



LAPORAN KERJA PRAKTIK

MEMBANGUN *PROXY SERVER* PADA JARINGAN PT. CROSS NETWORK INDONESIA DENGAN MENGGUNAKAN MIKROTIK

KERJA PRAKTIK

Program Studi

S1 Teknik Komputer

**INSTITUT BISNIS
DAN INFORMATIKA**

stikom
SURABAYA

Oleh:

ANDRE ARTA KURNIAWAN

16410200016

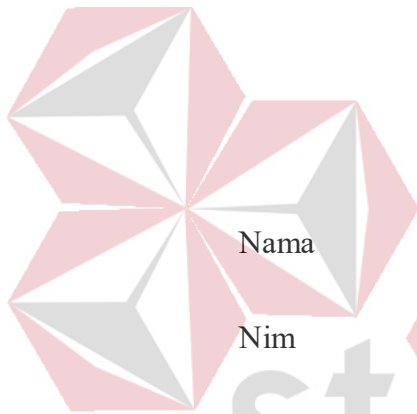
**FAKULTAS TEKNOLOGI DAN INFORMATIKA
INSTITUT BISNIS DAN INFORMATIKA STIKOM SURABAYA
2019**

LAPORAN KERJA PRAKTIK

MEMBANGUN *PROXY SERVER* PADA JARINGAN PT CROSS NETWORK INDONESIA DENGAN MENGGUNAKAN MIKROTIK

Diajukan sebagai salah satu syarat untuk menempuh ujian Tahap Akhir

Program Strata Satu (S1)



Disusun Oleh :

Nama : Andre Arta Kurniawan

Nim : 16.41020.0016

Program : S1 (Strata Satu)

Jurusan : Teknik Komputer

FAKULTAS TEKNOLOGI DAN INFORMATIKA

INSTITUT BISNIS DAN INFORMATIKA STIKOM SURABAYA

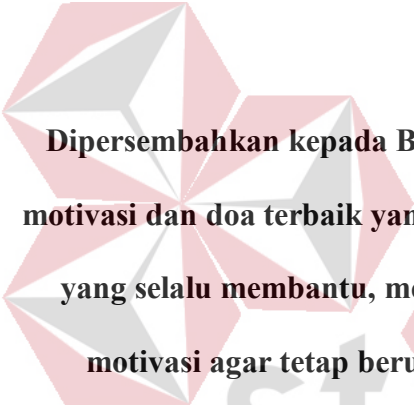
2019



“Learn From The Past”

Andre Arta Kurniawan

stikom
SURABAYA



Dipersembahkan kepada Bapak, Ibu dan Keluarga saya atas dukungan, motivasi dan doa terbaik yang diberikan kepada saya. Beserta semua orang yang selalu membantu, mendukung, memberi masukan, dan memberi motivasi agar tetap berusaha dan belajar agar menjadi lebih baik.

LAPORAN KERJA PRAKTIK
MEMBANGUN *PROXY SERVER* PADA JARINGAN PT CROSS
NETWORK INDONESIA DENGAN MENGGUNAKAN MIKROTIK

Laporan Kerja Praktik oleh

Andre Arta Kurniawan

NIM : 16.41020.0016

Telah diperiksa, diuji dan disetujui

Surabaya, 15 Maret 2019

Disetujui :

Dosen Pembimbing,

Penyelia,



Dr. Susijanto Tri Rasmana, S.Kom., M.T.

NIDN.0727097302


www.cross.net

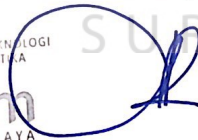
Kurniawan

Mengetahui :

Ketua Prodi S1 Teknik Komputer,



FAKULTAS TEKNOLOGI
DAN INFORMATIKA
stikom
SURABAYA



22
03 2019

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 : Andre Arta Kurniawan
NIM : 16410200016
Program Studi : SI Teknik Komputer
Fakultas : Fakultas Teknologi dan Informatika
Jenis Karya : Laporan Kerja Praktik
Judul Karya : **MEMBANGUN *PROXY SERVER* PADA JARINGAN
PT CROSS NETWORK INDONESIA DENGAN
MENGUNAKAN MIKROTIK**

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 di atas 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, 15 Maret 2019

Yang Menyatakan,



Andre Arta Kurniawan

NIM.16410200016

ABSTRAK

Banyaknya konten negatif di dalam dunia internet memang tidak bisa dihindari. Namun bukan berarti konten negatif tersebut tidak bisa dicegah. Sejak 2014 di Pemerintah Indonesia bekerja sama dengan seluruh *internet service provider* (ISP) di seluruh Indonesia telah menerapkan internet positif dimana seluruh akses internet akan diarahkan dulu ke *dns* milik pemerintah yang kemudian di *filter*, tetapi pada dasarnya setiap ISP akan menerapkan internet positif tanpa harus mengarahkan ke *dns* milik pemerintah Indonesia. Oleh karena itu, pada percobaan *project* ini diterapkan web proxy pada ISP Cross Network Indonesia yang kemudian akan dibandingkan dengan *system firewall* milik Cross Network Indonesia.

Dengan adanya kelebihan dan kekurangan pada metode yang digunakan maka akan dilakukan pula analisis pada *resources hardware* yang digunakan. Dan dari hasil pengerjaan *project* ini *web proxy* telah berhasil dibuat dan sistem *web proxy* telah berhasil memblokir *website* – *website* pada *blacklist* yang telah dibuat. Namun kelemahan dari *web proxy* yang didapat adalah *web proxy* tidak bisa memblokir *website* dengan koneksi HTTPS serta kinerja *resource* pada *hardware* saat *web proxy* diaktifkan meningkat sehingga untuk tingkat keberhasilan pada *project* ini bisa mencapai 100% apabila *web proxy* memblokir *blacklist website* yang berasal dari ketikan melalui *url* dan bukan dari mesin pencarian atau *search engine* (seperti *Google*, *Yahoo*, dan lain – lain).

Kata Kunci : MikroTik, proxy server, web proxy mikrotik

KATA PENGANTAR

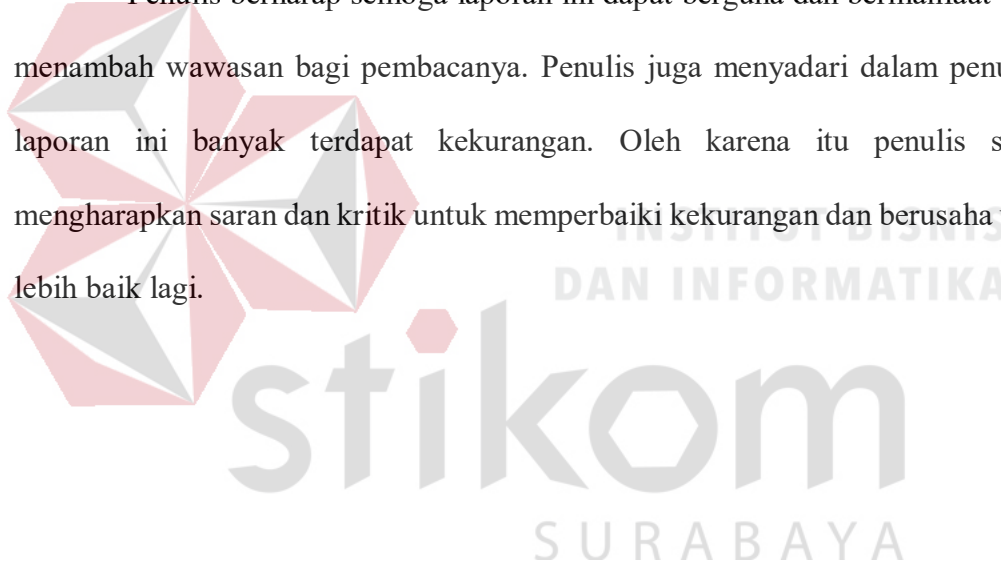
Puji syukur saya panjatkan kepada Tuhan Yesus Kristus atas segala berkat dan rahmat yang telah diberikan, sehingga penulis dapat menyelesaikan Laporan Kerja Praktik. Penulisan Laporan ini adalah sebagai salah satu syarat menempuh Tugas Akhir pada Program Studi S1 Teknik Komputer Institut Bisnis dan Informatika Stikom Surabaya.

Dalam usaha menyelesaikan penulisan Laporan Kerja Praktik ini penulis banyak mendapat bantuan dari berbagai pihak baik moral maupun materi. Oleh karena itu penulis mengucapkan terima kasih kepada :

1. Tuhan YME, karena berkat dan rahmatnya penulis dapat menyelesaikan Laporan Kerja Praktik ini.
2. Orang Tua dan Seluruh Keluarga penulis tercinta yang telah memberikan dorongan dan bantuan baik moral maupun materi sehingga penulis dapat menempuh dan menyelesaikan Kerja Praktik serta Laporan ini.
3. PT. CROSS NETWORK INDONESIA atas segala kesempatan dan pengalaman kerja yang telah diberikan kepada penulis selama melaksanakan Kerja Praktik.
4. Kepada Bapak Kurniawan selaku penyelia dan pembimbing. Terima kasih atas bimbingan yang diberikan dan kesempatannya serta tuntunan baik itu materi secara tertulis maupun lisan sehingga penulis dapat melaksanakan Kerja Praktik di PT. CROSS NETWORK INDONESIA.

5. Kepada Bapak Pauladie Susanto, S.Kom., M.T. selaku Ketua Program Studi Teknik Komputer Surabaya atas ijin yang diberikan untuk melaksanakan Kerja Praktik di PT. CROSS NETWORK INDONESIA.
6. Kepada Dr. Susijanto Tri Rasmana, S.Kom., M.T. selaku dosen pembimbing penulis sehingga dapat menyelesaikan Laporan Kerja Praktik.
7. Teman- teman seperjuangan Teknik Komputer angkatan 2016 serta rekan-rekan pengurus Himpunan Mahasiswa S1 Teknik Komputer Institut Bisnis dan Informatika Stikom Surabaya.

Penulis berharap semoga laporan ini dapat berguna dan bermanfaat untuk menambah wawasan bagi pembacanya. Penulis juga menyadari dalam penulisan laporan ini banyak terdapat kekurangan. Oleh karena itu penulis sangat mengharapkan saran dan kritik untuk memperbaiki kekurangan dan berusaha untuk lebih baik lagi.



