



**KONFIGURASI FIREWALL DAN VIRTUAL SERVER UNTUK
MODUL PEMBELAJARAN DI BADAN PEMERIKSAAN
KEUANGAN REPUBLIK INDONESIA (BPKRI)**



LAPORAN KERJA PRAKTIK

Program Studi

S1 Sistem Komputer

Oleh:

Rusli Ali Hasan

1341020115

**FAKULTAS TEKNOLOGI DAN INFORMATIKA
INSTITUT BISNIS DAN INFORMATIKA STIKOM
SURABAYA
2018**

LAPORAN KERJA PRAKTIK

KONFIGURASI FIREWALL DAN VIRTUAL SERVER UNTUK

MODUL PEMBELAJARAN DI BADAN PEMERIKSAAN

KEUANGAN REPUBLIK INDONESIA (BPKRI)

Diajukan sebagai salah satu syarat untuk menyelesaikan

Program Sarjana



UNIVERSITAS
Dinamika

Disusun Oleh :

Nama : Rusli Ali Hasan

NIM : 13.41020.0115

Program : S1 (Strata Satu)

Jurusan : Sistem Komputer

FAKULTAS TEKNOLOGI DAN INFORMATIKA

INSTITUT BISNIS DAN INFORMATIKA STIKOM SURABAYA

2018

“ But man is not made for defeat, a man can be destroyed but not defeated ”

-Ernest Hemmingway



UNIVERSITAS
Dinamika

Kupersembahkan Kepada

ALLAH SWT

**Ibu, Bapak dan seluruh keluarga tercinta, yang selalu mendukung,
memotivasi dan menyisipkan nama saya dalam doa-doanya.**

**Beserta orang-orang yang selalu membantu, mendukung dan memotivasi
agar tetap berusaha menjadi lebih baik dan dapat terus melangkah kedepan.**



UNIVERSITAS
Dinamika

LEMBAR PENGESAHAN

**KONFIGURASI FIREWALL DAN VIRTUAL SERVER
UNTUK MODUL PEMBELAJARAN DI BADAN PEMERIKSAAN
KEUANGAN REPUBLIK INDONESIA (BPKRI)**

Laporan Kerja Praktik oleh

Rusli Ali Hasan

NIM : 13.41020.0115

Telah diperiksa, diuji dan disetujui

Surabaya, 10 Januari 2018

Disetujui :

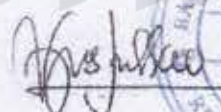
Dosen Pembimbing



Harianto, S.Kom., M.Eng.

NIDN : 0722087701

Penyelia



Mohammad Agus Prihandono

NIP : 198208072008081001

Mengetahui,

Ketua Program Studi

S1 Sistem Komputer



FAKULTAS TEKNOLOGI
DAN INFORMATIKA

stikom

Pauladie Susanto, S.Kom., M.T.

NIDN : 0729047501

SURAT PERNYATAAN

PERSETUJUAN PUBLIKASI DAN KEASLIAN KARYA ILMIAH

Sebagai Mahasiswa Institut Bisnis dan Informatika Stikom Surabaya, saya:

Nama : Rusli Ali Hasan

NIM : 13.41020.0115

Program Studi : S1 Sistem Komputer

Fakultas : Teknologi dan Informatika

Jenis Karya : Laporan Kerja Praktik

Judul Karya : **KONFIGURASI FIREWALL DAN VIRTUAL SERVER
UNTUK MODUL PEMBELAJARAN DI BADAN
PEMERIKSAAN KEUANGAN REPUBLIK INDONESIA
(BPKRI)**

Menyatakan dengan sesungguhnya bahwa:

1. Demi pengembangan Ilmu Pengetahuan, Teknologi dan Seni, saya menyetujui memberikan kepada Institut Bisnis dan Informatika Stikom Surabaya Hak Bebas Royalti Non-Eksklusif (Non-Exclusive Royalti Free Right) atas seluruh isi/ sebagian karya ilmiah saya tersebut di atas untuk disimpan, dialihmediakan, dan dikelola dalam bentuk pangkalan data (database) untuk selanjutnya didistribusikan atau dipublikasikan demi kepentingan akademis dengan tetap mencantumkan nama saya sebagai penulis atau pencipta dan sebagai pemilik Hak Cipta.
2. Karya tersebut diatas adalah karya asli saya, bukan plagiat baik sebagian maupun keseluruhan. Kutipan, karya atau pendapat orang lain yang ada dalam karya ilmiah ini adalah semata hanya rujukan yang dicantumkan dalam Daftar Pustaka saya.
3. Apabila dikemudian hari ditemukan dan terbukti terdapat tindakan plagiat pada karya ilmiah ini, maka saya bersedia untuk menerima pencabutan terhadap gelar kesarjanaan yang telah diberikan kepada saya.

Demikian surat pernyataan ini saya buat dengan sebenarnya.

Surabaya, Januari 2018

Yang menyatakan



Rusli Ali Hasan

NIM 13.41020.0115

ABSTRAK

Dalam sebuah perusahaan besar pada umumnya telah menggunakan jaringan yang berbasis Internet. Dalam membangun jaringan tersebut dibutuhkan beberapa komponen pembangun. Seperti Firewall dan Virtual Server yang fungsinya sebagai keamanan dan memaksimalkan pelayanan dalam jaringan.

Dari dua alat tersebut (Firewall dan Virtual Server) Bagi orang yang belum mengerti tentang bagaimana cara setting atau konfigurasinya akan terlihat susah untuk melakukannya, padahal melakukan konfigurasi dasar pada dua alat tersebut tidaklah serumit yang dipikirkan. Maka dari itu dibuatlah modul ini yang diharapkan dapat membantu bagi orang yang belum mengerti tentang cara konfigurasi dasar Firewall dan Virtual Server dapat terbantu setelah membaca modul ini.

Firewall adalah sebuah barrier yang dapat mengizinkan siapa saja yang dapat keluar-masuk. Firewall didesain untuk dapat menyaring pada level IP packet, atau mungkin pada protokol layer yang tinggi. Server adalah perangkat atau program komputer yang melayani program atau perangkat lain yang disebut *Client*. Server memiliki banyak fungsi seperti: *sharing data and resource* dan komputasi. Komputer yang digunakan sebagai server harus lebih kuat dan lebih handal dari komputer biasa. Alternatifnya dapat menggunakan cluster (gabungan beberapa node komputer) yang lebih simpel, dengan komponen yang dapat diganti. Beberapa contoh server misalnya: *database server, file server, mail server, print server, web server, application server*, dan sebagainya. Dari pembahasan dalam modul ini pembaca dapat mengerti tentang bagaimana cara konfigurasi dasar Firewall dan Virtual server yang merupakan komponen penting dari terhubungnya suatu jaringan.

Kata Kunci : Konfigurasi dasar, Jaringan, Firewall, Server, Virtual Server;

KATA PENGANTAR

Puji syukur kepada Allah atas segala rahmat yang telah memberikan kesehatan jasmani dan rohani, sehingga penulis dapat menyelesaikan Laporan Kerja Praktik ini. Penulisan Laporan ini adalah salah satu syarat untuk menempuh mata kuliah Kerja Praktik dan Tugas Akhir pada Program Studi S1 Sistem Komputer Institut Bisnis dan Informatika Stikom Surabaya.

1. Allah SWT karena dengan rahmatnya dan hidayahnya penulis dapat menyelesaikan Laporan Kerja Praktik ini.
2. Orang tua yang tidak pernah berhenti memberi dukungan penulis.
3. Bapak Pauladie Susanto, S.Kom., M.T., selaku Ketua Program Studi S1 Sistem Komputer Fakultas Teknologi Informatika Institut Bisnis dan Informatika Stikom Surabaya.
4. Bapak Harianto, S.Kom., M.Eng., selaku Dosen Pembimbing yang selalu memberi masukan dan saran dalam menyelesaikan laporan ini.
5. Bapak Iwan A.W selaku kepala bagian Teknologi Informasi di Badan Pemeriksa Keuangan Republik Indonesia (BPKRI).
6. Bapak Sugianto, Bapak Agus beserta seluruh Staf Bagian IT selaku pembimbing selama berjalannya Kerja Praktik di Badan Pemeriksa Keuangan Republik Indonesia (BPKRI).

Seluruh teman-teman S1 Sistem Komputer Institut Bisnis dan Informatika Stikom Surabaya dan semua pihak yang terlibat namun tidak dapat penulis sebutkan satu persatu atas bantuan dan dukungannya. Dengan segala kerendahan hati, penulis

menyadari bahwa penyusunan Laporan Kerja Praktik ini masih jauh dari kata sempurna, walaupun penulis telah berusaha dengan sungguh-sungguh menuangkan kemampuan yang dimiliki penulis dalam menyelesaikan Laporan Kerja Praktik ini. Dengan ini, penulis mengharapkan adanya kritik dan saran yang dapat penulis jadikan sebagai bahan acuan untuk penyusunan laporan-laporan yang selanjutnya agar bisa lebih baik lagi.

Surabaya, Oktober 2017



UNIVERSITAS Penulis
Dinamika

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSEMBAHAN	iii
HALAMAN PENGESAHAN	iv
HALAMAN PERNYATAAN.....	v
HALAMAN PUBLIKASI.....	vi
ABSTRAKSI.....	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR GAMBAR	xi
DAFTAR LAMPIRAN.....	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Tujuan Kerja Praktek.....	1
1.3 Perumusan Masalah.....	2
1.4 Batasan Masalah	2
1.5 Waktu dan Lama Kerja Praktek	2
1.6 Ruang Lingkup Kerja Praktek	2
1.7 Sistematika Penulisan Laporan	2
BAB II GAMBARAN UMUM PERUSAHAAN	4
2.1 Sejarah Singkat Perusahaan	4
2.2 Visi dan Misi Perusahaan.....	6
2.2.1 Visi.....	6
2.2.2 Misi	6
BAB III LANDASAN TEORI	8
3.1 Sejarah <i>Firewall</i>	8
3.1.1 Cyberoam CR100iNG.....	8
3.2 Virtualisasi	10
3.2.1 Hypervisor(Virtual Machine Monitor)	12
3.2.2 Virtual Machine	12
3.3 Server	12

3.3.1 Nutanix Server.....	13
BAB IV PEMBAHASAN.....	15
4.1 Langkah-langkah Penulisan Modul	15
4.2 Konfigurasi Hardware	15
4.2.1 Pengaturan Cyberoam CR100iNG melalui WebAdmin	14
4.2.2 Instalasi Acropolis Hypervisor pada Nutanix Server	21
4.2.3 Pengaturan Nutanix Server.....	26
4.3 Konfigurasi Software	30
4.3.1 Virtual Machine Pada AHV	31
BAB V KESIMPULAN.....	44
5.1 Kesimpulan	44
5.2 Saran	44
DAFTAR PUSTAKA	45



UNIVERSITAS
Dinamika

DAFTAR GAMBAR

Gambar 3.1 Antarmuka Cyberoam CR100iNG	9
Gambar 3.2 Perbedaan Arsitektur Komputer	11
Gambar 3.3 Arsitektur Komputer Virtual	12
Gambar 3.4 Node fisik tampak depan.....	14
Gambar 3.5 Node fisik tampak belakang	14
Gambar 4.1 Tampilan Login	15
Gambar 4.2 Tampilan pengaturan host	16
Gambar 4.3 Tampilan Pengaturan Service.....	17
Gambar 4.4 Tampilan pengaturan schedule	18
Gambar 4.5 Tampilan rule untuk Ipv4.....	19
Gambar 4.6 Pengaturan rule untuk Ipv4	19
Gambar 4.7 Tampilan pengaturan Gateway.....	20
Gambar 4.8 Pengaturan IP address pada PC	21
Gambar 4.9 Tampilan terminal.....	22
Gambar 4.10 Pilihan Device controller.....	22
Gambar 4.11 Pengaturan IP address pada Foundation VM	23
Gambar 4.12 Ping ke IP Foundation VM.....	23
Gambar 4.13 Login pada WinSCP	24
Gambar 4.14 Proses Copy file Nutanix OS 4.5.0.2.....	25
Gambar 4.15 Proses copy file phoenix 4.5.0.2.iso	25
Gambar 4.16 Global Configuration	26
Gambar 4.17 Block Node Configuration	27
Gambar 4.18 Node Imaging	28
Gambar 4.19. Cluster creation.....	29
Gambar 4.21 Login WinSCP ke PRISM	30
Gambar 4.22 Tampilan Login PRISM.....	31
Gambar 4.23 Dashboard PRISM.....	32
Gambar 4.24 Tampilan VM table list	32
Gambar 4.25 Tampilain Create VM	33
Gambar 4.26 Tampilan Add Disk.....	34

Gambar 4.27 Windows Setup	35
Gambar 4.28 Pilihan OS	36
Gambar 4.29 Custom Install.....	37
Gambar 4.30 Load driver	38
Gambar 4.31 Browse driver	39
Gambar 4.32 Browse folder	40
Gambar 4.33 Nutanix VirtIO Driver.....	41
Gambar 4.34 Select Windows Installation Drive	42
Gambar 4.35 Login Windows	43



UNIVERSITAS
Dinamika

DAFTAR LAMPIRAN

Lampiran 1. Surat Balasan Perusahaan.....	46
Lampiran 2. Acuan Kerja (Form KP-5).....	47
Lampiran 3. Log Harian (Form KP-6).....	49
Lampiran 4. Kehadiran Kerja Praktik (Form KP-7).....	50
Lampiran 5. Kartu Bimbingan Kerja Praktik (Form KP-8).....	51
Lampiran 6. Biodata Penulis	52



UNIVERSITAS
Dinamika

BAB I

PENDAHULUAN

1.1. Latar Belakang

Badan Pemeriksa Keuangan Republik Indonesia (BPKRI) adalah suatu lembaga yang bergerak dibidang keuangan yang ada di Negara Indonesia. Pada lembaga ini terdapat bagian yang penting yaitu bagian IT yang bertugas memantau dan mengawasi jaringan kantor BPKRI sendiri dan BPK daerah daerah lain. Pentingnya bagian ini diikuti oleh keharusan karyawan untuk mengetahui jaringan di kantor BPKRI sehingga karyawan dapat memaksimalkan fasilitas dan kinerja mereka.

Modul yang akan dibuat ini diharapkan dapat menjadi pegangan bagi pegawai yang ingin mempelajari tentang bagaimana cara setting atau konfigurasi dasar Server dan Firewall. Dimana pada modul ini telah dijelaskan secara singkat bagaimana cara mengkonfigurasi Server dan Firewall. Diharapkan nantinya bagi modul ini agar dapat dipahami oleh pegawai bagian lain yang ingin mempelajari tentang bagaimana cara mengkonfigurasi dasar Server dan Firewall.

1.2. Tujuan Kerja Praktik

Tujuan Kerja Praktik di Badan Pemeriksa Keuangan Republik Indonesia (BPKRI) adalah sebagai berikut :

1. Tujuan Umum
 - a. Memperoleh pengetahuan mengenai struktur, organisasi, standar, dan etika kerja di Badan Pemeriksa Keuangan Republik Indonesia (BPKRI)
 - b. Meningkatkan efektivitas dan efisiensi proses pendidikan dan pelatihan kerja berkualitas.
 - c. Dapat memecahkan permasalahan pada bagian yang ditempati kerja praktik.
 - d. Menambah wawasan dan pengetahuan untuk mempersiapkan diri baik secara teoritis maupun secara praktis.

2. Tujuan Khusus

Tujuan dari penelitian ini adalah untuk mempermudah pegawai dari bagian lain untuk mengerti apa dan bagaimana cara konfigurasi Virtual Server dan Firewall.

1.3. Perumusan Masalah

Dari latar belakang, maka dapat dirinci perumusan masalah sebagai berikut:

1. Bagaimana membuat materi tentang konfigurasi Virtual Server dan Firewall.
2. Bagaimana membuat materi tentang Virtual Server dan Firewall).

1.4. Batasan Masalah

Batasan masalah pada pelaksanaan Kerja Praktik ini adalah sebagai berikut:

1. Server yang digunakan adalah Nutanix Server.
2. Firewall yang digunakan adalah Cyberoam CR100iNG.
3. Software yang digunakan adalah Nutanix Foundation 3.0

1.5. Waktu dan Lama Kerja Praktik

Kerja Praktik di Badan Pemeriksa Keuangan Republik Indonesia dilaksanakan mulai tanggal 23 Januari 2017 – 17 Februari 2017.

