server Port dan IP Forward dengan IPTables Pada Infrastruktur Jaringan Virtualisasi

.Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar sarjana Teknik pada Program Studi Teknik Komputer, Departemen Teknik Elektro, Fakultas Teknik, Universitas Indonesia.

DEWAN PENGUJI

Pembimbing : Muhammad Salman, S.T., M.IT ( )

Penguji : Yan Maraden, S.T., M.Sc ( )

Penguji : I Gde Dharma Nugraha, S.T., MT ( )

Ditetapkan di : Depok

Tanggal : 11 Juli 2012

UCAPAN TERIMA KASIH

Puji syukur saya panjatkan kehadirat Allah SWT sebab atas segala rahmat dan hidayah-Nya, saya dapat menyelesaikan skripsi ini. Saya menyadari bahwa skripsi ini tidak dapat diselesaikan tanpa bantuan dari banyak pihak. Oleh karena itu, saya mengucapkan terima kasih kepada:

1) Bapak Muhammad Salman S.T. , MIT selaku pembimbing skripsi saya. Terima kasih atas pengarahan, koreksi, dukungan, dan waktu yang telah diberikan selama saya mengerjakan skripsi ini.
2) Orang tua dan keluarga saya yang telah memberikan dukungan baik moril maupun materil sehingga saya dapat menyelesaikan skripsi ini.
3) Teman – teman dari Departemen Teknik Elektro dalam memberikan masukan – masukan kepada penulis.
4) Addina Fitriatika Daraini yang telah selalu memberikan semangat selama proses pembuatan skripsi ini.

Akhir kata, semoga Tuhan berkenan membalas kebaikan dari semua pihak yang telah berbaik hati membantu saya dan semoga skripsi ini dapat bermanfaat bagi perkembangan teknologi dan ilmu pengetahuan.

Depok, 11 Juli 2012

Achmad Farisy

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini :

Nama	:	Achmad Farisy
NPM	:	0806338992
Program Studi	:	Teknik Komputer
Departemen	:	Teknik Elektro
Fakultas	:	Teknik
Jenis Karya	:	Tugas Akhir

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Nonekslusif** (*Non-exclusive Royalty-Free Right*) atas karya ilmiah saya yang berjudul :

IMPLEMENTASI DAN ANALISA KINERJA XEN VIRTUAL SERVER DENGAN METODE IP FORWARD DAN PORT FORWARD PADA INFRASTRUKTUR JARINGAN BERBASIS VIRTUALISASI

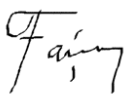
Dengan Hak Bebas Royalti Nonekslusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian persetujuan ini saya buat dengan sebenarnya.

Dibuat di : Depok

Pada tanggal : Juli 2012

yang menyatakan,



(Achmad Farisy)

ABSTRAK

Nama : Achmad Farisy

Program Studi : Teknik Komputer

Judul : Implementasi dan Analisa Kinerja Xen Virtual Server dengan Metode IP Forward dan Port Forward pada Infrastruktur Jaringan Berbasis Virtualisasi

Teknologi Virtualisasi semakin meningkat kepentingannya dalam dunia IT sebagai salah satu metode dalam penghematan dalam penggunaan perangkat keras yang ada dan pemanfaatan Alamat IP Publik pun semakin banyak sehingga tidak akan lama akan penuh. Xen sebagai salah satu sistem opensource yang turut berkontribusi besar dalam virtualisasi dan dapat bersaing dengan para pengembang virtualisasi komersial sehingga virtualisasi dengan Xen bisa dibilang salah satu solusi untuk menuju virtualisasi server serta dengan pemanfaatan *packet filter* pada IPTables dengan tujuan mengurangi pemanfaatan *IP Publik* dengan membuat *IP Private* server Internal menjadi dapat di akses oleh Publik. Dari hasil penelitian ini untuk penggunaan *CPU Usage* dan RAM Usage dengan metode *Port Forward* lebih efisien sekitar 30% dan 1,125% terhadap *IP Forward*, dan persentase secara keseluruhan dari pengujian kedua metode ini didapatkan nilai efisiensi 23,3625% dengan metode *Port Forward* terhadap *IP Forward*

Kata kunci :
Virtualisasi Server, Xen, IPTables, IP Publik, IP Forward, Port Forward, CPU Usage, RAM Usage

ABSTRACT

Name : Achmad Farisy

Study Program : Computer Engineering

Title : Implementation and Performance Analysis of Xen Virtualization Server using IP Forward and Port Forward Methods on Virtualization based Network Infrasrtructure

Virtualization technology increasing its importance in the world of IT as one methods of saving in the using existing hardware and utilization of public IP address is much so will not long shall be full. Xen as one system opensource that contribute large in virtualization and can compete with the developers virtualization commercial so virtualization through xen pass as a solution for toward virtualization server, and from the utilization packet filter to iptables with the purpose of reducing utilization ip at public made lp private server internal be can be in access by the public. From the results of this research for use of CPU Usage and RAM Usage with more efficient methods of Port Forward around 30% and 1,125% against IP Forward, and the overall percentage of testing both of these methods are obtained value efficiency 23,3625% with the method of Port Forward than IP Forward

Key words :

Virtualization Server, Xen,IPTablesl, IP Public , Port Forward, IP Forward, CPU Usage, RAM Usage

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dengan ledakan pertumbuhan internet dan perannya yang semakin penting dalam kehidupan kita, lalu lintas di internet pun meningkat secara dramatis. Beban di situs-situs internet yang popular pun meningkat pesat dimana sautu situs tersebut mendapatkan puluhan juta pengunjung per harinya. Hal ini menyebabkan banyak administrator menemukan masalah tentang bottleneck pada kinerja server mereka dimana dengan mudahnya access request ke server mengakibatkan kelebihan beban dalam waktu singkat. Saat ini, semakin banyak perusahaan yang lebih memfokuskan bisnis mereka di internet sehingga behenti atau adanya intrupsi dari pelayanan di suatu server yang mengakibatkan bisnis merugi, dan ketersediaan pelayanan suatu server yang meningkat mengakibatkan server menjadi semakin penting.

Dengan meningkatnya kebutuhan penggunaan suatu sever yang memiliki kemampuan :

- Peningkatan skalabilitas
- Ketersediaan 24 x 7
- Efektifitas biaya

Mengakibatkan banyak yang mencari solusi untuk masalah ini salah satunya yaitu *virtualisasi server*. Yaitu suatu teknologi yang memungkinkan beberapa virtual mesin dapat berjalan pada server tunggal secara fisik. Dengan melakukan virtualisai ini dapat mengurangi biaya operasional dan meningkatkan kemampuan serta kemudahan beroperasi suatu server dengan infrastruktur IT lainnya.

Teknologi vrtualisasi juga berdampak positif pada sisi system keamanannya dimana terdapat suatu system yang khusus melakukan isolasi atau pemisahan dari beberapa mesin virtual yang dibuat oleh hypervisor yaitu perangkat lunak yang berfungsi membuat mesin virtual. Lalu dengan penambahan firewall pada hypervisor yang terhubung pada server virtual bisa meningkatkan keamanan dari sisi server virtual itu sendiri.

1.2 Tujuan Penelitian

Tujuan dari penulisan ini adalah :

1. Membangun jaringan virtualisasi dengan konsep Virtualisasi Server
2. Mengukur kinerja Xen Virtual Server dengan penggunaan 1 dan 2 IP Public untuk 2 Virtual Server
3. Menggunakan Netfilter/IPTables sebagai Packet Filter

1.3 Batasan Masalah

Pembatasan masalah pada perancangan server virtual ini, adalah :

- Penggunaan Xen Hypervisor sebagai perangkat lunak untuk membuat mesin virtual
- Penggunaan IPTables pada Host Server sebagai pengaturan jaringan untuk Virtualisasi server.
- Xen-Ubuntu 12.02 LTS 32-Bit sebagai Host.

1.4 Metodologi Penulisan

1. Studi Literatur

   Studi literature melalui buku – buku, jurnal, forum ataupun dari situs – situs di internet yang berhubungan dengan keamanan pada server virtual dengan penggunaan Ubuntu 12.04 LTS 32-Bit dan Xen Hypervisor.
2. Konsultasi dengan Dosen Pembimbing

   Pertemuan pada rapat pleno setiap seminggu sekali membantu memberikan pengarahan kepada penulis.
3. Analisa

   Melakukan analisa terhadap berbagai informasi yang diperoleh dengan tujuan untuk peningkatan kinerja pada Virtual Server.

1.5 Sistematika Penulisan

Skripsi ini dibagi menjadi 4 bab, yaitu :

1. BAB 1 : Pendahuluan

Berisi latar belakang masalah, tujuan, pembatasan masalah, metodologi dan sistematika penulisan.

2. BAB 2 : DASAR TEORI

   Membahas tentang hal yang melatarbelakangi virtualisasi, Hypervisor, virtual server dan firewall.

3. BAB 3 : PERANCANGAN

   Bab ini mencakup penjelasan mengenai perangkat, metode serta prosedur yang akan digunakan pada saat pelaksanaan penelitian.

4. BAB 4 : PENGUJIAN

   Bab ini menjelaskan metode pengujian yang dilakukan dalam penelitian.

5. BAB 5 : KESIMPULAN

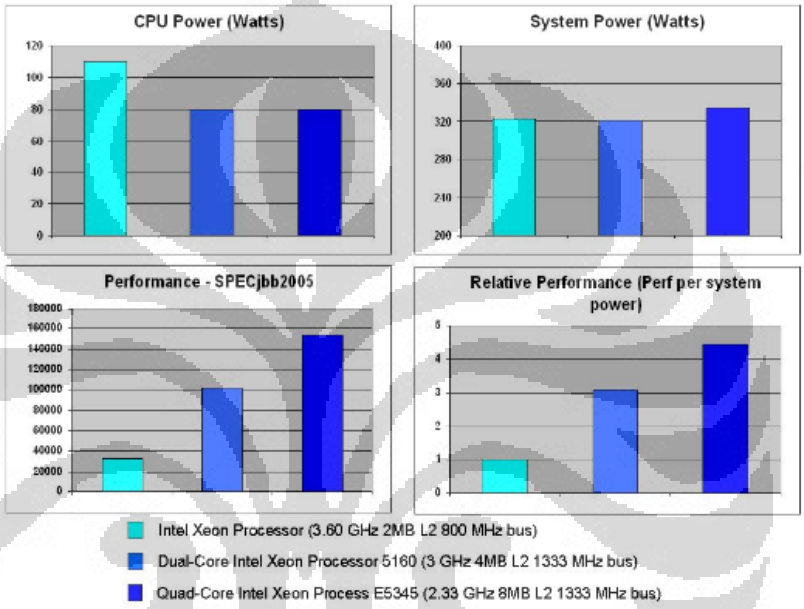
   Bab ini berisikan kesimpulan dari hasil pengujian da penelitian.

BAB 2

LANDASAN TEORI

2.1 Konsolidasi Virtualisasi untuk Penghematan Energi

Peralihan dari bentuk fisik ke virtualisasi didasarkan karena konsumsi daya dari suatu CPU sebanding dengan performance. Dari gambar terlihat perbandingan konsumsi daya dan performance

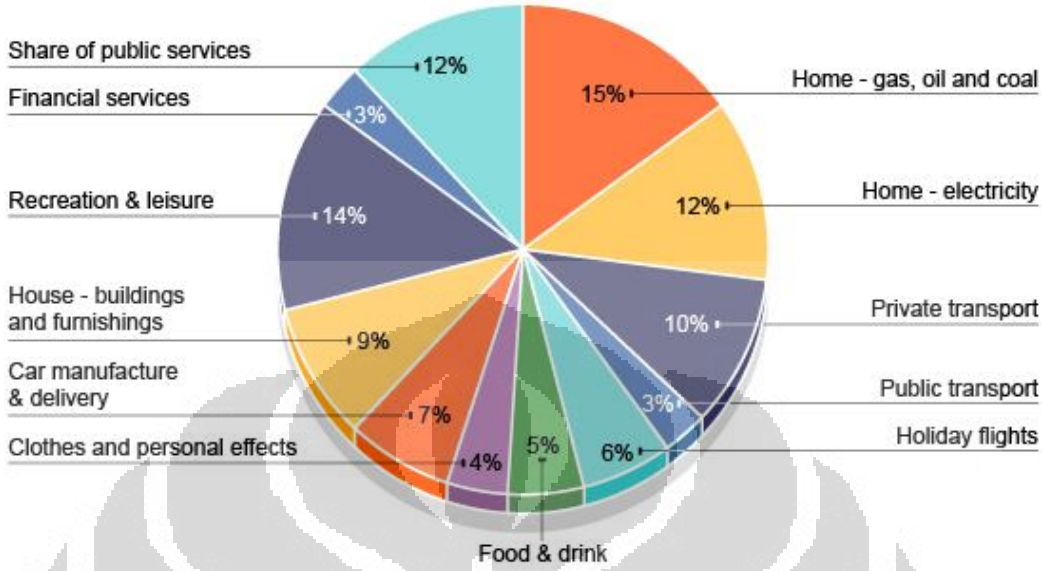


Gambar 2.1 Daya dari CPU dan Performanya

Sumber: Meeting Green Computing Challenges, David Wang, Ph.D.

Berdasarkan gambar bisa dikatakan efiiensi energy merupakan aspek yang penting dalam mengurangi pemborosan energy. Menurut World Energy Council (WEC) ada tiga sektor utama yang bertanggung jawab pada konsumsi energi negara-negara di dunia diantaranya mesin industri sebanyak 45%, pencahayaan sekitar 15%, peralatan rumah tangga dan elektronik sekitar 15%. Diketahui bahwa prosentase penggunaan daya untuk mesin sangat besar. Hal ini dikarenakan mayoritas keputusan yang diambil oleh pelaku bisnis saat membeli mesin lebih mengutamakan harga yang murah sementara di sisi lain terdapat pemakaian daya yang tinggi. Lalu berdasarkan dari data yang berasal dari penduduk yang hidup di

negara *MEDCS* dengan tingkat pembangunan yang sangat tinggi bisa dilihat dari pie chart dibawah ini.



Gambar 1

Gambar 2.2 *Pie Chart* dari penduduk yang tinggal dalam negara *MEDCS*

Berdasarkan sebuah jurnal yang ditulis oleh sejumlah peneliti dari Sweden's Royal Institute of Technology, menempatkan jumlah dari emisi CO_2 yang didapatkan dari sektor ICT yang berkontribusi sebesar 1,3% dari total emisi karbon di dunia. ICT pun turut bertanggung jawab dalam 3.9 persen dari pemakaian energi di dunia. Tabel di bawah ini menunjukkan jumlah yang berbeda dari setiap area di dalam ICT.

Table 2.1 Dampak Lingkungan dari Berbagai Elektronik

Table 4. Operational Electricity (TWh) and Total CO_2-eq Emissions (Mt) Relating to Information and Communication Technology (ICT) and Its Subsectors in 2007

ICT	*Operational electricity [TWh]*	*Total CO_2-eq emissions [Mt]*
Mobile telecom	**60**	**80**
Mobile networks, operation	50	46
Mobile networks, manufacturing (incl. also sites, etc.)	n.a.	9
Mobile phones, operation	9	5
Mobile phones, manufacturing	n.a.	21
Fixed telecom	**160**	**120**
Fixed networks, operation	72	54
Fixed networks, manufacturing (incl. also sites, etc.)	n.a.	10
Cordless phones, operation	22	13
BB modems and routers, operation	35	21
PBXs, faxes and various business systems, operation	35	20
End-user telecom equipment, manufacturing	n.a.	6
PCs	**260**	**250**
PCs, operation	258	155
PCs, manufacturing	n.a.	97
Data centers, enterprise networks and transport networks	226	170
Data centers, operation	180	108
Enterprise networks, operation	29	17
Transport networks, operation	17	10
Data hardware, manufacturing	n.a.	30
Total	**710**	**620**

Note: n.a. = not applicable. Operational electricity for manufacturing not assessed. BB = broadband; PBX = private branch exchange.

Sektor ICT mencakup dua aspek yakni teknologi informasi yang meliputi segala hal yang berkaitan dengan pengelolaan informasi dan teknologi komunikasi yang berkaitan dengan penransferan data dari satu perangkat ke perangkat lain. Dapat dilihat pada tabel bahwa untuk teknologi informasi memakan porsi yang lebih besar dibandingkan dengan teknologi komunikasi dengan data bahwa operasional PC dan *data center* mengambil porsi yang terbesar dibandingkan penggunaan lainnya begitu pula dengan penggunaan – penggunaan lain di dalam teknologi informasi yang apabila diakumulasikan akan lebih tinggi dibandingkan dengan teknologi komunikasi. Terlihat pada kolom paling kanan yakni total emisi karbon yang dihasilkan, tentunya peantara teknologi informasi akan jauh lebih mengungguli dibandingkan dengan teknologi komunikasi. Sebab semakin banyak energi yang digunakan tentunya akan berbanding lurus dengan emisi karbon yang dihasilkan.

Dengan kondisi dimana dunia semakin terjadi krisis energi, diperlukan sebuah perilaku yang dapat mengurangi terjadinya krisis energi. Pada tahun 1992,

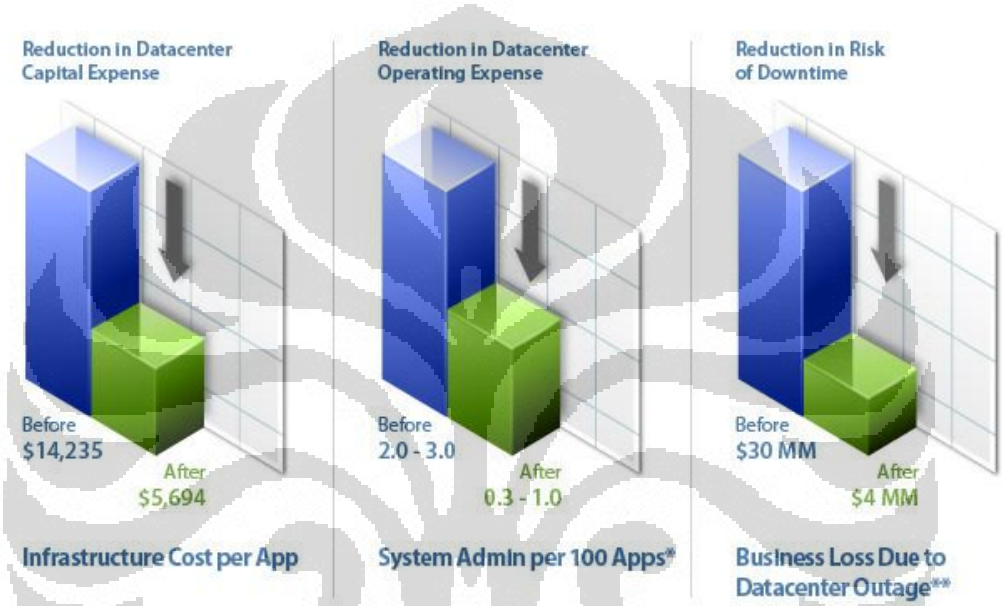
telah hadir di beberapa negara maju seperti Amerika sebuah program yang bernama *Energy Star*. Program *Energy Star* mendorong produsen untuk menciptakan perangkat yang hemat energi dan hanya membutuhkan energi yang minim untuk dapat dioperasikan. Program *Energy Star* merupakan salah satu regulasi metode dari *green computing*. *Green computing* didefinisikan sebagai studi dan praktek dari perancangan, manufaktur, penggunaan, dan pembuangan dari komputer, *server*, dan *subsystems* yang terkait seperti *monitor, printer*, *storage devices*, dan *networking and communications systems* dengan penggunaan konsumsi sumber daya yang dapat berkurang dan pembuangan yang tepat dari elektronik sampah. Dalam bidang komputasi, *green computing* adalah sebuah konsep global yang memerlukan *system architecture, system software, parallel and distributed computing*, dan *computer network.* Hal ini bertujuan untuk mengurangi konsumsi daya dari sistem komputer, menyediakan layanan yang efisien, dapat diandalkan, dan mencapai tujuan dari sistem IT dengan daya rendah. Konsumsi daya dari sebuah sistem komputer ditentukan dari konsumsi daya dari *hardware*, efisiensi *runtime* dari task, dan kebijakan konfigurasi dari sumber daya.