Surabaya, 15 Maret 2019

Penulis

DAFTAR ISI

Halaman

SURAT PERNYATAAN.....	Error! Bookmark not defined.
PERSETUJUAN PUBLIKASI DAN KEASLIAN KARYA ILMIAH.....	Error! Bookmark not defined.
ABSTRAK	vii
KATA PENGANTAR	viii
DAFTAR ISI	x
DAFTAR TABEL	xiii
DAFTAR GAMBAR	xiv
DAFTAR LAMPIRAN.....	xvi
BAB I.....	1
PENDAHULUAN	1
1.1. Latar Belakang Masalah.....	1
1.2. Perumusan Masalah	2
1.3. Batasan Masalah	2
1.4. Tujuan	2
1.5. Kontribusi.....	3
BAB II.....	4
GAMBARAN UMUM PERUSAHAAN.....	4
2.1. Sejarah Singkat PT. CROSS NETWORK INDONESIA	4

2.2.	Visi dan Misi PT. CROSS NETWORK INDONESIA.....	5
2.2.1.	Visi.....	5
2.2.2.	Misi.....	6
2.3.	Lokasi Perusahaan	6
2.4.	Struktur Organisasi PT. CROSS NETWORK INDONESIA.....	7
BAB III.....		8
LANDASAN TEORI.....		8
3.1.	Konsep Dasar Jaringan Komputer	8
3.2.	TCP/IP (Transmission Control Protocol/Internet Protocol).....	11
3.3.	Firewall	13
3.4.	NAT (Network Address Translation)	14
3.5.	Router.....	15
3.6.	MikroTik RouterOS.....	17
3.7.	Winbox	20
3.8.	Proxy Server.....	21
3.8.1.	Web Proxy MikroTik.....	25
3.8.2.	Squid Proxy Server Linux.....	25
BAB IV		27
DESKRIPSI KERJA PRAKTIK		27
4.1.	Prosedur Penelitian	27
4.1.1.	Analisa Kebutuhan	27

4.1.2.	Desain	29
4.1.3.	Simulasi.....	29
4.1.4.	Implementasi	30
4.1.5.	Analisa Hasil	30
4.2.	<i>Flowchart</i> Cara Kerja	31
4.3.	Perancangan.....	33
4.3.1.	Topologi Jaringan.....	33
4.3.2.	Konfigurasi MikroTik.....	34
4.3.3.	Konfigurasi <i>Web Proxy</i> Pada MikroTik	40
4.4.	Hasil dan Pembahasan	50
BAB V.....		57
PENUTUP.....		57
5.1.	Kesimpulan.....	57
5.2.	Saran	58
DAFTAR PUSTAKA		59
LAMPIRAN		61
BIODATA PENULIS		69

DAFTAR TABEL

	Halaman
Tabel 4.1 Kebutuhan Perangkat Lunak.....	28
Tabel 4.2 Kebutuhan Perangkat Keras.....	29
Tabel 4.3 Hasil penjadwalan waktu akses <i>social media</i>	52
Tabel 4.4 Tabel hasil pengujian (1)	54
Tabel 4.5 Tabel hasil pengujian (2)	55



DAFTAR GAMBAR

	Halaman
Gambar 2.1 Lokasi PT. Cross Network Indonesia	6
Gambar 2.2 Struktur Organisasi PT. CROSS NETWORK INDONESIA	7
Gambar 3.1 <i>TCP/IP Models</i>	12
Gambar 3.2 <i>TCP/IP Protocols</i>	13
Gambar 3.3 NAT diagram.....	15
Gambar 3.4 Cisco <i>Router</i>	17
Gambar 3.5 MikroTik <i>Router</i>	17
Gambar 3.11 RB433 yang digunakan sebagai <i>web proxy</i>	19
Gambar 3.12 Tampilan Winbox	20
Gambar 3.13 Tampilan Winbox setelah masuk kedalam MikroTik	21
Gambar 3.14 Cara Kerja <i>Proxy</i>	25
Gambar 4.1 Tahapan Pengerjaan.....	27
Gambar 4.2 Flowchart Cara Kerja (1)	31
Gambar 4.3 Flowchart Cara Kerja (2)	32
Gambar 4.4 Topologi Jaringan	33
Gambar 4.5 Konfigurasi <i>IP Address</i>	36
Gambar 4.6 Konfigurasi DNS	37
Gambar 4.7 Konfigurasi NAT <i>Masquerade</i>	38
Gambar 4.8 Konfigurasi <i>Gateway</i>	39
Gambar 4.9 Hasil <i>ping google.com</i>	40
Gambar 4.10 Konfigurasi <i>Web Proxy</i>	41
Gambar 4.11 Konfigurasi <i>Transparent Web Proxy</i> (1)	43

Gambar 4.12 Konfigurasi <i>Transparent Web Proxy</i> (2)	43
Gambar 4.13 <i>Blacklist web</i> yang diblokir	45
Gambar 4.14 <i>Script</i> untuk mengaktifkan <i>web proxy</i>	46
Gambar 4.15 <i>Script</i> untuk menonaktifkan <i>web proxy</i>	47
Gambar 4.16 Penjadwalan untuk <i>script</i> blok-youtube.....	48
Gambar 4.17 Penjadwalan untuk <i>script</i> buka-youtube	49
Gambar 4.18 Pengujian <i>web proxy</i>	50
Gambar 4.19 Jumlah <i>counter</i> pada <i>hits</i> yang terus bertambah.....	51
Gambar 4.20 Hasil <i>filtering website</i> menggunakan <i>firewall</i>	53
Gambar 4.21 <i>Update blacklist web proxy</i>	56



DAFTAR LAMPIRAN

	Halaman
Lampiran 1 Form KP-3 (Surat Balasan Perusahaan).....	61
Lampiran 2 Form KP-5 (Acuan Kerja).....	62
Lampiran 3 Form KP-6 (Log Harian dan Catatan Perubahan Acuan Kerja).....	64
Lampiran 4 Form KP-7 (Kehadiran Kerja Praktik).....	66
Lampiran 5 Kartu Bimbingan Kerja Praktik	68



BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Internet di era sekarang menjadi kebutuhan yang penting untuk menunjang kegiatan sehari – hari. Dalam penggunaannya internet bisa bermanfaat bagi banyak orang yang menggunakan namun di lain sisi internet juga bisa bersifat menghancurkan. Internet dengan mudah memberikan kebebasan banyak orang untuk mengakses segala sesuatu yang berada di internet, dan dengan kemudahan mengakses internet semua orang bisa menikmati konten konten yang beredar di internet.

Dengan adanya kebebasan mengakses internet tidak menutup kemungkinan seseorang bisa mengakses konten konten negatif yang beredar di internet. Maka dari itu dibutuhkan filter untuk memblock koneksi internet agar tidak dapat mengakses konten negatif. Upaya ini dapat dilakukan dengan membuat sebuah *firewall* yang dapat mengurangi koneksi untuk mengakses konten konten negatif.

Berdasarkan permasalahan tersebut dibutuhkan sebuah *firewall*, adapun cara yang dapat digunakan tidak membutuhkan proses instalasi yang rumit dan administrasi yang mudah yaitu dengan membuat sebuah *proxy server*, karena pada PT CROSS NETWORK INDONESIA menggunakan perangkat MikroTik RouterOS maka bisa dibuat sebuah *web proxy* yang nantinya akan berfungsi sebagai *firewall* dan *filtering* untuk memfilter konten konten negatif yang beredar di internet.

1.2. Perumusan Masalah

Bagaimana cara merancang dan Membangun *Proxy Server* pada jaringan ISP PT. Cross Network Indonesia dengan menggunakan *Web Proxy* berbasis *MikroTik RouterOS*?

1.3. Batasan Masalah

Melihat permasalahan yang ada, maka penulis membatasi masalah dari kerja praktik, yaitu:

1. Menggunakan RB433 sebagai perangkat *router*
2. Menggunakan *router* dengan sistem operasi *MikroTik*
3. Menggunakan 1 jalur internet milik ISP Cross Network Indonesia

1.4. Tujuan

Tujuan dari kegiatan Kerja Praktik yang dilaksanakan oleh mahasiswa adalah agar mahasiswa dapat melihat secara langsung bagaimana kondisi dan kenyataan di lapangan. Serta melatih analisa, tentang bagaimanakah cara menyelesaikan permasalahan menggunakan ilmu yang didapatkan pada perkuliahan. Tujuan khusus adalah sebagai berikut :

1. Mengkonfigurasi *web proxy* pada *MikroTik routerOS*
2. Memahami topologi jaringan yang ada pada ISP PT CROSS NETWORK INDONESIA
3. Mencoba dan menganalisa hasil konfigurasi dan hasil *web proxy*
4. Memberikan cara konfigurasi dan proses pada router yang telah dikonfigurasi

1.5. Kontribusi

Memberikan kontribusi ke PT. CROSS NETWORK INDONESIA dengan mengkonfigurasi *web proxy* sehingga dapat berfungsi sebagai *firewall* untuk koneksi ke internet dan *memblock* koneksi internet ke *webpage* yang tidak diinginkan.



BAB II

GAMBARAN UMUM PERUSAHAAN

2.1. Sejarah Singkat PT. CROSS NETWORK INDONESIA

Sejarah CrossNet bermula dari pada tahun 1992, berawal dari sebuah kelompok programmer dengan nama xsoft yang kemudian menjadi xnet, pada tahun 1995 menjadi sebuah toko komputer dengan spesialisasi di bidang grafis dan networking di Tenggilis Mejoyo blok AC-20 yang melayani kebutuhan mahasiswa dan dosen Universitas Surabaya mulai kebutuhan hardware sampai ke pelatihan atau bimbingan skripsi, yang kemudian melayani beberapa perusahaan terutama untuk pembuatan software dan local area network di perusahaan baik di surabaya dan beberapa kota lainnya.

Seiring dengan berkembangnya informasi Teknologi khususnya internet yang menjadi tujuan berbagai kalangan untuk saling berbagi informasi ini maka pada tanggal 17 Agustus 2004 CroosNet mulai memberikan komitmen untuk melayani kebutuhan dan solusi di bidang LT. Dengan MOTTO "THE RIGHT WAY FOR I.T SOLUTION". Diawali dengan C.V Cross Network Mitra Lestari menyediakan berbagai solusi IT bagi perusahaan maupun secara yang kemudian pada tanggal 28 agustus 2006 menjadi P.T Cross Network Indonesia dan telah mendapatkan Ijin Operasi berdasarkan Keputusan Direktur Jenderal Pos dan Telekomunikasi Nomor : 226/Dirjen/2010 tanggal 05 Juli 2010 tentang izin Penyelenggaraan Jasa Akses Internet (Internet Service Provider) oleh Menteri Komunikasi dan Informatika Republik Indonesia serta ijin keterangan layak operasi di Manado Nomor

1304/DJPT.1/Kominfo/6/2010. Dalam perjalanan CrossNet mengembangkan pelayanan IT yang tepat guna bagi perusahaan baik dalam bentuk pengembangan jaringan maupun software, maka CrossNet mendapatkan kepercayaan dari berbagai perusahaan untuk menjadi partner dalam pengembangan solusi IT. Saat ini CrossNet memfokuskan kegiatan pada Internet Service Provider dengan bekerja sama dengan operator terkemuka di tanah air dengan menggunakan multiple backbone melalui media fiber optic (FO) ke gateway internasional dan memakai V S A T (Very Small Apperature Terminal) untuk menjangkau tempat terpencil.