1.6. Ruang Lingkup Kerja Praktik

Sasaran Kerja Praktik adalah agar mahasiswa mendapatkan pengalaman saat mempelajari Server dan Firewall serta membuat materi Server dan Firewall, maka dapat dijabarkan ruang lingkup Kerja Praktik adalah sebagai berikut:

1. Konfigurasi dasar Firewall Cyberoam
2. Instalasi software pada Server

3. Konfigurasi dasar Virtual Server
4. Pembuatan modul tentang konfigurasi dan instalasi Firewall dan Virtual Server

1.7. Sistematika Penulisan Laporan

Berikut ini adalah sistematika penulisan laporan hasil Kerja Praktik di Badan Pemeriksa Keuangan Republik Indonesia:

1. HALAMAN JUDUL
2. PENGESAHAN
3. KATA PENGANTAR
4. DAFTAR ISI
5. BAB I PENDAHULUAN

Pada bab pendahuluan berisi latar belakang Kerja Praktik, rumusan masalah, batasan masalah, tujuan Kerja Praktik, waktu dan jangka waktu Kerja Praktik, ruang lingkup Kerja Praktik, dan sistematika penulisan.

6. BAB II GAMBARAN UMUM PERUSAHAAN

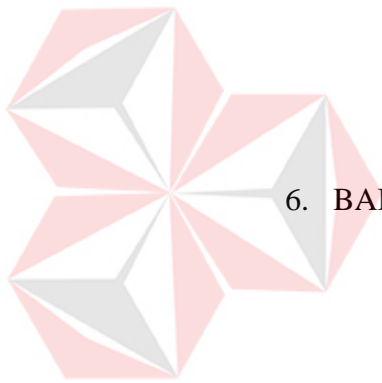
Pada BAB II berisi penjabaran tentang sejarah perusahaan yaitu Badan Pemeriksa Keuangan Republik Indonesia. Pengenalan unit kerja dan budaya masyarakat, pemahaman proses bisnis yang meliputi visi dan misi perusahaan.

7. BAB III LANDASAN TEORI

Pada BAB III berisi tentang Virtual Server dan Firewall, beserta penjelasan, teori fitur-fitur Hardware yang digunakan.

8. BAB IV PEMBAHASAN
9. BAB V PENUTUP

Pada BAB Penutup membahas tentang kesimpulan dan saran dari seluruh isi laporan ini yang disesuaikan dengan hasil dan pembahasan pada bab-bab sebelumnya.



BAB II

GAMBARAN UMUM PERUSAHAAN

2.1 Sejarah Singkat Perusahaan

Pasal 23 ayat (5) UUD Tahun 1945 menetapkan bahwa untuk memeriksa tanggung jawab tentang Keuangan Negara diadakan suatu Badan Pemeriksa Keuangan yang peraturannya ditetapkan dengan Undang-Undang. Hasil pemeriksaan itu disampaikan kepada Dewan Perwakilan Rakyat.

Berdasarkan amanat UUD Tahun 1945 tersebut telah dikeluarkan Surat Penetapan Pemerintah No.11/OEM tanggal 28 Desember 1946 tentang pembentukan Badan Pemeriksa Keuangan, pada tanggal 1 Januari 1947 yang berkedudukan sementara di kota Magelang. Pada waktu itu Badan Pemeriksa Keuangan hanya mempunyai 9 orang pegawai dan sebagai Ketua Badan Pemeriksa Keuangan pertama adalah R. Soerasno. Untuk memulai tugasnya, Badan Pemeriksa Keuangan dengan suratnya tanggal 12 April 1947 No.94-1 telah mengumumkan kepada semua instansi di Wilayah Republik Indonesia mengenai tugas dan kewajibannya dalam memeriksa tanggung jawab tentang Keuangan Negara, untuk sementara masih menggunakan peraturan perundang-undangan yang dulu berlaku bagi pelaksanaan tugas Algemene Rekenkamer (Badan Pemeriksa Keuangan Hindia Belanda), yaitu ICW dan IAR.

Dalam Penetapan Pemerintah No.6/1948 tanggal 6 Nopember 1948 tempat kedudukan Badan Pemeriksa Keuangan dipindahkan dari Magelang ke Yogyakarta. Negara Republik Indonesia yang ibukotanya di Yogyakarta tetap mempunyai Badan Pemeriksa Keuangan sesuai pasal 23 ayat (5) UUD Tahun 1945; Ketuanya diwakili oleh R. Kasirman yang diangkat berdasarkan SK Presiden RI tanggal 31 Januari 1950 No.13/A/1950 terhitung mulai 1 Agustus 1949.

Dengan terbentuknya Negara Kesatuan Republik Indonesia Serikat (RIS) berdasarkan Piagam Konstitusi RIS tanggal 14 Desember 1949, maka dibentuk Dewan Pengawas Keuangan (berkedudukan di Bogor) yang merupakan salah satu alat perlengkapan negara RIS, sebagai Ketua diangkat R. Soerasno mulai tanggal 31 Desember 1949, yang sebelumnya menjabat sebagai Ketua Badan Pemeriksa Keuangan di Yogyakarta. Dewan Pengawas Keuangan RIS berkantor di Bogor

menempati bekas kantor Algemene Rekenkamer pada masa pemerintah Netherland Indies Civil Administration (NICA).

Dengan kembalinya bentuk Negara menjadi Negara Kesatuan Republik Indonesia pada tanggal 17 Agustus 1950, maka Dewan Pengawas Keuangan RIS yang berada di Bogor sejak tanggal 1 Oktober 1950 digabung dengan Badan Pemeriksa Keuangan berdasarkan UUDS 1950 dan berkedudukan di Bogor menempati bekas kantor Dewan Pengawas Keuangan RIS. Personalia Dewan Pengawas Keuangan RIS diambil dari unsur Badan Pemeriksa Keuangan di Yogyakarta dan dari Algemene Rekenkamer di Bogor.

Pada Tanggal 5 Juli 1959 dikeluarkan Dekrit Presiden RI yang menyatakan berlakunya kembali UUD Tahun 1945. Dengan demikian Dewan Pengawas Keuangan berdasarkan UUD 1950 kembali menjadi Badan Pemeriksa Keuangan berdasarkan Pasal 23 (5) UUD Tahun 1945.

Meskipun Badan Pemeriksa Keuangan berubah-ubah menjadi Dewan Pengawas Keuangan RIS berdasarkan konstitusi RIS Dewan Pengawas Keuangan RI (UUDS 1950), kemudian kembali menjadi Badan Pemeriksa Keuangan berdasarkan UUD Tahun 1945, namun landasan pelaksanaan kegiatannya masih tetap menggunakan ICW dan IAR.

Dalam amanat-amanat Presiden yaitu Deklarasi Ekonomi dan Ambeg Parama Arta, dan di dalam Ketetapan MPRS No. 11/MPRS/1960 serta resolusi MPRS No. 1/Res/MPRS/1963 telah dikemukakan keinginan-keinginan untuk menyempurnakan Badan Pemeriksa Keuangan, sehingga dapat menjadi alat kontrol yang efektif. Untuk mencapai tujuan itu maka pada tanggal 12 Oktober 1963, Pemerintah telah mengeluarkan Peraturan Pemerintah Pengganti Undang-undang No. 7 Tahun 1963 (LN No. 195 Tahun 1963) yang kemudian diganti dengan Undang-Undang (PERPU) No. 6 Tahun 1964 tentang Badan Pemeriksa Keuangan Gaya Baru.

Untuk mengganti PERPU tersebut, dikeluarkanlah UU No. 17 Tahun 1965 yang antara lain menetapkan bahwa Presiden, sebagai Pemimpin Besar Revolusi pemegang kekuasaan pemeriksaan dan penelitian tertinggi atas penyusunan dan pengurusan Keuangan Negara. Ketua dan Wakil Ketua BPK RI berkedudukan masing-masing sebagai Menteri Koordinator dan Menteri.

Akhirnya oleh MPRS dengan Ketetapan No.X/MPRS/1966 Kedudukan BPK RI dikembalikan pada posisi dan fungsi semula sebagai Lembaga Tinggi Negara. Sehingga UU yang mendasari tugas BPK RI perlu diubah dan akhirnya baru direalisasikan pada Tahun 1973 dengan UU No. 5 Tahun 1973 Tentang Badan Pemeriksa Keuangan.

Dalam era Reformasi sekarang ini, Badan Pemeriksa Keuangan telah mendapatkan dukungan konstitusional dari MPR RI dalam Sidang Tahunan Tahun 2002 yang memperkuat kedudukan BPK RI sebagai lembaga pemeriksa eksternal di bidang Keuangan Negara, yaitu dengan dikeluarkannya TAP MPR No.VI/MPR/2002 yang antara lain menegaskan kembali kedudukan Badan Pemeriksa Keuangan sebagai satu-satunya lembaga pemeriksa eksternal keuangan negara dan peranannya perlu lebih dimantapkan sebagai lembaga yang independen dan profesional.

Untuk lebih memantapkan tugas BPK RI, ketentuan yang mengatur BPK RI dalam UUD Tahun 1945 telah diamandemen. Sebelum amandemen, BPK RI hanya diatur dalam satu ayat (pasal 23 ayat 5). Kemudian dalam Perubahan Ketiga UUD 1945 dikembangkan menjadi satu bab tersendiri (Bab VIII A) dengan tiga pasal (23E, 23F, dan 23G) dan tujuh ayat.

Untuk menunjang tugasnya, BPK RI didukung dengan seperangkat Undang-Undang di bidang Keuangan Negara, yaitu;

- UU No.17 Tahun 2003 Tentang Keuangan Negara
- UU No.1 Tahun 2004 Tentang Perbendaharaan Negara
- UU No.15 Tahun 2004 Tentang Pemeriksaan Pengelolaan dan Tanggung Jawab Keuangan Negara

2.2 Visi dan Misi Perusahaan

2.2.1 Visi

Menjadi pendorong pengelolaan keuangan negara untuk mencapai tujuan negara melalui pemeriksaan yang berkualitas dan bermanfaat.

2.2.2 Misi

1. Memeriksa pengelolaan dan tanggung jawab keuangan negara secara bebas dan mandiri; dan

2. Melaksanakan tata kelola organisasi yang berintegritas, independen, dan profesional.

2.3 Tujuan Strategis

Dalam memastikan tercapainya visi dan misi, maka ditetapkan dua tujuan strategis, yaitu:

1. Meningkatkan manfaat hasil pemeriksaan dalam rangka mendorong pengelolaan keuangan negara untuk mencapai tujuan negara; dan
2. Meningkatkan pemeriksaan yang berkualitas dalam mendorong pengelolaan keuangan negara untuk mencapai tujuan negara.



UNIVERSITAS
Dinamika

BAB III

LANDASAN TEORI

3.1 Sejarah Firewall

Firewall pertama kali muncul pada akhir era 1980 yaitu berupa perangkat router yang dipakai untuk memisahkan suatu network jaringan menjadi jaringan local (LAN) yang lebih kecil, dimana penggunaan firewall hanya dimaksudkan untuk mengurangi masalah kelebihan data dari LAN keseluruhan jaringan, atau aplikasi yang terlalu banyak digunakan oleh pengguna. Penggunaan firewall untuk keperluan keamanan pertama kali digunakan pada awal 1990, berupa router IP dengan aturan filter tertentu. Aturan pada tahun 1990an dapat dikatakan masih sederhana karena masih mengizinkan siapa yang dapat keluar dari dalam, dan siapa yang dapat masuk dari luar.

Firewall generasi selanjutnya, yaitu firewall yang disebut “Bastion Host”. Firewall komersial yang pertama dari tipe ini, yang menggunakan filter dan gateway aplikasi Firewall komersial pertama di konfigurasi untuk pelanggan pertama dari sebuah perusahaan kimia besar yang berbasis di pantai timur AS pada 13 Juni 1991.

Firewall adalah sebuah barrier yang dapat mengizinkan siapa saja yang dapat keluar-masuk. Firewall didesain untuk dapat menyaring pada level IP packet, atau mungkin pada protokol layer yang tinggi.

Firewall dapat menggunakan satu atau beberapa metode untuk mengontrol sebuah jaringan:

- Packet filtering

Paket (bagian dari data pada jaringan) di analisis terhadap suatu saringan(aturan).

Paket yang lolos saringan akan dikirim ke sistem penerima, sisanya dibuang.

- Proxy service

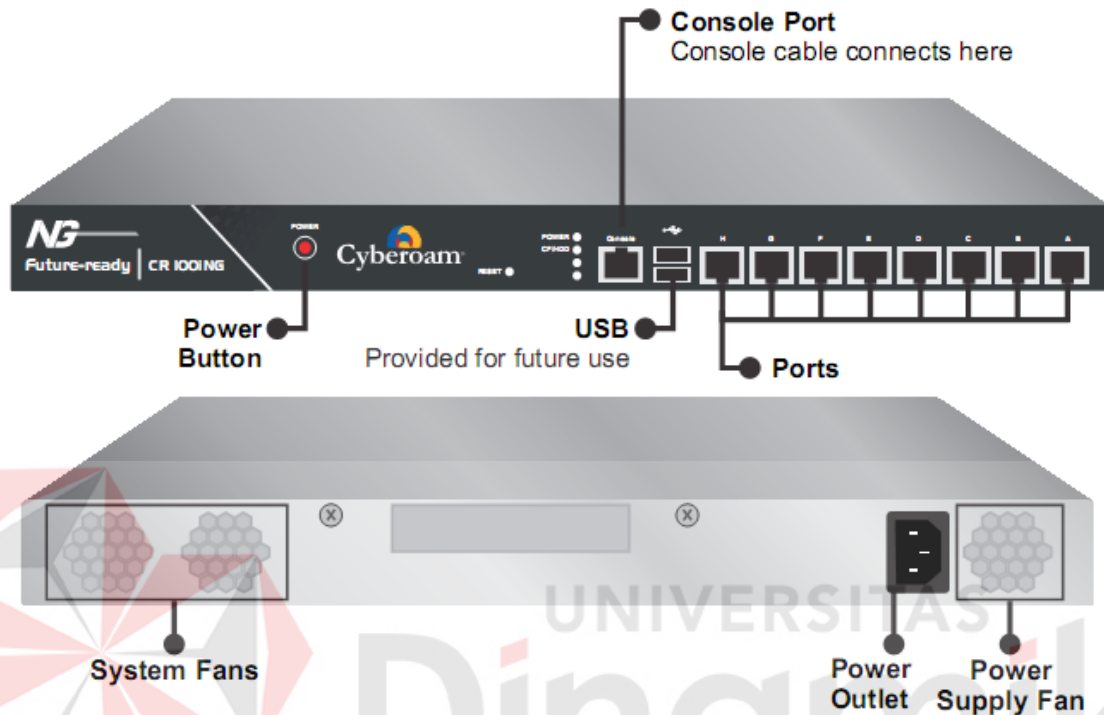
Informasi dari internet diterima oleh firewall dan dikirim ke penerima, juga sebaliknya.

- Stateful Inspection

Membandingkan beberapa bagian dari paket ke database yang berisi informasi yang terpercaya. Jika perbandingan menghasilkan kecocokan yang masuk akal, informasi akan diijinkan lewat. Jika tidak cocok, dibuang. (Oktaviani: 2007, 2)

3.1.1 Cyberoam CR100iNG

Adalah salah satu produk Firewall dari seri UTM (Unified Threat Management) yang menawarkan keamanan, konektivitas, dan produktivitas dengan performa yang dibutuhkan jaringan untuk masa depan. Pada antarmuka (gambar 3.1) terdapat sebuah console port, 2 usb port, dan 8 ethernet port. (Cyberoam: 2017)



Gambar 3.1 Antarmuka Cyberoam CR100iNG

Beberapa fitur Cyberoam CR 100i NG adalah:

- Layer 8 (User - Identity) Firewall
- Multiple Security Zones
- Location-aware and Device-aware Identity-based Access Control Policy
- Access Control Criteria (ACC): User-Identity, Source and Destination Zone, MAC and IP address, Service
- Security policies - IPS, Web Filtering, Application Filtering, Anti-virus, Anti-spam and QoS
- Country-based Traffic Control
- Access Scheduling
- Policy based Source and Destination NAT, Gateway Specific NAT Policy
- H.323, SIP NAT Traversal
- DoS and DDoS attack prevention
- MAC and IP-MAC filtering
- Spoof Prevention
- VPN
- Bandwidth Management
- Logging/Monitoring

3.2 Virtualisasi

Menurut Kamus Besar Bahasa Indonesia, virtual berarti (secara) nyata, sedangkan akhiran –isasi menyatakan makna melakukan, proses, usaha, atau kegiatan. Berarti virtualisasi adalah proses menyatakan atau membuat sesuatu menjadi nyata.