Berikut adalah beberapa metode pendekatan dalam pengehematan sumber daya energy :

1. Pemanfaatan energi alternatif
2. Penggunaan sistem teknologi virtualisasi
3. Pengaturan penggunaan sumber daya
4. Penggunaan *hardware* yang *low power*
5. Pemanfaatan sistem daur ulang

Dari kelima metode di atas, virtualisasilah yang akan dibahas di dalam skripsi ini. Seperti yang telah diketahui bersama bahwa bidang teknologi informasi dan komunikasi diakui tidak sedikit mengambil konsumsi energi seperti contoh untuk menghidupkan layar monitor CRT berukuran 17” diperlukan daya 200 Watt, untuk mengaktifkan *cooler fan*, *removable disk*, dan *CD ROM* diperlukan daya sebesar 100 Watt, dan daya untuk *hard disk* sebesar 250 GB memerlukan daya 25 Watt dalam pemakaiannya.

Dengan teknologi virtualisasi, dimungkinkan untuk menjalankan lebih dari satu mesin komputer di dalam satu fisik mesin komputer. Tentu saja dengan teknologi virtualisasi, dapat terjadi pengurangan pada pemakaian perangkat keras secara fisik dan pemaksimalan penggunaan perangkat keras itu sendiri.lalu berdasarkan dari hasil literature yang didapat juga terdapat grafik yang menunjukkan keuntungan bagi suatu perusahaan dalam penggunaan teknologi virtualisasi



Gambar 2.3 Penhematan dengan Virtualisasi

Menyadari bahwa perkembangan teknologi saat ini yang sudah menjadi kebutuhan utama serta penggunaan komputer yang akan selalu bertambah dari waktu ke waktu harus disertai dengan pertimbangan akan tetap menjaga aspek lingkungan tetap bersih, sehat, dan tidak tercemar oleh bahan – bahan berbahaya, dapat lebih baik untuk memiliki sikap peduli terhadap segala aspek dengan harapan agar terhindar dari pemborosan energi yang dapat berdampak kepada pencemaran lingkungan.

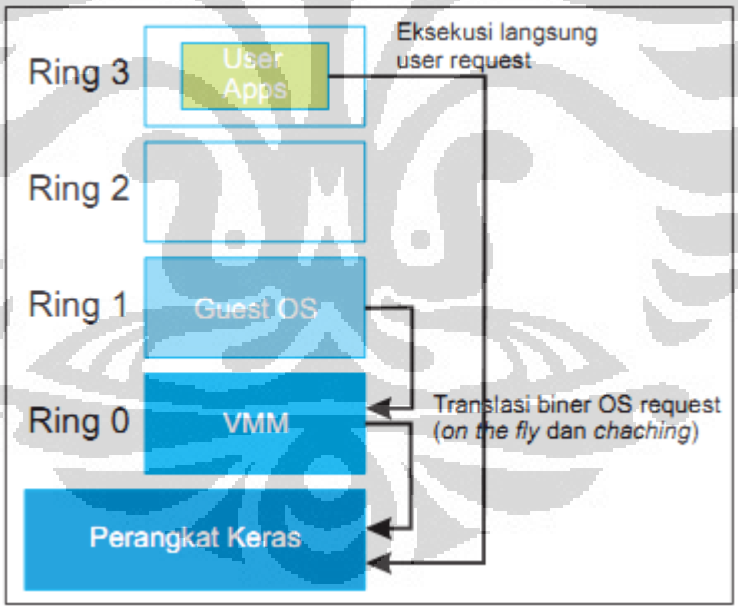
2.2 Teknologi Virtualisasi

Virtualisasi adalah metode untuk mengoperasikan beberapa system operasi virtual yang independen pada sebuah computer fisik tunggal. Ini adalah cara untuk

memaksimalkan suatu sumber daya fisik sebagai pemaksimalan investasi pada perangkat keras. Dalam membuat suatu computer fisik tunggal terdapat tekniknya, yaitu *full virtualization, partial virtualization, dan paravirtualization.*

2.2.1 **Full Virtualization**

Teknik ini menggunakan translasi biner dan eksekusi langsung. Dengan menempatkan VMM di ring 0, mengakibatkan guest OS, yaitu sistem operasi yang divirtualisasi, terpisah dari sumber daya perangkat keras. Hal ini mengakibatkan guest OS tidak menyadari sedang divirtualisasi, tanpa modifikasi terhadap OS tersebut. Instruksi-instruksi sensitif ditranslasi biner menjadi sebarisan instruksi yang dapat dieksekusi di perangkat keras. Translasi instruksi tersebut dan instruksi OS dilakukan secara langsung sehingga dapat dilakukan dengan cepat. Sementara instruksi di tingkat pengguna diteruskan dan dieksekusi secara langsung tanpa melalui translasi VMM agar performanya terjaga. Dapat dilihat pada gambar.



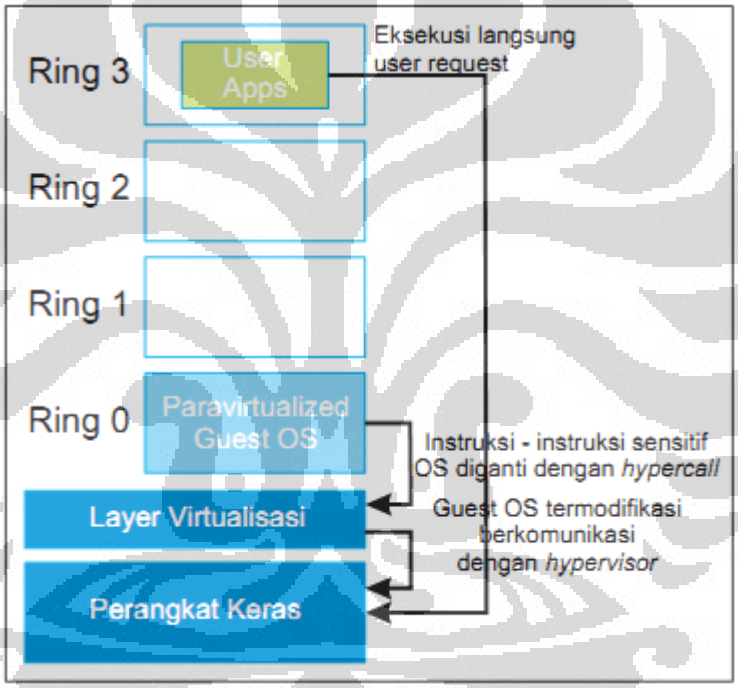
Gambar 2.4 Full-Virtualization

Sumber : Vmware

2.2.2 **ParaVirtualization**

Teknik ini disebut juga dengan OS Assisted Virtualization. Teknik ini dilakukan dengan memodifikasi OS untuk mengganti instruksi-instruksi sensitif

dengan hypercall yang dapat berkomunikasi secara langsung dengan lapisan virtualisasi hypervisor. Paravirtualization memiliki kelebihan dan kekurangan dibandingkan full virtualization. Paravirtualization memiliki kelebihan berupa overhead yang lebih sedikit. Kekurangan dari teknik ini adalah performa yang tergantung dari jenis beban kerja. Selain itu, paravirtualization tidak dapat mendukung OS tanpa modifikasi seperti Windows XP, sehingga kompatibilitasnya rendah. Apabila dilihat dari sisi pengembangan, modifikasi OS relatif lebih mudah daripada membuat metode translasi biner untuk mendukung full virtualization.



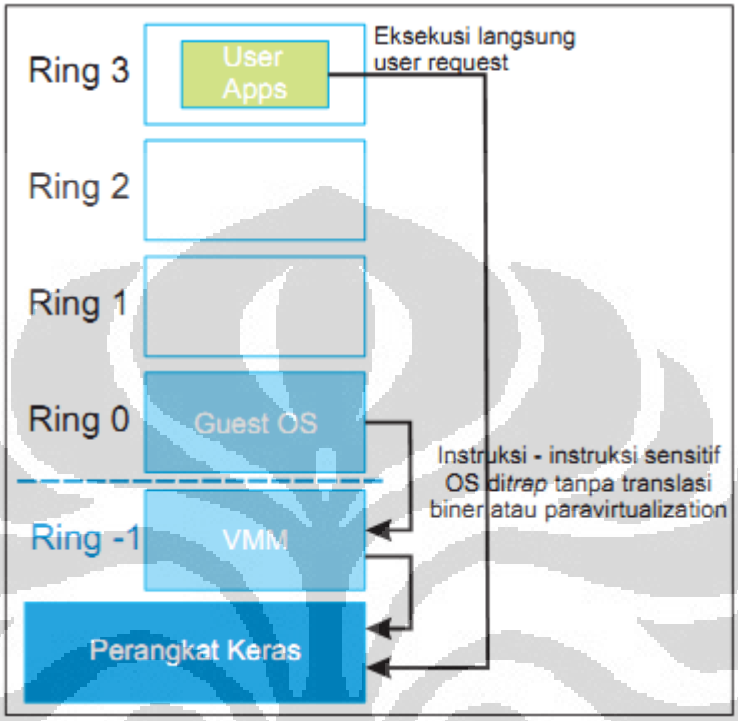
Gambar 2.5 Paravirtualization

Sumber : Vmware

2.2.3 **Hardware Assisted Virtualization**

Teknik ini menggunakan bantuan perangkat keras prosesor. Dua tipe prosesor yang telah mendukung instruksi virtualisasi adalah Intel-VT dan AMD-V. Keduanya menyediakan modus eksekusi CPU bagi instruksi-instruksi sensitive dengan membuat VMM berjalan di bawah ring 0, yang dapat disebut ring -1.

Instruksi-instruksi sensitive secara otomatis dikenali kemudian di-trap ke hypervisor, sehingga tidak memerlukan translasi biner atau paravirtualization. Hal ini dapat dilihat pada Gambar dibawah.



Gambar 2.6 Hardware Assisted Virtualization

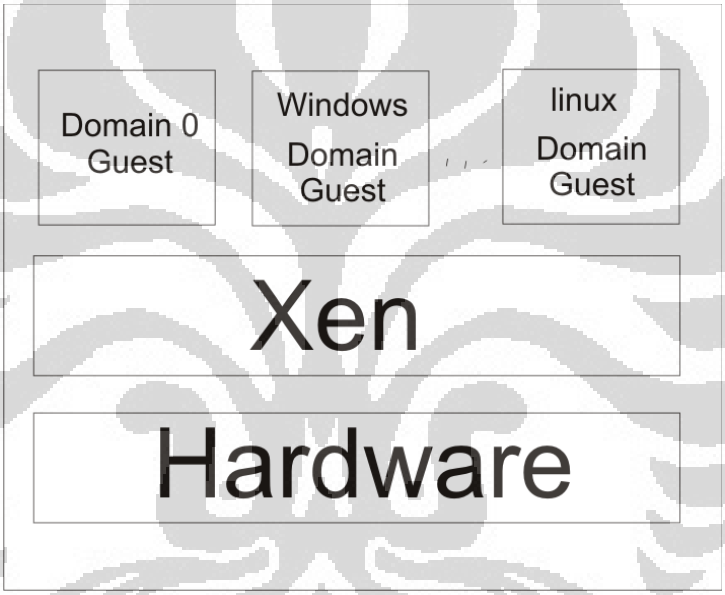
Sumber : VMware

2.3 Xen Hypervisor

Xen Hypervisor adalah layer perangkat lunak yang berjalan secara langsung pada perangkat keras yang menggantikan system operasi sehingga memungkinkan perangkat keras computer tersebut untuk menjalankan beberapa *guest* system operasi secara bersamaan. Beberapa processor yang mendukung antara lain x86-64, Itanium, Power PC, dan processor ARM membuat Xen Hypervisor memungkinkan untuk berjalan di berbagai perangkat computer dan saat ini didukung oleh Linux, NetBSD, FreeBSD, Solaris, Windows dan system operasi umum lainnya yang sebagai *Guest* pada Hypervisor. Komunitas Xen.org mengembangkan dan memelihara Xen Hypervisor sebagai solusi gratis yang berlisensi dibawah GNU General Public License.

Sebuah computer yang menjalankan Xen Hypervisor mengandung tiga komponen:

1. Xen Hypervisor
2. Domain 0, privileged Domain – privileged guest yang berjalan pada Hypervisor dengan akses langsung ke perangkat keras dan memiliki tanggung jawab untuk memanajemen guest.
3. Multiple Domain U, Unprevilaged Domain Guest (DomU) – Unprevilaged Guest yang berjalan pada Hypervisor tidak memiliki akses langsung ke perangkat keras.(misal disk, memory, dll)



Gambar 2.7 Xen

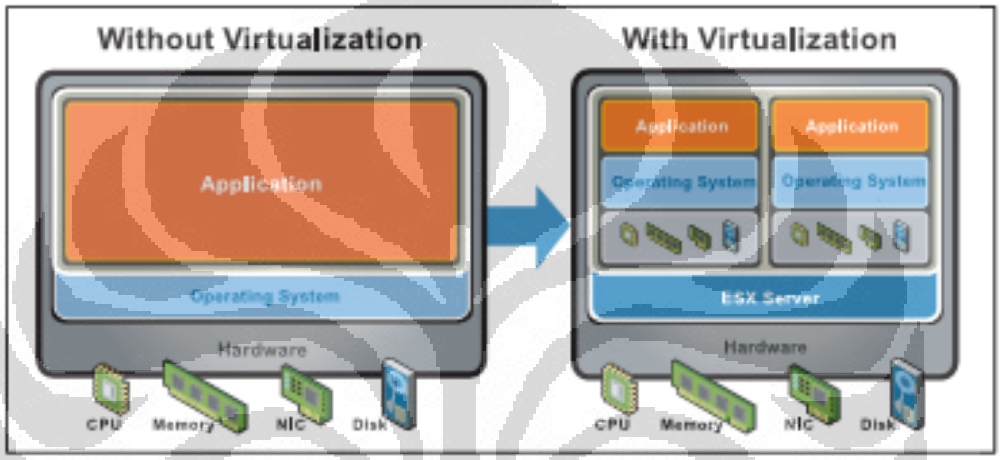
Xen Hypervisor berjalan secara langsung pada perangkat keras dan tatap muka langsung terhadap semua permintaan pernagkat keras seperti CPU, I/O dan Disk untuk system operasi tamu/Guest OS. Dengan memisahkan Guest dari perangkat keras, Xen Hypervisor dapat menjalankan beberapa system operasi dengan aman dan independen.

Domain 0 guest disebut sebagai Dom0 yang berhubungan langsung dengan Xen Hypervisor selama system awal start-up dan dapat dijalankan oleh system operasi kecuali *windows.* Dom0 memiliki hak unik untuk mengakses Xen Hypervisor dan tidak dapat dialokasikan dengan Domain guest lainnya. Hak ini

memungkinkan untuk mengelola semua aspek Domain guest seperti memulai, berhenti, permintaan I/O, dll. Seorang administrator system dapat login ke Dom0 dan mengelola seluruh system computer.

Beberapa Domain guest disebut sebagai DomUs yang berasal dan dikontrol oleh Dom0 dan bersifat independen beroperasi pada system.

2.4 Virtual Server



Gambar 2.8 tradisional dan virtual server (anonym 2009)

Virtualisasi Server adalah teknologi yang telah terbukti memungkinkan beberapa virtual mesin untuk dijalankan pada server fisik tunggal. Setiap mesin virtual benar – benar terisolasi dari mesin virtual lain dan dipisahkan dari host dengan *thin layer* dan hypervisor. Hal ini memungkinkan setiap mesin virtual untuk menjalankan system operasi dan aplikasi yang berbeda. Karena mesin telah tepisahkan dari host, guest juga dapat dipindahkan dari satu host server fisik ke yang lainnya saat berjalan, ini dikenal sebagai *Live migration*.

Teknologi virtualisasi server sebagai teknologi yang masih berkembang memiliki sejumlah kelebihan dan permasalahan. Kelebihan yang diharapkan dari teknologi virtualisasi server antara lain :

1. Peningkatan utilisasi perangkat keras,
2. Peningkatan efektifitas manajemen infrastruktur server,
3. Perbaikan proses pemulihan bencana,

4. Pengurangan kebutuhan energi,
5. Pengurangan kebutuhan tempat,
6. Pengurangan beban jaringan,
7. Pengurangan biaya test and development perangkat lunak.

Secara garis besar virtualisasi server memberikan keuntungan dalam beberapa aspek, yaitu:

1. Fleksibilitas.

   Sebuah host dapat digunakan untuk beberapa sistem operasi, migrasi VM dapat dilakukan dan alokasi sumber daya perangkat keras dapat disesuaikan dengan kebutuhan VM,
2. Ketersediaan.

   Ketersediaan layanan dapat dijaga walaupun host mengalami masalah atau secara sengaja dimatikan untuk maintenance,
3. Skalabilitas.

   Penggunaan klaster memungkinkan penambahan atau pengurangan host dengan mudah, guna menyesuaikan kebutuhan,
4. Keamanan.

   Virtualisasi memungkinkan pemisahan layanan pada masing-masing VM sehingga ketika terjadi masalah pada suatu layanan, layanan yang lain tidak mengalami gangguan,
5. Utilisasi perangkat keras.

   Konsolidasi server mengakibatkan sumber daya perangkat keras yang tidak digunakan oleh VM idle, dapat digunakan oleh VM lain.

Selain memiliki sejumlah aspek keuntungan, teknologi virtualisasi server juga memiliki beberapa permasalahan yang dapat muncul apabila perencanaannya tidak matang. Beberapa hal yang harus diperhatikan antara lain :

1. Daya Listrik.

   Walaupun secara umum virtualisasi server akan mengurangi biaya penggunaan daya listrik, dibutuhkan perencanaan yang matang terkait dengan instalasi kelistrikan. Sebuah mesin server yang di dalamnya

terdapat banyak VM, mengkonsumsi energi listrik relatif lebih banyak dari mesin server normal. Sehingga diperlukan instalasi kelistrikan yang memadai, berupa redundansi power supply dan keluaran daya yang lebih besar untuk tiap kabinetnya,

2. Backup.

   Dalam infrastruktur virtualisasi server, data yang harus di-backup sangat besar sehingga perusahaan membutuhkan sistem backup yang dapat mengirimkan data dalam jumlah besar dengan cara yang cepat.