Pada tahun 2006 CrossNet telah melebarkan sayap ke beberapa kota besar di Indonesia Timur. Sampai sekarang CrossNet telah hadir dan melayaniii kebutuhan masyarakat akan jaringan internet di 10 kota besar di Indonesia, seperti surabaya, malang, Probolinggo, Kupang, Luwuk, Manado, Kotamobagu, Tondano, Bitung serta Sarong dan terus memperluas ke kotakota yang lain. CrossNet percaya dalam perjalanannya yang selalu mengutamakan kepuasan pelanggan dengan cara mendengarkan dan mengerti apa yang menjadi kebutuhan menjadi kunci dalam pengembangannya. CrossNet juga memberikan produk produk yang inovatif, costomisable dan tepat guna sesuai dengan kebutuhan pelanggan baik itu perusahaan ataupun personal.

2.2. Visi dan Misi PT. CROSS NETWORK INDONESIA

2.2.1. Visi

Menjadi perusahaan yang dapat memberikan solusi IT secara tepat guna dan menjadi salah satu Internet Service Provider yang baik di Indonesia

2.2.2. Misi

1. Memberikan dan mengembangkan pelayanan terbaik dan tepat kepada seluruh pelanggan
2. Mengembangkan berbagai produk guna memberikan solusi terhadap permasalahan yang di hadapi oleh konsumen
3. Mengembangkan CrossNet ke berbagai kota di Indonesia guna memberikan layanan IT secara lebih luas

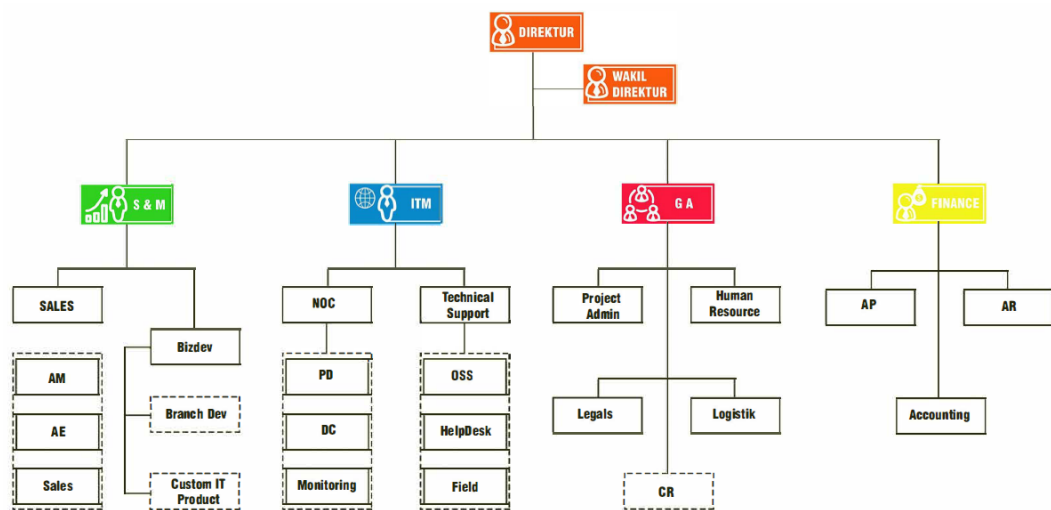
2.3. Lokasi Perusahaan

Lokasi PT. Cross Network Indonesia yaitu di Intiland Tower Building 10th Floor Suite 01-D Jalan Panglima Sudirman No. 101-103 Surabaya. Berikut adalah peta dari lokasi PT. Cross Network Indonesia:



Gambar 2.1 Lokasi PT. Cross Network Indonesia

2.4. Struktur Organisasi PT. CROSS NETWORK INDONESIA



Gambar 2.2 Struktur Organisasi PT. CROSS NETWORK INDONESIA



BAB III

LANDASAN TEORI

3.1. Konsep Dasar Jaringan Komputer

Dalam dunia komputer, jaringan Dasar adalah praktik menghubungkan dua atau lebih perangkat komputer dalam suatu sistem jaringan secara bersama-sama untuk tujuan berbagi data. Jaringan dibangun atas dasar sistem jaringan komputer yaitu perpaduan antara perangkat keras Jaringan komputer, perangkat lunak Jaringan komputer dan protokol jaringan komputer. (jaringankomputer.org, 2019)

Dan seiring berkembangnya jaman, jaringan komputer sudah tak hanya lagi menghubungkan beberapa perangkat komputer yang ada namun sekarang jaringan komputer dengan adanya koneksi internet sudah bisa menghubungkan seluruh orang di dunia dengan berbagai macam perangkat yang bisa terhubung ke internet.

Internet (kependekan dari *interconnection-networking*) adalah seluruh jaringan komunikasi yang menggunakan media elektronik, yang saling terhubung menggunakan standar sistem global Transmission Control Protocol/Internet Protocol Suite (TCP/IP) sebagai protokol pertukaran paket (packet switching communication protocol) untuk melayani miliaran pengguna di seluruh dunia. Rangkaian internet yang terbesar dinamakan Internet. Cara menghubungkan rangkaian dengan kaidah ini dinamakan internetworking ("antarjaringan").

Saat ini telah banyak berbagai macam model jaringan yang ada, untuk klasifikasinya dapat dibedakan menjadi beberapa, yaitu :

1. Berdasarkan distribusi sumber informasi/data

a. **Jaringan terpusat**

Jaringan ini terdiri dari komputer klient dan server yang mana komputer klient yang berfungsi sebagai perantara untuk mengakses sumber informasi/data yang berasal dari satu komputer server

b. **Jaringan terdistribusi**

Merupakan perpaduan beberapa jaringan terpusat sehingga terdapat beberapa komputer server yang saling berhubungan dengan klient membentuk sistem jaringan tertentu.

2. Berdasarkan jangkauan geografis dibedakan menjadi

a. **LAN (*Local Area Network*)**

jaringan yang menghubungkan 2 komputer atau lebih dalam cakupan seperti laboratorium, kantor dan lain lain

b. **MAN (*Metropolitan Area Network*)**

Cakupan jaringan dalam 1 kota besar yang saling terhubung.

c. **WAN (*Wide Area Network*)**

Cakupan jaringan seluruh dunia

3. Berdasarkan peranan dan hubungan tiap komputer dalam memproses data

a. **Jaringan Client-Server**

Pada jaringan ini terdapat 1 atau beberapa komputer server dan komputer client. Komputer yang akan menjadi komputer server maupun menjadi komputer client dan diubah-ubah melalui software jaringan pada protokolnya. Komputer client sebagai perantara untuk dapat mengakses data pada komputer server sedangkan

komputer server menyediakan informasi yang diperlukan oleh komputer client.

b. Jaringan *Peer-To-Peer*

Pada jaringan ini tidak ada komputer client maupun komputer server karena semua komputer dapat melakukan pengiriman maupun penerimaan informasi sehingga semua komputer berfungsi sebagai client sekaligus sebagai server.

4. Berdasarkan media transmisi data

a. Jaringan Berkabel (*Wired Network*)

Pada jaringan ini, untuk menghubungkan satu komputer dengan komputer lain diperlukan penghubung berupa kabel jaringan. Kabel jaringan berfungsi dalam mengirim informasi dalam bentuk sinyal listrik antar komputer jaringan.

b. Jaringan Nirkabel (*Wireless Network*)

jaringan dengan medium berupa gelombang elektromagnetik. Pada jaringan ini tidak diperlukan kabel untuk menghubungkan antar komputer karena menggunakan gelombang elektromagnetik yang akan mengirimkan sinyal informasi antar komputer jaringan.

Dalam dunia jaringan komputer juga terdapat macam – macam topologi yang digunakan salah satunya yang paling umum digunakan yaitu, topologi *star*.

Macam – macam topologi jaringan komputer yang ada diantaranya :

1. Topologi *Ring*
2. Topologi *Bus*
3. Topologi *Star*

4. Topologi *Mesh*
5. Topologi *Tree*
6. Topologi *Linier*
7. Topologi *Hybrid*
8. Topologi *Peer-To-Peer*

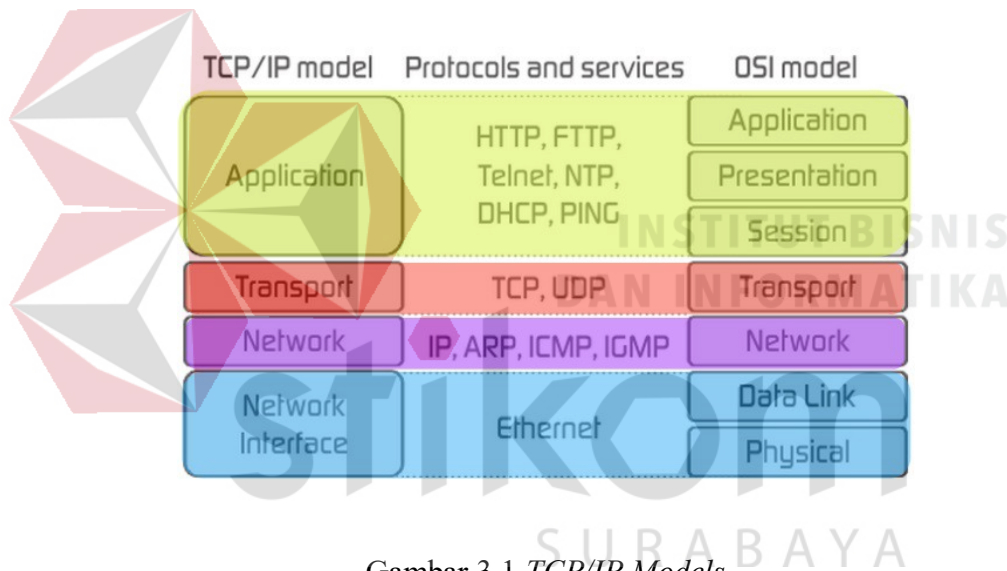
3.2. TCP/IP (Transmission Control Protocol/Internet Protocol)