Sedangkan dalam ilmu komputer, virtualisasi bisa diartikan sebagai pembuatan suatu bentuk simulasi dari sesuatu yang asalnya bersifat fisik, misalnya sistem operasi, perangkat penyimpanan data atau sumber daya jaringan. Definisi lainnya adalah "sebuah teknik untuk menyembunyikan karakteristik fisik dari sumber daya komputer dari bagaimana cara sistem lain, aplikasi atau pengguna berinteraksi dengan sumber daya tersebut. Hal ini termasuk membuat sebuah sumber daya tunggal (seperti server, sebuah sistem operasi, sebuah aplikasi, atau peralatan penyimpanan terlihat berfungsi sebagai beberapa sumber daya logikal; atau dapat juga termasuk definisi untuk membuat beberapa sumber daya fisik (seperti beberapa peralatan penyimpanan atau server) terlihat sebagai satu sumber daya logikal."

Dalam ilmu komputer, Ada dua jenis virtualisasi yaitu virtualisasi penuh dan virtualisasi paruh. Virtualisasi penuh maksudnya mensimulasikan secara lengkap hal-hal yang mendasari suatu perangkat, sedangkan virtualisasi paruh hanya mensimulasikan beberapa hal dari perangkat tersebut. Virtualisasi paruh lebih mudah dijalankan daripada virtualisasi penuh, akan tetapi virtualisasi paruh memiliki kekurangan dalam hal compatibility/kesesuaian.

Virtualisasi dapat diimplementasikan ke dalam berbagai bentuk, antara lain:

1. Network Virtualization : VLAN, Virtual IP (untclustering), Multilink
2. Memory Virtualization : pooling memory dari node-node di cluster
3. Grid Computing : banyak komputer = satu
4. Application Virtualization : Dosemu, Wine
5. Storage Virtualization : RAID, LVM
6. Platform Virtualization : virtual computer

Pembahasan selanjutnya dalam buku ini akan terkonsentrasi pada platform virtualization alias virtual computer. Platform virtualization digambarkan sebagai berikut: ada sebuah hardware komputer dengan sistem operasinya (host; control program) yang menciptakan simulasi dari komputer yang lain dengan sistem operasinya sendiri sebagai guest software-nya. Guest

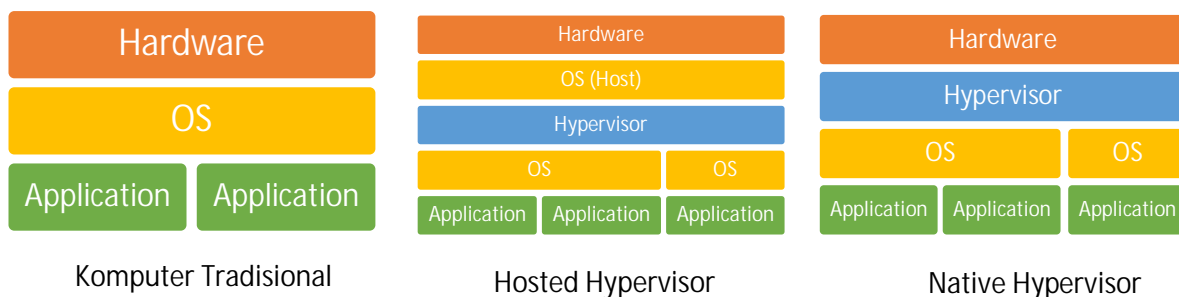
software tidak selalu dibatasi oleh aplikasi pengguna, banyak host yang mengizinkan host mengeksekusi secara lengkap sistem operasinya. Nantinya guest software akan bekerja terhubung dengan hardware yang dimiliki komputer host. Akses dari guest ke system resources seperti akses jaringan, keyboard, disk storage dan sebagainya secara umum akan dikontrol oleh host dengan penggunaan prosesor dan sistem memori yang terbatas.

Beberapa alasan virtualisasi:

1. Dalam hal penggabungan server, banyak server kecil yang digantikan dengan satu server besar dengan tujuan untuk mengurangi jumlah hardware yang memiliki harga tinggi seperti CPU. Meskipun hardware dijadikan satu seperti itu, sistem operasinya tidak digabung. Masing-masing sistem operasi yang berjalan pada satu server tersebut akan menjadi sebuah sistem operasi yang berjalan sendiri secara virtual. Jadi satu server yang besar itu dapat menjadi host bagi beberapa guest.
2. Dengan penggabungan hardware seperti yang diterangkan diatas, kita juga dapat mengurangi penggunaan energi.
3. kita akan lebih mudah mengontrol mesin virtual daripada mengontrol hardware yang sebenarnya, konfigurasi bagi mesin virtual juga lebih fleksibel.
4. Mesin virtual dapat diletakkan pada komputer host lain sesuai kebutuhan kita.
5. Error yang terjadi pada mesin virtual tidak akan membahayakan sistem komputer host, sehingga mesin virtual sangat cocok bagi orang yang hobi utak-atik sistem operasi.

(Hidayati: 2007, 1-3)

Aplikasi komputer dengan arsitektur tradisional menggunakan hardware secara langsung melalui OS. Sedangkan komputer dengan arsitektur virtualisasi menggunakan hardware yang di kelola oleh hypervisor. Untuk lebih jelasnya dapat dilihat pada gambar 3.2.



Gambar 3.2 Perbedaan Arsitektur Komputer

Pada gambar 3.2 terdapat dua tipe virtualisasi yaitu *Native* dan *Hosted*. *Native Hypervisor* mengelola langsung hardware yang kemudian digunakan oleh OS virtualnya. *Hosted Hypervisor* mengelola hardware melalui OS Host seperti aplikasi biasa, sedangkan OS virtual berjalan sebagai *process*.

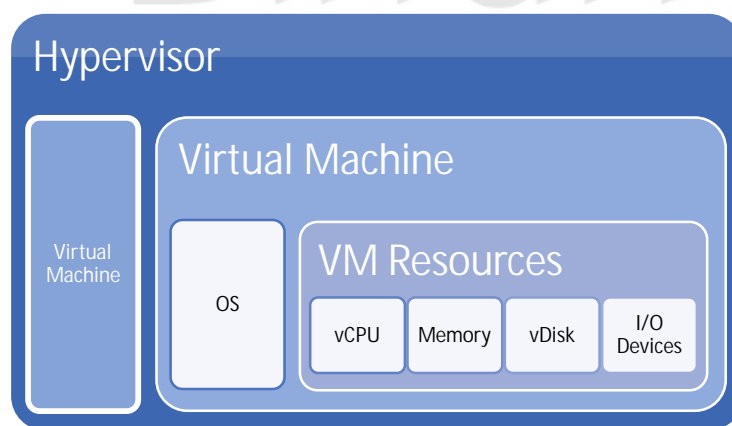
3.2.1 Hypervisor (Virtual Machine Monitor)

Adalah *software*, *hardware* atau *firmware* yang membuat dan menjalankan *virtual machine*. Istilah hypervisor dimaksudkan sebagai supervisor dari supervisor. Terdapat beberapa hypervisor yang dipakai secara umum seperti: Microsoft HyperV, Linux KVM, VMWare ESXi, Nutanix AHV, dan sebagainya.

AHV (Acropolis Hypervisor) adalah salah satu hypervisor gratis yang dirancang untuk infrastruktur hyperconverged Nutanix Server.

3.2.2 Virtual Machine

Virtual machine adalah komputer yang bersifat virtual; mempunyai arsitektur dan fungsi seperti komputer fisik tetapi tidak memiliki fisik secara langsung, bergantung pada fisik host. Adapun arsitekturnya dapat dilihat pada gambar 3.3.



Gambar 3.3 Arsitektur Komputer Virtual

3.3 Server

Server adalah perangkat atau program komputer yang melayani program atau perangkat lain yang disebut *Client*. Server memiliki banyak fungsi seperti: *sharing data and resource* dan

komputasi. Komputer yang digunakan sebagai server harus lebih kuat dan lebih handal dari komputer biasa. Alternatifnya dapat menggunakan cluster (gabungan beberapa node komputer) yang lebih simpel, dengan komponen yang dapat diganti. Beberapa contoh server misalnya: *database server*, *file server*, *mail server*, *print server*, *web server*, *application server*, dan sebagainya.

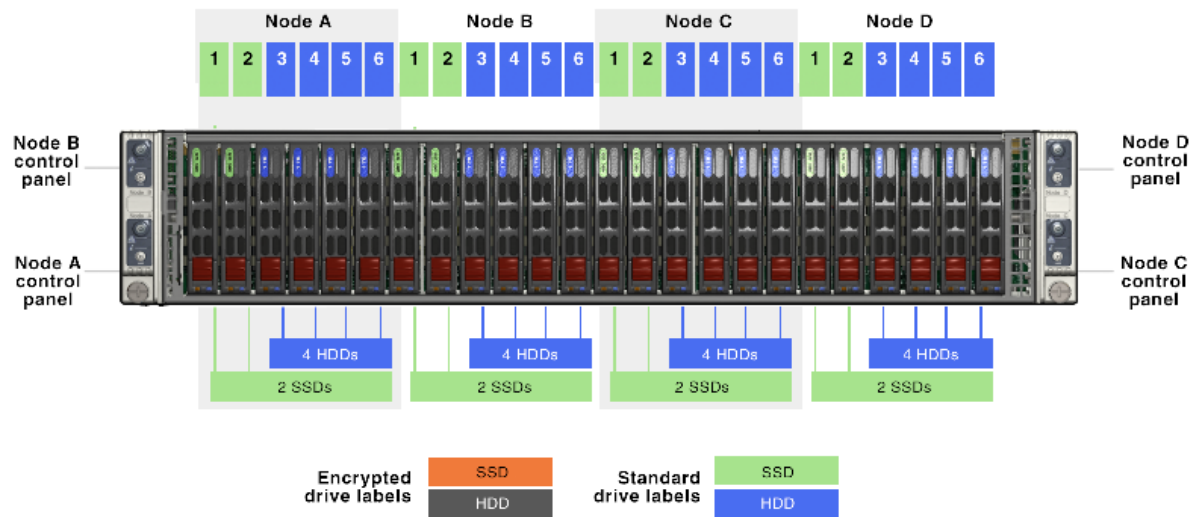
3.3.1. Nutanix Server

Nutanix server adalah salah satu merk server yang mengedepankan *high availability* dan *hyperconverged*. *High availability* adalah tingkat kehandalan yang tinggi, maksudnya server mempunyai *down time* (waktu mati) yang sangat rendah. Hal tersebut dapat dicapai dengan mengaplikasikan *backup device*. Sedangkan *hyperconverged* adalah sistem penyatuan server dan storage dalam satu perangkat. Tujuannya adalah membuat platform yang sederhana dan mudah didistribusikan untuk virtualisasi.

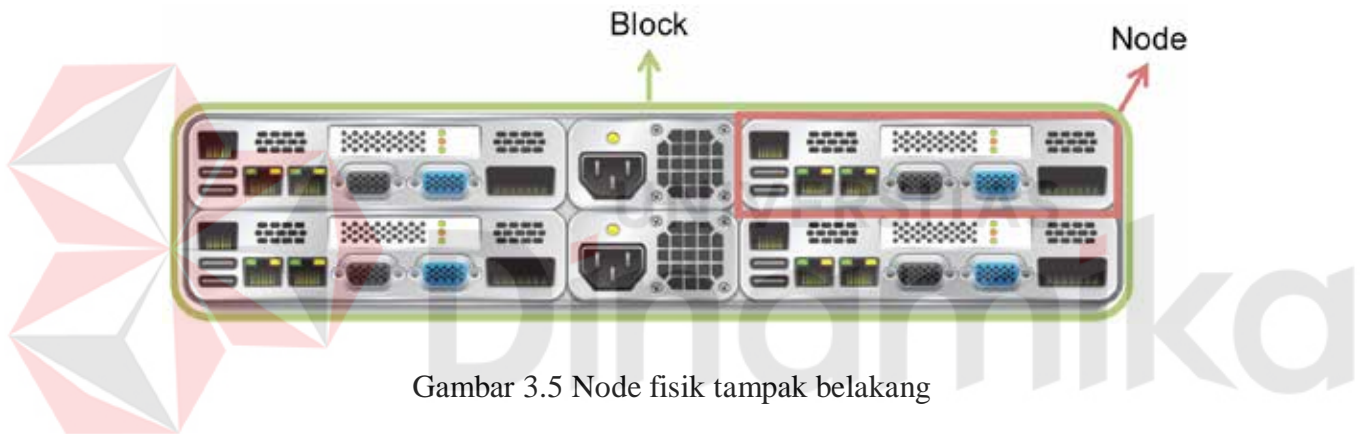
Pada perkembangannya, infrastruktur data center mengalami banyak perubahan. Sistem yang kompleks membutuhkan banyak tempat dan biaya untuk tetap berjalan. Semakin lama, kebutuhan data center semakin besar. Kemudian muncullah ide untuk membuat sistem yang terintegrasi. Sistem ini menyatukan server dan penyimpanan (*converged*). Pada perkembangan berikutnya, seluruh infrastruktur telah disatukan dalam sebuah *resource pool* (*hyper-converged*).

Keuntungan infrastruktur hyperconverged ialah mengurangi biaya dari peralatan, sambungan kabel, biaya operasional dari manajemen dan infrastruktur. Dari segi fisik, infrastruktur juga semakin sederhana dan memakan sedikit tempat, mengurangi kerumitan sambungan kabel dari berbagai sumber.

Untuk menerapkan hyper-converged dan high availability, nutanix menyatukan seluruh sistem dan dibagi kedalam beberapa **node** seperti pada gambar 3.5 dan gambar 3.6. Setiap node menjalankan sebuah *hypervisor* yang berisi hardware komputer (processor, memory, network interface, dan penyimpanan lokal (SSD dan HDD)). Kumpulan node dikelola dalam sebuah **block**. (Nutanix: 2017)



Gambar 3.4 Node fisik tampak depan



Gambar 3.5 Node fisik tampak belakang

BAB IV

PEMBAHASAN

4.1. Langkah-langkah Penulisan Modul

Berikut ini adalah langkah-langkah penulisan modul:

1. Riset dan kajian pustaka

Penulis melakukan riset dan kajian pustaka mengenai definisi Firewall dan Server, konsep virtualisasi, dan fitur-fitur hardware.

2. Praktik konfigurasi pada Hardware dan Software

Pada tahap ini dilakukan instalasi dan konfigurasi pada hardware firewall dan server dan pengecekan konfigurasi agar tepat guna.

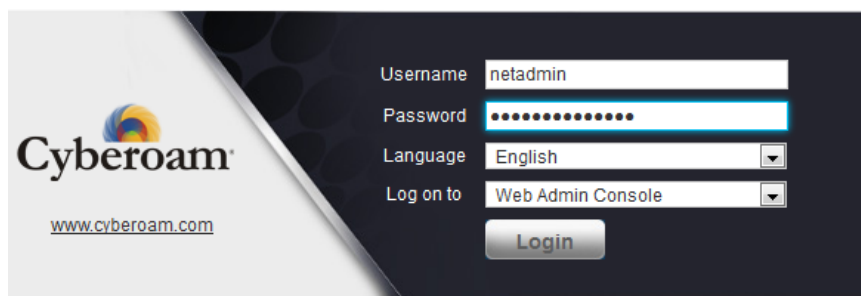
3. Penulisan modul

Penulisan buku termasuk merancang kerangka buku hingga penulisan.

4.2. Konfigurasi pada Hardware

4.2.1. Pengaturan Cyberoam CR100iNG melalui WebAdmin

Login ke cyberoam WebAdmin seperti pada gambar 4.1 (default address: 172.16.16.16, username: admin, password: admin)



Gambar 4.1 Tampilan Login

Pengaturan Host

Mengatur IP Host, IP Host Group, MAC Host, dan lainnya untuk nantinya dijadikan target sebuah rule (aturan) seperti pada gambar 4.2.