3. Jaringan.

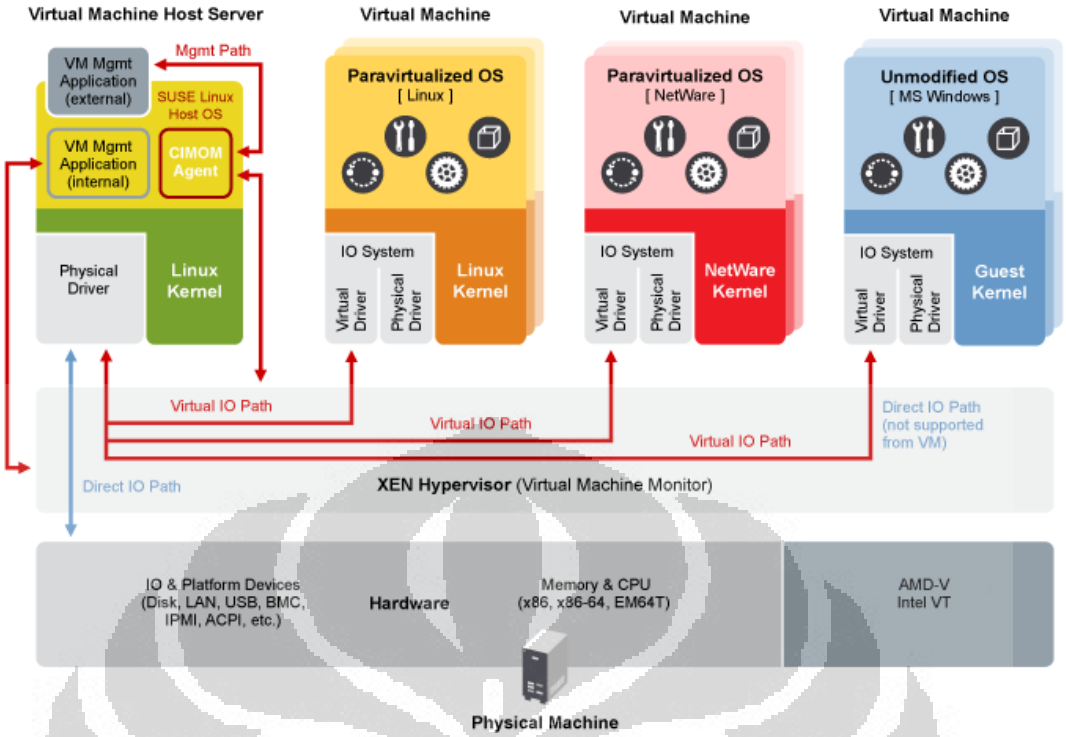
   Virtualisasi server dapat menyebabkan lalu lintas paket data yang sangat tinggi (very high packet per second) pada kartu jaringan dan port switch. Buffer pada switch dapat penuh, yang berakibat pada banyak paket hilang dan pengiriman ulang paket sehingga dibutuhkan Gigabit switch berkualitas,

4. Performa.

Konsolidasi server akan meningkatkan utilisasi prosesor, sehingga disk I\O request akan semakin meningkat. Hal ini berpotensi untuk menimbulkan bottleneck, karena kecepatan akses disk jauh lebih lambat dibandingkan kecepatan prosesor. Kemudian frekuensi akses disk yang tinggi juga dapat menyebabkan fragmentasi (penempatan blok data di disk yang tidak rapi) yang menyebabkan penurunan performa, sehingga dibutuhkan sistem penyimpanan data (storage) yang baik dan memori yang cukup.

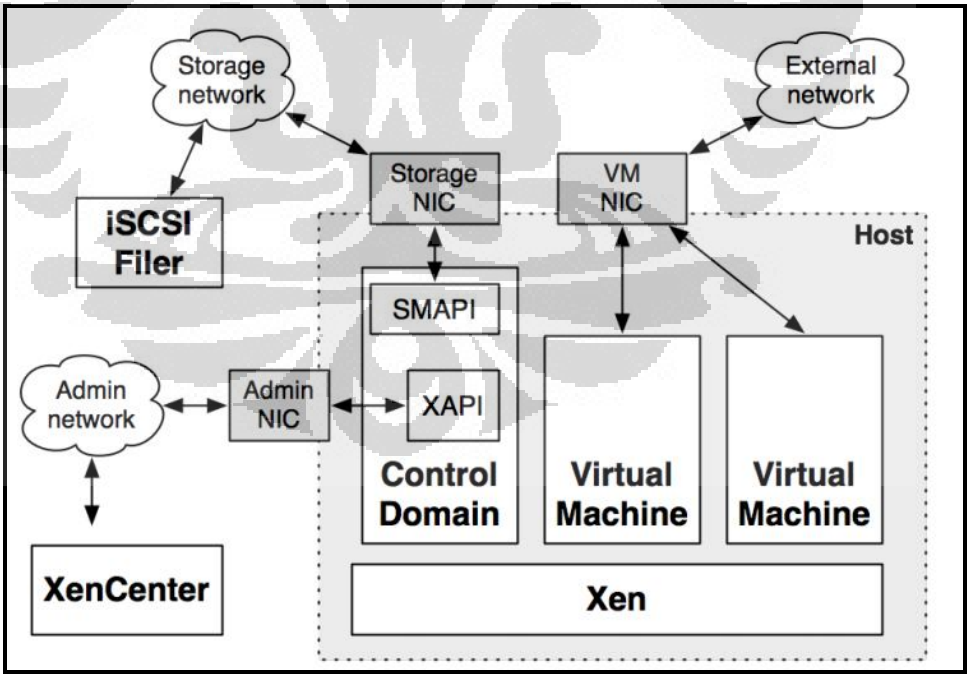
2.4.1 **XenServer**

XenServer adalah sebuah virtualisasi server platform yang dapat menjalankan beberapa sistem operasi secara bersamaan. Konsolidasi ini dapat mengurangi biaya operasional dan meningkatkan kelincahan yang berhubungan dengan menjalankan infrastruktur IT. Meskipun XenServer bertujuan untuk menjadi aman secara default dan memerlukan sedikit out-of-the-box konfigurasi sehubungan dengan keamanan.



Gambar 2.9 skema Xen

2.4.2 **Arsitektur XenServer**



Gambar 2.10 arsitektur XenServer

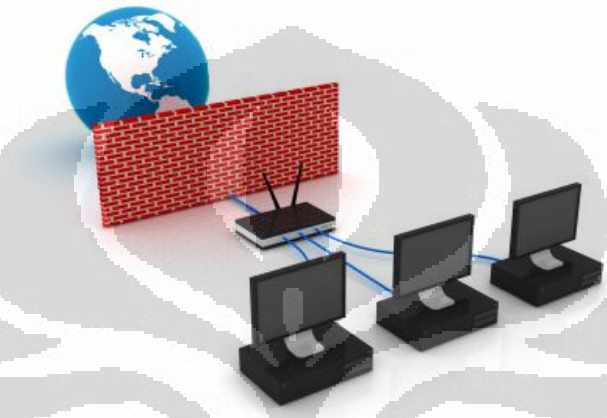
XenServer terdiri dari beberapa komponen yang berbeda:

- Xen hypervisor adalah perangkat lunak pertama yang menerima beban ketika boot XenServer. Berjalan di mode 64-bit dan virtualizes CPU, interupt dan memori host. Xen adalah *thin layer* dari perangkat lunak yang tidak memiliki driver perangkat apapun di luar port serial, dan terdiri dari sekitar 150.000 baris kode.
- Domain kontrol boot, yang merupakan 32-bit berbasis distribusi Linux. Domain kontrol adalah VM XenServer normal dan memiliki hak previlages yang diberikan untuk memungkinkan mengontrol perangkat keras host dan juga membuat domain guest.
- XAPI manajement Stack berjalan di dalam domain kontrol dan mengelola semua sumber daya yang diperlukan untuk menjalankan domain guest. XAPI terdiri dari distribusi database dan kontrol perangkat lunak yang terdapat pada interface administrasi untuk klien XenAPI yang memberikan kontrol instruksi.
- Storage Manager (SMAPI) berjalan di dalam domain0 dan menyediakan antarmuka yang konsisten untuk berbagai backends penyimpanan, seperti Fibre Channel, iSCSI, disk berbasis file VHD, atau penyimpanan lokal.
- User interface XenCenter adalah sebuah aplikasi Windows yang user-friendly untuk mengelola host XenServer dalam jumlah besar.
- XenServer dapat berjalan pada beberapa Mesin Virtual pada host yang sama, masing-masing menyediakan perhitungan yang seluruhnya terisolasi, penyimpanan dan jaringan untuk sistem operasi berjalan di dalamnya.
- Beberapa XenServer host dapat dikelompokkan ke dalam *resource pool* yang bertindak sebagai satu unit administrasi di mesin cluster.

2.5 Firewall

Firewall adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Umumnya, sebuah firewall diimplementasikan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (gateway) antara jaringan lokal dan jaringan lainnya. Firewall umumnya juga digunakan untuk mengontrol

akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar. Saat ini, istilah firewall menjadi istilah generik yang merujuk pada sistem yang mengatur komunikasi antar dua jaringan yang berbeda. Mengingat saat ini banyak perusahaan yang memiliki akses ke Internet dan juga tentu saja jaringan korporat di dalamnya, maka perlindungan terhadap aset digital perusahaan tersebut dari serangan para hacker, pelaku spionase, ataupun pencuri data lainnya, menjadi esensial.



Gambar 2.11 Firewall

Jadi, firewall adalah suatu mekanisme untuk melindungi keamanan jaringan komputer dengan menyaring paket data yang keluar dan masuk di jaringan. Paket data yang "baik" diperbolehkan untuk melewati jaringan dan paket dapa yang dianggap "jahat" tidak diperbolehkan melewati jaringan. Firewall dapat berupa perangkat lunak atau perangkat keras yang ditanam perangkat lunak yang dapat menfilter paket data. Firewall dapat juga berupa suatu sikap yang ditanam dan diajarkan kepada staf IT suatu perusahaan untuk tidak membocorkan data perusahaan kepada perusahaan. Ini untuk mencegah salah satu jenis hacking yaitu social enggeneering.

2.5.1 **Jenis – Jenis Firewall**

Tipe-tipe Firewall, antara lain

1. Packet-Filtering Firewall

   Packet-Filtering Firewall adalah tipe firewall yang memeriksa dan membandingkan alamat sumber dari paket lewat dengan aturan atau kebijakan

yang telah terdaftar pada filtering firewall. Pada firewall tipe ini akan diatur apakah paket data tersebut akan diperbolehkan lewat atau menolaknya.

Aturan atau kebijakan pemeriksaan didasarkan informasi yang dapat ditangkap dari packet header, yaitu antara lain :

a. IP address sumber dan tujuan
b. Nomor port TCP/UDP sumber dan tujuan
c. Tipe ICMP message

Tabel 2.2 contoh rule packet filtering firewall

from	to	src port	dst port	proto	rule
*	www	*	80	tcp	allow
*	mail-gw	*	25	tcp	allow
squids	proxy	*	8080, 3128	*	allow
mynet	*	*	*	*	allow
*	*	*	*	*	deny

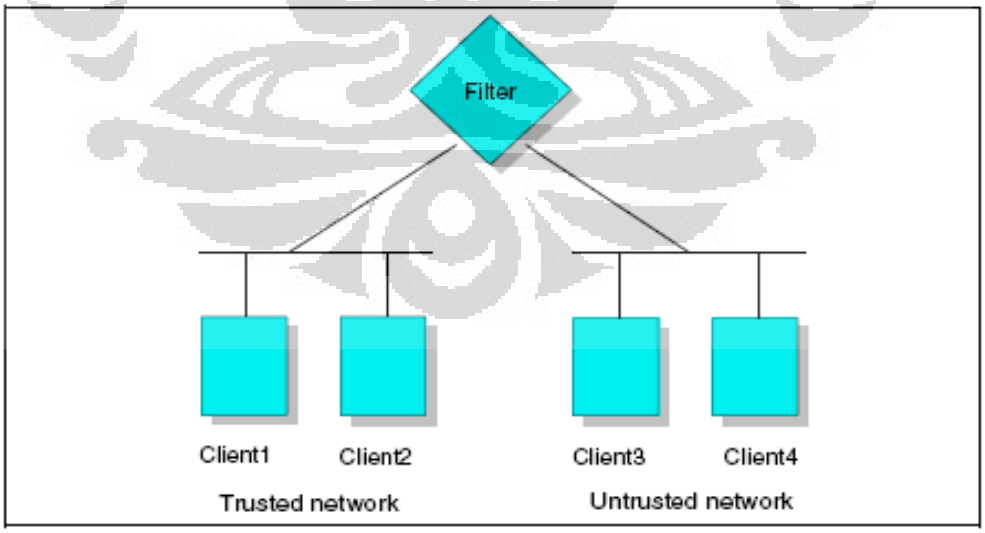
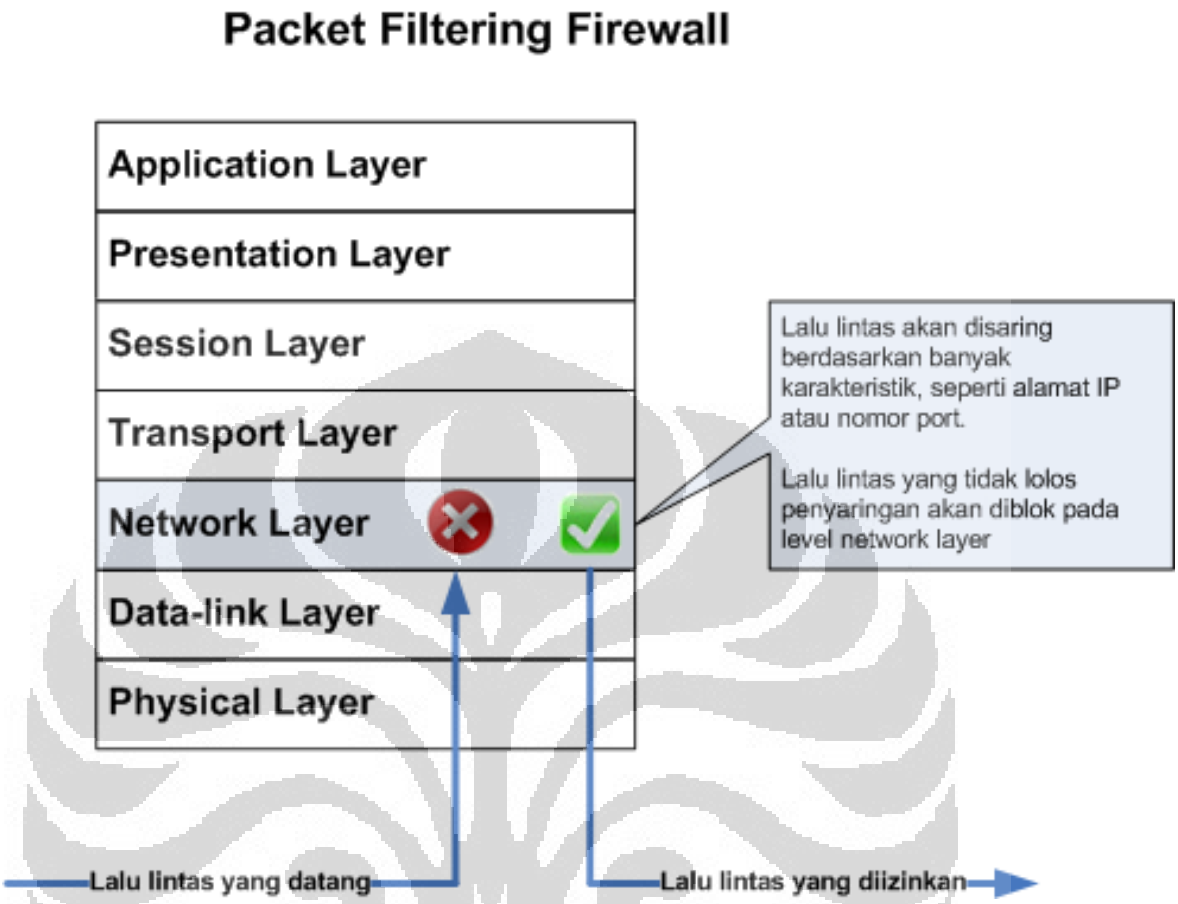


Figure 268. Packet filtering router

Gambar 2.12 Ilustrasi cara kerja packet filtering firewall



Gambar 2.13 ilustrasi packet filtering firewall

Contoh satu aturan pada firewall jenis adalah melakukan penonaktifan port 23 yaitu protokol yang digunakan untuk telnet. Ini bertujuan untuk mencegah pengguna internet untuk mengakses layanan yang terdapat pada jaringan yang di firewallkan. Firewall ini juga dapat melakukan pengecualian terhadap aplikasi-aplikasi yang dapat berdapat berjalan di jaringan. Inilah salah satu kerumitan pada packet filtering tipe firewall, dikarena sulitnya menbuat aturan atau kebijakan yang akan diberlakuan untuk firewall.

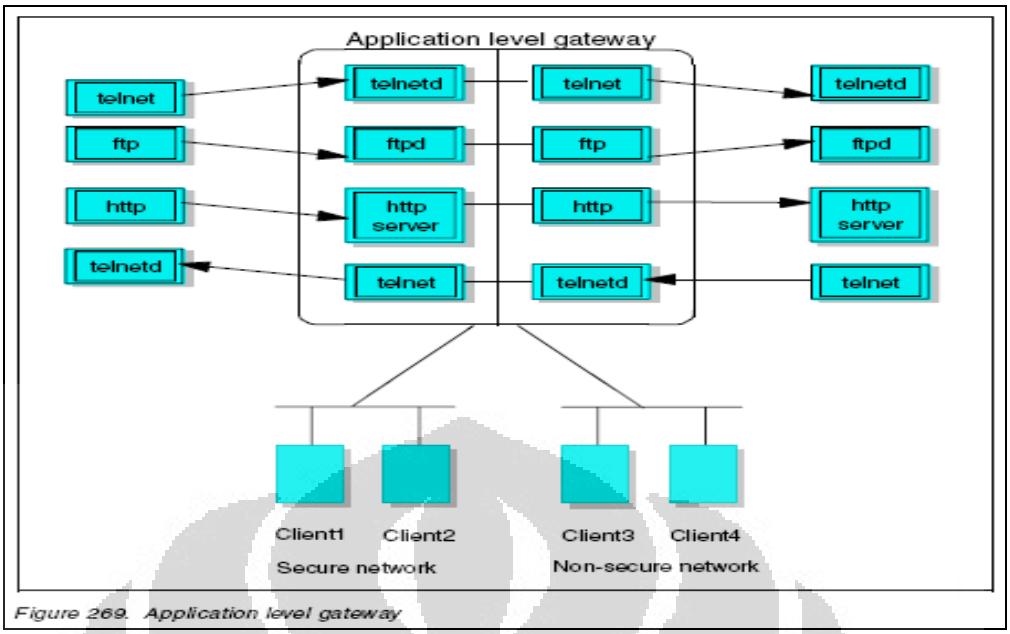
Kelebihan packet filtering firewall antara lain relatif mudah dalam pengimplementasikannya, tranparan untuk pengguna, dan relatif lebih cepat. Adapun kekurangan tipe firewall ini antara lain sulit dalam membuat aturan dan kebijakan pada packet filtering firewall ini secara tepat guna dan aturan tersebut

akan semakin banyak seiiring dengan banyak alamat IP sumber dan tujuan, port sumber dan tujuan yang dimasukan dalam kebijakan packet filtering firewall ini.