Protokol adalah spesifikasi formal yang mendefinisikan prosedur-prosedur yang harus diikuti ketika mengirim dan menerima data (Werner, 1996). Protokol mendefinisikan jenis, waktu, urutan dan pengecekan kesalahan yang digunakan dalam jaringan. Transmission Control Protocol/Internet Protocol (TCP/IP) merupakan protokol untuk mengirim data antar komputer pada jaringan. Protokol ini merupakan protokol yang digunakan untuk akses Internet dan digunakan untuk komunikasi global. TCP/IP terdiri atas dua protokol yang terpisah. TCP/IP menggunakan pendekatan lapisan (layer) pada saat membangun protokol ini. Dengan adanya pendekatan berlapis ini memungkinkan dibangunnya beberapa layanan kecil untuk tugas-tugas khusus. TCP/IP terdiri dari lima layer, yaitu:

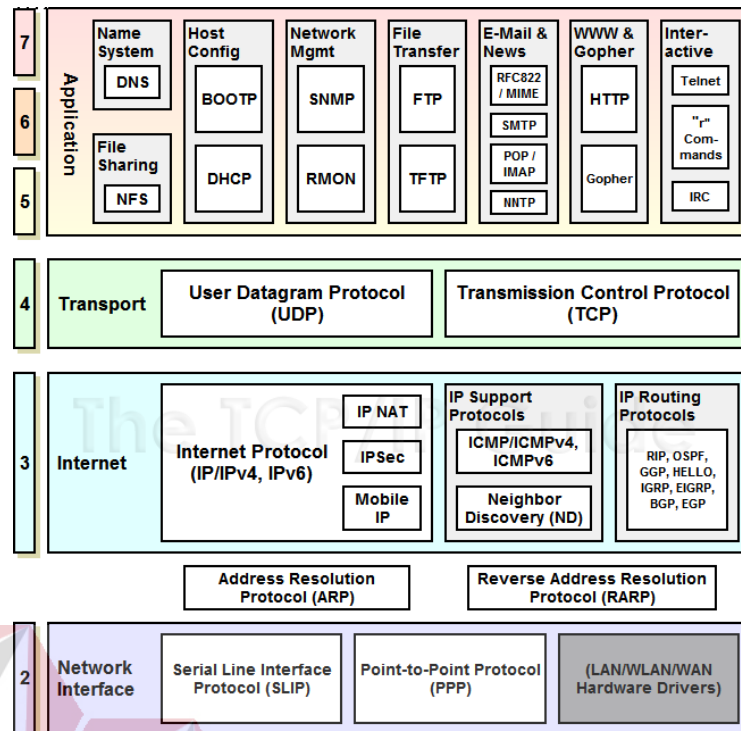
- a. Layer Application, di dalam layer ini aplikasi seperti FTP, Telnet, SMTP, dan NFS dilaksanakan.
- b. Layer Transport, di dalam layer ini TCP dan UDP menambahkan data transport ke paket dan melewatkannya ke layer Internet.
- c. Layer Internet, layer ini mengambil paket dari layer transport dan menambahkan informasi alamat sebelum mengirimkannya ke layer network interface.

- d. Layer Network Interface, di dalam layer ini data dikirim ke layer physical melalui device jaringan.
- e. Layer Physical, layer ini merupakan sistem kabel yang digunakan untuk proses mengirim dan menerima data.

TCP/IP dikirimkan ke setiap jaringan lokal sebagai subnet yang masing-masing subnet telah diberi alamat. IP yang menggunakan pengalamatan disebut dengan IP Address. IP Address ini digunakan untuk mengidentifikasi subnet dan host secara logik di dalam TCP/IP. (Staff of Linux Journal, 2004)



Gambar 3.1 *TCP/IP Models*



Gambar 3.2 TCP/IP Protocols

3.3. Firewall

Firewall adalah sebuah sistem atau kelompok sistem yang menerapkan sebuah access control policy terhadap lalu lintas jaringan yang melewati titik-titik akses dalam jaringan. Tugas firewall adalah untuk memastikan bahwa tidak ada tambahan diluar ruang lingkup yang diizinkan. Firewall bertanggung jawab untuk memastikan bahwa acces control policy yang diikuti oleh semua pengguna di dalam jaringan tersebut. Firewall sama seperti alat-alat jaringan lain dalam hal untuk mengontrol aliran lalu lintas jaringan. Namun, tidak seperti alat-alat jaringan lain, sebuah firewall harus mengontrol lalu lintas network dengan memasukkan faktor pertimbangan bahwa tidak semua paket-paket data yang dilihatnya adalah apa yang seperti terlihat. Firewall digunakan untuk mengontrol akses antara network internal sebuah organisasi Internet. Sekarang ini firewall semakin menjadi fungsi standar

yang ditambahkan untuk semua host yang berhubungan dengan network. (Purbo, 2000)

Fungsi-fungsi umum firewall adalah sebagai berikut:

- a. Static packet filtering (penyaringan paket secara statis)
- b. Dynamic packet filtering (penyaringan paket secara dinamis)
- c. Stateful filtering (penyaringan paket berdasarkan status)
- d. Proxy

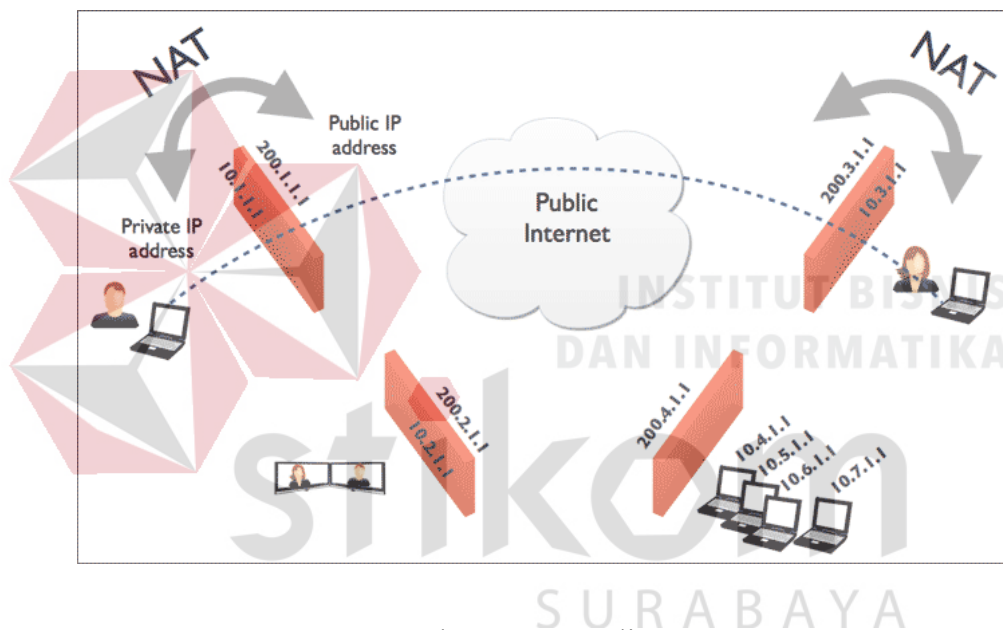
3.4. NAT (Network Address Translation)

Network Address Translation (NAT) adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet menggunakan satu alamat IP. NAT merupakan teknologi yang memungkinkan IP Private dapat membagi koneksi akses internet jaringan yang didesain untuk menyederhanakan IP address, dan berperan juga untuk melindungi jaringan dan kemudahan serta fleksibilitas dalam administrasi jaringan. Banyaknya penggunaan metode ini disebabkan karena ketersediaan alamat IP Address yang terbatas. NAT berlaku sebagai penerjemah antara dua jaringan. (Taringaan, 2009)

IP address sebagai sarana pengalamatan di internet semakin menjadi barang mewah dan eksklusif. Tidak sembarangan orang sekarang ini bisa mendapatkan IP address yang valid dengan mudah. Oleh karena itulah dibutuhkan suatu mekanisme yang dapat menghemat IP address. Logika sederhana untuk penghematan IP address adalah dengan membagi suatu nomor IP address valid ke beberapa client IP address lainnya. Atau dengan kata lain, beberapa komputer bisa mengakses

internet walau hanya memiliki satu IP address yang valid. Salah satu mekanisme itu disediakan oleh NAT. (Riadi, 2011)

NAT bekerja dengan jalan mengkonversikan IP address ke satu atau lebih IP address lain. IP address dikonversi adalah IP address yang diberikan untuk tiap mesin dalam jaringan internal. IP address yang menjadi hasil konversi terletak di luar jaringan internal tersebut dan merupakan IP address legal yang valid. (Husaini, 2008)



Gambar 3.3 NAT diagram

3.5. Router

Router adalah suatu perangkat keras pada jaringan komputer yang berfungsi untuk menghubungkan beberapa jaringan, baik itu jaringan yang sama maupun jaringan yang berbeda dari sisi teknologinya.

Ada juga yang menjelaskan bahwa pengertian router adalah suatu hardware jaringan komputer yang berfungsi untuk mengirimkan paket data melalui jaringan

atau internet dari satu perangkat komputer ke perangkat lainnya, dimana proses tersebut disebut dengan routing.

Fungsi utama dari setiap router adalah untuk menghubungkan 2 jaringan atau lebih agar dapat mendistribusikan paket data dari satu jaringan ke jaringan lainnya.

Jenis – jenis router :

1. Berdasarkan pengaplikasiannya

- a. **Router Aplikasi**

suatu aplikasi yang dapat diinstal oleh user pada sistem operasi komputer sehingga sistem operasi komputer tersebut dapat bekerja layaknya router.

- b. **Router Hardware**

hardware yang mempunyai kemampuan seperti router

- c. **Router PC**

yaitu suatu komputer dengan spesifikasi tinggi yang dimodifikasi sehingga dapat berfungsi sebagai router

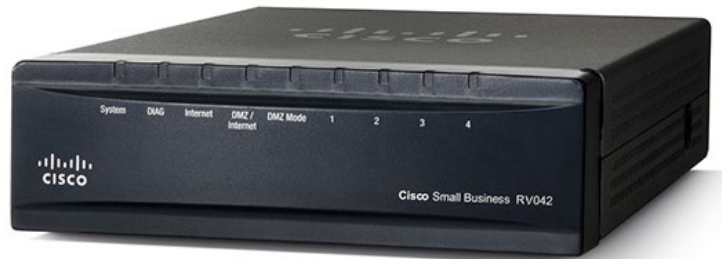
2. Berdasarkan Mekanismenya

- a. **Router Statis**

router yang mampu untuk melakukan proses routing (penghalaan) dari suatu jaringan dimana prosesnya dilakukan secara manual oleh seorang administrator.

b. Router Dinamis

router yang dapat melakukan proses routing (penghalaan) dapat berjalan secara otomatis dan dinamis setelah melalui pengaturan oleh seorang administrator jaringan.