Cyberoam
CR100iNG - 10.6.2 MR-1

IP Host | IP Host Group | MAC Host | FQDN Host | FQDN Host Group | Country Host

OBJECTS

- **Hosts**
- Services
- Schedule
- File Type

NETWORK

IDENTITY

FIREWALL

VPN

IPS

WEB FILTER

APPLICATION FILTER

WAF

IIM

QoS

ANTI VIRUS

Add **Delete**

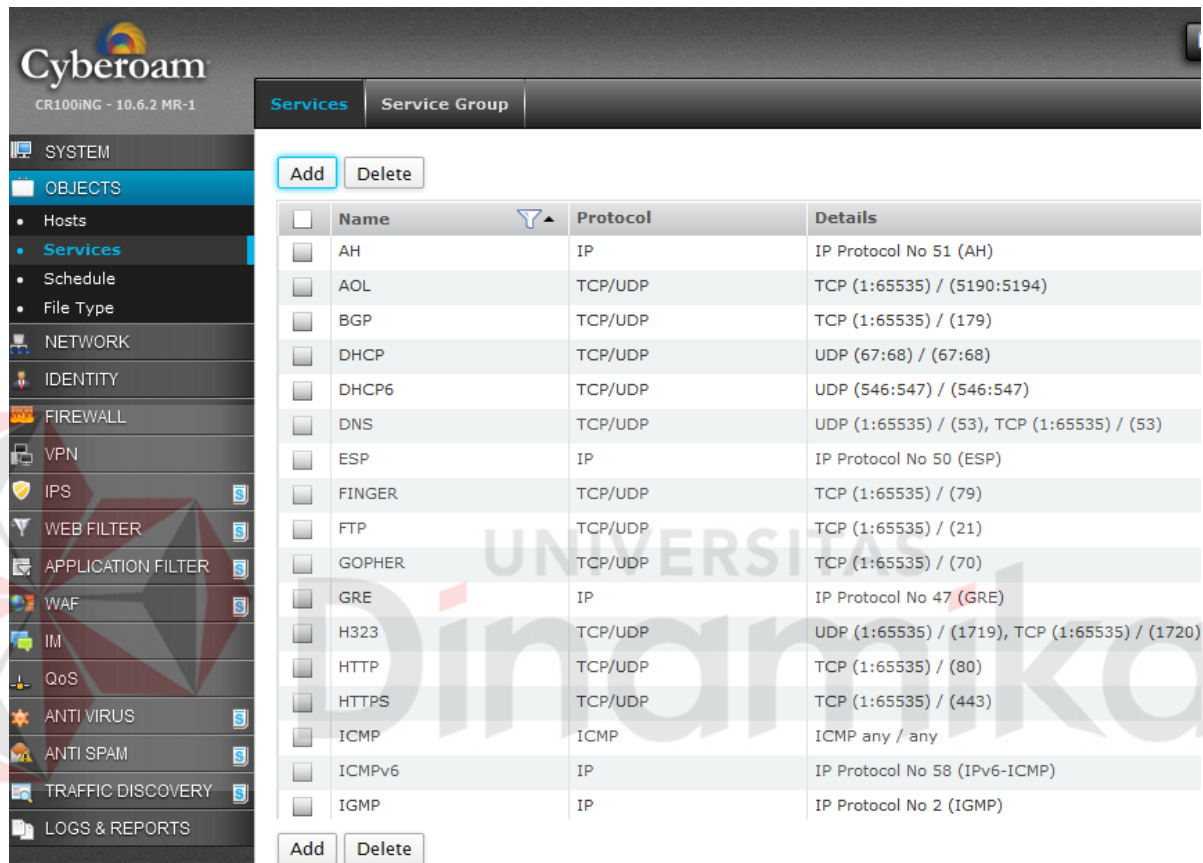
<input type="checkbox"/>	Name	Type	Address Detail
<input type="checkbox"/>	##ALL_IPSEC_RW	System Host	NA
<input type="checkbox"/>	##ALL_RW	System Host	NA
<input type="checkbox"/>	##ALL_SSLVPN_RW	System Host	NA
<input type="checkbox"/>	#PortA	System Host	172.16.16.16/255.255.255.255
<input type="checkbox"/>	#PortB	System Host	10.117.15.1/255.255.255.255
<input type="checkbox"/>	#PortC	System Host	NA
<input type="checkbox"/>	#PortD	System Host	NA
<input type="checkbox"/>	#PortE	System Host	NA
<input type="checkbox"/>	#PortF	System Host	NA
<input type="checkbox"/>	#PortG	System Host	NA
<input type="checkbox"/>	#PortH	System Host	36.66.127.58/255.255.255.255

Add **Delete**

Gambar 4.2 Tampilan pengaturan host

Pengaturan Service

Service mengatur Protokol dan Port dari sebuah service yang nantinya dapat diatur dalam rule seperti pada gambar 4.3. Service dapat juga diatur dalam sebuah service group. Service group memungkinkan pengaturan beberapa service dalam 1 grup.

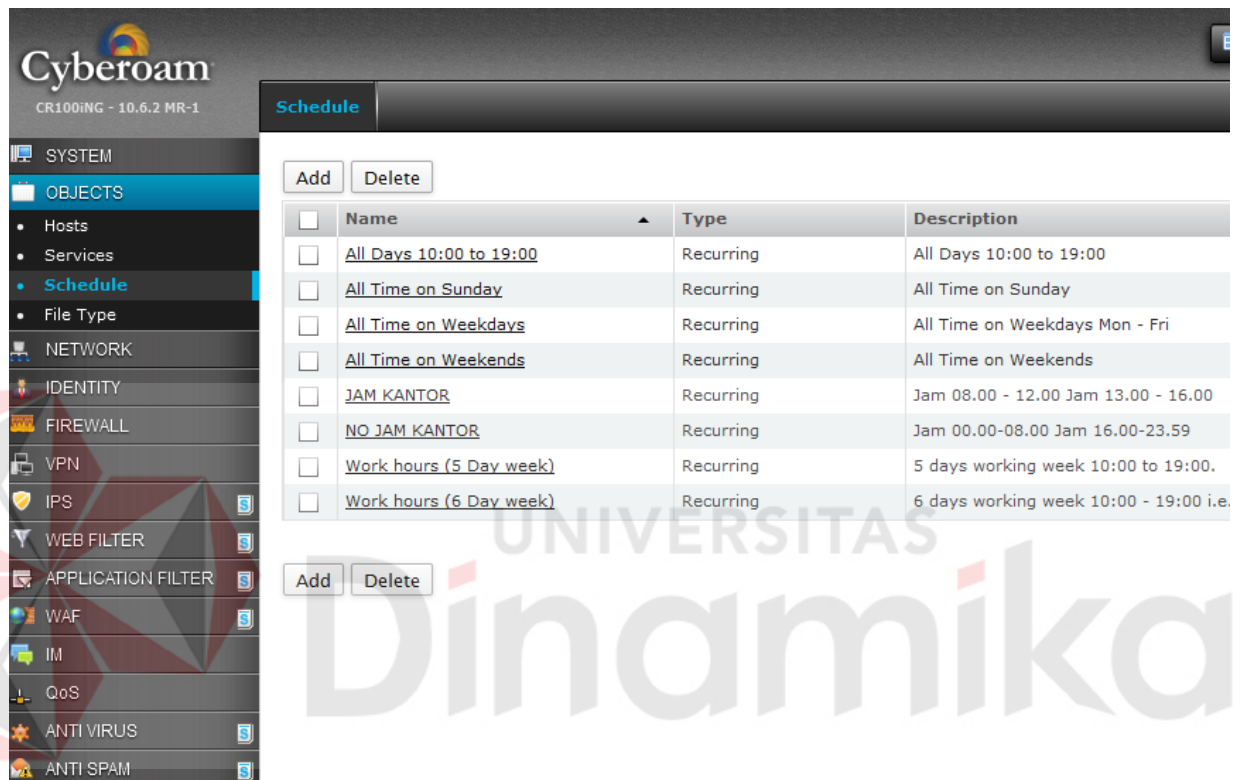


Gambar 4.3 Tampilan Pengaturan Service

Pengaturan Schedule

Schedule adalah jadwal untuk kapan rule akan diterapkan. Dapat menentukan jadwal pada tanggal dan jam spesifik atau berulang pada hari dan jam tertentu.

Misalnya, pada gambar 4.4 di atur jam kantor yaitu jam 8.00 -12.00 dan 13.00-



16.00.

Gambar 4.4 Tampilan pengaturan schedule

Pengaturan Firewall Rule

Membuat peraturan yang membatasi lalu lintas jaringan. gambar 4.5 menampilkan rules yang telah dibuat. Dapat mengatur Network/Host dari asal dan tujuan, Service yang di atur, kapan peraturan berlaku, serta aksi yang dilakukan (**Accept** (Terima/Boleh), **Drop** (Tolak/Larang tanpa balasan), atau **Reject** (Tolak/Larang dengan balasan)). Selain itu juga dapat diatur kebijakan keamanan seperti Aplikasi dan Web filter, IPS (Intrusion Prevention System), Qos (Quality of Services), Routing Policy, dan Log Traffic. Dapat mengatur akses dari IPv4 dan

IPv6. Pada gambar 4.6 adalah pengaturan perizinan akses http, https, dan icmp setiap waktu.

IPv4 Rule		IPv6 Rule					
Add		Delete		Clear All Filters		All Zones ▼ to All Zones ▼ Go	
<input type="checkbox"/>	ID	Rule Name	Enable	Source	Destination	Service	Action
LAN - WAN (Total 4)							
<input type="checkbox"/>	4	ALLOW_DNS	<input checked="" type="checkbox"/>	Any Host	Any Host	DNS	Accept
<input type="checkbox"/>	3	ALLOW_HTTP/S	<input checked="" type="checkbox"/>	Any Host	Any Host	HTTP, HTTPS, ICMP	Accept
<input checked="" type="checkbox"/>	2	#LAN_WAN_LiveUserTraffic	<input checked="" type="checkbox"/>	Any Host	Any Host	Any Service	Drop
<input checked="" type="checkbox"/>	1	#LAN_WAN_AnyTraffic	<input checked="" type="checkbox"/>	Any Host	Any Host	Any Service	Drop
LAN - DMZ (Total 1)							
<input type="checkbox"/>	5	LAN-LAN	<input checked="" type="checkbox"/>	Any Host	Any Host	Any Service	Accept

Gambar 4.5 Tampilan rule untuk Ipv4

Dashboard

IPv4 Rule IPv6 Rule

General Settings

Rule Name

Name * ALLOW_HTTP/S

Description user hanya boleh http/s

Basic Settings

Source

Destination

Zone * LAN

WAN

Attach Identity ☐

Network / Host * Any IP Address

Any IP Address

Services * HTTP,HTTPS,ICMP

Schedule All The Time

Action * ☒ Accept ☐ Drop ☐ Reject

☒ Apply NAT MASQ

Advanced Settings (Security Policies, QoS, Routing Policy, Log Traffic)

Security Policies

Application Filter None

Web Filter General Corporate Policy

IPS None

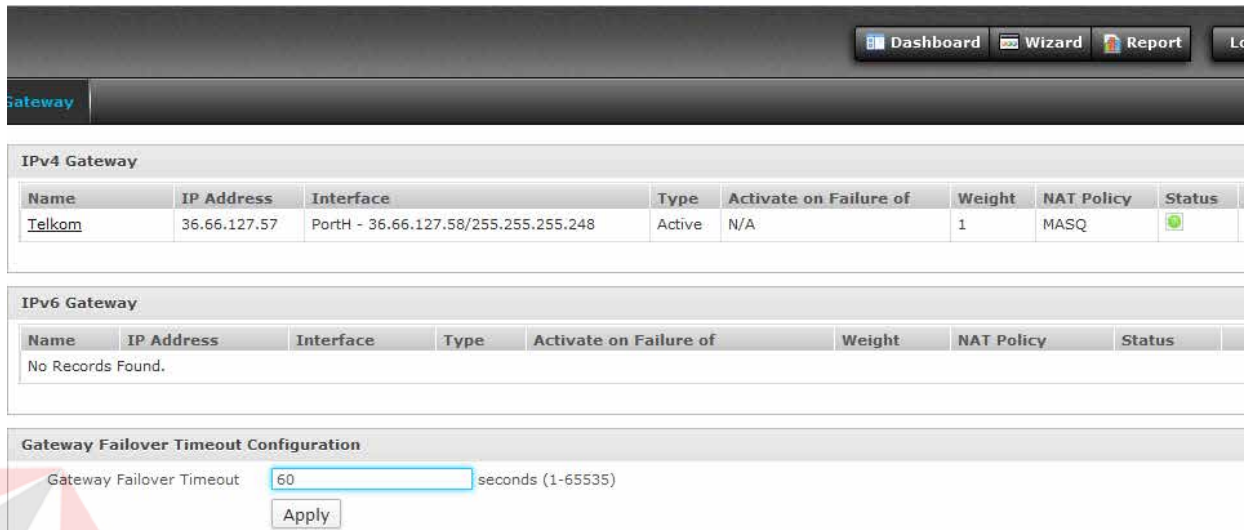
☐ Apply Application based QoS Policy

☐ Apply Web Category based QoS Policy

Gambar 4.6 Pengaturan rule untuk Ipv4


Pengaturan Gateway

Mengatur IP Address serta interface eksternal (jaringan luar) dari jaringan lain atau Internet Service Provider (ISP). Pada gambar 4.7 diatur ISP dari telkom dengan IP 36.66.127.57 ke port H dengan IP 36.66.127.58 dan netmask



The screenshot shows the Mikrotik WinBox Gateway configuration interface. At the top, there are navigation buttons: Dashboard, Wizard, Report, and Log. Below this is a 'Gateway' tab. The main content area is divided into three sections: IPv4 Gateway, IPv6 Gateway, and Gateway Failover Timeout Configuration.

IPv4 Gateway

Name	IP Address	Interface	Type	Activate on Failure of	Weight	NAT Policy	Status
Telkom	36.66.127.57	Porth - 36.66.127.58/255.255.255.248	Active	N/A	1	MASQ	

IPv6 Gateway

Name	IP Address	Interface	Type	Activate on Failure of	Weight	NAT Policy	Status
No Records Found.							

Gateway Failover Timeout Configuration

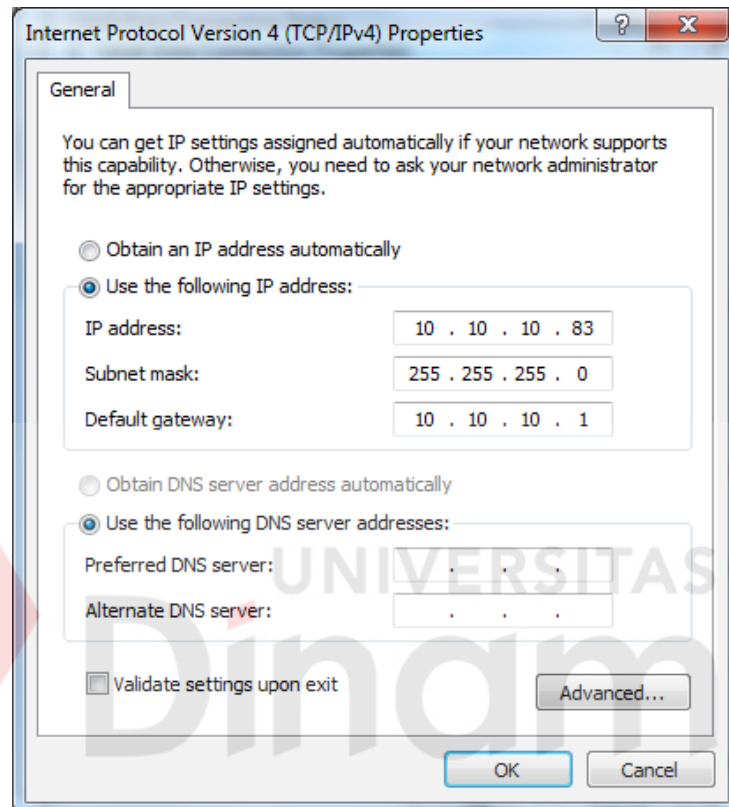
Gateway Failover Timeout: seconds (1-65535)

255.255.255.248.