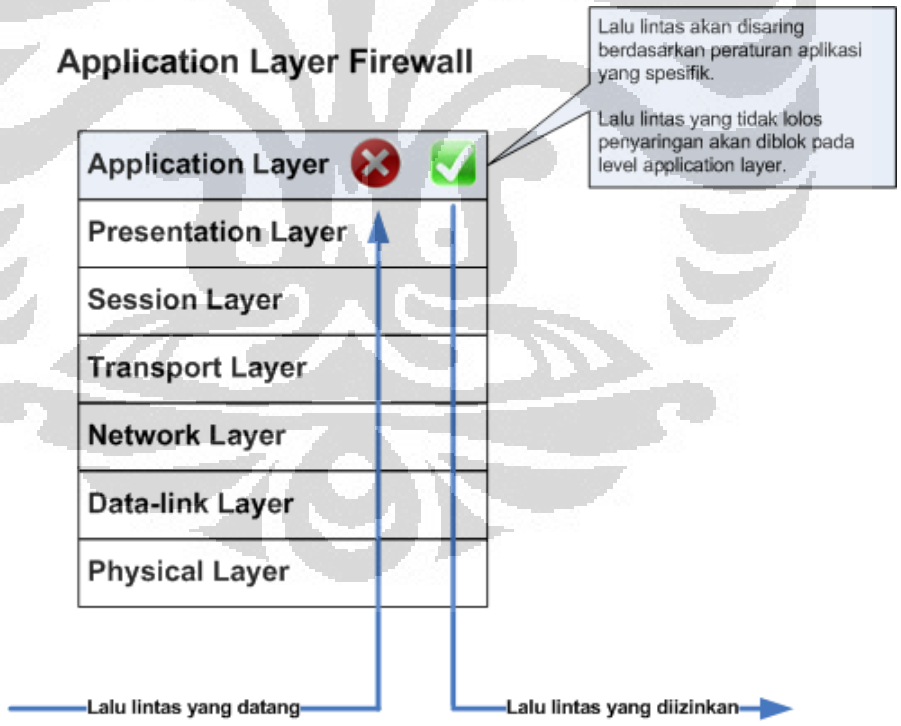
2. Application-Level Gateway (Proxy)

Application-levet gateway sering juga disebut application level firewall atau proxy firewall. Firewall ini tidak memperbolehkan paket data yang datang untuk melewati firewall sacara langsung. Applicatin level gateway menyediakan kontrol tingkat tinggi pada traffic antara dua jaringan yang isi layanan tertentu didalamnya dapat dimonitor dan difilter sesuai dengan kebijakan keamanan jaringan. Firewall tipe ini akan mengatur semua yang berkaitan dengan layer aplikasi, seperti ftp, telner, dll.

Kebanyakan, proxy firewall ini akan melakukan autentifikasi terhadap pengguna sebelum pengguna dapat melewati jaringan. firewall ini juga melakukan mekanisme pencatatan (logging) sebagai bagian dari aturan dan kebijakan keamanan yang diterapkannya. Contohnya apabila ada pengguna salah satu aplikasi seperti telnet untuk mengakses secara remote, maka gateway akan meminta pengguna untuk memasukan alamat remote host. Ketika pengguna mengirimkan username dan password serta informasi lain maka gateway akan melakukan pemeriksaan dan melakukan hubungan terhadap aplikasi tersebut yang sesuai dengan remote host. Apabila tidak sesuai, firewall tidak akan meneruskan dan menolak data tersebut.



Gambar 2.14 Ilustrasi cara kerja application layer firewall



Gambar 2.15 ilustrasi application layer firewall

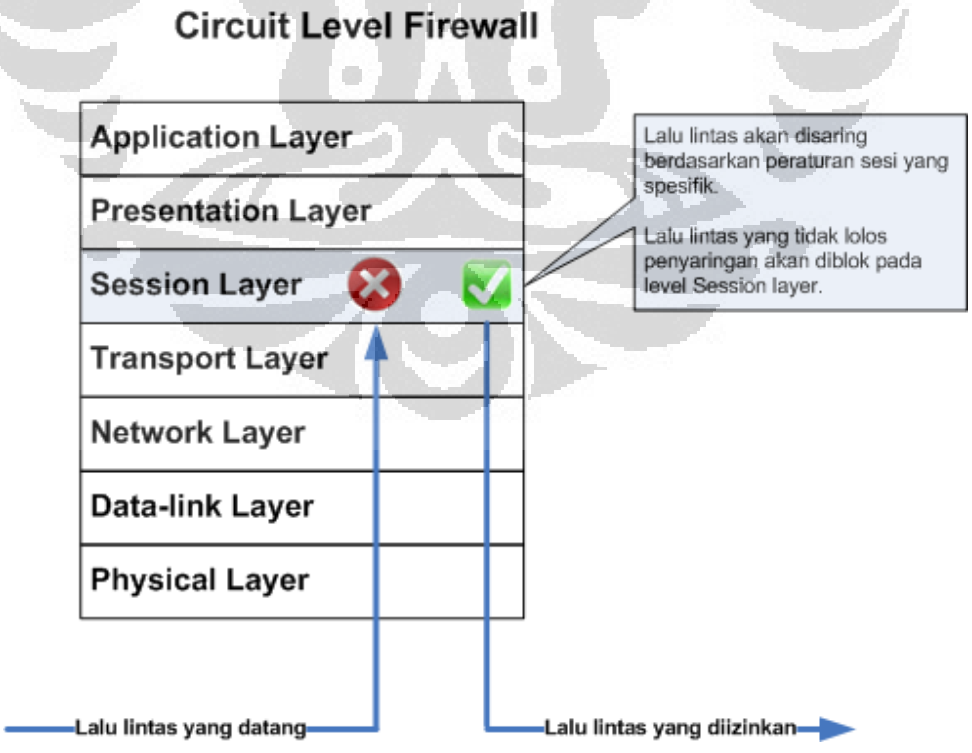
Kelebihan application layer firewall antara lain : relatif lebih aman dibandingkan dengan packet filtering firewall, adanya pencatatan log setiap transaksi yang terjadi pada level aplikasi.

Kekurangan application layer firewall antara lain : pemrosesan tambahan yang berlebih pada setiap hubungan yang akan mengakibatkan terdapat dua buah sambungan koneksi antara pengguna dan gateway, dimana gateway akan memeriksa dan meneruskan semua arus dari dua arah.

3. Circuit Level Gateway

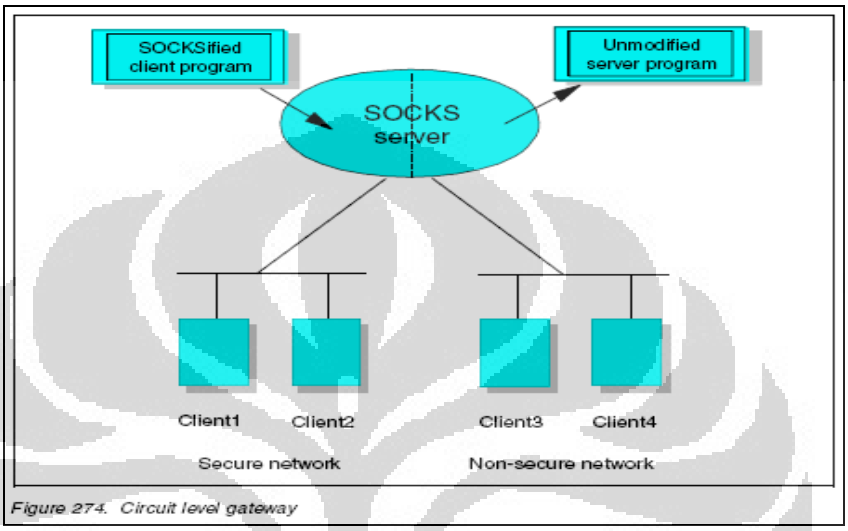
Circuit lavel gateway dapat dikatakan sebagai tipe khusus dari proxy karena proxy dapat dikonfigurasi untuk melewatkan semua informasi pengguna yang sudah di authentifikasi sebagai circuit level gatewai. Circuit level gateway meng*handle* koneksi TCP dan tidak menyediakan paket tambahan seperti prosessing atau filtering. Firewall jenis akan menyembunyikan jaringan dari pengguna ketika koneksi akan terjadi dari pengguna. Pengguna akan berhadapan langsung dengan firewall pada saat proses pembuatan koneksi dan firewall akan membentuk koneksi dengan sumber daya di jaringan yang hendak di akses oleh pengguna setelah mengubah alamat IP dari paket yang ditransmisikan oleh dua belah pihak

Firewall jenis ini bekerja pada lapisan session layer.



Gambar 2.16 Circuit Level Firewall

Kelebihan firewall jenis ini antara lain lebih aman dibandingkan dengan jenis packet filtering firewall karena pengguna luar tidak dapat melihat alamat IP jaringan internal dalam paket-paket yang ia terima, melainkan alamat IP dari firewall. Protokol yang populer digunakan sebagai Circuit-Level Gateway adalah SOCKS v5.



Gambar 2.17 Ilustrasi Circuit Level Gateway

2.5.2 **Fungsi Firewall**

Fungsi firewall, antara lain :

2. Mengontrol dan mengawasi paket data yang mengalir di jaringan

   Firewall harus dapat mengatur, memfilter dan mengontrol lalu lintas data yang diizin untuk mengakses jaringan privat yang dilindungi firewall. Firewall harus dapat melakukan pemeriksaan terhadap paket data yang akan melawati jaringan privat.

   Beberapa kriteria yang dilakukan firewall apakah memperbolehkan paket data lewati atau tidak, antara lain :

   a. Alamat IP dari komputer sumber
   b. Port TCP/UDP sumber dari sumber
   c. Alamat IP dari komputer tujuan

d. Port TCP/UDP tujuan data pada komputer tujuan
e. Informasi dari header yang disimpan dalam paket data

3. Melakukan autentifikasi terhadap akses.
4. Applikasi proxy

   Firewall mampu memeriksa lebih dari sekedar header dari paket data, kemampuan ini menuntut firewall untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi

5. Mencatat semua kejadian di jaringan

   Mencatat setiap transaksi kejadian yang terjadi di firewall. Ini memungkinkan membantu sebagai pendeteksian dini akan kemungkinan penjebolan jaringan.

2.5.3 Cara Kerja Firewall

Cara kerja firewall pada umumnya :

Cara-cara firewall dalam melindungi jaringan komputer internal, antara lain :

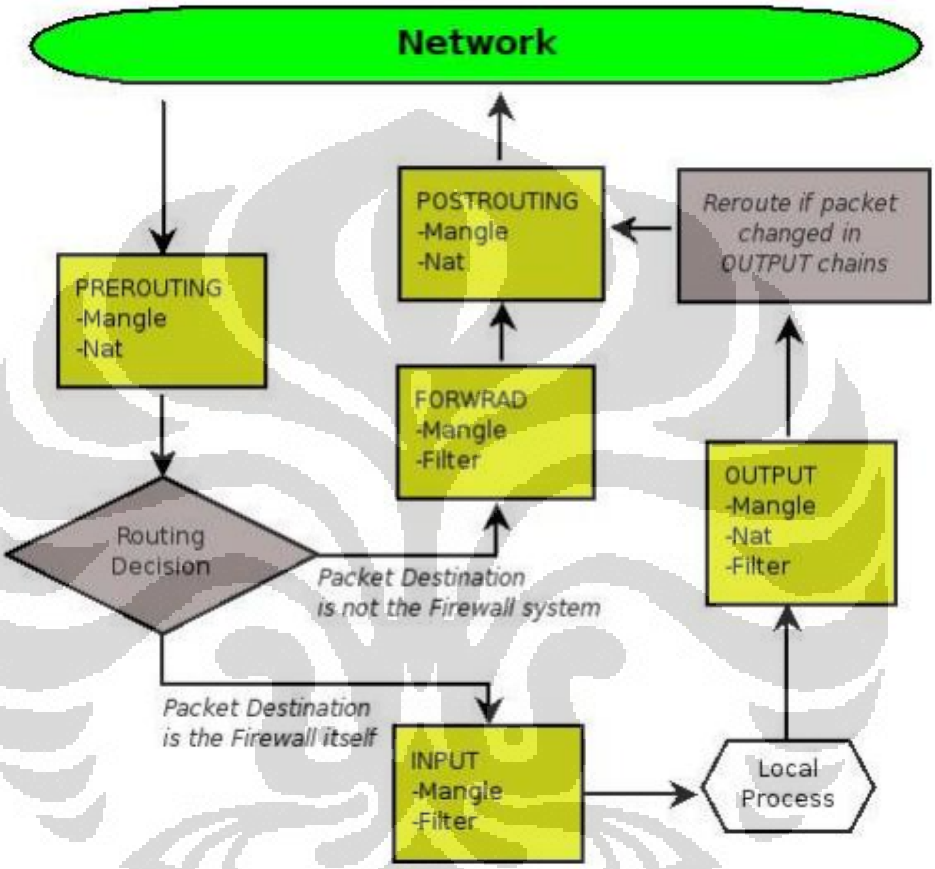
1. Menolak dan memblokir paket data yang datang berdasarkan sumber dan tujaun yang tidak diinginkan.
2. Menolak dan menyaring paket data yang berasal dari jaringan intenal ke internet. Contoh nya ketika ada pengguna jaringan internel akan mengakses situs-situs porno.
3. Menolak dan menyaring paket data berdasakan konten yang tidak diinginkan. Misalnya firewall yang terintegrasi pada suatu antivirus akan menyaring dan mencegah file yang sudah terjangkit virus yang mencoba memasuki jaringan internal.
4. Melaporkan semua aktivitas jaringan dan kegiatan firewall.

2.5.4 **IPTables**

Iptables adalah salah satu tools firewall default pada system operasi linux. Iptables ini bekerja baik di kernel 2.4.x-2.6.x sedangkan untuk kernel 2.2.x masih

menggunakan ipchains. Perintah 'iptables' digunakan untuk mengelola, memaintain, menginspeksi rule-rule IP packet filter dalam kernel linux.

Diagram Iptables



Gambar 2.18 Diagram IPTables

Table adalah tempat rule - rule yang dibuat . Ada 3 buah table, secara general dapat definisikan:

- Table filter, adalah tempat rule - rule yang berkaitan dengan boleh/tidaknya suatu paket

  network melewati sebuah CHAIN .

- Table NAT, adalah singkatan dari Network Address Translation, yaitu table tempat rule - rule yang berkaitan dengan manipulasi suatu paket

network ketika melewati CHAIN PREROUTING, POSTROUTING, dan OUTPUT.

- Table mangle, adalah tempat rule - rule yang berkaitan dengan manipulasi suatu paket network untuk keperluan advance, seperti QOS (quality of service), packet marking, dan lain - lain.

Konsep chain :

1. **PREROUTING**, adalah Titik dimana bisa memanipulasi paket network sebelum dia memasuki keputusan routing, apakah ia akan masuk ke dalam Linux kita atau hanya sekedar 'lewat'.
2. **INPUT**, adalah Titik dimana bisa melakukan pemeriksaan terhadap paket network yang akan MASUK ke dalam Linux kita.
3. **OUTPUT**, adalah Titik dimana kita melakukan pemeriksaan terhadap paket network yang dihasilkan oleh Linux kita KELUAR sebelum routing.
4. **FORWARD**, adalah Titik dimana kita melakukan pemeriksaan terhadap paket network yang hanya menumpang LEWAT Linux kita.
5. **POSTROUTING**, adalah Titik dimana kita bisa melakukan manipulasi terhadap paket yang akan keluar dari Linux kita.

Perintah umum iptables :

$iptables [-t table] command [match] [target/jump]

Berikut beberapa option dasar yang cukup sering dalam mengkonfigurasi iptables

- -A

  Tambahan aturan ini ke rantai aturan yang ada. Rantai atau chain yang valid adalah INPUT, FORWARD, dan OUTPUT. Biasanya lebih banyak menggunakan rantai INPUT yang berdampak pada paket data yang masuk

- -L

  Memperlihatkan daftar aturan yang telah dipasang di iptables.

- -m state

  Menjelaskan daftar dari kondisi / state bagi aturan untuk di bandingkan. Beberapa state yang valid, adalah :

  NEW => sambungan baru dan belum pernah terlihat sebelumnya

  RELATED => sambungan baru, tapi berhubungan dengan sambungan lain telah diizinkan.

  ESTABLISHED => sambungan yang telah terjadi.

  INVALID => lalu lintas paket data yang karena berbagai alasan tidak bisa di identifikasi

- -m limit

  Dibutuhkan oleh aturan jika ingin melakukan pembandingan dan pencocokan dalam waktu / jumlah tertentu. Mengizinkan penggunaan option –limit. Berguna untuk membatasi aturan logging.

- --limit

  Kecepatan maksimum pencocokan, diberikan dalam bentuk angka yang diikuti oelh ”/seconf”,”/minute”,”/hour”, atau ”/day” tergantung seberapa sering kita ingin melakukan pencocokan aturan. Jika option ini tidak digunakan maka secara defaultnya adalah ”3/hour”

- -p

  Protokol yang digunakan untuk sambungan.

- --dport

  Port tujuan yang digunakan oleh aturan iptables. Bisa berupa satu port, bisa juga satu batasan jangkauan ditulis sebagai start:end, yang akan mencocokan semua port start sampai end

- -j

  Jump ke target yang spesifik. Iptables mempunyai empat target default, yaitu :

ACCEPT

- ⇨ Accept / menerima paket dan berhenti memproses aturan dalam rantai aturan ini.

REJECT

- ⇨ Reject /tolak paket data dan beritahu ke pengirim bahwa aturan firewall menolak paket data tersebut, stop pemrosesan aturan dalam rantai aturan ini

DROP

- ⇨ Diam-diam mengacuhkan paket ini, dan stop pemrosesan aturan di rantai aturan ini.

LOG

- ⇨ Log/catat paket, dan teruskan pemrosesan aturan di rantai aturan ini.
- ⇨ Mengijinkan penggunaan option --log –prefix dan --log -level

- --log –prefix

  Jika pencatatan dilakukan, letakan text atau tulisan sebelum catatan.

- --log –level

  Pencatatan menggunakan syslog level.

- -i

  Melakukan pencocokan jika paket yang masuk dari interface tertentu.

- -I

  Memasukan aturan ke iptables.