Gambar 3.4 Cisco Router



Gambar 3.5 MikroTik Router

3.6. MikroTik RouterOS

Mikrotik adalah sistem operasi independen berbasis Linux khusus untuk komputer yang difungsikan sebagai router. Mikrotik didesain untuk mudah digunakan dan sangat baik digunakan untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga yang kompleks.

Mikrotik mulai didirikan tahun 1995 yang pada awalnya ditujukan untuk perusahaan jasa layanan Internet (Internet Service Provider, ISP) yang melayani pelanggannya menggunakan teknologi nirkabel. Saat ini MikroTik memberikan layanan kepada banyak ISP nirkabel untuk layanan akses Internet di banyak negara di dunia dan juga sangat populer di Indonesia.

Mikrotik pada standar perangkat keras berbasiskan Personal Computer (PC) dikenal dengan kestabilan, kualitas kontrol dan fleksibilitas untuk berbagai jenis paket data dan penanganan proses rute (routing). Mikrotik yang dibuat sebagai router berbasiskan komputer banyak bermanfaat untuk sebuah ISP yang ingin menjalankan beberapa aplikasi mulai dari hal yang paling ringan hingga tingkat lanjut. Selain routing, Mikrotik dapat digunakan sebagai manajemen kapasitas akses (bandwidth, firewall, wireless access point (WiFi), backhaul link, sistem hotspot, Virtual Private Network server dan masih banyak lainnya. (Tanautama, 1996)

Mikrotik bukanlah perangkat lunak yang gratis jika ingin memanfaatkannya secara penuh, dibutuhkan lisensi dari MikroTik untuk dapat menggunakannya dengan cara membayar. Mikrotik dikenal dengan istilah Level pada lisensinya.

Tersedia mulai dari Level 0 kemudian 1, 3 hingga 6, untuk Level 1 adalah versi Demo Mikrotik dapat digunakan secara gratis dengan fungsi-fungsi yang sangat terbatas. Tentunya setiap level memiliki kemampuan yang berbeda-beda sesuai dengan harganya, Level 6 adalah level tertinggi dengan fungsi yang paling lengkap. Secara singkat dapat dijelaskan sebagai berikut:

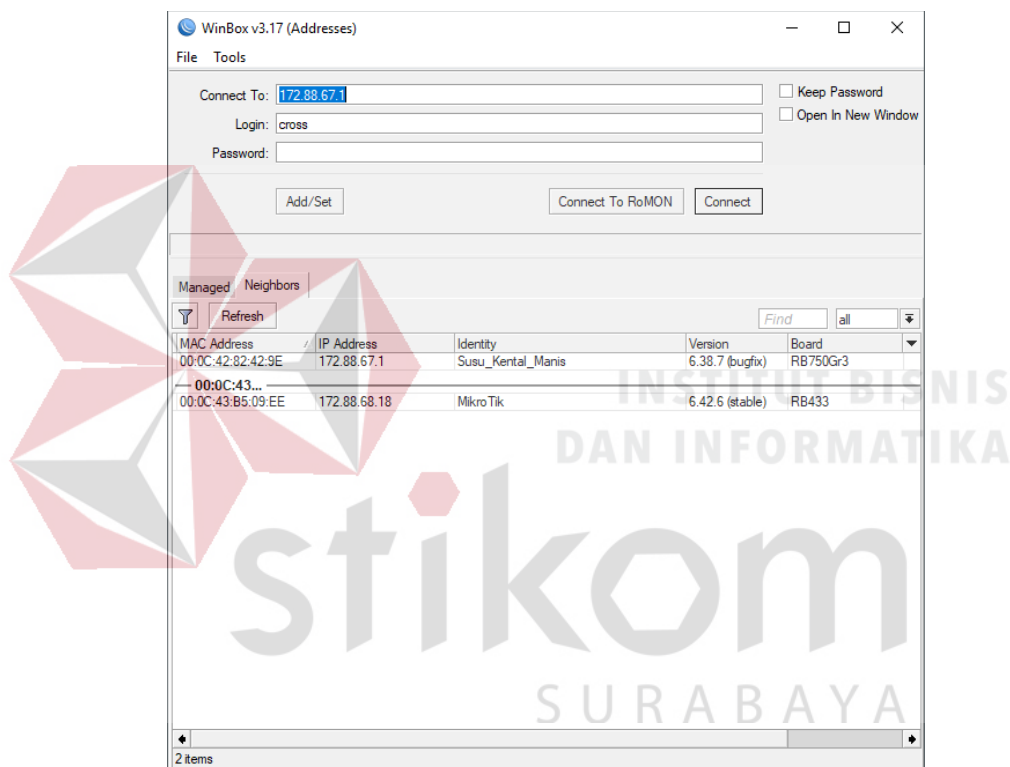
- a. Level 0 (gratis), tidak membutuhkan lisensi untuk menggunakannya dan penggunaan fitur hanya dibatasi selama 24 jam setelah instalasi dilakukan.
- b. Level 1 (demo), pada level ini kamu dapat menggunakannya sbg fungsi routing standar saja dengan 1 pengaturan serta tidak memiliki limitasi waktu untuk menggunakannya.
- c. Level 3, sudah mencakup level 1 ditambah dengan kemampuan untuk manajemen segala perangkat keras yang berbasis Kartu Jaringan atau Ethernet dan pengelolaan perangkat wireless tipe client.
- d. Level 4, sudah mencakup level 1 dan 3 ditambah dengan kemampuan untuk mengelola perangkat wireless tipe access point.
- e. Level 5, mencakup level 1, 3 dan 4 ditambah dengan kemampuan mengelola jumlah pengguna hotspot yang lebih banyak.
- f. Level 6, mencakup semua level dan tidak memiliki limitasi atau batasan apapun.



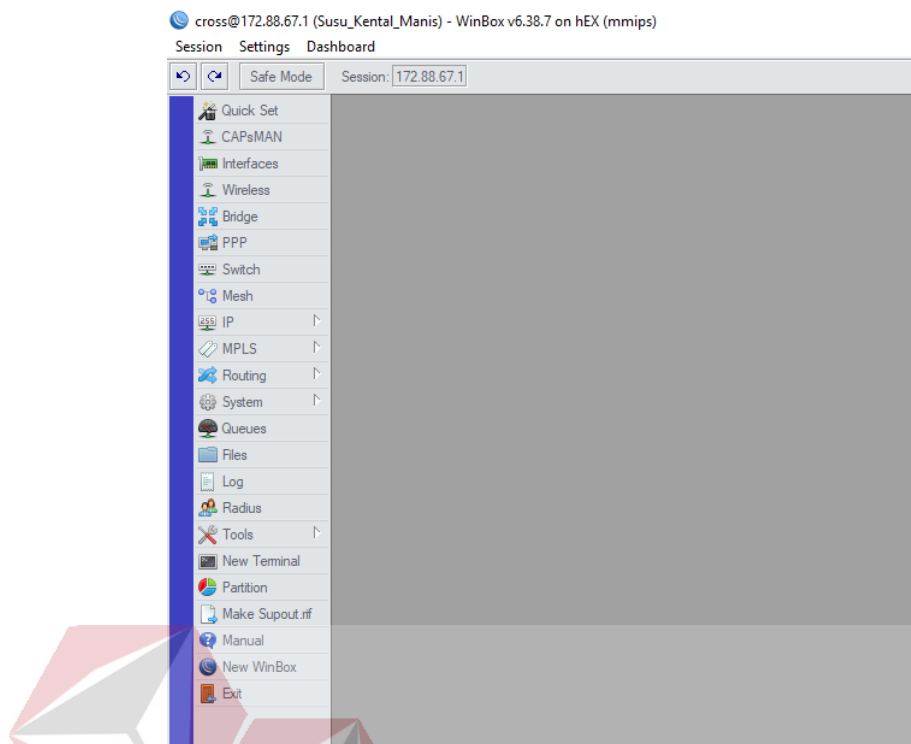
Gambar 3.6 RB433 yang digunakan sebagai *web proxy*

3.7. Winbox

Winbox adalah sebuah *utility* atau software yang digunakan untuk meremote dan/atau mengkonfigurasi MikroTik kedalam mode GUI (*Graphical User Interface*). Selain itu MikroTik dapat diremote dan/atau dikonfigurasi dengan mode CLI (*Command Line Interface*) dengan mengakses MikroTik melalui SSH atau telnet.



Gambar 3.7 Tampilan Winbox



Gambar 3.8 Tampilan Winbox setelah masuk kedalam MikroTik

3.8. Proxy Server

Proxy memiliki pengertiannya sebagai perantara, bekerja dalam berbagai jenis protokol komunikasi jaringan dan dapat berada pada level-level yang berbeda pada hirarki layer protokol komunikasi jaringan. Suatu perantara dapat saja bekerja pada layer Data-Link, layer Network dan Transport, maupun layer Aplikasi dalam hirarki layer komunikasi jaringan menurut OSI. Namun pengertian Proxy Server sebagian besar adalah untuk menunjuk suatu server yang bekerja sebagai Proxy pada layer Aplikasi (Arjuni, 2010), sedangkan *server* adalah suatu sistem komputer yang menyediakan jenis layanan (*service*) tertentu dalam suatu jaringan komputer. Server didukung dengan prosesor yang bersifat *scalable* dan RAM yang besar, juga dilengkapi dengan sistem operasi khusus, yang disebut sebagai sistem operasi jaringan (*network operating system*).

Proxy Server sendiri suatu server komputer yang menyediakan layanan untuk meneruskan permintaan user ke server lainnya yang berada di internet. Dengan adanya proxy server maka sebuah komputer bisa dihubungkan dengan komputer lainnya melalui internet.

Pada umumnya proxy server digunakan untuk mengamankan jaringan komputer pribadi yang terhubung dengan jaringan publik. Jadi, dari proxy server tersebut maka biasanya server diletakkan di antara aplikasi server dengan aplikasi client, dimana aplikasi client berupa web browser, client FTP dan lainnya sedangkan aplikasi server berupa server FTP dan web server. (Maxmanroe, 2019)

Fungsi *Proxy Server*:

1. Fungsi *Connection Sharing*

Proxy Server berfungsi secara teknis untuk menjadi sebuah gateway dimana berperan untuk membatasi penggunaan jaringan lokal dan jaringan luar.