Gambar 4.7 Tampilan pengaturan Gateway

4.2.2. Instalasi Acropolis Hypervisor pada Nutanix Server

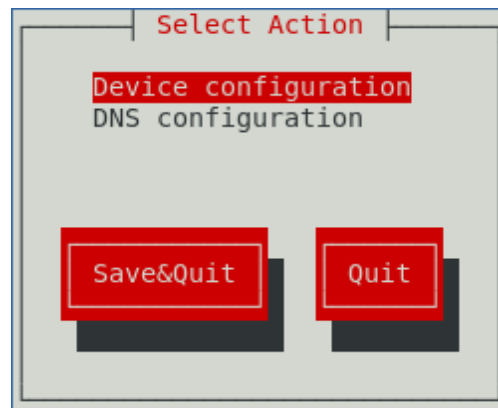
1. Import Foundation VM 3.0 pada VirtualBox
2. Jalankan VM Foundation
3. Konfigurasi IP address pada PC dan Foundation VM dalam satu jaringan
4. Konfigurasi IP address pada PC seperti pada gambar 4.8.



Gambar 4.8 Pengaturan IP address pada PC

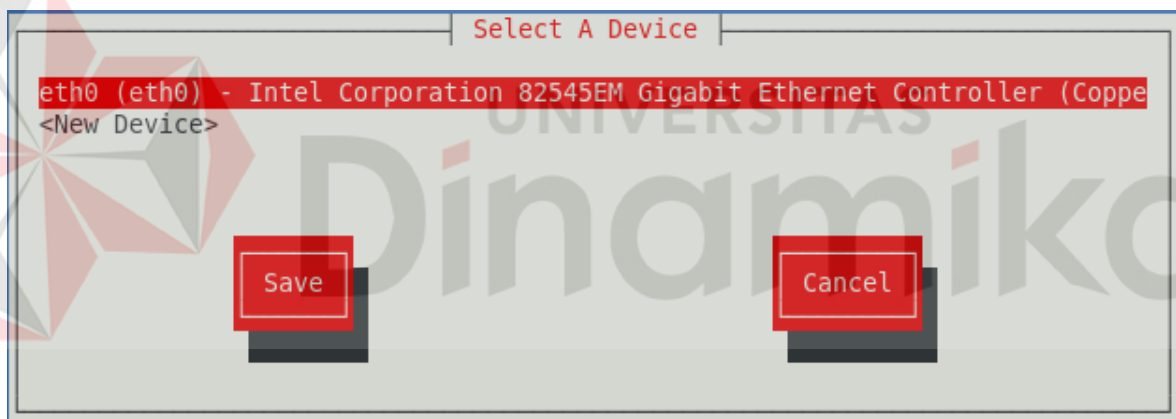
5. Konfigurasi IP address Foundation VM:
 - 5.1. Buka kembali VirtualBox dan login menggunakan user: **nutanix** dan password: **nutanix/4u**
 - 5.2. Klik kanan file **set_foundation_ip_address** pada desktop
 - 5.3. Pilih **run in terminal**

5.4. Setelah muncul terminal dengan tampilan pada gambar 4.9, Pilih **Device configuration** dan tekan enter



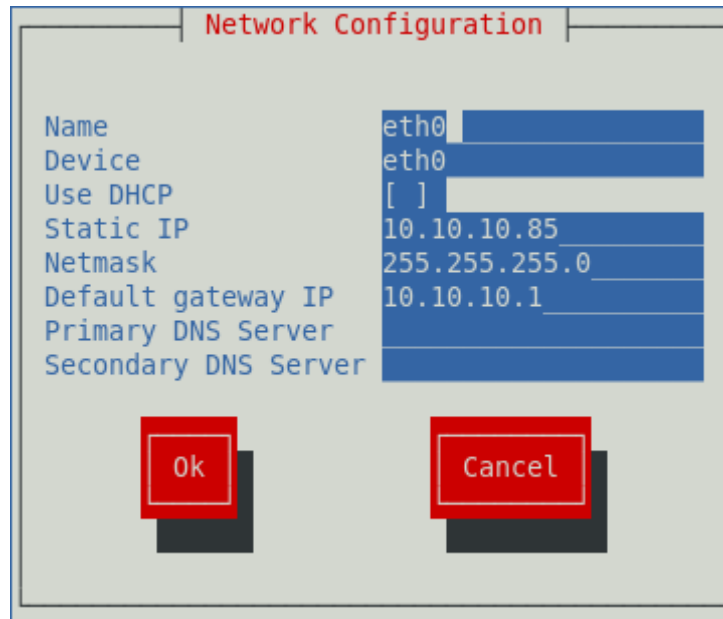
Gambar 4.9 Tampilan terminal

5.5. Pilih device controller yang akan di atur. Pada gambar 4.10 menunjukkan pilihan eth0 (ethernet port 0) dan tekan enter



Gambar 4.10 Pilihan Device controller

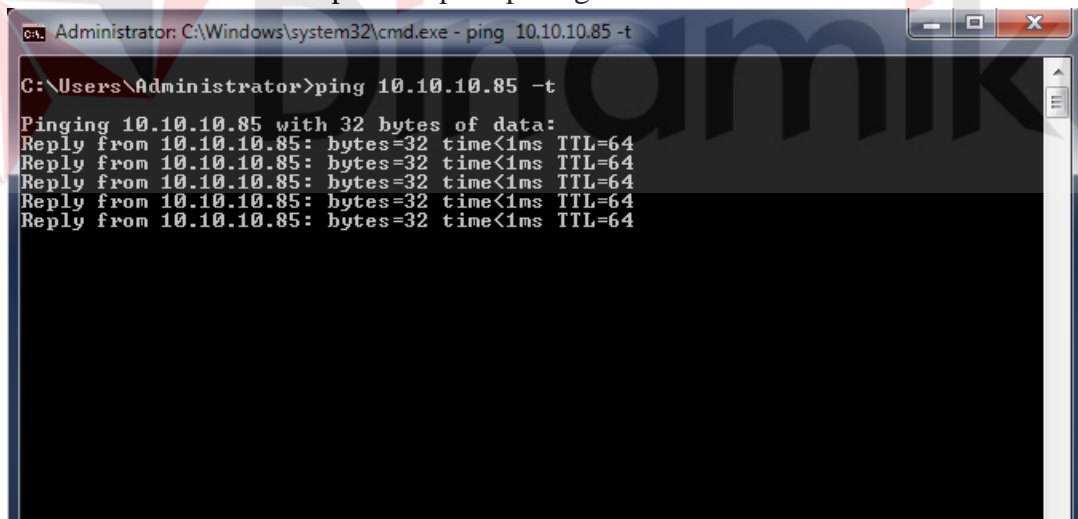
5.6. Isi Network Configuration Foundation VM (**Static IP, Netmask, Default gateway IP**) seperti pada gambar 4.11.



Gambar 4.11 Pengaturan IP address pada Foundation VM

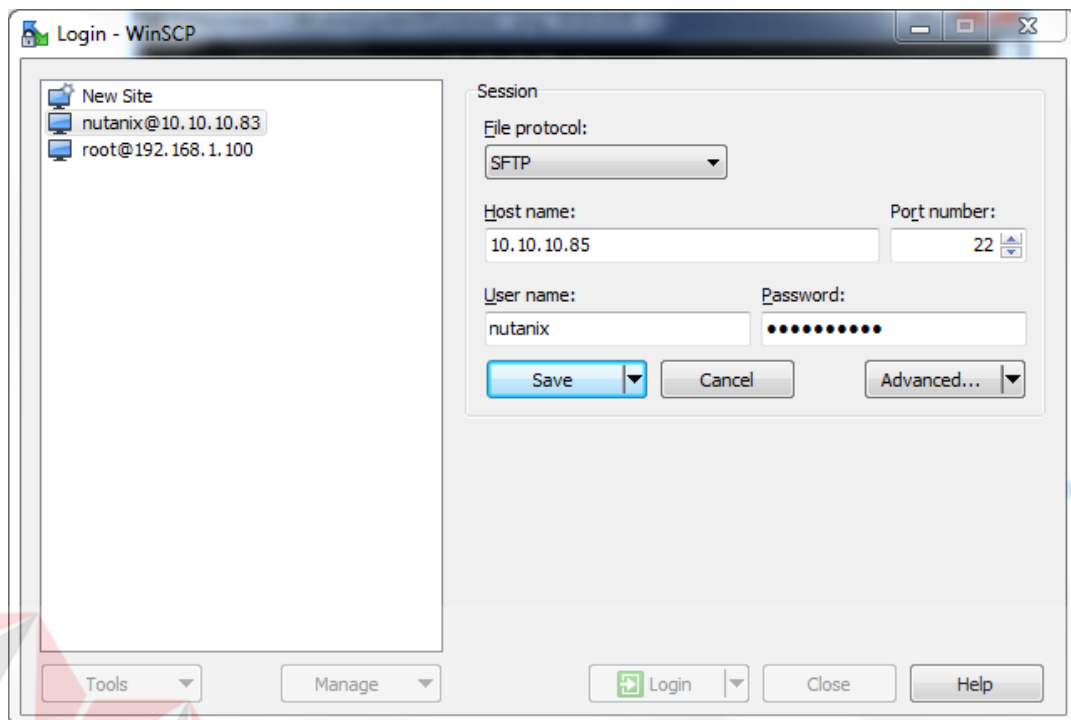
5.7. Enter tombol Ok. Dan tunggu sampai konfigurasi selesai.

5.8. Setelah itu lakukan tes dengan cara ping IP Foundation VM melalui Command Prompt PC seperti pada gambar 4.12.



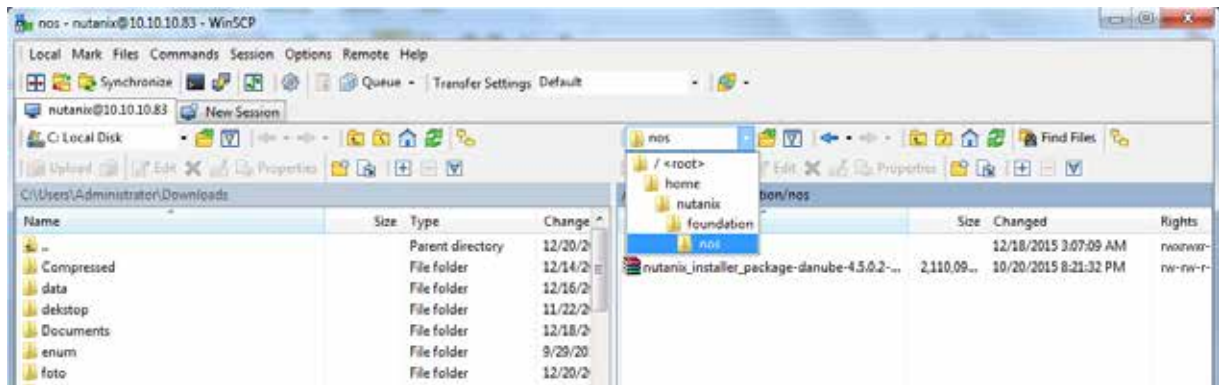
Gambar 4.12 Ping ke IP Foundation VM

5.9. Jika proses tes berhasil, Copy file NOS dan Phoenix yang diperlukan untuk proses deploy seperti pada gambar 4.13



Gambar 4.13 Login pada WinSCP

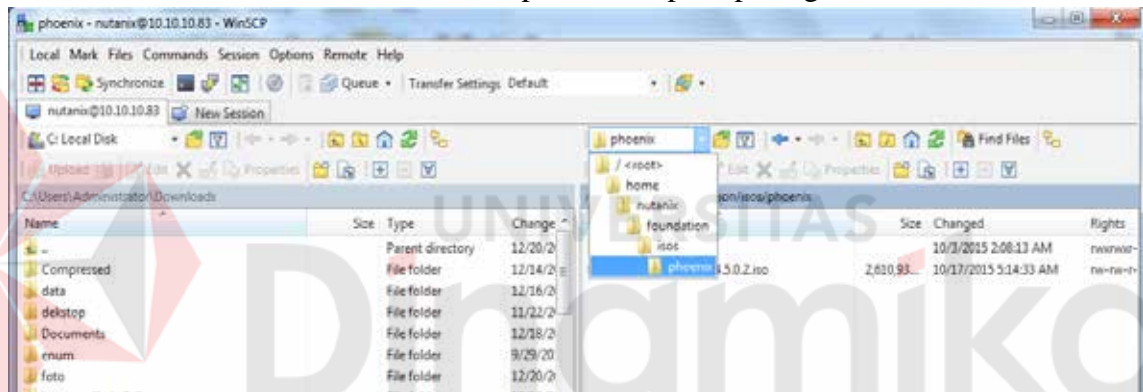
- 5.10. Buka aplikasi WinSCP
- 5.11. Masukkan IP address dari Foundation VM
- 5.12. Save Kemudian klik tombol login. Jika ada perintah untuk memasukkan password isikan dengan **nutanix/4u**
- 5.13. Copy file Nutanix OS 4.5.0.2 ke dalam directory `/home/nutanix/foundation/ nos/` seperti pada gambar 4.14



Gambar 4.14 Proses Copy file Nutanix OS 4.5.0.2

5.14. Copy file Phoenix ke dalam directory

/home/nutanix/foundation/isos/ phoenix/ seperti pada gambar 4.15



Gambar 4.15 Proses copy file phoenix 4.5.0.2.iso

5.15. Jika semua proses copy sudah selesai, Selanjutnya yaitu melakukan deploy ke nutanix.

4.2.3 Pengaturan Nutanix Server

Buka aplikasi firefox ke address **localhost:8000/gui/index.html**. Isikan Global Configuration (Gambar 4.16) dengan gateway dan netmask. Untuk username diisi ADMIN dan password diisi ADMIN. Memory pada CVM diisi

Nutanix Foundation - Mozilla Firefox

Nutanix Foundation

localhost:8000/gui/index.html

Google

ist Visited Centos Wiki Documentation Forums

Global Configuration

Block Common Configuration

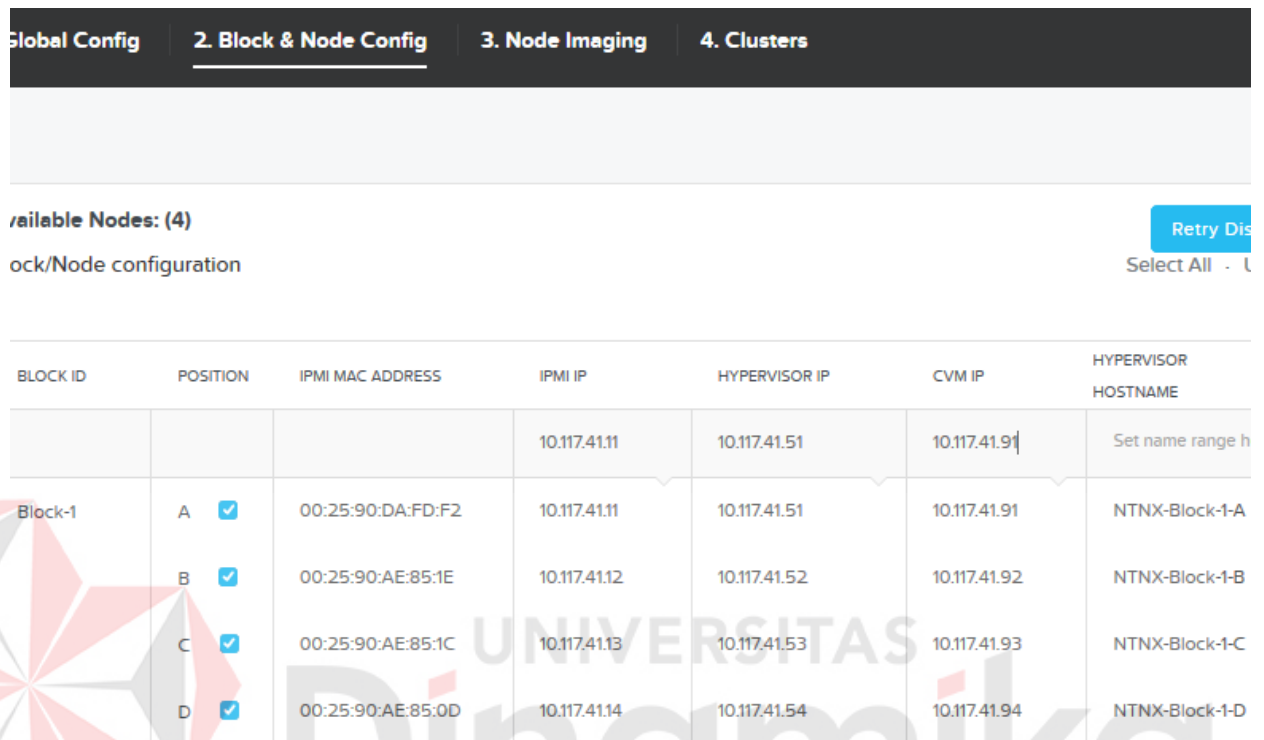
IPMI	HYPERVISOR	CVM
NETMASK: 255.255.255.0	NETMASK: 255.255.255.0	NETMASK: 255.255.255.0
GATEWAY: 10.10.10.1	GATEWAY: 10.10.10.1	GATEWAY: 10.10.10.1
USERNAME: ADMIN	DNS SERVER IP: 10.10.10.1	MEMORY: 24 GB
PASSWORD: ***** Show		

24GB.