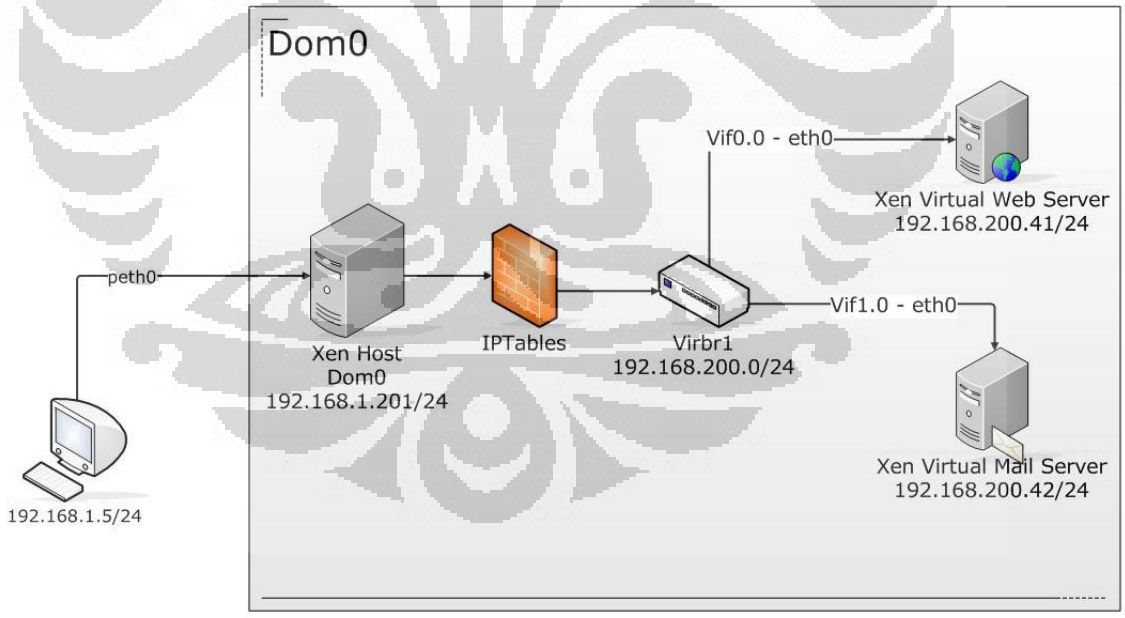
- -v

  Menampilkan lebih banyak informasi di layar Option diatas adalah hanya sedikit dari option yang terdapat pada iptables.

BAB 3
PERANCANGAN MODEL INFRASTRUKTUR JARINGAN VIRTUALISASI SERVER

3.1 Topologi Jaringan

Model topologi jaringan yang dirancang untuk pengujian tugas akhir ini terdiri dari satu perangkat komputer desktop sebagai Host Server Xen dimana didalamnya terdapat dua virtual server, satu firewall/IPTables dan Virtual Bridge (virbr1) yang terhubung dengan Netbook sebagai User Client. Dua Virtual Server yaitu Web Server dan Mail Server terhubung dengan satu Virtual Bridge dimana interface pada Virtual Bridge yaitu vif0.0 dan vif1.0 yang menghubungkan dengan Virtual Server, lalu antara Virtual Bridge dengan Xen Host terdapat firewall/iptables yang berguna mengatur lalu lintas jaringan virtual.



Gambar 3.1 Topologi Virtualisasi Server Xen

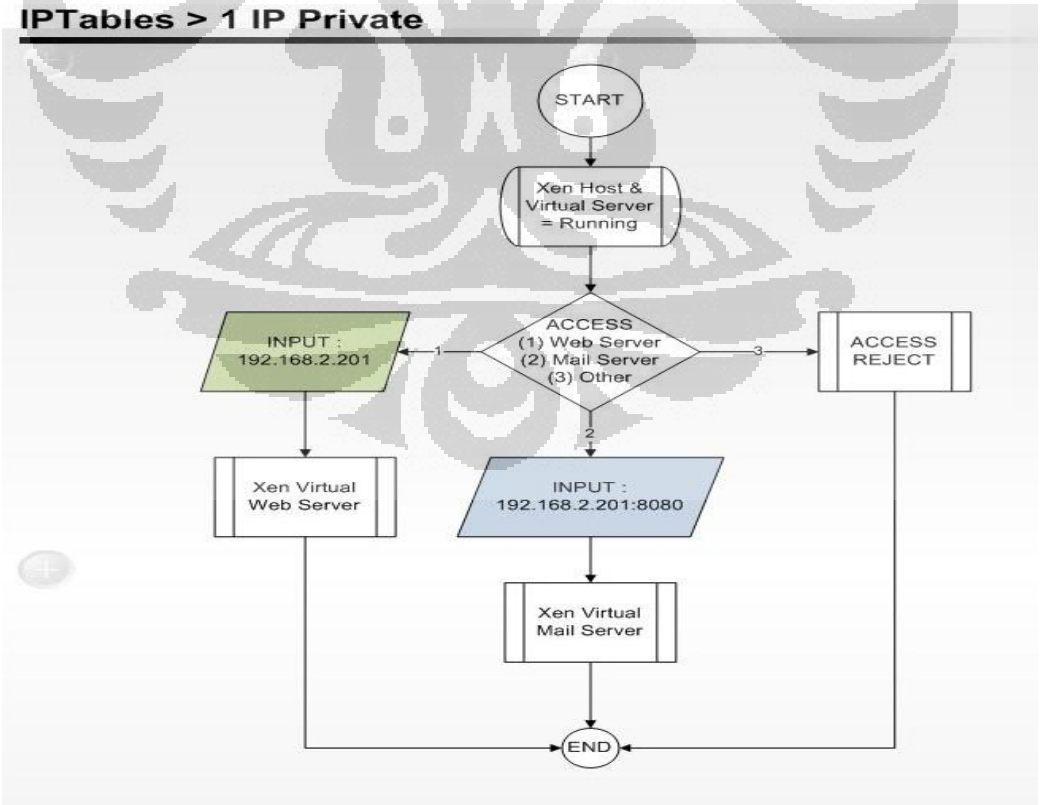
Tabel 3.1 Daftar alamat IP pada Perangkat Xen Virtual Server

No	Nama Perangakat	Alamat IP/Netmask
1	Xen Host (Dom0)	192.168.1.201/24
2	Xen Virtual Web Server	192.168.200.41/24
3	Xen Virtual Mail Server	192.168.200.42/24
4	Virbr1	192.168.200.1/24
5	Client	192.168.1.5/24

3.2 Perancangan Aturan - aturan IPTables

Dalam perancangan aturan pada IPTables pada Virtual Server ini terdapat dua aturan yaitu pengaturan untuk jaringan dengan menggunakan 1 IP Private untuk 2 Virtual Server dan pengaturan dengan 2 IP Private untuk 2 Virtual Server.

3.1.1. Perancangan Aturan pada IPTables dengan 1 IP Private



Gambar 3.2 Flowchart Aturan IPTables 1 IP Private

Pada pengaturan ini IPTables mengarahkan client yang mengakses web server dengan port 80 , 443 dengan melalui Alamat IP 192.168.1.201 akan di FORWARD ke Xen Virtual Web Server sedangkan saat client yang ingin mengakses mail server dengan port 25, 110, 143 dan input URL : 192.168.1.201:8080 (web mail : 80, 443) akan langsung di FORWARD ke Xen Virtual Mail Server. karena pada pembuatan Virtual Machine ini dengan metode NAT pada virtual networkingnya maka diperlukan modifikasi pada aturan di IPTables diantaranya pada CHAIN PREROUTING dan FORWARD dengan tujuan memberikan izin akses dari luar network untuk memasuki internal network.

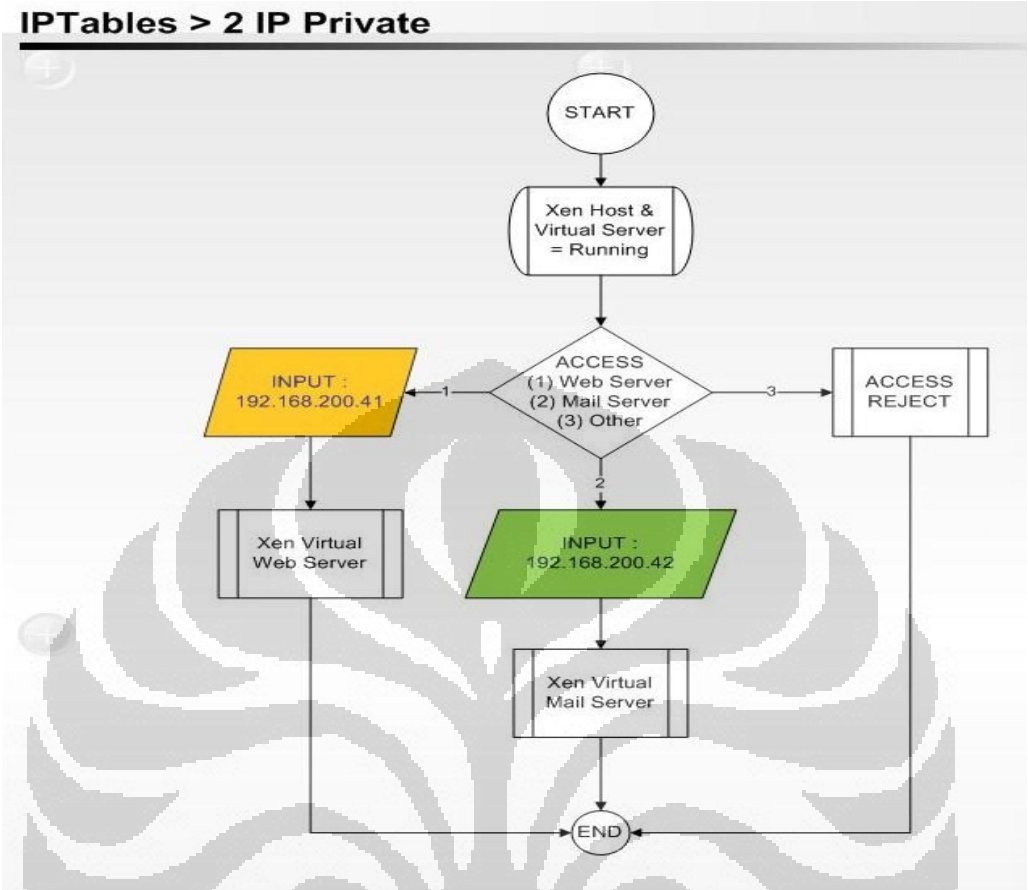
```
# mengarahkan lalu lintas jaringan dari port 80 & 443 ke Virtual Web Server
# iptables -t nat -A PREROUTING -p tcp -i eth0 --destination-port 80 -j DNAT --to-destination
192.168.200.41
# iptables -t nat -A PREROUTING -p tcp -i eth0 --destination-port 443 -j DNAT --to-destination
192.168.200.41
```

```
# mengarahkan lalu lintas jaringan dari port 25, 110, dan 143 ke Virtual Mail Server

# iptables -t nat -A PREROUTING -p tcp -i eth0 --destination-port 25  -j DNAT --to-destination
192.168.200.42

# iptables -t nat -A PREROUTING -p tcp -i eth0 --destination-port 110 -j DNAT --to-destination
192.168.200.42

# iptables -t nat -A PREROUTING -p tcp -i eth0 --destination-port 143 -j DNAT --to-destination
192.168.200.42
```

```
# mengarahkan lalu lintas jaringan dari port 8080 & 8443 ke Virtual Mail Server

# iptables -t nat -A PREROUTING -p tcp -i eth0 --destination-port 8080 -j DNAT --to-
destination 192.168.200.42:80

# iptables -t nat -A PREROUTING -p tcp -i eth0 --destination-port 8443 -j DNAT --to-
destination 192.168.200.42:443
```

```
#supaya ext network dapat mengakses ke dalam virtual server di INPUT aturan di baris atas

# iptables -I FORWARD -i eth0 -o virbr0 -p tcp -m state --state NEW -j ACCEPT
```

3.2.1 Perancangan Aturan pada IPTables dengan 2 IP Private



Gambar 3.3 Flowchart Aturan IPTables 2 IP Private

Pada perancangan ini pengaturan pada IPTables lebih sederhana dibanding perancangan aturan IPTables dengan menggunakan 1 IP Private. dari pihak client yang ingin mengakses wen server dan mail server pada Xen Virtual Server pada penelitian ini melalui IP Virtual Server itu sendiri dikarenakan penggunaannya 2 IP Private. Pada rancangan aturan IPTables ini, hanya terdapat dua virtual server yang digunakan sehingga jika client ingin mengakses port selain port untuk ke webs server dan mail server akan di REJECT oleh IPTables. Misalkan client ingin mengakses web server pada Xen Virtual Server maka client memasukan URL http://192.168.200.41 dan untuk mengakses mail server client memasukkan URL http://192.168.200.42.

Dalam perancangan ini hal pertama yang harus dilakukan adalah aktifkan terlebih dahulu etho:0 dan eth0:1, lalu berikan alamat IP masing - masing yaitu :

#alamat IP untuk eth0:0

#ifconfig eth0:0 192.168.1.211

```
#alamat IP untuk eth0:1

#ifconfig eth0:1 192.168.1.212
```

jadi saat client ingin melakukan akses ke Web Server dengan alamat IP 192.168.1.211 dan untuk alamat IP Mail Server 192.168.1.212. Untuk konfigurasinya sebagai berikut :

```
-A PREROUTING -d 192.168.1.211 -i eth0 -p tcp -j DNAT --to-destination 192.168.200.41

-A PREROUTING -d 192.168.1.212 -i eth0 -p tcp -j DNAT --to-destination 192.168.200.42
```

IPTables memberikan akses jaringan untuk packet data yang melalui Alamat IP 192.168.1.211 akan di *FORWARD* ke alamat IP 192.168.1.200.41 dimana sebagai Xen Virtual Web Server, sedangkan untuk client yang mengakses Alamat IP 192.168.1.212 akan di *FORWARD* ke alamat IP 192.168.1.42 dimana sebagai Xen Virtual Mail Server.

Lalu untuk akses keluar dari system Xen menggunakan *POSTROUTING*. konfigurasinya sebagai berikut :

```
-A POSTROUTING -s 192.168. 200.41 -d ! 192.168.122.0/255.255.255.0 -j SNAT --to-source 192.168.1.211

-A POSTROUTING -s 192.168. 200.42 -d ! 192.168.122.0/255.255.255.0 -j SNAT --to-source 192.168.1.212
```

Dalam konfigurasi ini setiap data packet yang keluar dari Virtual Server akan di ubah alamat IP nya saat keluar dimana kebalikan dari alamat sebelumnya yaitu 192.168.1.211 dan 192.168.1.212.

3.3 Komponen Perangkat Lunak

3.3.1 Sistem Operasi

Sistem Operasi untuk Xen Host yang digunakan pada penelitian ini adalah LINUX Ubuntu 12.04 LTS 32-Bit (Precise Pangolin) dimana merupakan versi terbaru dari Ubuntu LTS(Long Term Support) yang akan secara reguler diperbaharui hingga lima tahun kedepan dari tangal perilisan versi ini. Hal ini sesuai dengan infrastruktur pada Xen Virtual Server yang dibangun dan terus dikembangkan untuk jangka panjang. Alasan lain penggunaan versi ini adalah sebagai uji coba untuk penggunaan versi Ubuntu terbaru ini dan kompatibilasnya dengan Xen Hypervisor terbaru 4.x dimana kernelnya sudah 3.x.x. Sedangkan sistem operasi untuk Virtual Servernya yaitu Ubuntu 8.04 (Hardi Heron) dimana untuk versi ini yang sudah lama sehingga membuat lebih ringan pada Xen Host.

Hal ini dikarenakan pada penelitian ini Komputer Desktop yang digunakan merupakan komputer desktop dengan spesifikasi rata - rata. Untuk spesifikasi Virtual Server itu sendiri dibuat memiliki CPU dengan 1 Core dan 1 Gb RAM.

3.3.2 Aplikasi Virt-Manager

Virtual Machine Manager atau disingkat Virt-Manager adalah suatu aplikasi dekstop pengelola virtual machine dengan berbasiskan tampilan GUI. pada aplikasi ini juga dapat memonitoring penggunaan CPU, RAM, I/O dan jaringan secara real-time dalam bentuk grafik sehinggan mempermudah dalam pembuatan virtual machine baru dan monitoring sistem pada virtual machine serta melakukan konfigurasi pada sistem.

Aplikasi ini dibuat dengan bahasa pemprograman phyton dan UI dengan Glade dan Gtk+ dimana dibuat oleh libvirt. alasan penggunaan aplikasi ini adalah kontribusi libvirt yang dalam pembuatan aplikasi monitoring virtual machine diawali pada hypervisor Xen sehingga lebih kompeten dalam aplikasi monitoring virtual machine.

Gambar 3.4 Tampilan Virt-Manager

3.4 Komponen Perangkat Keras

Komponen perangkat keras yang digunakan dalam pembuatan sistem untuk tugas akhir ini adalah sebagai berikut :

- Satu Komputer Desktop dengan spesifikasi komponen :

  CPU : AMD Phenom II X2 555, 45nm, core 2, 3,2 GHz

  RAM : V-Gen 4 Gb DDR3

  PSU : Corsair CX500 500 Watt

- Satu Netbook HP Mini sebagai client dengan spesifikasi :

  CPU : Intel Atom 1,67 GHz

  RAM : 1 Gb

  OS : Windows 7 32-bit

- Satu kabel UTP Cross over sebagai penghubung antara Xen Host Server dengan Client

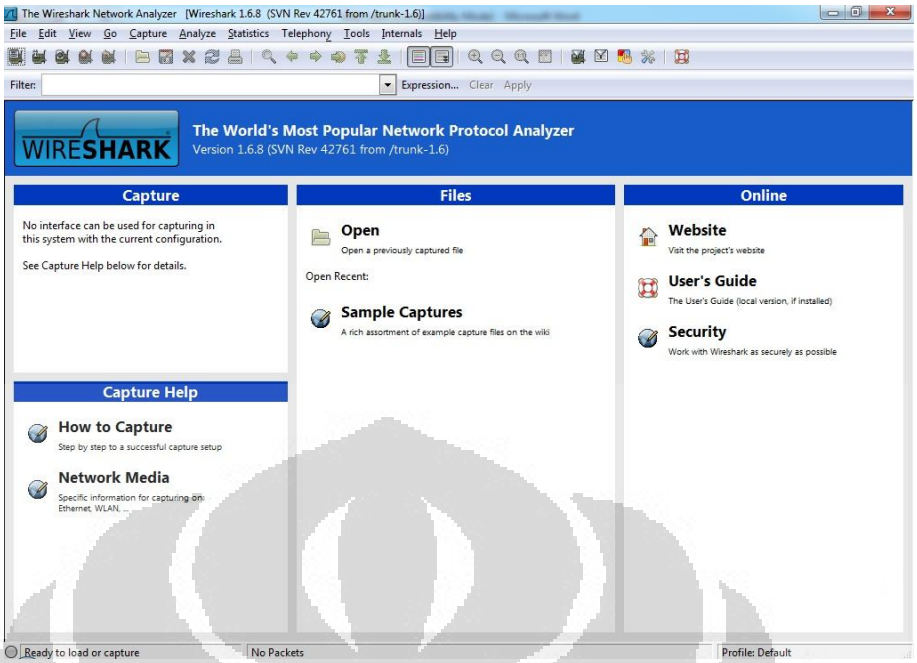
3.5 Perangkat Pengujian

3.5.1 Wireshark

Wireshark adalah tool untuk menganalisa paket pada jaringan. Wireshark dapat menangkap paket pada jaringan dan menampilkan paket dengan informasi yang detail diantaranya adalah dapat mengetahui Throughput, Packet Loss, dan lain - lan, dengan Wireshark dapat menjadi sebagai suatu perangkat pengukuran pada jaringan kabel seperti layaknya voltmeter yang digunakan oleh tukang listrik dan aplikasi ini opensource.