2. Fungsi *Filtering*

Proxy Server bertindak seperti Firewall sebagai media penyaringan atau filtering sebuah jaringan internet dimana setiap paket-paket data yang ditransmisikan akan discan dan difilter untuk mengurangi kegagalan.

3. Fungsi *Caching*

Proxy Server dapat menyimpan objek dan data yang pernah di cari atau diminta user saat *browsing* menggunakan aplikasi internet. Misalnya ketika Anda melakukan pencarian pada situs tertentu maka data-data tersebut akan disimpan dalam bentuk cache.

Manfaat *Proxy Server* :

1. Menghemat Bandwidth

Proxy server bisa dimanfaatkan untuk menghemat penggunaan bandwidth dari koneksi internet user karena adanya proses caching yang menyimpan cookies dari situs-situs yang pernah dikunjungi.

2. Meningkatkan Kinerja Internet

Proxy server dapat membantu meningkatkan kinerja jaringan internet user karena adanya penghematan bandwidth.

3. Memblokir Situs Tertentu

Proxy server dapat secara otomatis memblokir situs-situs yang mengandung sara atau situs yang tidak diinginkan dengan adanya fitur filtering. Sehingga dengan manfaat ini bisa menghindari karyawan membuka situs-situs terlarang melalui jaringan internet lokal perusahaan.

4. Keamanan Jaringan Komputer

proxy server dapat meningkatkan keamanan komputer dari serangan virus dan gangguan malware. Meskipun proxy bermanfaat besar bagi keamanan jaringan komputer namun masih terdapat kekurangan

penggunaan proxy. Salah satunya adalah sering terjadi kesalahpahaman terhadap suatu situs yang dianggap harus diblokir oleh server sehingga perlu dilakukan pembukaan blokir secara manual.

Jenis – jenis *Proxy Server* :

1. *Anonymous Proxy*

Jenis *proxy* yang memberikan informasi mengenai komputer pengguna. Saat pengguna melakukan request pada sebuah *website*, maka *website* itu tidak akan mengetahui alamat IP pribadi si pengguna, hanya mengetahui IP *proxy* nya saja.

2. *High Anonymity Proxy*

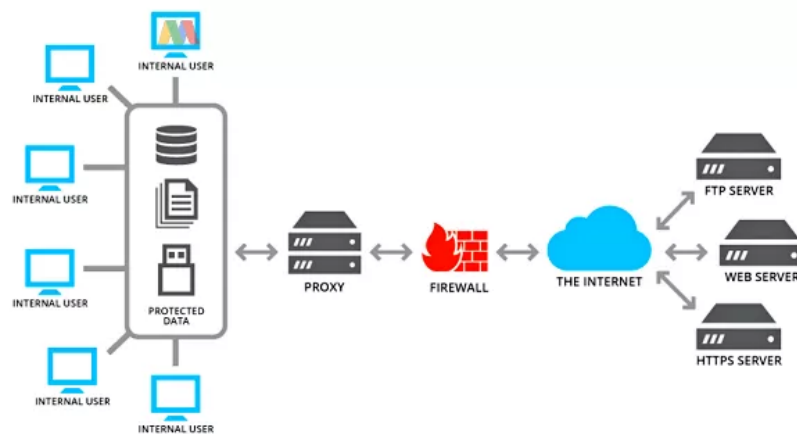
Jenis *proxy* yang tidak mengidentifikasi dirinya sebagai *proxy server* dan tidak menyediakan alamat IP original.

3. *Transparent Proxy*

Jenis *proxy* yang melanjutkan permintaan pengguna ke sumber yang diinginkan tanpa mengungkap informasi komputer si pengguna. Pada umumnya *proxy* jenis ini banyak dipakai pada komputer di perkantoran.

4. *Reverse Proxy*

Jenis *proxy* yang digunakan untuk mencegah *client* terhubung dengan data/informasi sensitif. Dan ketika *caching* pada *proxy* jenis ini diaktifkan maka trafik jaringan akan menurun.



Gambar 3.9 Cara Kerja *Proxy*

Dalam penggunaannya, *Proxy* bisa diterapkan ke dalam *router* langsung ataupun *server* seperti *Linux*. Untuk *router* sendiri salah satu aplikasinya adalah *web proxy* milik MikroTik sedangkan untuk *server* aplikasi yang bisa digunakan yaitu *squid*.

3.8.1. *Web Proxy MikroTik*

Mikrotik memiliki fitur *Web proxy* yang bisa digunakan sebagai *proxy server* yang nantinya akan menjadi perantara antara *browser user* dengan *web server* di internet.

3.8.2. *Squid Proxy Server Linux*

Squid adalah suatu *daemon* yang digunakan sebagai *proxy server* dan *web cache*. *Squid* memiliki banyak jenis penggunaan, mulai dari mempercepat *server web* dengan melakukan *caching* permintaan yang berulang-ulang, *caching DNS*, *caching situs web*, dan *caching* pencarian komputer di dalam jaringan untuk sekelompok komputer yang menggunakan sumber daya jaringan yang sama, hingga pada membantu keamanan dengan cara melakukan penyaringan (*filter*) lalu lintas. Meskipun seringkali

digunakan untuk protokol HTTP dan FTP, *Squid* juga menawarkan dukungan terbatas untuk beberapa protokol lainnya termasuk *Transport Layer Security* (TLS), *Secure Socket Layer* (SSL), *Internet Gopher*, dan HTTPS. Versi *Squid* 3.1 mencakup dukungan protokol IPv6 dan *Internet Content Adaptation Protocol* (ICAP)

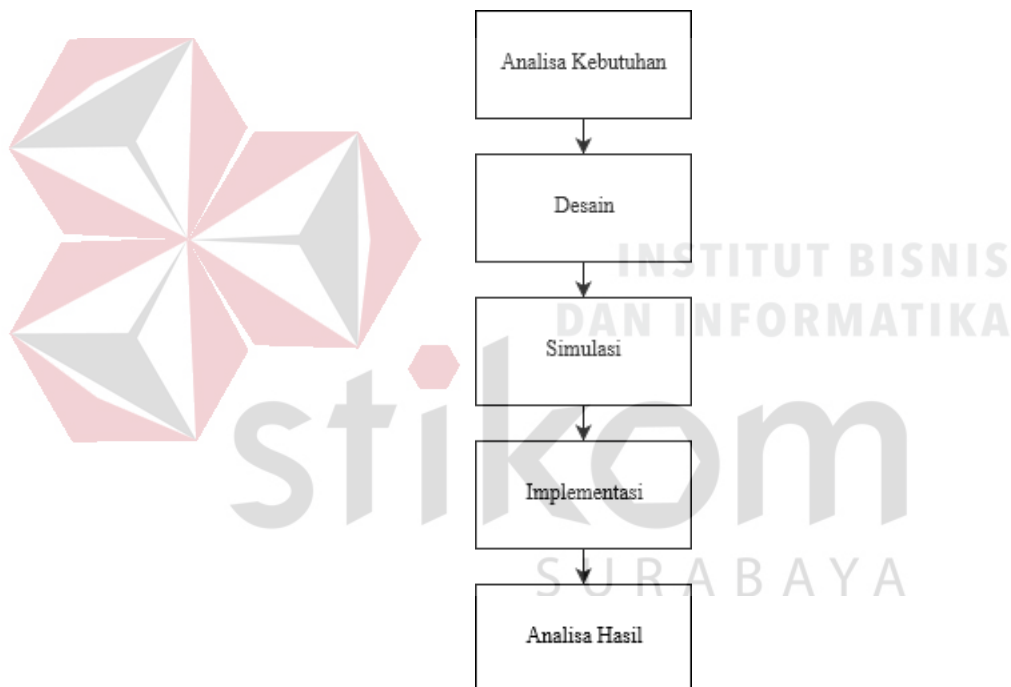


BAB IV

DESKRIPSI KERJA PRAKTIK

4.1. Prosedur Penelitian

Pada pengerjaan *project ini* dibutuhkan prosedur penelitian untuk mengerjakan dan menentukan tahapan yang akan dilalui untuk mengerjakan *project* serta kebutuhan yang dibutuhkan untuk mengerjakan *project*.



Gambar 4.1 Tahapan Pengerjaan

4.1.1. Analisa Kebutuhan

Analisa kebutuhan ini dibutuhkan sebagai bagian awal untuk mengidentifikasi masalah serta kebutuhan yang dibutuhkan untuk menyelesaikan masalah yang ada. Kebutuhan ini bisa berupa metode dan

kebutuhan sistem yang akan digunakan, untuk kebutuhan sistem sendiri berupa *software* dan *hardware*.

A. Analisa Kebutuhan Perangkat Lunak

Adapun kebutuhan perangkat lunak yang dibutuhkan dalam pengerjaan *project* ini :

Tabel 4.1 Kebutuhan Perangkat Lunak

No.	Nama	Fungsi
Client		
1	Linux Ubuntu 18.04	Sebagai sistem operasi yang digunakan pada client
2	Windows 10	
Server		
3	MikroTik	Sebagai sistem operasi yang digunakan pada router
Konfigurasi		
4	Winbox	Aplikasi bawaan MikroTik yang digunakan untuk mengkonfigurasi Router
Simulator		
5	GNS3 Network Simulator	Aplikasi yang digunakan untuk membuat simulasi jaringan
6	Oracle VM Virtualbox Manager	

B. Analisa Kebutuhan Perangkat Keras

Adapun kebutuhan perangkat keras yang dibutuhkan dalam pengerjaan *project* ini :

Tabel 4.2 Kebutuhan Perangkat Keras

No.	Nama
1	Laptop / PC
2	MikroTik RB433
3	Kabel UTP
4	<i>Access Point</i>

C. Analisa Kebutuhan Topologi Jaringan

Untuk kebutuhan topologi jaringan disini menggunakan topologi jaringan yang sudah terdapat pada PT. Cross Network Indonesia, dimana untuk seluruh jaringan PT. Cross Network Indonesia menggunakan topologi *hybrid* yang mengkombinasikan lebih dari 1 macam topologi jaringan. Sedangkan untuk skala jaringan kecil menggunakan topologi *star*, pada skala jaringan kecil ini lah yang akan di implementasikan *proxy server*.