Gambar 4.16 Global Configuration

1. Pengaturan Block dan Node

Jumlah node dalam block dapat diatur pada **Node & Block Config**. Pada gambar 4.17 diatur 4 node dalam 1 block.



Global Config 2. Block & Node Config 3. Node Imaging 4. Clusters						
Available Nodes: (4)						
Block/Node configuration						
BLOCK ID	POSITION	IPMI MAC ADDRESS	IPMI IP	HYPERVISOR IP	CVM IP	HYPERVISOR HOSTNAME
Block-1	A	00:25:90:DA:FD:F2	10.117.41.11	10.117.41.51	10.117.41.91	Set name range h
	B	00:25:90:AE:85:1E	10.117.41.12	10.117.41.52	10.117.41.92	NTNX-Block-1-B
	C	00:25:90:AE:85:1C	10.117.41.13	10.117.41.53	10.117.41.93	NTNX-Block-1-C
	D	00:25:90:AE:85:0D	10.117.41.14	10.117.41.54	10.117.41.94	NTNX-Block-1-D

Gambar 4.17 Block Node Configuration

IPMI (Intelligent Platform Management Interface) adalah kumpulan dari interfaces pada komputer untuk manajemen dan pengawasan tiap CPU, firmware (BIOS atau UEFI), dan OS dari sistem. IPMI dapat diakses melalui MAC Address dan IP tiap node. MAC address dari node tertulis dibawah network interface. **Hypervisor IP** adalah alamat dari Hypervisor tiap node. **CVM** adalah Controller VM yang bertugas untuk mengakses PCI yang umumnya tersambung pada disk tiap node. Untuk mengakses CVM pada jaringan dibutuhkan **CVM IP**. Isikan IPMI IP dengan 10.117.41.11 - 14. Hypervisor IP dengan 10.117.41.91 – 94.

2. Node Imaging

Node Imaging adalah proses menginstall hypervisor yang diinginkan pada setiap node. Pada gambar 4.18 menunjukkan cara pemasangan AHV, Acropolis Hypervisor untuk server Nutanix. Pada tahap node imaging ditentukan File acropolis package pada folder /foundation/nos dan File hypervisor iso image pada folder /foundation/isos/hypervisor.

Global Config 2. Block & Node Config 3. Node Imaging 4. Clusters

Node Imaging

ISO Selection

AHV Refr

ACROPOLIS PACKAGE ~ /foundation/nos nutanix_installer_package-release-danube-4.6.

HYPERVISOR ISO IMAGE ~ /foundation/isos/hypervisor host-bundle-el6.nutanix.20160217.tar.gz

< Prev

Gambar 4.18 Node Imaging

3. Menentukan Cluster

Cluster adalah kelompok host(node) untuk menjaga server agar tetap bersifat highly available.

Assign Nodes and Blocks to created clusters

Cluster creation

CLUSTER NAME	EXTERNAL IP	CVM DNS SERVERS	CVM NTP SERVERS	HYPERVISOR NTP SERVERS	MAX REDUNDANCY FACTOR	DEL
CL-NUTANIX	10.117.41.10	10.199.21.254	10.199.252.5	10.199.252.5	2	X

Create New Cluster

Post Image Testing

☐ Diagnostics ☐ NCC

Assigned to CL-NUTANIX (Based on the redundancy factor, select at least 3 nodes.) Select All - Unselect All

BLOCK AND NODES	IPMI MAC ADDRESS	IPMI IP	HYPERVISOR IP	CVM IP	HOST NAME	
Block-1	<input checked="" type="checkbox"/>					
A	<input checked="" type="checkbox"/>	00:25:90:DA:FD:F2	10.117.41.11	10.117.41.51	10.117.41.91	NTNX-Block-1-A
B	<input checked="" type="checkbox"/>	00:25:90:AE:85:1E	10.117.41.12	10.117.41.52	10.117.41.92	NTNX-Block-1-B
C	<input checked="" type="checkbox"/>	00:25:90:AE:85:1C	10.117.41.13	10.117.41.53	10.117.41.93	NTNX-Block-1-C
D	<input checked="" type="checkbox"/>	00:25:90:AE:85:00	10.117.41.14	10.117.41.54	10.117.41.94	NTNX-Block-1-D

Gambar 4.19. Cluster creation

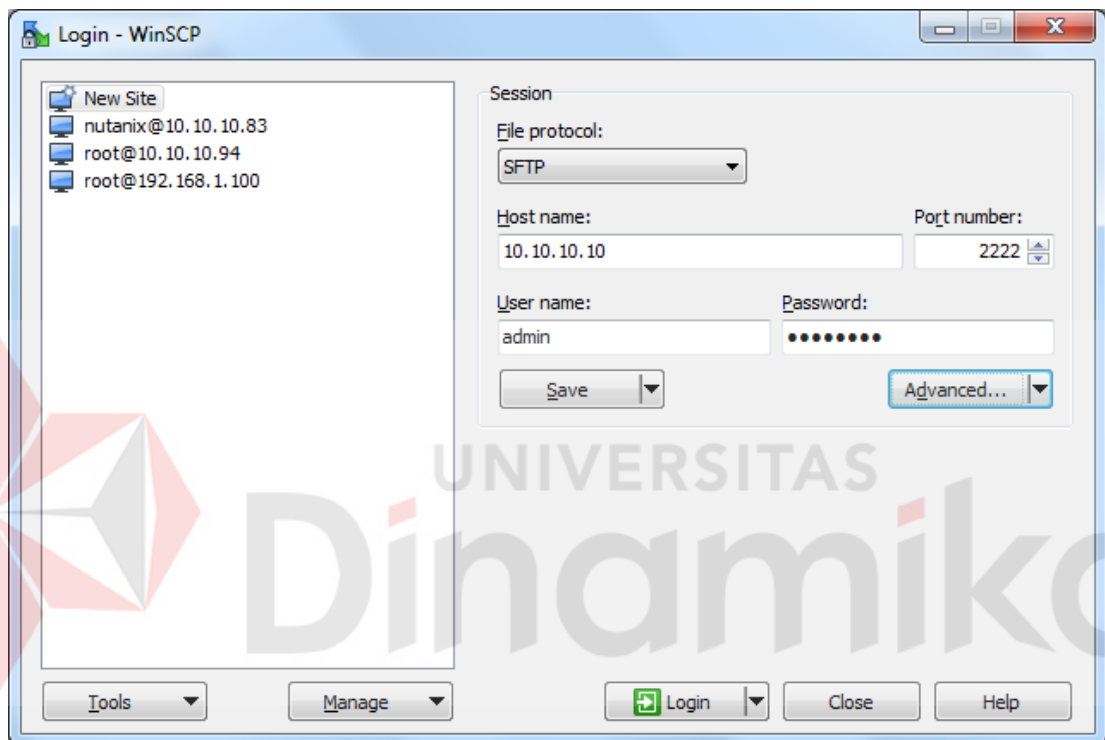
Pada gambar 4.19, **CVM DNS Server** adalah alamat server DNS pada jaringan, **CVM NTP Server** adalah alamat NTP server pada jaringan. **Max redundancy factor** (Slave Host) adalah jumlah host backup maksimum untuk menjaga redundansi data dari host utama (Master Host). Setelah menentukan Pengaturan dasar Cluster, selanjutnya memilih block dan node yang akan digunakan pada cluster tersebut. Misal dalam satu cluster mempunyai max redundancy factor bernilai 2, maka minimal cluster harus mempunyai minimal 3 node (1 Master Host + 2 Slave Host).

Setelah selesai klik tombol “Run Installation” pada pojok kanan atas, tunggu proses sampai selesai. Jika proses deploy gagal, coba lakukan konfigurasi dari awal dan cek kembali IPMI MAC ADDRESS apakah sudah benar. Selanjutnya lakukan tes dengan membuka web browser pada PC dengan memasukkan alamat cluster: 10.10.10.10:9440 untuk mengakses halaman dari prism web console dari Nutanix atau dengan alamat tiap VM: 10.10.10.31, 10.10.10.32, 10.10.10.33, 10.10.10.34.

4.3. Konfigurasi Software

Untuk men-copy file iso OS dengan menggunakan WINSCP dapat dilihat pada gambar 4.22.

1. Masukkan Hostname. (Masukkan IP Cluster dari Nutanix)
2. Masukkan port 2222
3. Masukkan username dan password yang digunakan ketika autentikasi pada prism. (username: admin & password: nutanix/4u)
4. Klik tombol login.
5. Dan copy kan file iso pada container.

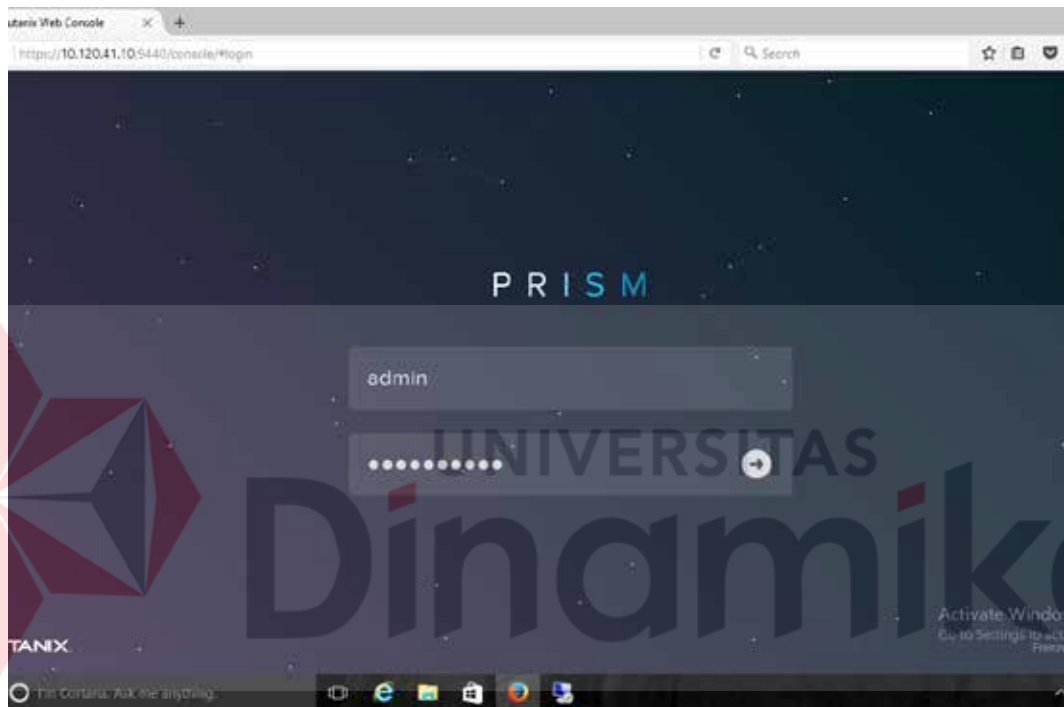


Gambar 4.21 Login WinSCP ke PRISM

4.3.1. *Virtual Machine pada AHV*

Pembuatan Virtual Machine pada UI Prism cukup mudah, hanya memasukkan data-data yang menyangkut spesifikasi komputer virtual sesuai keperluan. Berikut panduan membuat virtual machine dari *ISO* yang sudah ada.

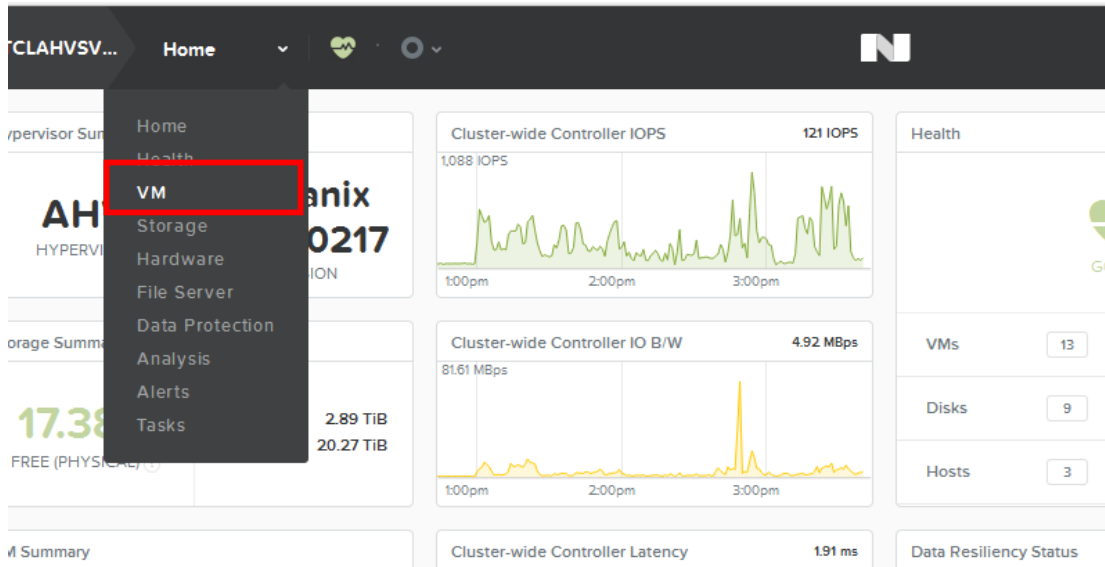
1. Buka browser dan akses link Prism <https://10.134.41.10:9440/console> seperti pada gambar 4.22.



Gambar 4.22 Tampilan Login PRISM

2. Masukkan username: admin dan password: nutanix/4u
3. Tekan enter.

4. Kemudian akan muncul halaman dashboard prism nutanix seperti pada gambar 4.23 dan klik menu VM.



Gambar 4.23 Dashboard PRISM

5. Kemudian klik Tab Table.
6. Setelah itu klik tombol + Create VM yang berada di pojok kanan atas.

The screenshot shows the 'VM' tab selected in the Prism dashboard. At the top right, the '+ Create VM' button is highlighted with a red box. Below the navigation bar, there is a table listing VMs. The table has columns for USED STORAGE, CPU USAGE, CONTROLLER READ IOPS, CONTROLLER WRITE IOPS, CONTROLLER IO BANDWIDTH, CONTROLLER AVG IO LATENCY, and BACKUP A... The table contains 10 rows of data, with the first row showing 20.24 GiB storage usage and 13.27% CPU usage.

USED STORAGE	CPU USAGE	CONTROLLER READ IOPS	CONTROLLER WRITE IOPS	CONTROLLER IO BANDWIDTH	CONTROLLER AVG IO LATENCY	BACKUP A...
20.24 GiB	13.27%	0	6	88 KBps	1.27 ms	Yes
1.68 TiB	17.63%	70	14	3.43 MBps	1.97 ms	Yes
8.13 GiB	-	-	-	-	-	Yes
1.83 GiB	-	-	-	-	-	Yes
1.82 GiB	-	-	-	-	-	Yes
8.16 GiB	-	-	-	-	-	Yes

Gambar 4.24 Tampilan VM table list



General Configuration

NAME
JKTTEST

DESCRIPTION
Optional

Compute Details

VCPUS
2

NUMBER OF CORES PER VCPU
2

MEMORY
4 GIB

Disks
+ Add new disk

TYPE	ADDRESS	PARAMETERS
CDROM		EMPTY=true; BUS=ide

Volume Groups
+ Add volume group

Network Adapters (NIC)
+ Add new NIC

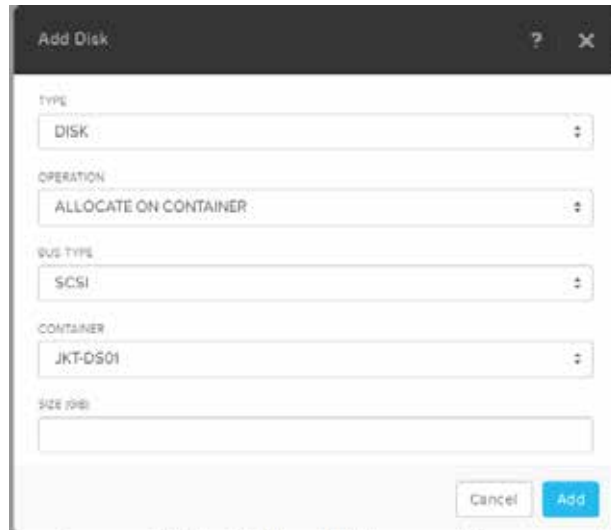
☐ Custom Script

Cancel Save

Gambar 4.25 Tampilain Create VM

Kemudian akan muncul tampilan Create VM seperti pada gambar 4.25. **VCPU** adalah Virtual CPU, yaitu CPU yang digunakan secara logis dari sejumlah CPU fisik. **Cores per CPU** adalah jumlah core per CPU yang digunakan. **Memory** adalah jumlah memory (RAM) dalam GigaByte. **Disks** untuk media penyimpanan disini menggunakan virtual disk atau vDisk.