Beberapa contoh penggunaan Wireshark diantaranya :

- Digunakan oleh admin jaringan sebagai troubleshoot pada masalah jaringan
- Memeriksa masalah keamanan jaringan oleh Teknisi Keamanan jaringan
- Untuk implementasi debug protocol oleh para Developer
- dan orang - orang menggunakan untuk edukasi pada internal jaringan



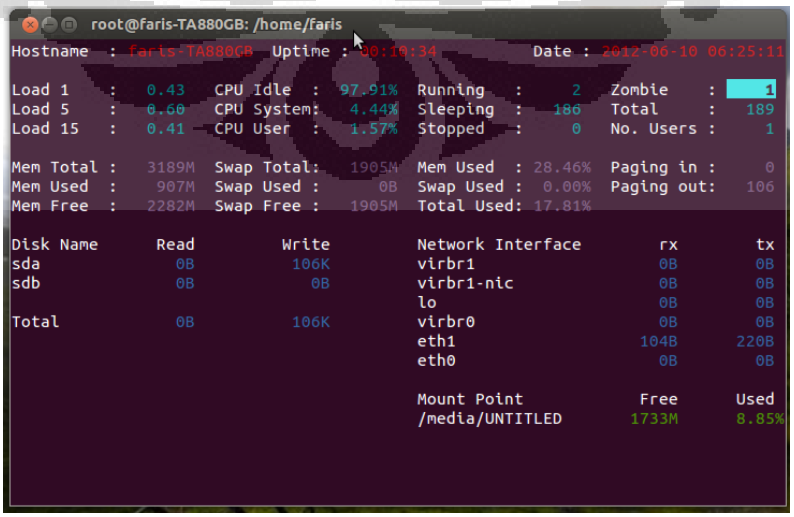
Gambar 3.5 Tampilan Wireshark

Penggunaan wireshark pada penelitian ini adalah untuk memanfaatkan fungsi analisa | summary untuk mendapatkan nilai Troughput dan Delay

3.5.2 Saidar

Saidar adalah tool berbasis CLI dengan library libstatgrab yang berfungsi untuk mengumpulkan informasi tentang keadaan sistem komputer yang berjalan. Diantaranya yaitu informasi interface jaringan, penggunaan memori, penggunaan CPU, proses yang berjalan, Disk read/write access. Saidar ini berjalan pada di LINUX dan distro Ubuntu untuk proses instalasi :

```
#apt-get install saidar
```



Gambar 3.6 Tampilan Saidar CLI

Penggunaan Saidar ini dalam penelitian ialah untuk mengetahui informasi penggunaan CPU dan Memori pada komputer Host dan Virtual Machine.

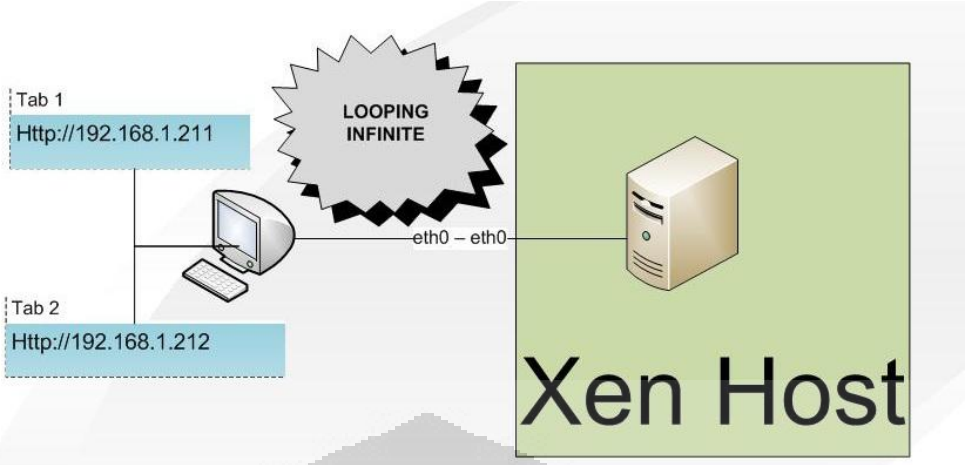
3.6 Skenario Pengujian

Setelah perancangan dan selesai melakukan konfigurasi pada IPTables, maka akan dilakukan pengujian terhadap kinerja jaringan.

3.6.1 Uji Kinerja Xen Virtual Server dengan Penggunaan 1 & 2 IP Private

Dalam skenario pengujian ini dari pihak client yang sudah terhubung dengan Xen Host Server membuka Web Browser dimana sebelumnya dari sisi Server keduanya telah dibuat script PHP supaya saat client mengakses ke Server terjadi perulangan terus - menerus. Hal ini membuat client dan server akan terus terhubung dan saling terus mengirim dan menerima data secara terus - menerus.

Gambar 3.7 Skenario uji Virtual Server 1 IP Private



Gambar 3.8 Skenario uji Virtual Server 2 IP Private

Setiap pengujian yang dilakukan diberikan waktu 10 menit dan dilakukan pengujian selama 10x. Pengujian pertama yaitu dengan pemanfaatan 1 IP Private dan kemudian pengujian selanjutnya dengan 2 IP Private.

Tabel 3.2 Skenario uji akses Virtual Server

Virtual Server yang di akses	Waktu 10 Menit tiap percobaan									
	1	2	3	4	5	6	7	8	9	10
Web Server & Mail Server	X	X	X	X	X	X	X	X	X	X

Setiap pengujian berlangsung tool Wireshark dijalankan di Xen Host, Virtual Web Server , dan Virtual Mail Server serta dijalankan pula saidara pada Terminal masing - masing.

3.7 Parameter Pengujian

3.7.1 CPU Usage

CPU Usage adalah jumlah waktu CPU yang digunakan untuk mengolah proses yang berlangsung pada sistem komputer secara *real time*. Bila dikatakan suatu proses menghabiskan 50% CPU, maka yang sebenarnya terjadi adalah tools menemukan sebanyak 50% proses sedang aktif di CPU dari keseluruhan nilai sample yang diambilnya. CPU adalah mesin dengan keadaan diskrit, karena itu sebenarnya tidak ada istilah literal penggunaan 50% CPU karena pada keadaan riil

kerja CPU hanyalah 100% mengeksekusi atau 0% menunggu untuk mengeksekusi proses. Peran CPU pada Virtual Server Xen ini sangat berperan khusunya untuk penggunaan sumber daya VM dari Host.

3.7.2 RAM Usage

Memori merupakan faktor penting dari infrastruktur Virtual Server Xen. Memori dalam Virtualisasi Xen ini bisa diatur pada tool Virt-manager dengan batas maksimal berdasarkan dari penggunaan memori pada Xen Host.

3.7.3 Throughput

Throughput adalah tingkat rata-rata pengiriman *message* yang berhasil melalui saluran komunikasi. Data ini dapat disampaikan melalui link fisik atau logis, atau melewati node jaringan tertentu. Throughput biasanya diukur dalam bit per detik (bit / s atau bps), dan kadang-kadang dalam paket data per paket kedua atau data per slot waktu. *Throughput* ini berpengaruh besar untuk pengukuran uji kinerja karena memberikan informasi untuk analisa pada penelitian ini.

3.7.4 Delay

Delay adalah tenggang waktu yang dibutuhkan mulai mengirim data sampai

dengan data diterima. Parameter ini merupakan beberapa parameter yang penting untuk melihat informasi dari penelitian ini.

BAB 4

PENGUJIAN DAN ANALISIS SISTEM

3.8 Pengukuran dan Analisis Kinerja Virtual Server Xen

Seperti yang sudah dijelaskan pada bagian sebelumnya, pengujian akan dilakukan dalam interval waktu 10 menit dan diulang 10 kali untuk kedua skenario yaitu Virtual Server Xen dengan satu IP Private dan dua IP Private. Dari sisi client akan membuka dua *web browser* dan masing - masing mengakses ke Virtual Web Server dan Mail Server. Pada pengukuran kinerja, client akan membuka dua *web browser* melalui netbook yang telah terhubung dengan Xen host komputer desktop yang terhubung oleh kabel UTP Crossover. pengukuran ini dilakukan selama 10 menit dan sebelum client mengakses ke *Xen Host*, masing - masing Virtual Server menjalankan tooll *Wireshark* dan pada terminal *Saidar*. Dalam skenario pengujian pertama ini yang akan di ambil datanya ialah *CPU Usage*, *RAM Usage*, Nilai *Throughput*, dan *Delay*. keempat parameter inilah ayng kemudian akan dianalisa setelah data didapat.

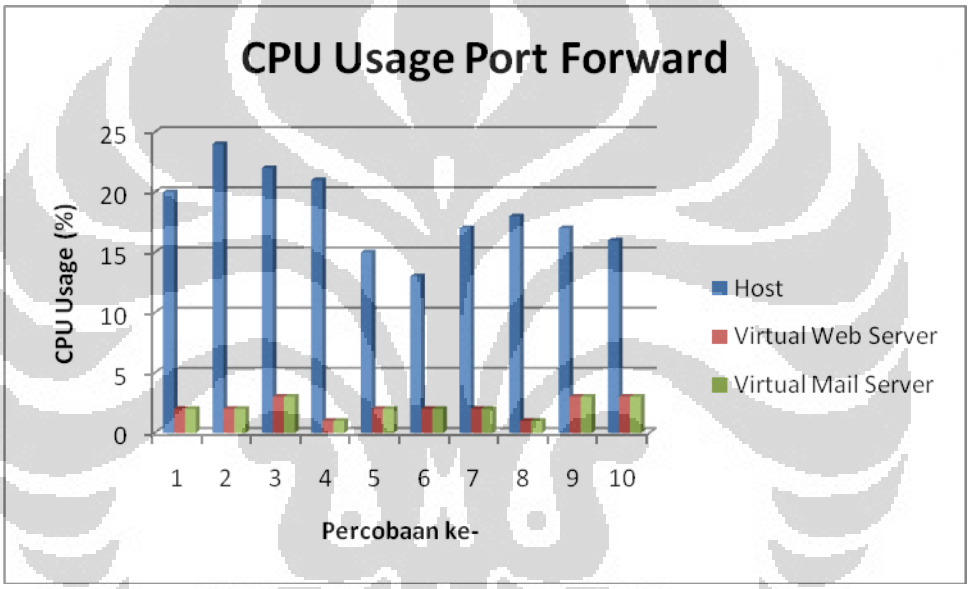
Client pada Web Browser memasukkan URL http://192.168.1.201 untuk mengakses Xen Virtual Web Server dan kemudian pada Tab Browser lain memasukkan URL Http://192.168.1.201:8080 ini untuk melakukan akses ke Xen Virtual Mail Server. Dengan menggunakan tool Saidar yang berbasis CLI diperoleh data dari sepuluh kali percobaan yaitu CPU Usage.

3.8.1 CPU Usage

Tabel 4.1 CPU Usage (%) Port Forwarding

Percobaan ke	Host	Virtual Web Server	Virtual Mail Server
1	20	2	1
2	24	2	2
3	22	3	3

4	21	1	4
5	15	2	5
6	13	2	6
7	17	2	7
8	18	1	8
9	17	3	3
10	16	3	3

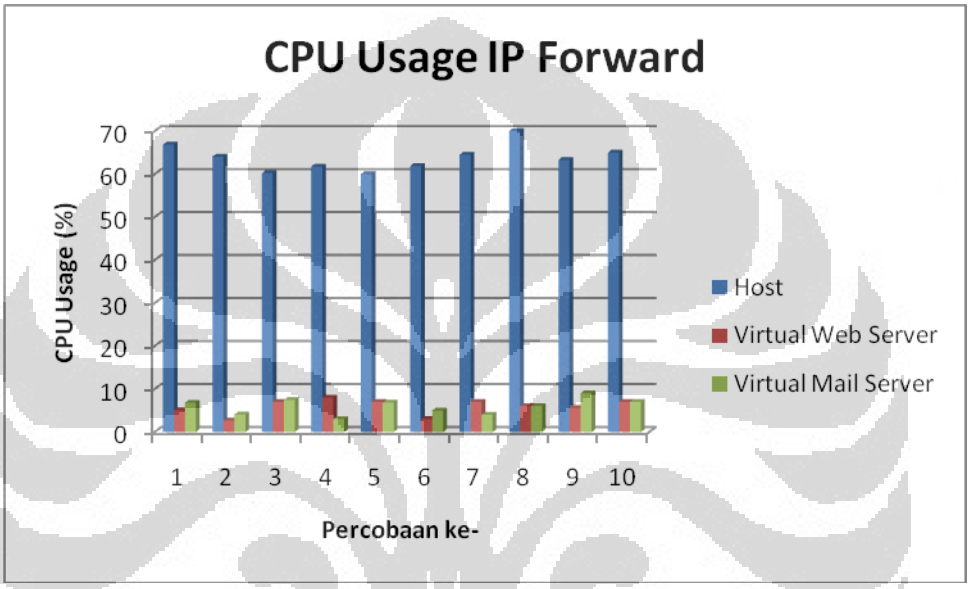


Gambar 4.1 Grafik CPU Usage Port Forward

Tabel 4.2 CPU Usage IP Forwarding

Percobaan	Host	Virtual Web Server	Virtual Mail Server
1	66.84	5.05	6.8
2	64.04	2.67	4.05
3	60.2	7	7.45
4	61.75	8	3
5	60	7	6.84

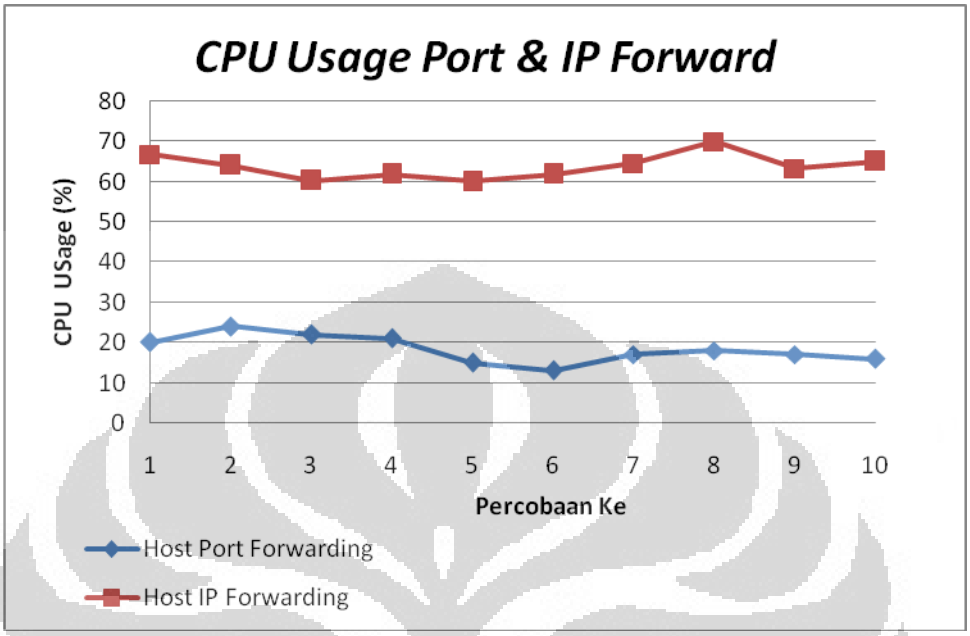
6	61.87	3.02	5
7	64.52	7	4
8	70	6	6
9	63.3	5.56	9
10	65	7	7



Gambar 4.2 grafik CPU Usage IP Forwad

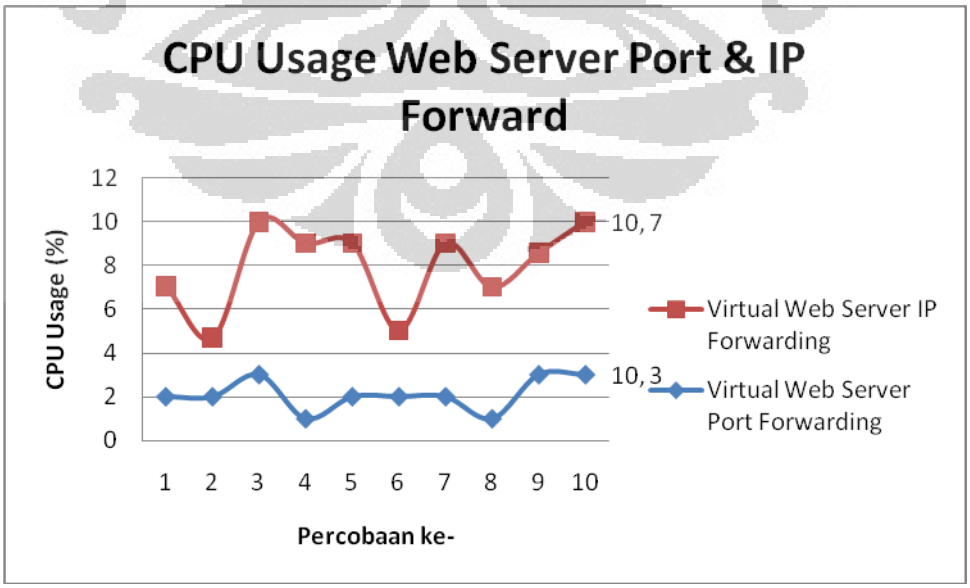
Dari sepuluh kali percobaan didapatkan data untuk CPU Usage seperti pada Gambar Grafik 4.2 diketahui bahwa penggunaan CPU Usage oleh Host sangat besar jika dibandingkan dengan Virtualisasi Servernya dengan perbandingan selisihnya sebesar 60%, hal ini dikarenakan model virtualisasi yang digunakan adalah Virtualisasi Penuh sehingga penggunaan resource lebih di bebankan kepada Host. Kemudian jika dibandingkan CPU Usage antara metode Port Forward dengan IP Forward seperti pada Gambar 4.3 terdapat perbedaan yaitu selisih sekitar 30% dimana dengan metode Port Forward dengan penggunaan *CPU Usage* berkisar 10% - 30% dari resource system, sedangkan metode IP Forward kisaran 60% - 70% terhadap *CPU Usage* CPU , hal ini terjadi bisa dikarenakan pada proses IP Forward terdapat dua proses SNAT (Source

NAT) sehingga CPU melakukan dua kali proses pada SNAT dibandingan metode Port Forward hanya terdapat satu proses SNAT.

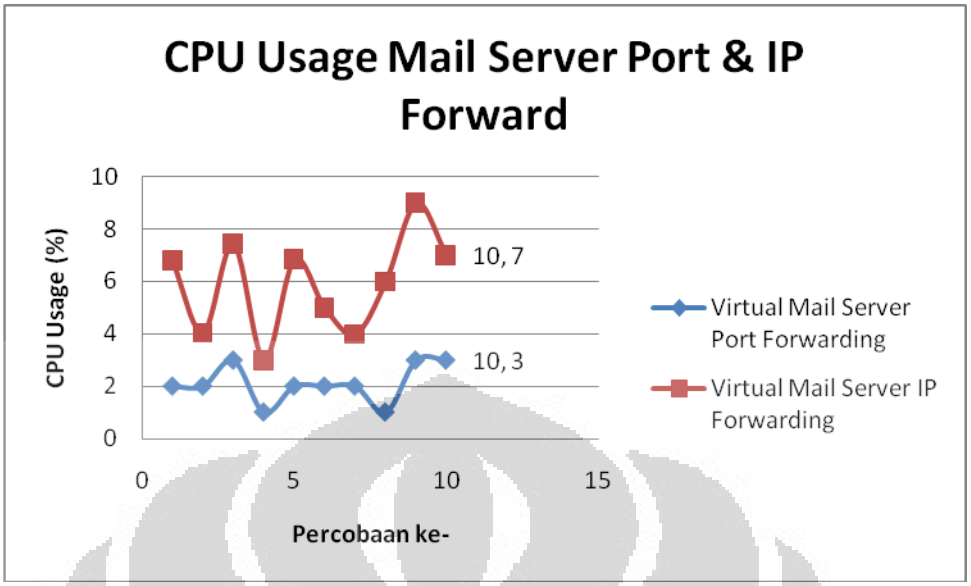


Gambar 4.3 Grafik CPU Usage Port & IP Forward

Sedangkan untuk Virtualisasi Servernya jika dibandingkan, dengan metode dengan Port Forward lebih sedikit penggunaan *CPU Usage* - nya, seperti pada gambar 4.4 dan gambar 4.5.