4.1.2. Desain

Pada proses desain akan dibuat alur sistem kerja yang akan digunakan. dimana pada alur sistem kerja ini diharapkan dapat memberikan gambaran mengenai kebutuhan dari *project* yang akan dikerjakan. Desain alur sistem kerja yang akan dibuat nantinya berupa topologi jaringan, dengan adanya topologi jaringan diharapkan akan dapat memberikan gambaran mengenai *project* yang dikerjakan.

4.1.3. Simulasi

Sebelum *project* diterapkan atau diimplementasikan ada baiknya jika *project* tersebut dilakukan dengan membuat sebuah simulasi. Pada *project* ini penulis menggunakan aplikasi *GNS3 Network Simulator* untuk membuat

simulasi topologi dan *project* yang akan digunakan. Setelah membuat simulasi nantinya akan ada pertimbangan jika *project* yang dikerjakan tersebut masih memiliki kekurangan dan lain sebagainya.

4.1.4. Implementasi

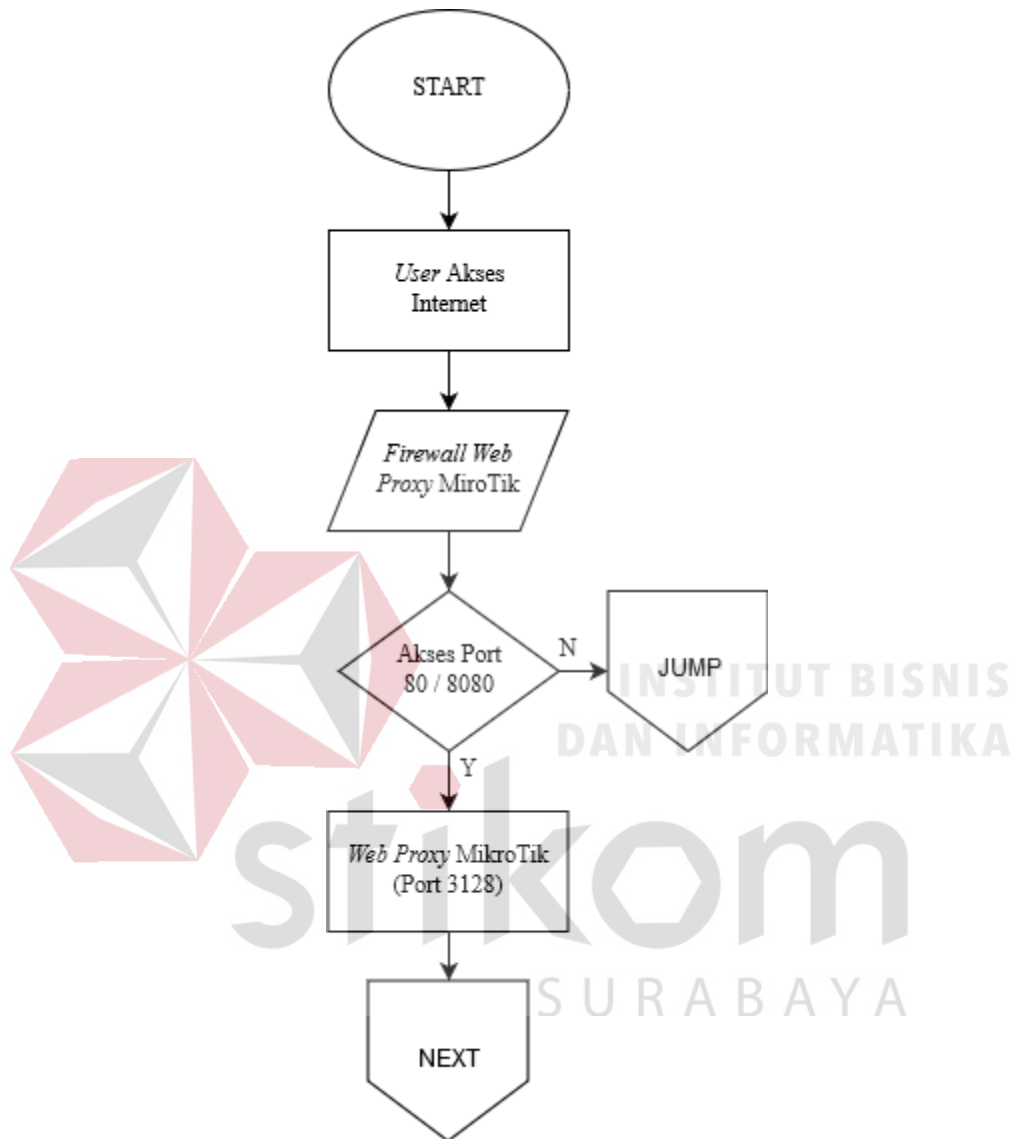
Dalam tahap ini rancangan yang dibuat akan diterapkan pada PT. Cross Network Indonesia. Pada tahap ini akan dilakukan beberapa kegiatan seperti:

- A. Menggunakan topologi jaringan yang sudah terdapat pada PT. Cross Network Indonesia.
- B. Mengkonfigurasi MikroTik RB433.
- C. Implementasi *web proxy* pada MikroTik RB433.

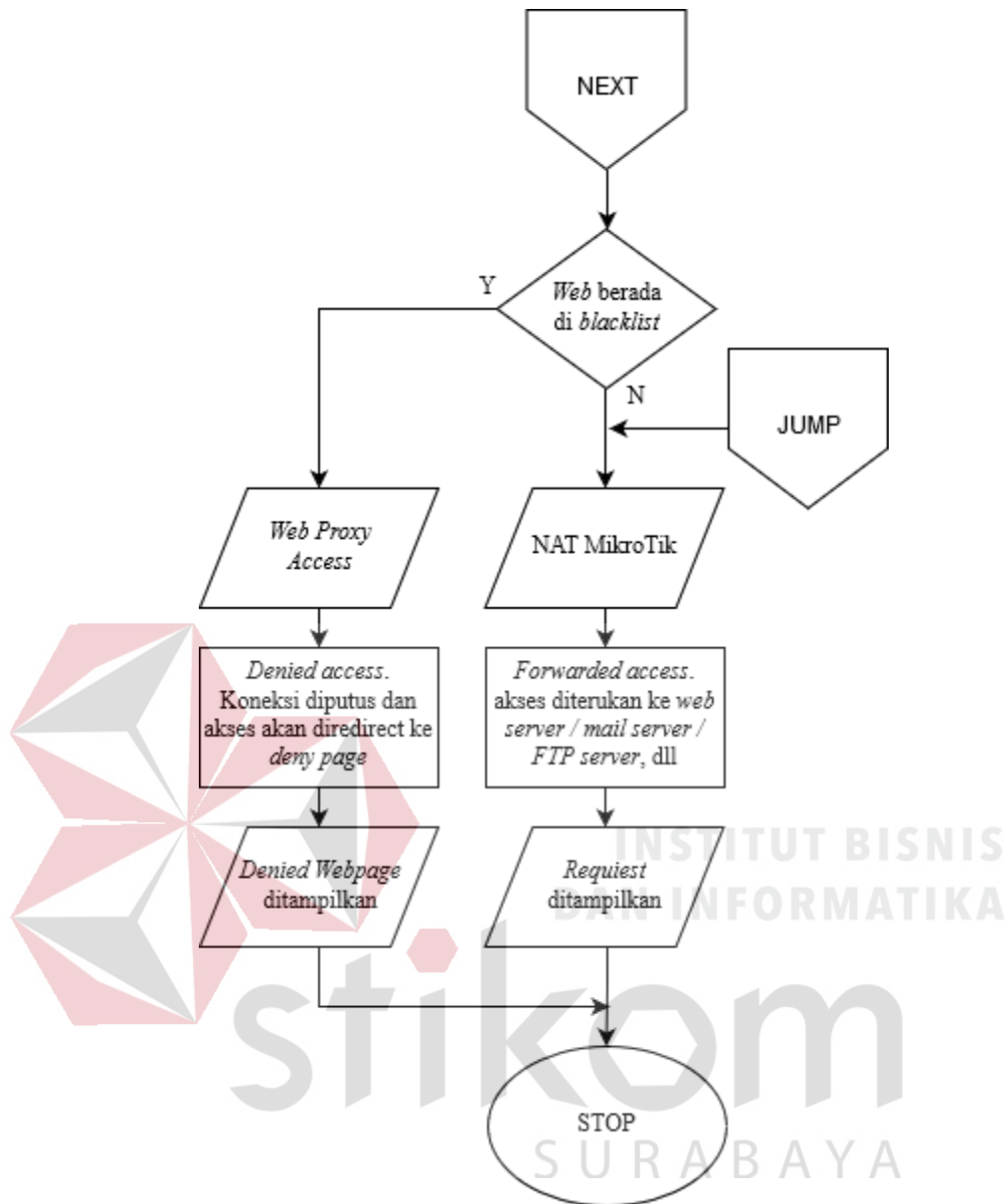
4.1.5. Analisa Hasil

Pada tahap yang terakhir nantinya akan dilakukan Analisa hasil, dimana pada percobaan di tahap simulasi akan di implementasikan yang kemudian akan diambil hasil dari percobaan pada tahap implementasi. Setelah itu hasil akan dianalisa dan disimpulkan. Nantinya hasil analisa berupa nilai yang telah ditentukan menjadi *point* penting. Dan dari analisa tersebut akan dapat dibuktikan apakah *web proxy* dapat berjalan dengan baik atau tidak. Selain itu, untuk kebutuhan analisa *QoS*, penulis akan menggunakan *throughput* sebagai bahan analisa juga.