Gambar 4.26 Tampilan Add Disk

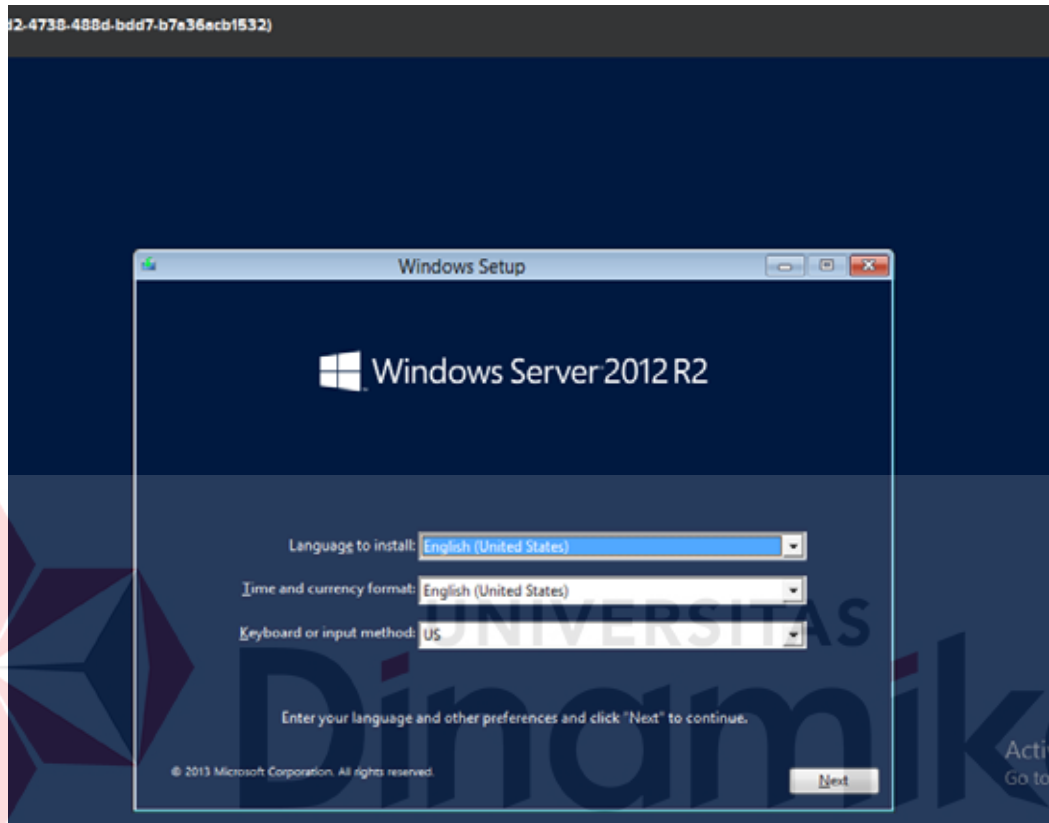


vDisk adalah virtualisasi dari disk fisik. Gambar 4.26 menunjukkan pengaturan penambahan disk. Layaknya disk fisik, vDisk mempunyai karakteristik: **Type** disk, CDRom atau disk. **Operation** adalah cara pembuatan disk, apakah dialokasikan pada container atau pada file iso. **Container** adalah segmentasi logika dari storage pool. Dapat berisi VM atau file (vDisk).

Fungsi utama **Storage pool** adalah sebagai kelompok dari penyimpanan secara fisik misalnya PCIe SSD, SSD, dan HDD untuk cluster. Hanya satu storage pool digunakan pada kebanyakan pengaturan karena storage pool dapat digunakan antar node. Untuk type disk mempunyai karakter: **Bus type**, SCSI atau IDE. **Size**, ukuran disk. **Network Adapter (NIC)** disini adalah kartu jaringan virtual untuk Virtual Machine agar dapat tersambung pada jaringan yang telah diatur pada hypervisor.

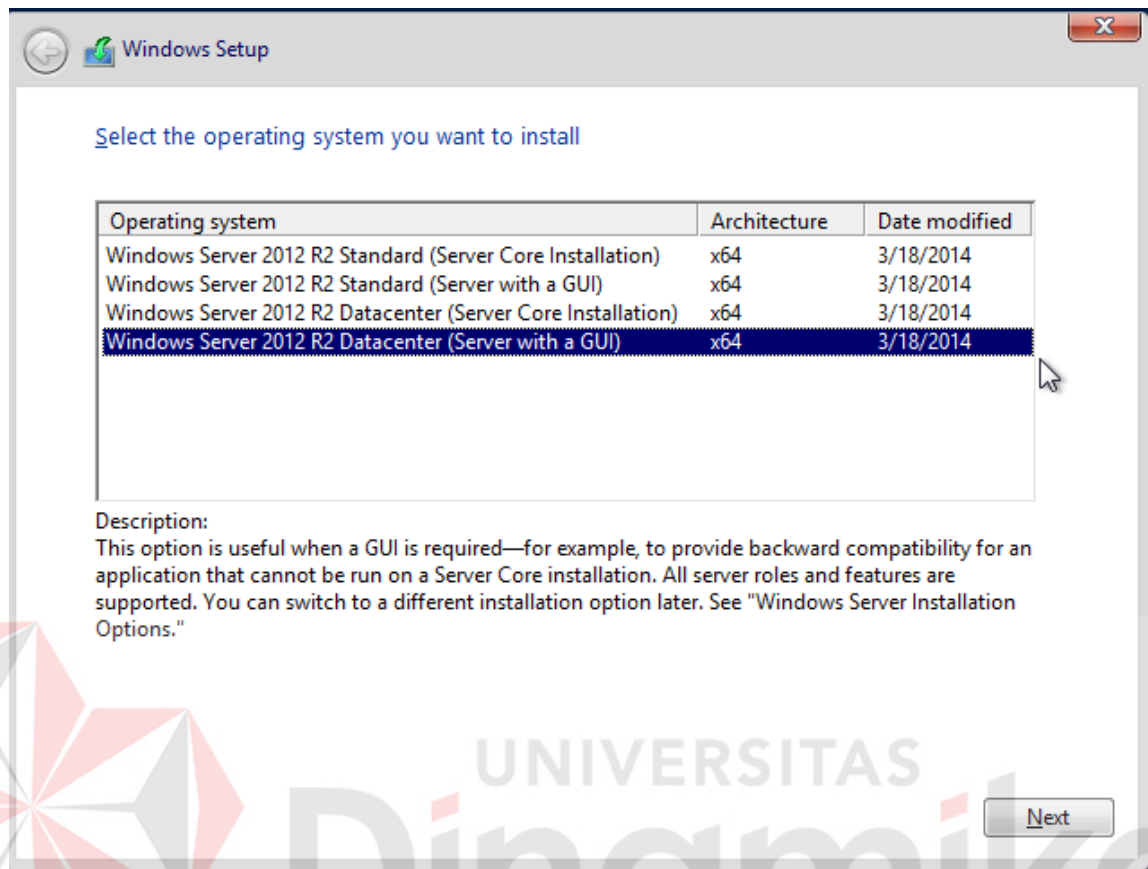
Setelah pengaturan VM selesai, klik save.

7. Klik Power on dan Launch Console. Dan tunggu untuk proses installasi.
8. Pada gambar 4.27 klik Next, kemudian Install Now.



Gambar 4.27 Windows Setup

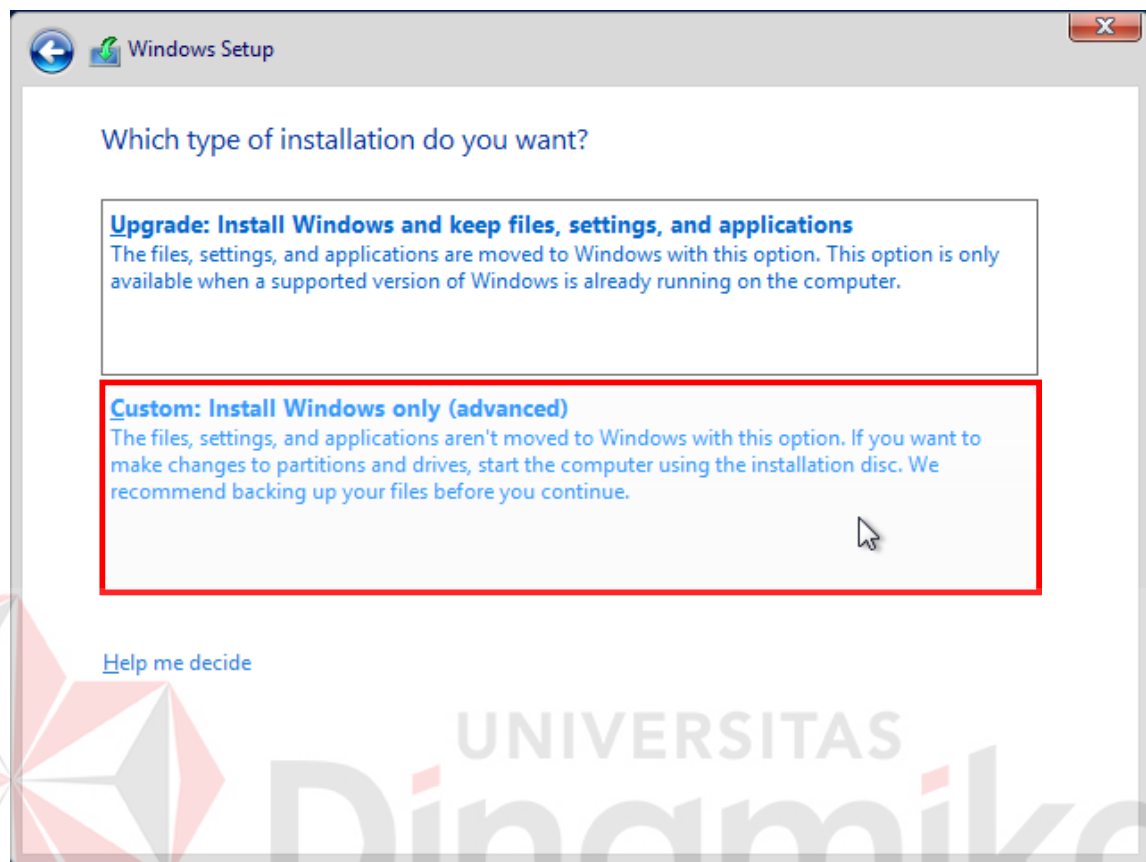
9. Pilih OS yang diinginkan. Dan klik tombol Next seperti pada gambar 4.28



Gambar 4.28 Pilihan OS

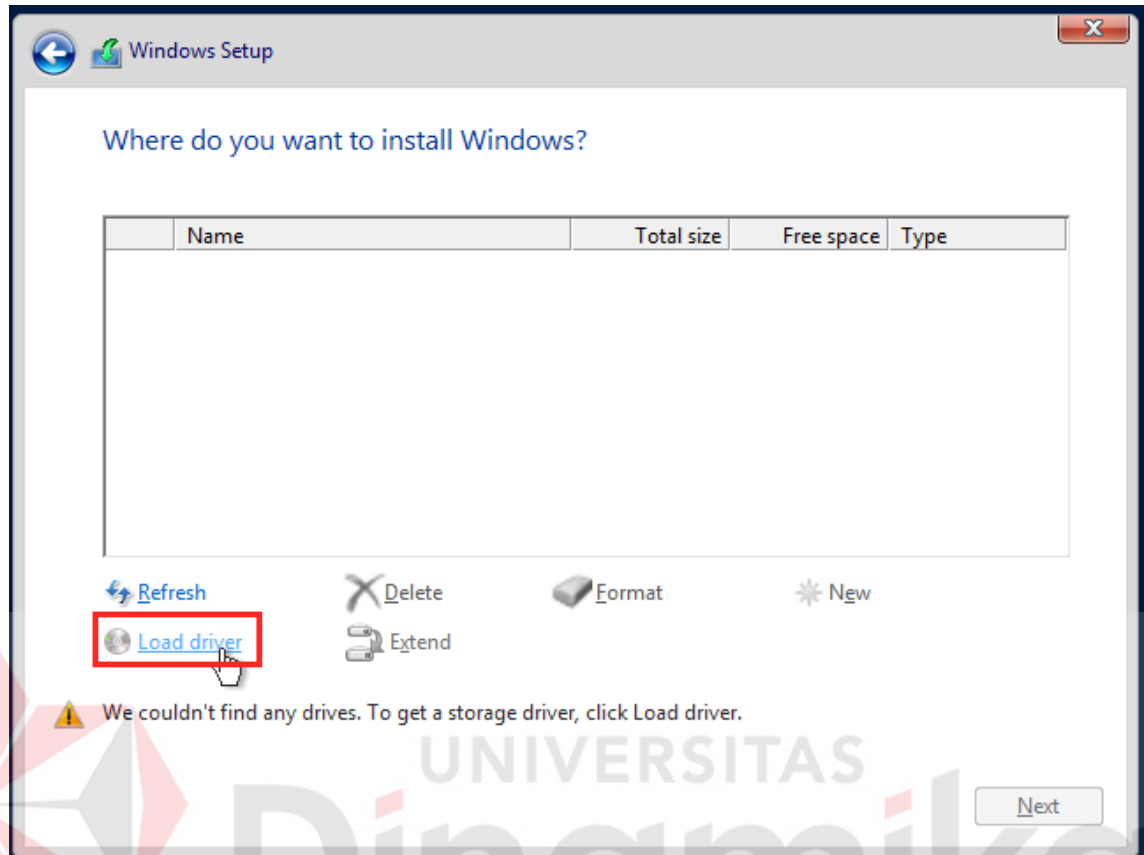
10. Ceklist I Accept the license terms. Dan klik Next.