Gambar 4.4 Grafik CPU Usage Web Server Port & IP Forward



Gambar 4.5 Grafik CPU Usage Mail Server Port & IP Forward

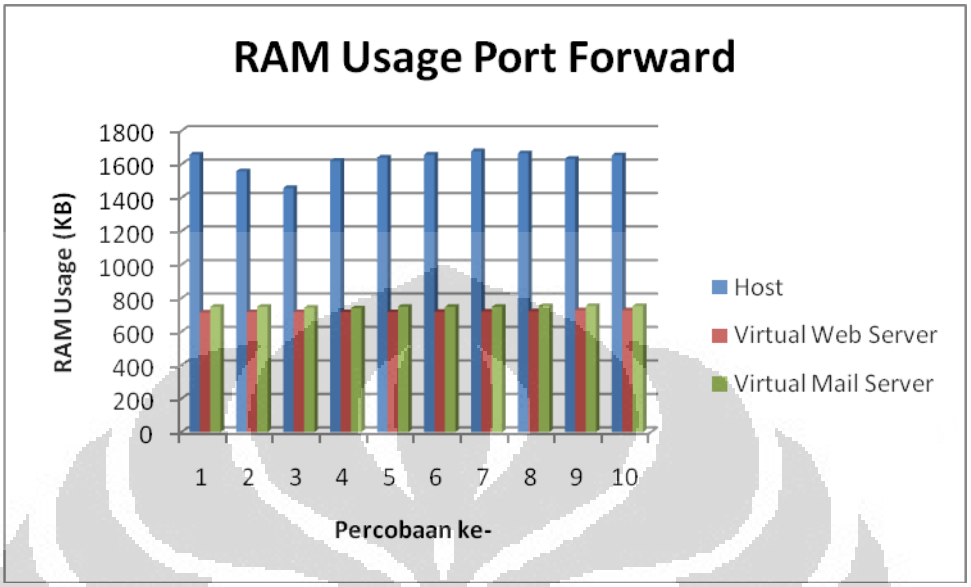
3.8.2 RAM Usage

Pada pembuatan Virtualisasi dengan Virt-manager, alokasi penggunaan RAM untuk kedua Virtual Server sebesar 1024 Gb. lalu setelah dilakukan pengambilan data metode Port Forward dan IP Forward dan kemudian diolah seperti pada gambar 4.6.

Tabel 4.3 RAM Usage Port Forward

Percobaan	Host	Virtual Web Server	Virtual Mail Server
1	1658	714	748
2	1558	716	748
3	1458	716	743
4	1621	717	740
5	1640	717	748
6	1657	718	748
7	1678	720	748
8	1666	721	753
9	1632	727	753

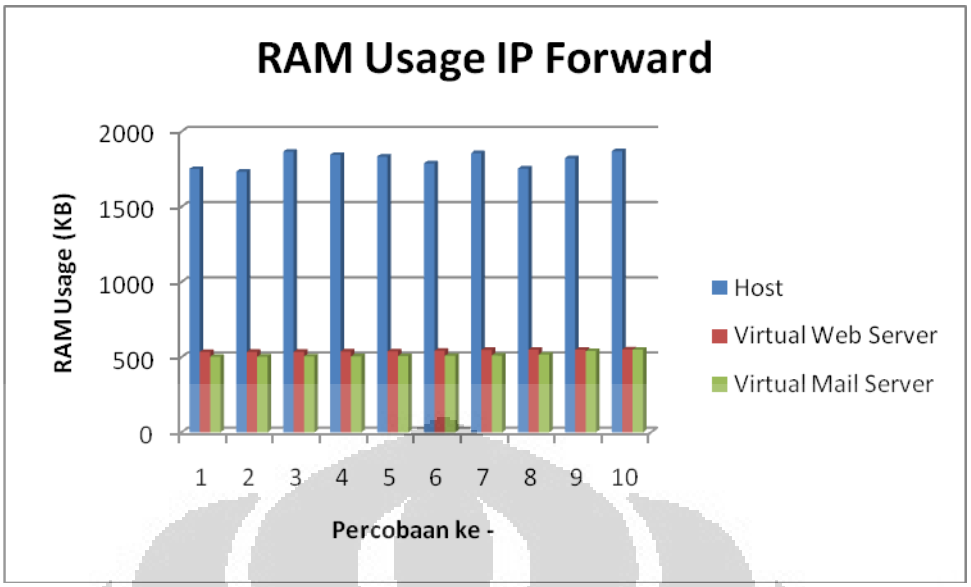
10	1654	727	753



Gambar 4.6 Grafik RAM Usage Port Forward

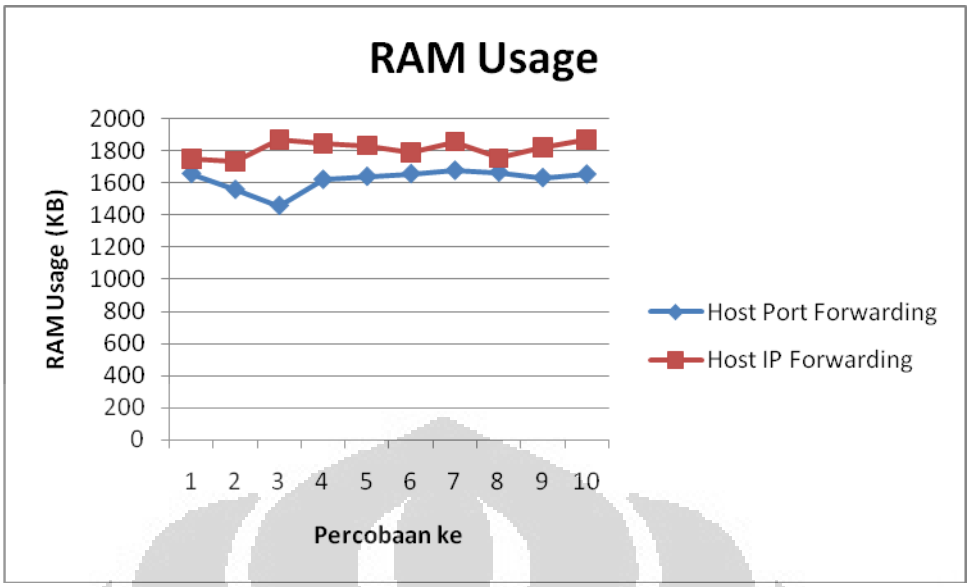
Tabel 4.4 RAM Usage IP Forward

Percobaan	Host	Virtual Web Server	Virtual Mail Server
1	1751	534	502
2	1733	535	503
3	1866	535	504
4	1845	537	505
5	1833	538	507
6	1788	542	509
7	1856	548	510
8	1754	549	517
9	1822	549	540
10	1869	551	549

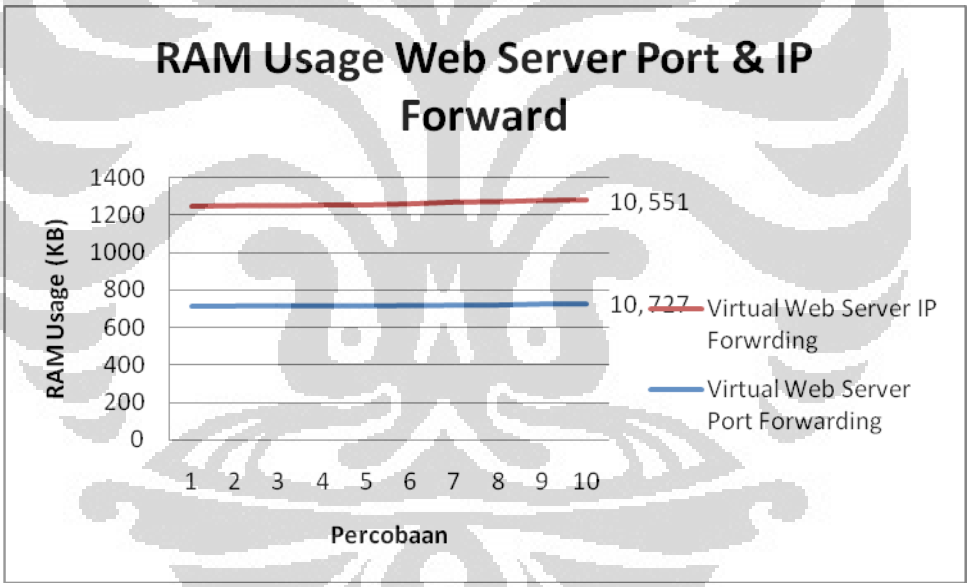


Gambar 4.7 Grafik RAM Usage IP Forward

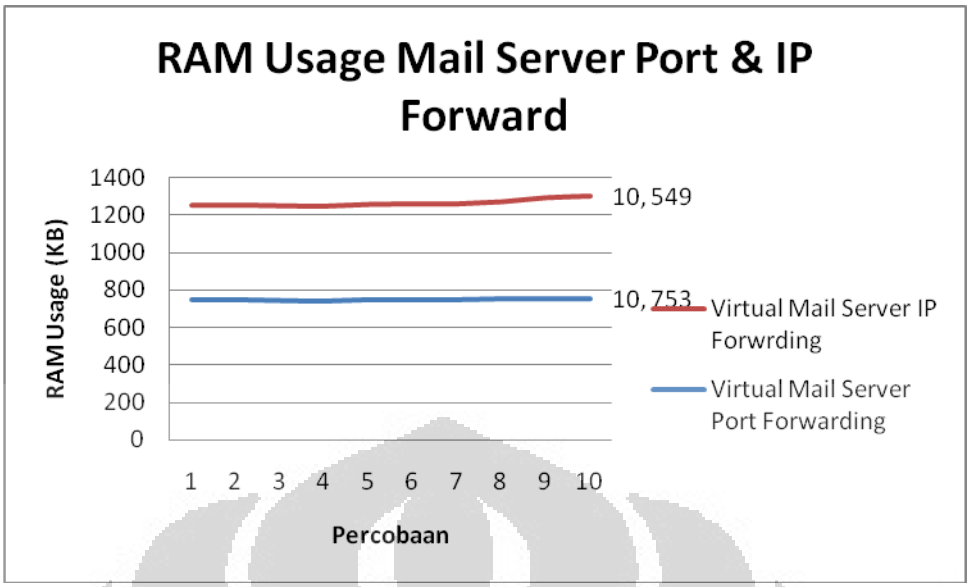
Dari kedua pengujian tersebut dimana dengan metode yang berbeda dapat diketahui bahwa penggunaan memori kedua metode menjelaskan jika penggunaan memori pada Host adalah yang lebih besar bebannya jika dibandingkan dengan Virtualisasinya. Lalu dari pengujian pada penggunaan memori dengan kedua metode jika dibandingkan seperti pada Gambar 4.7 4.8 ; 4.9 , diketahui jika dengan metode filtering packet IPTables dengan Port Forward lebih efisien sekitar 100 Kb - 200 Kb jika dibandingkan dengan IP Forward baik dari sisi Host ataupun virtualisasi dengan perkiraan persentase metode Port Forward lebih efisien 1,125% terhadap metode IP Forward.



Gambar 4.7 Grafik RAM Usage Hst IP & Port Forward



Gambar 4.8 Grafik RAM Usage Web Server dengan metode Port Forward dan IP Forward



Gambar 4.9 Grafik RAM Usage Mail Server dengan metode Port Forward dan IP Forward

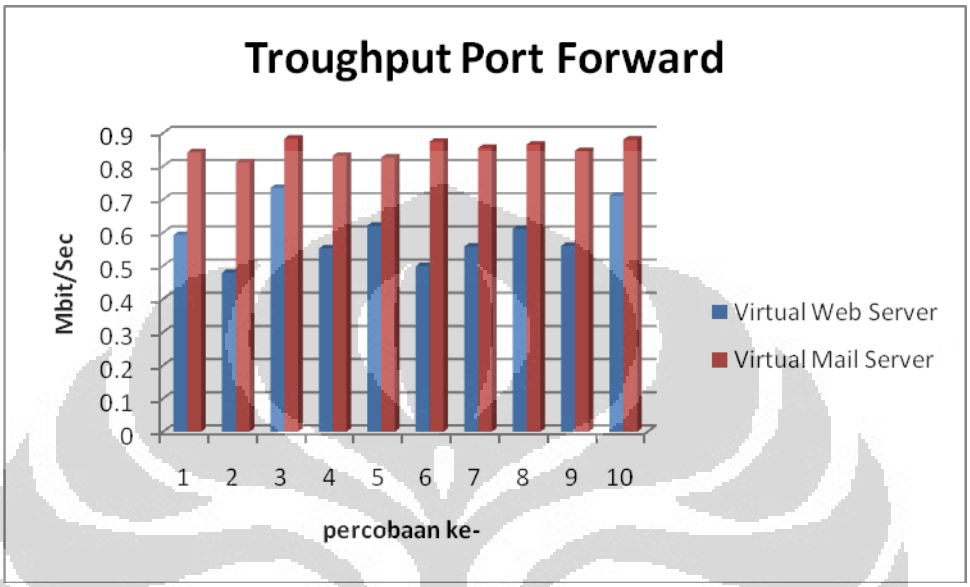
3.8.3 Troughput

Kemudian dalam pengujian diperoleh data nilai Throughput untuk kedua metode yaitu Port Forwar dan IP Forward. berdasar tabel [Tabel 4.5] dari 10 kali percobaan menunjukkan nilai Troughput Mail Server lebih besar terhadap Web Server hal ini bersifat kebalikan terhadap data yang diperoleh dari hasil pengukuran Delay.

Tabel 4.5 Troughput Port Forward

Percobaan	Virtual Web Server	Virtual Mail Server
1	0.593	0.842
2	0.479	0.811
3	0.735	0.883
4	0.552	0.831
5	0.621	0.826
6	0.499	0.874
7	0.558	0.855

8	0.611	0.865
9	0.56	0.846
10	0.711	0.88



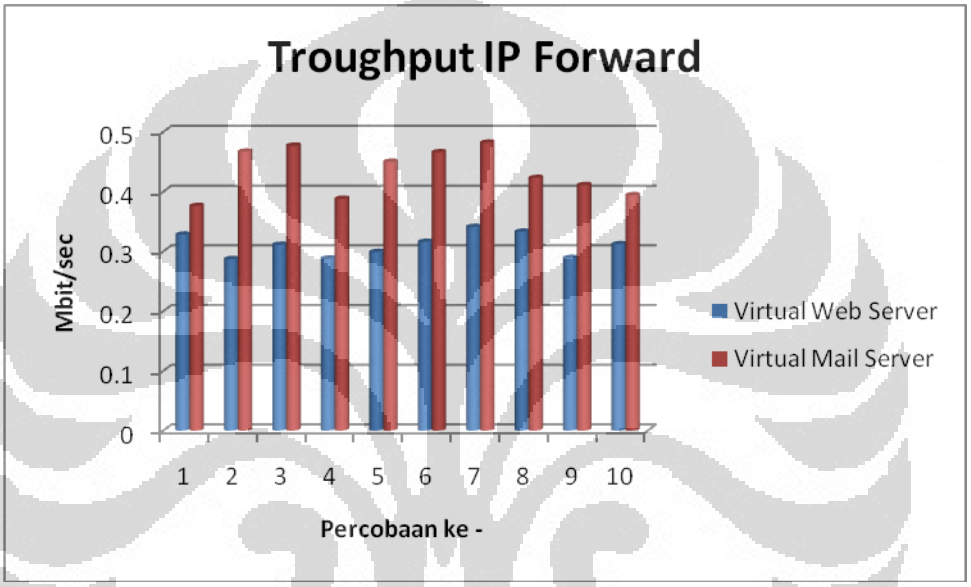
Gambar 4.10 Grafik Troughput Port Forward

Lalu jika pada pengujian dengan metode IP Forward diperoleh data yang tidak jauh beda dengan menggnakan metode Port Forward hanya saja jika dengan metode IP Forward nilai Troughput pada mail server tertinggi adalah 0.482 Mbit/sec dan nilai Troughput tertinggi pada web server ialah 0.333 Mbit/sec. Jika dianalisa, baik dengan penggunaan metode Port Forward ataupun dengan metode IP Forward didapat bentuk grafik yang hampir sama dimana nilai Troughput Mail Server selalu lebih besar dibandingkan dengan Web Server.

Tabel 4.6 Troughput IP Forward

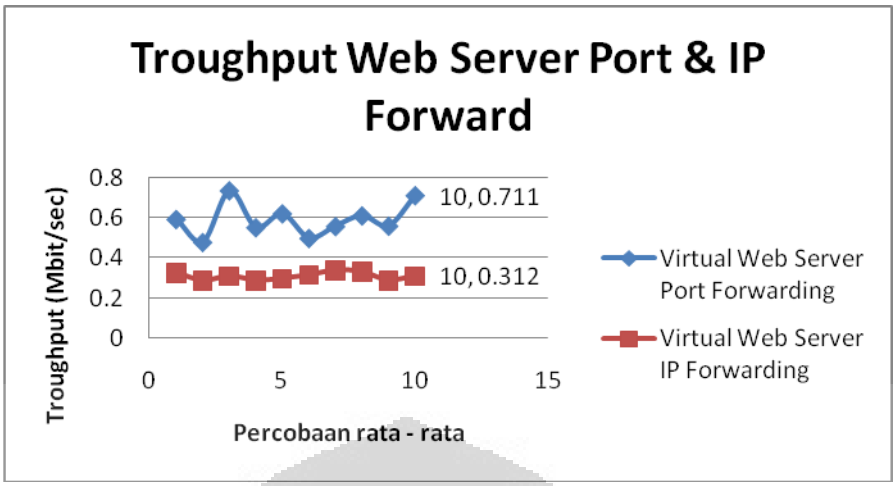
No	Virtual Web Server	Virtual Mail Server
1	0.328	0.376
2	0.287	0.467
3	0.311	0.477
4	0.288	0.388

5	0.299	0.45
6	0.316	0.466
7	0.341	0.482
8	0.333	0.423
9	0.289	0.411
10	0.312	0.394

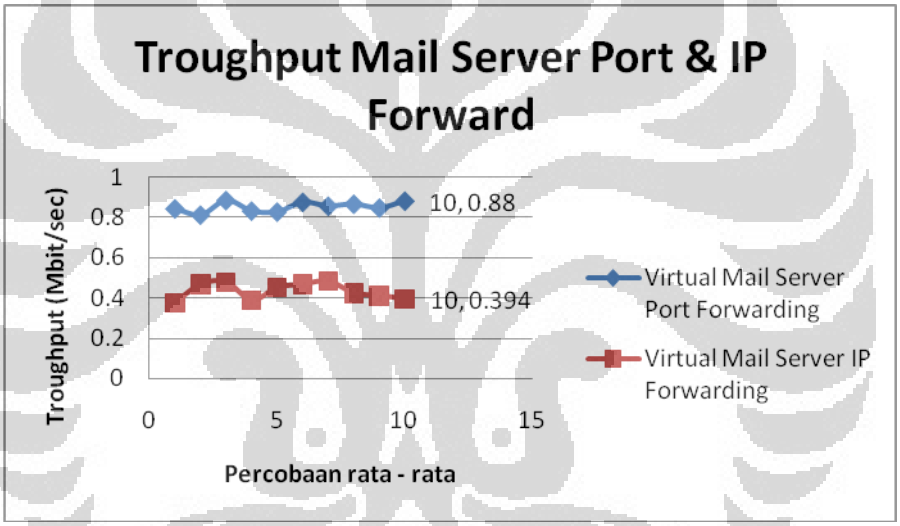


Gambar 4.11 Grafik Troughput IP Forward

Kemudian jika dibandingkan Troughput antara metode Port Forward dengan IP Forward seperti pada grafik [Gambar 4.13] dan grafik [Gambar 4.14] diketahui jika kedua grafik menunjukkan penggunaan metode Port Forward lebih besar nilai Troughputnya terhadap metode IP Forward dengan selisih antara 0.1 - 0,3 MBit/sec . jika dianalisa hal ini membuktikan bahwa penggunaan SNAT pada kedua metode sangat berpengaruh pada kinerja antara lain nilai Troughput. Port Forward dimana menggunakan satu saja SNAT sehingga proses packet filtering oleh Host menjadi lebih cepat jika dibandingkan dengan metode IP Forward yang menggunakan dua SNAT karena terdapat dua interface yang harus di Forward packet secara bersamaan sehingga beban proses pada sisi server pun lebih besar.