11. Pilih Custom: Install Windows only (Advanced) seperti pada gambar 4.29.



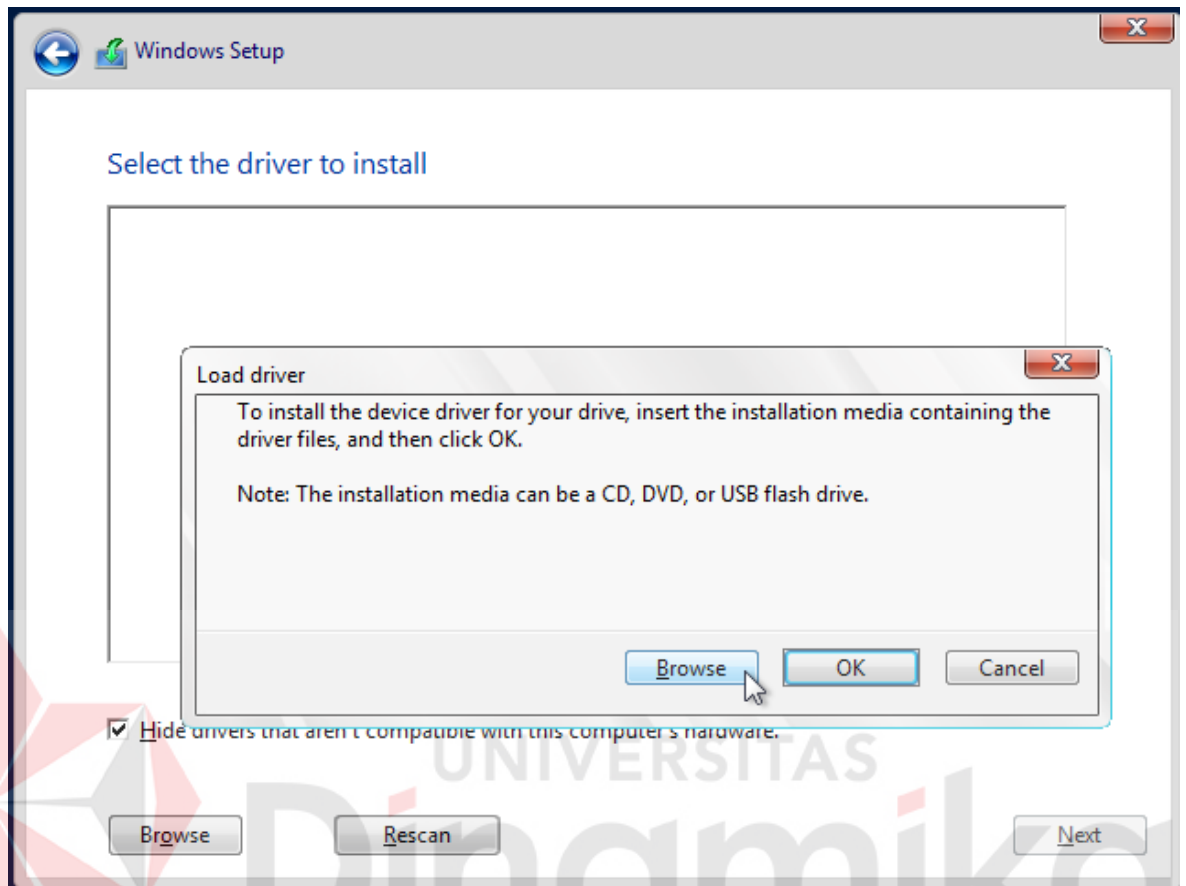
Gambar 4.29 Custom Install

12. Klik Load driver seperti pada gambar 4.30.



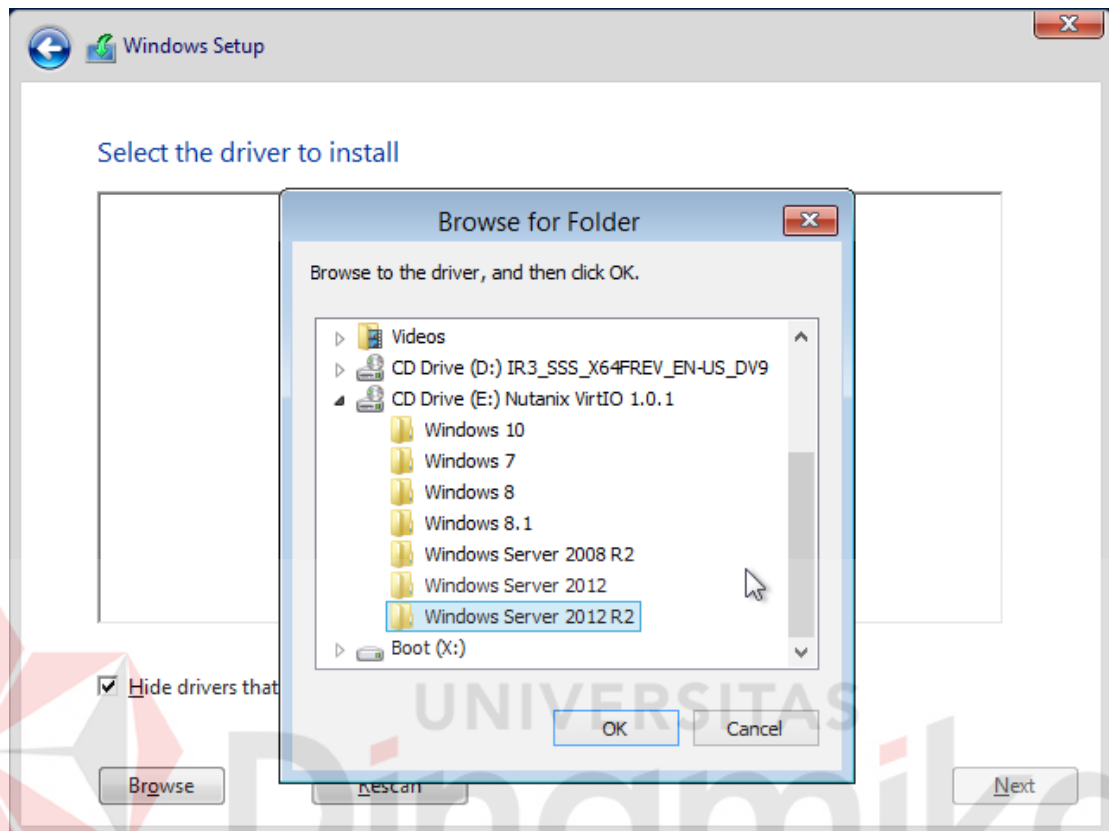
Gambar 4.30 Load driver

13. Klik Browse seperti pada gambar 4.31.



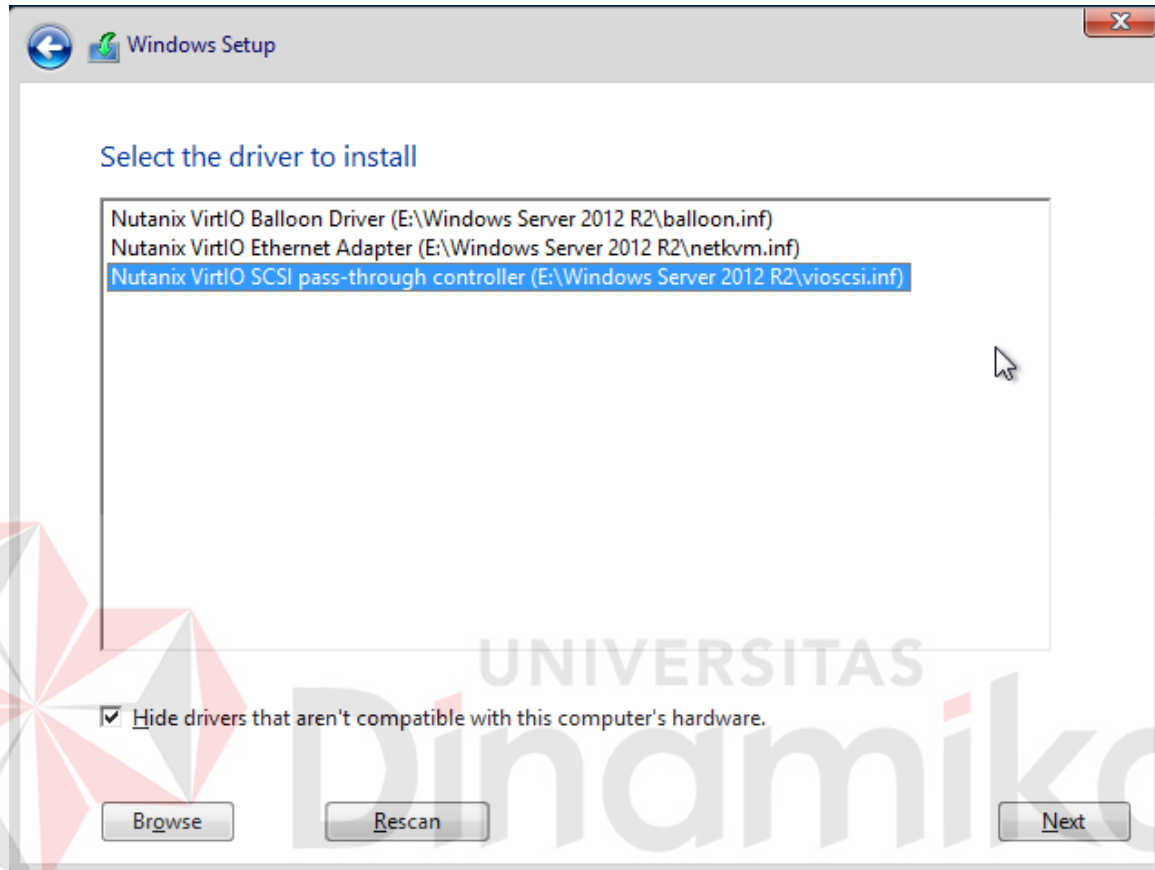
Gambar 4.31 Browse driver

14. Kemudian lihat list seperti pada gambar 4.32 dan pilih versi windows.
(Contoh windows 2012 R2). Klik OK.



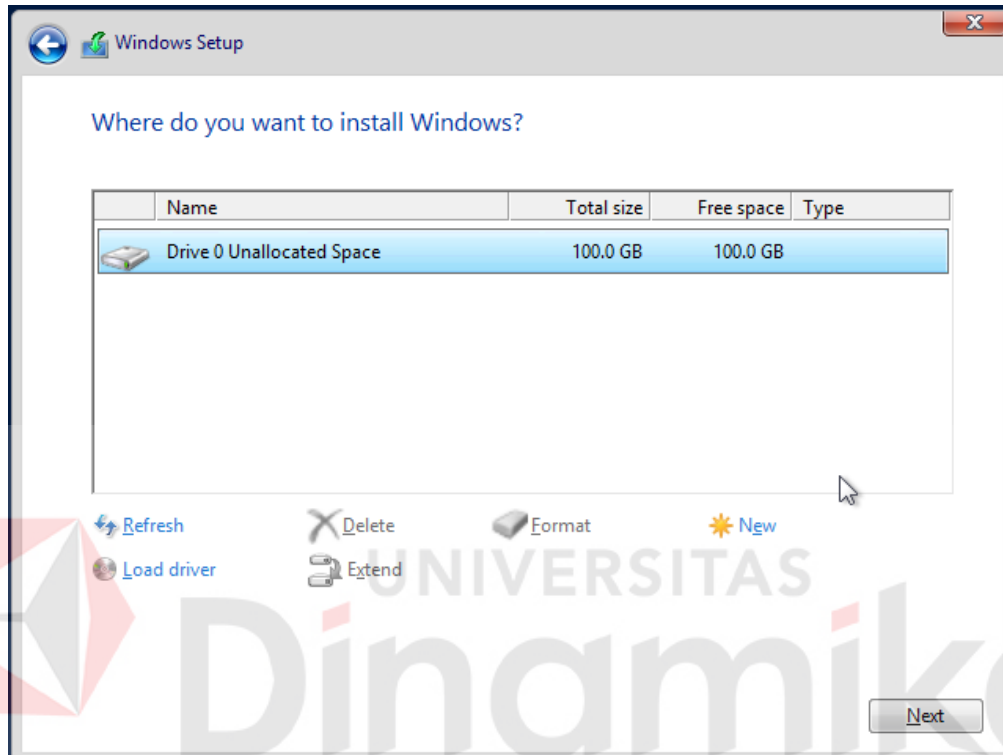
Gambar 4.32 Browse folder

15. Setelah di klik OK. Akan muncul pilihan lagi seperti pada gambar pilih Nutanix VirIO SCSI pass-through controller (E:\Windows Server 2012 R2\vioscsi.inf), kemudian klik Next dan tunggu prosesnya selesai.



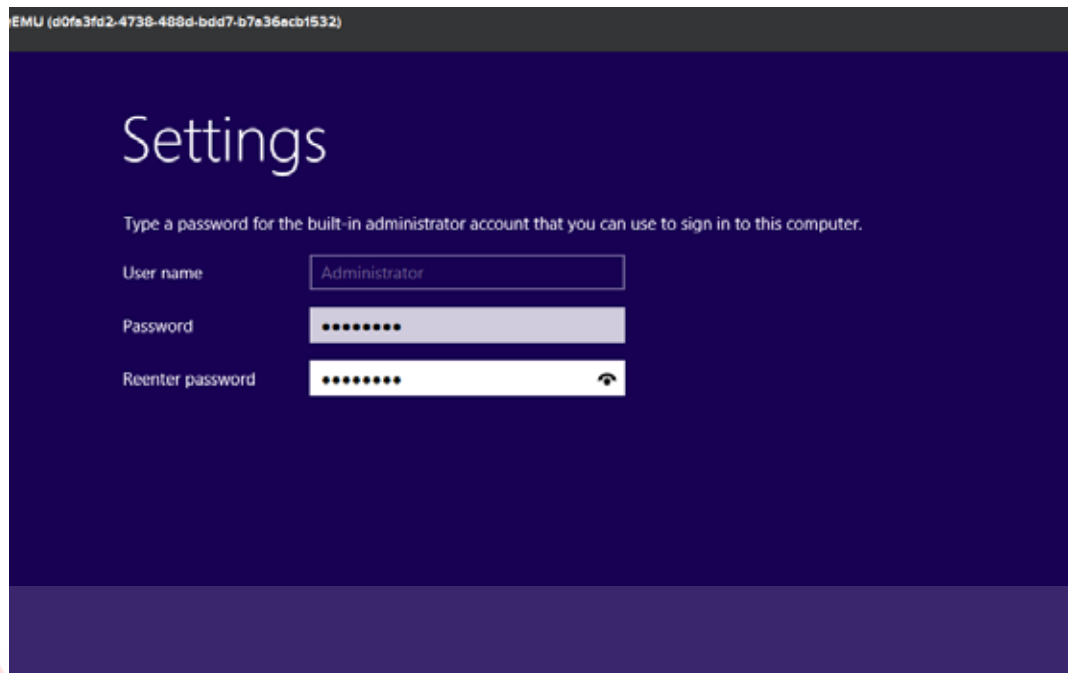
Gambar 4.33 Nutanix VirtIO Driver

16. Kemudian akan muncul pengaturan disk untuk menginstall OS Seperti pada gambar 4.34.
17. Pilih Disk untuk lokasi install windows. Dan klik Next, kemudian tunggu instalasi sampai selesai.



Gambar 4.34 Select Windows Installation Drive

18. Setelah selesai. Masukkan password user



Gambar 4.35 Login Windows

19. Klik tombol finish dan OS siap digunakan.



UNIVERSITAS
Dinamika

BAB V

KESIMPULAN

Pada bab ini membahas mengenai kesimpulan dan saran dari pembuatan buku pada Badan Pemeriksa Keuangan Republik Indonesia.

5.1. Kesimpulan

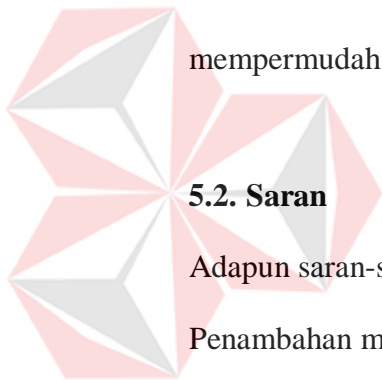
Kesimpulan yang diperoleh selama pembuatan buku di Badan Pemeriksa Keuangan Republik Indonesia adalah :

Pembuatan buku materi Konfigurasi Firewall dan Virtualisasi Server untuk mempermudah pembelajaran atau sosialisasi jaringan pada BPKRI.

5.2. Saran

Adapun saran-saran bila ada penambahan ialah sebagai berikut:

Penambahan materi lain terkait jaringan, mulai dari konsep dasar jaringan hingga fisik jaringan.



UNIVERSITAS
Dinamika

DAFTAR PUSTAKA

Badan Pemeriksa Keuangan. Diakses oktober 2017. bpk.go.id

Cyberoam. Diakses oktober 2017.

<https://www.cyberoam.com/downloads/datasheet/CyberoamCR100iNG.pdf>

Ingham, Kenneth, Stephanie Forrest. *Network Firewall*. University of New Mexico.

Diakses oktober 2017. <https://www.cs.unm.edu/~forrest/publications/firewalls-05.pdf>.

Nutanix. Diakses oktober 2017. <https://www.nutanix.com/hyperconverged-infrastructure/>

Oktaviani. 2007. *Mengenal Sistem Firewall*. Gunadarma University. Oktober 2016

<http://oktaviani.staff.gunadarma.ac.id/Publications/files/2158/mengenal+firewall.pdf>.

Stallings, William. 2007. *Network Security Essentials : Applications and Standards Third Edition*. USA : Pearson Prentice Hall



UNIVERSITAS
Dinamika