Gambar 4.12 Grafik Troughput Web Server Port & IP Forward



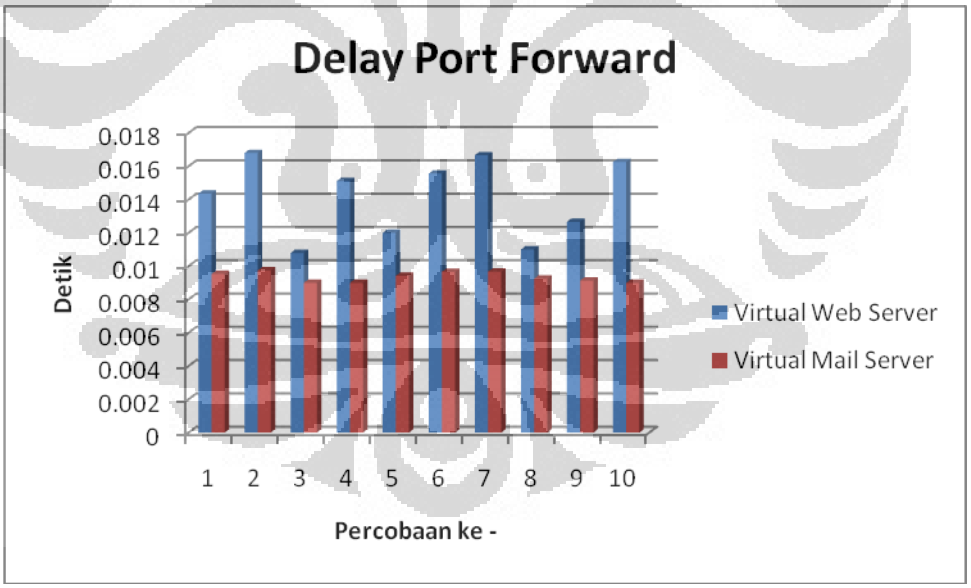
Gambar 4.13 Grafik Troughput Mail server Port & IP Forward

3.8.4 Delay

Dalam pengukuran niali Delay ini berbanding terbalik dengan nilai troughput dimana nilai troughput besar maka nilai delay akan kecil, dan hal ini terbukti dengan setelah pengambilan data antara metode Port Forward dan IP Forward. jika berdasarkan data yang diperoleh diketahui pada grafik [Gambar 4.13] dengan metode Port Forward nilai Delay Web Server terlihat begitu besar nilai Delay nya terhadap nilai Delay Mail Server. hal ini bisa terjadi bisa dikarenakan pada sisi Mail Server lebih cepat dalam melakukan proses atau terdapat gangguan dalam pengiriman paket ke sisi Web Server sehingga nilai Delay pada Web Server lebih besar terhadap Mail Server.

Tabel 4.7 Delay Port Forward

Percobaan	Virtual Web Server	Virtual Mail Server
1	0.014361776	0.009532
2	0.016795873	0.009747124
3	0.010789948	0.008994956
4	0.015112347	0.008995641
5	0.012003895	0.009421
6	0.015564413	0.00966123
7	0.016664128	0.009666451
8	0.011003641	0.009245783
9	0.012664139	0.009133895
10	0.016259613	0.00899733

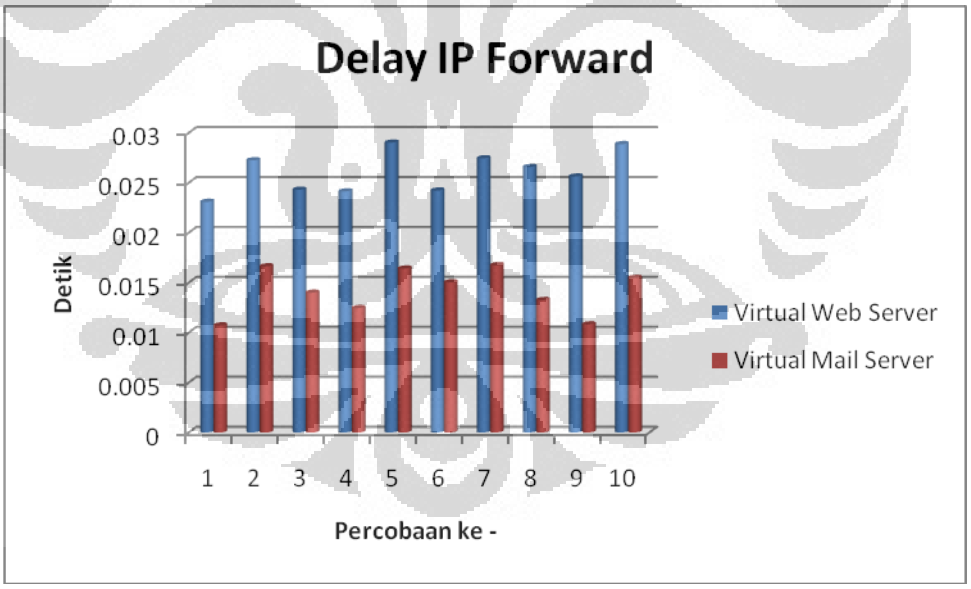


Gambar 4.13 Grafik Delay Port Forward

Pada nilai Delay dengan metode IP Forward juga memiliki bentuk pola delay yang hampir sama dengan metode Port Forward dimana niali Delay Mail Server lebih kecil delay nya.

Tabel 4.8 Delay IP Forward

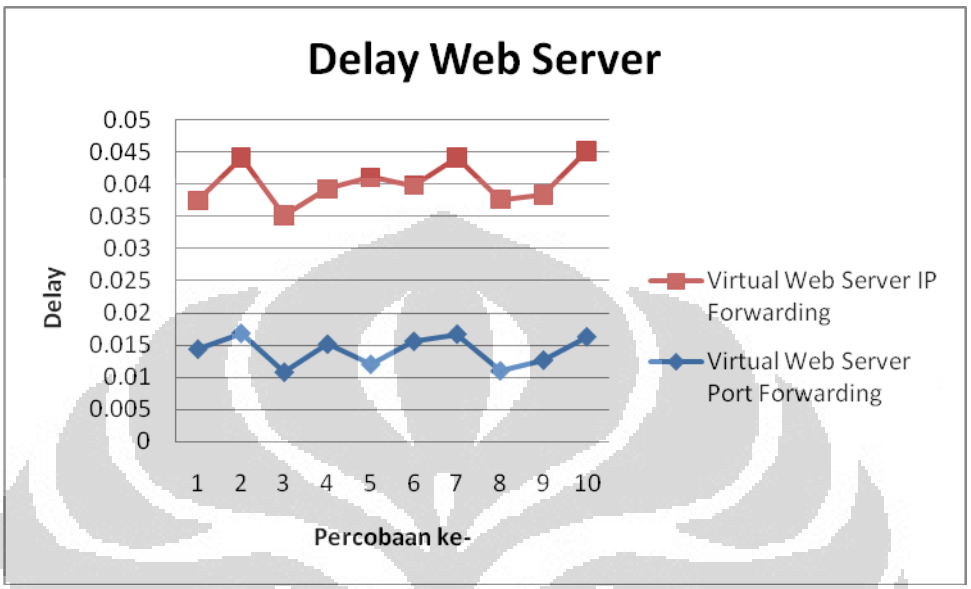
No	Virtual Web Server	Virtual Mail Server
1	0.023092591	0.010719053
2	0.027252179	0.016633153
3	0.0243	0.014
4	0.024134851	0.012456232
5	0.029022645	0.016412572
6	0.024225741	0.015033413
7	0.027452111	0.016745222
8	0.026584122	0.013255411
9	0.025633986	0.010823644
10	0.028874123	0.015477712



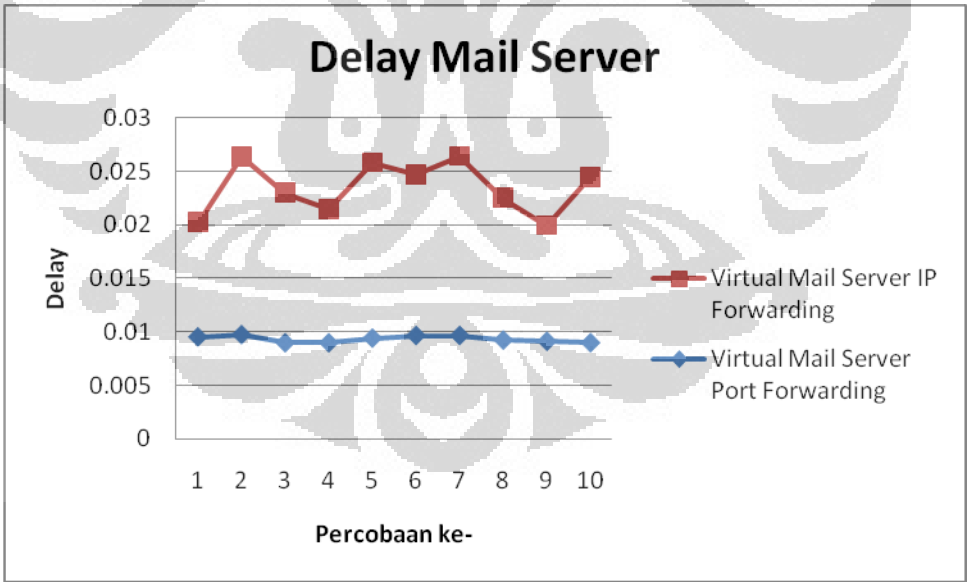
Gambar 4.13 *grafik* Delay IP Forward

Kemudian setelah data kedua metoe didapatkan kemudian dibandingkan antara metode Port Forward dengan IP Forward seperti pada grafik [Gambar 4.14 & 4.15] menunjukkan bahwa nilai delay dengan menggunakan metode Port Forward nilai delay nya lebih kecil dibandingkan dengan nilai delay IP Forward,

baik dari perbandingan antara mail Server maupun Web Server keduanya memiliki kesamaan yang menunjukkan bahwa dengn metode Port Forward memberikan nilai Delay yang kecil.



Gambar 4.14 Grafik Delay Web Server Port & IP Forward



Gambar 4.15 Grafik Delay Port & IP Forward

Secara keseluruhan setelah melakukan pengujian yang dilakukan baik dengan metode Port Forward maupun IP Forward dapat diketahui jika dengan menggunakan Port Forward adalah yang terbaik dari penggunaan CPU, RAM

serta nilai Troughput dan Delay nya. hal ini bisa dijadikan bahan pertimbangan jika dalam pembuatan suatu server virtualisasi dengan dengan hanya memiliki satu IP Public bisa menggunakan metode Port Forward.

BAB 5

KESIMPULAN

Dari pengujian yang telah dilakukan dapat disimpulkan :

1. Virtual Server adalah adalah teknologi yang telah terbukti memungkinkan beberapa virtual mesin untuk dijalankan pada server fisik tunggal.
2. Setiap mesin virtual benar – benar terisolasi dari mesin virtual lain dan dipisahkan dari host dengan *thin layer* hypervisor. Hal ini memungkinkan setiap mesin virtual untuk menjalankan system operasi dan aplikasi yang berbeda.
3. Hasil pengujian menunjukkan *CPU Usage* dengan metode Port Forward lebih rendah sekitar 30% dibandingkan dengan *IP Forward*. Hal ini menandakan proses yang terjadi dengan metode Port Forward lebih sedikit
4. Hasil pengujian menunjukkan penggunaan *memori* pada *Host* lebih besar terjadi pada metode *IP Forward* dengan selisih antara 100-200 KiloBytes/sec terhadap metode *Port Forward* atau sekitar 1,125% lebih efisien metode Port Forward terhadap IP Forward . Hal ini menandakan dimungkinkan bahwa proses yang berjalan terjadi penumpukan secara berlanjut sehingga mebebankan kepada proses yang sebelumnya.
5. Hasil pengujian menunjukkan nilai *Troughput* 0,1 - 0,3 MBit/sec lebih besar dengan metode *Port Forward*. Hal ini menandakan proses ini yang terdapat konfigurasi dua SNAT mempengaruhi nilai *Throughput*.
6. Berdasarkan dari semua pengujian, metode *Port Forward* lebih efisien *CPU dan RAM Usage* serta kinerjanya lebih baik dengan persentase lebih efisiensinya sebesar 23,3625% dibandingkan dengan metode *IP Forward.*

DAFTAR REFERENSI

[1]. http://www.cyberkomputer.com/Jaringan-Komputer/pengertian-dan-fungsi-firewall-dalam-suatu-jaringan-komputer-lan-dan-wan diakses pada 18 desember 2011

[2]. http://searchcloudsecurity.techtarget.com/definition/virtual-firewall diakses pada 18 desember 2011

[3]. http://wiki.xen.org/wiki/XenDomUSupport diakses pada 25 desember 2011

[4]. http://wiki.xen.org/wiki/XenDom0Kernels diakses pada 25 desember 2011

[5]. Gaurav Somani and Sanjay Chaudhary, "Application Performance Isolation in Virtualization" , 2009 IEEE International Conference on Cloud .

[6]. Xen Server Installation Guide 5.5.0, published June 2009.

[7]. Vassilis Prevelakis, "The Virtual Firewall".

[8]. www.xen.org

[9]. XenServer 5.5.0 User Security, published on June 2009

[10]. Sebastian Vogl, "Secure hypervisor".

[11]. http://virt-manager.org/index.html diakses pada 25 desember 2011

[12]. http://vavai.com/2010/01/25/teknologi-virtualisasi-virtualbox-xen-hypervisor-full-virtualization-paravirtualization/ diakses pada 13 Januari 2012

[13]. http://www.pc-tips-and-tricks.com/how-does-a-firewall-work.html diakses pada 13 januari 2012

[14]. http://www.copiouscom.com/2011/09/how-to-build-an-802-1q-lacp-trunk-for-xen-in-centos-5-5/ diakses pada 13 januari 2012

[15].http://cooker.techsnail.com/index.php/XEN,_KVM,_Libvirt_and_IPTables#Introduction diakses pada 13 Juni 2012

[16]. http://www.frozentux.net/iptables-tutorial/iptables-tutorial.html diakses pada 13 juni 2012

[17].http://ubuntuforums.org/showthread.php?s=2bc8163e9b0da7c3e19f602a8a07d0b8&t=159661 diakses pada 13 Juni 2012

[18]. https://help.ubuntu.com/community/IptablesHowTo#Basic_iptables_howto diakses pada 13 juni 2012

[19]. http://www.cyberciti.biz/faq/rhel-fedorta-linux-iptables-firewall-configuration-tutorial/ diakses pada 13 Juni 2012

[20]. http://bodhizazen.net/Tutorials/iptables/#Overview diakses pada 13 Juni 2012

[21]. Panduan Praktis Firewall dengan IPTables http://linux2.arinet.org diakses pada 2 Juni 2012

[22]. http://www.beyondlinux.com/2011/11/02/install-xen-4-1-and-setup-your-cloud-os-on-ubuntu-11-10/ diakses pada 1 mei 2012

LAMPIRAN

[A]. Instalasi Xen pada Distro LINUX Ubuntu 12.04 LTS (Precise Pangolin) :

#sudo apt-get install xen-hypervisor-4.1-i386 xen-utils-4.1 xenwatch xen-tools xen-utils-common xenstore-utils virtinst virt-viewer virt-manager

(optional)apt-get install linux-image-server

Restart os, choose the xen kernel,

verify xen installation. hold shift button if grub nothing

xm info

brctl show

Config your xend

$ sudo nano /etc/xen/xend-config.sxp

comment out (xend-unix-server yes) at the file, that means make sure the following line

(xend-unix-server yes)

#nano ~/.bashrc , add the following line:export VIRSH_DEFAULT_CONNECT_URI="xen:///"

Restart, choose the xen kernel, and verify libvirt

virsh version

Compiled against library: libvir 0.8.3

Using library: libvir 0.8.3

Using API: Xen 3.0.1

Running hypervisor: Xen 4.0.0

Run virtual machine manager to manage your vms.

virt-manager

[B] IPTables

Port Forward

- -A PREROUTING -i eth0 -p tcp -m tcp --dport 80 -j DNAT --to-destination 192.168.200.41
- -A PREROUTING -i eth0 -p tcp -m tcp --dport 443 -j DNAT --to-destination 192.168. 200.41
- -A PREROUTING -i eth0 -p tcp -m tcp --dport 25 -j DNAT --to-destination 192.168. 200.42
- -A PREROUTING -i eth0 -p tcp -m tcp --dport 110 -j DNAT --to-destination 192.168.200.42
- -A PREROUTING -i eth0 -p tcp -m tcp --dport 143 -j DNAT --to-destination 192.168. 200.42
- -A PREROUTING -i eth0 -p tcp -m tcp --dport 8080 -j DNAT --to-destination 192.168. 200.42:80
- -A PREROUTING -i eth0 -p tcp -m tcp --dport 8443 -j DNAT --to-destination 192.168. 200.42:443
- -A POSTROUTING -s 192.168.122.0/255.255.255.0 -d ! 192.168.122.0/255.255.255.0 -j SNAT --to-source 192.168.1.201

IP Forward

- -A PREROUTING -d 192.168.1.211 -i eth0 -p tcp -j DNAT --to-destination 192.168.200.41
- -A PREROUTING -d 192.168.1.212 -i eth0 -p tcp -j DNAT --to-destination 192.168.200.42
- -A POSTROUTING -s 192.168. 200.41 -d ! 192.168.122.0/255.255.255.0 -j SNAT --to-source 192.168.1.211
- # -A POSTROUTING -s 192.168. 200.42 -d ! 192.168.122.0/255.255.255.0 -j SNAT --to-source 192.168.1.212