4.2. Flowchart Cara Kerja



Gambar 4.2 Flowchart Cara Kerja (1)



Gambar 4.3 Flowchart Cara Kerja (2)

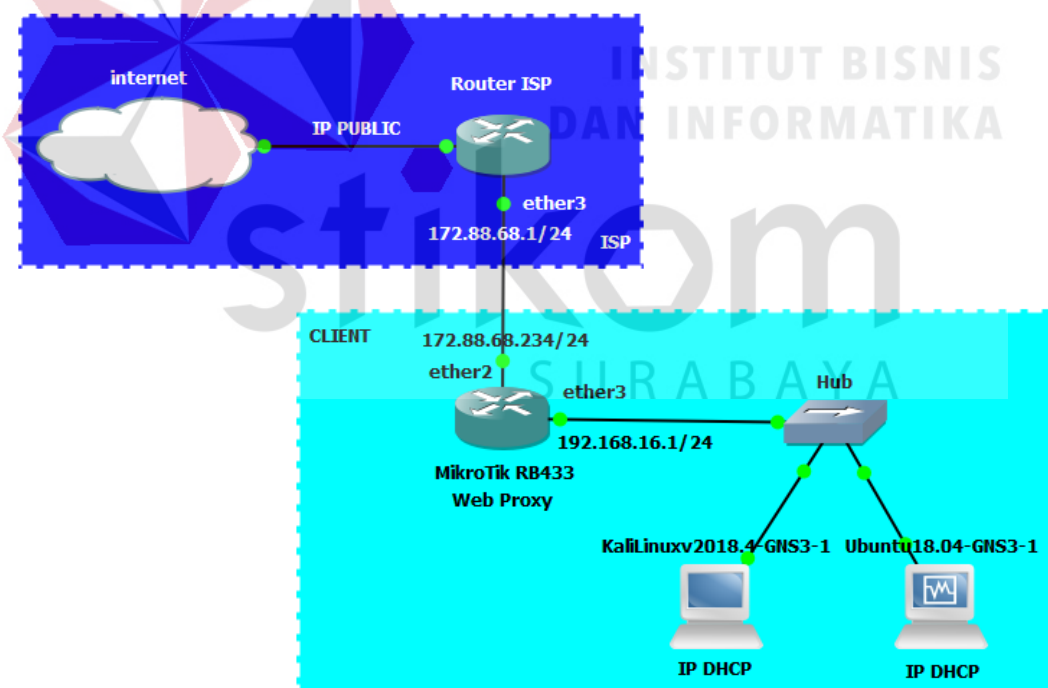
Dari Gambar 4.2 dan Gambar 4.3 dapat dijelaskan cara web proxy bekerja. Ketika user mengakses internet, firewall web proxy pada MikroTik akan melakukan pengecekan, apakah user akan mengakses sebuah webpage atau mengakses internet dengan menggunakan port 80 atau 8080. Jika benar user mengakses sebuah webpage atau mengakses internet dengan menggunakan port 80 atau 8080 maka terlebih dahulu akan melewati web proxy pada MikroTik. Jika user tidak

mengakses sebuah webpage atau mengakses internet dengan menggunakan port 80 atau 8080 maka user akan di bypass melewati web proxy dan akan langsung diarahkan ke internet dengan tujuan yang sesuai dengan yang diminta user.

Ketika akses user melewati web proxy, pada web proxy akan dilakukan pengecekan kembali. Jika webpage yang diakses berada di blacklist web yang akan diblokir maka akses ditolak dan akses internet akan diputus. Jika webpage yang diakses tidak berada di blacklist web maka akses akan langsung diteruskan ke webpage yang dituju.

4.3. Perancangan

4.3.1. Topologi Jaringan



Gambar 4.4 Topologi Jaringan

Pada pengerjaan *project* ini penulis menggunakan topologi jaringan yang sudah ada pada PT. Cross Network Indonesia. Dan untuk jaringan yang akan

digunakan adalah jaringan skala kecil milik PT. Cross Network Indonesia dalam artian bukan seluruh jaringan internet milik PT. Cross Network Indonesia atau jaringan dengan skala besar.

Pada Gambar 4.4 dapat dilihat rancangan topologi yang akan digunakan untuk pengerjaan *project*. Topologi jaringan tersebut juga merupakan simulasi yang akan dilakukan sebelum masuk ke tahap implementasi. Pada topologi jaringan tersebut pada bagian ISP, internet akan terhubung ke *router* ISP. ISP disini yang digunakan adalah milik PT. Cross Network Indonesia yang berarti nantinya IP *public* yang digunakan juga berasal dari PT. Cross Network Indonesia. *Router* ISP ini akan berada di kantor PT. Cross Network Indonesia dan nantinya untuk implementasi *project* akan dilakukan di kantor PT. Cross Network Indonesia.

Pada *router* bagian *client*, nantinya akan mendapat koneksi *internet* dari *router* ISP dimana pada *router* inilah yang akan dilakukan konfigurasi. *Router* pada bagian *client* ini menggunakan MikroTik RB433 dan konfigurasi *web proxy* akan diterapkan didalam *router* tersebut. Untuk *client - client* yang terhubung nantinya juga akan mendapatkan IP secara otomatis dari *router* karena pada *router* akan dikonfigurasi juga DHCP *server*. Jadi nantinya, pada saat *client* melakukan akses internet jalur yang akan dilewati harus melewati *web proxy* yang terdapat pada MikroTik RB433 kemudian ke internet melalui *router* ISP.

4.3.2. Konfigurasi MikroTik

Untuk konfigurasi MikroTik ini pada dasarnya hanya akan melakukan konfigurasi dasar pada MikroTik. Nantinya konfigurasi ini akan menjadikan

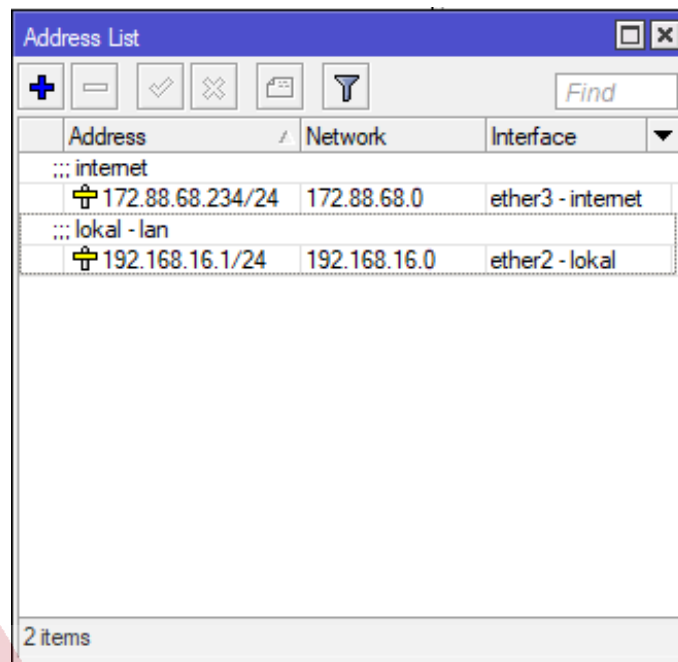
Router MikroTik menjadi *internet gateway* yang dapat menghubungkan *client* ke internet.

Langkah awal untuk melakukan konfigurasi ini terlebih dahulu harus masuk ke dalam *router* MikroTik bisa dengan mode GUI atau CLI. Pada pengerjaan *project* ini penulis menggunakan kedua mode yaitu GUI dan CLI.

Konfigurasi awal adalah dengan masuk ke *router* MikroTik dan kemudian mengkonfigurasi *IP Address*. Untuk konfigurasi *IP Address* yang digunakan hanya 2 *ethernet* dari MikroTik. *Ethernet* pertama digunakan untuk koneksi ke internet, sedangkan *ethernet* kedua digunakan untuk ke lokal lan *client*. Untuk konfigurasi melalui *winbox* masuk ke menu IP lalu pilih *Addresses* kemudian tambahkan seperti pada Gambar 4.5. Untuk konfigurasi melalui terminal atau mode CLI, berikut perintah yang digunakan.

```
[admin@MikroTik@WebProxy] > ip add address=172.88.68.234/24  
interface="ether3 - internet"
```

```
[admin@MikroTik@WebProxy] > ip add address=192.168.16.1/24  
interface="ether2 - lokal"
```

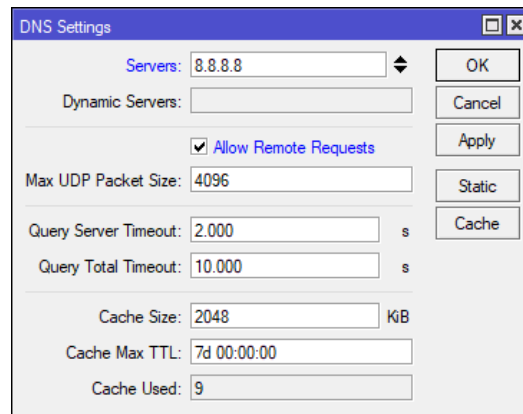


Gambar 4.5 Konfigurasi *IP Address*

Pada Gambar 4.5 dapat dilihat hasil konfigurasi untuk *IP Address*, terdapat 2 *IP address* yang ditambahkan, *IP address* 172.88.68.234/24 ditempatkan pada *ether3* dan digunakan sebagai koneksi ke internet dan *IP address* 192.168.16.1/24 ditempatkan pada *ether2* dan digunakan untuk *IP* lokal LAN.

Langkah selanjutnya, mengkonfigurasi DNS pada Mikrotik ini digunakan agar ketika *user* mengakses internet dapat menggunakan nama *domain* tanpa harus menggunakan IP. Untuk konfigurasi melalui *winbox* masuk ke menu IP lalu pilih *DNS* kemudian tambahkan seperti pada Gambar 4.6. Untuk konfigurasi melalui terminal atau mode CLI, berikut perintah yang digunakan.

```
[admin@MikroTik@WebProxy] > ip dns set servers=8.8.8.8 allow-remote-requests=yes
```

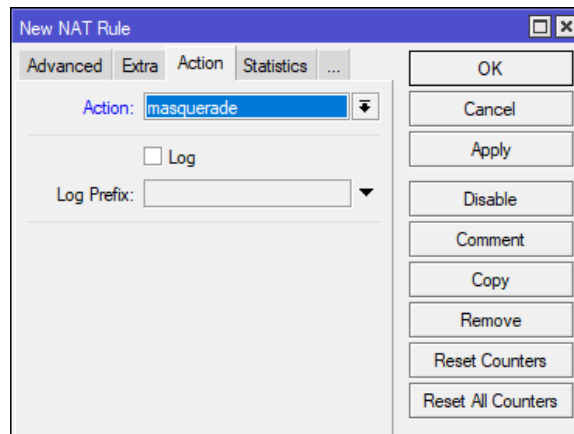


Gambar 4.6 Konfigurasi DNS

Pada Gambar 4.6 dapat dilihat hasil konfigurasi untuk mengatur DNS, DNS yang digunakan dapat disesuaikan dengan kebutuhan. Pada *project* ini DNS yang digunakan adalah DNS milik *Google*. Centang pada bagian *Allow Remote Requests* ini berfungsi agar MikroTik dapat digunakan sebagai DNS *cache*.

Selanjutnya mengkonfigurasi NAT untuk konfigurasi melalui *winbox* masuk ke menu IP lalu pilih *firewall* lalu pilih *tab* NAT kemudian tambahkan seperti pada Gambar 4.7. Untuk konfigurasi melalui terminal atau mode CLI, berikut perintah yang digunakan.

```
[admin@MikroTik@WebProxy] > ip firewall nat add action=masquerade
chain=srcnat
```

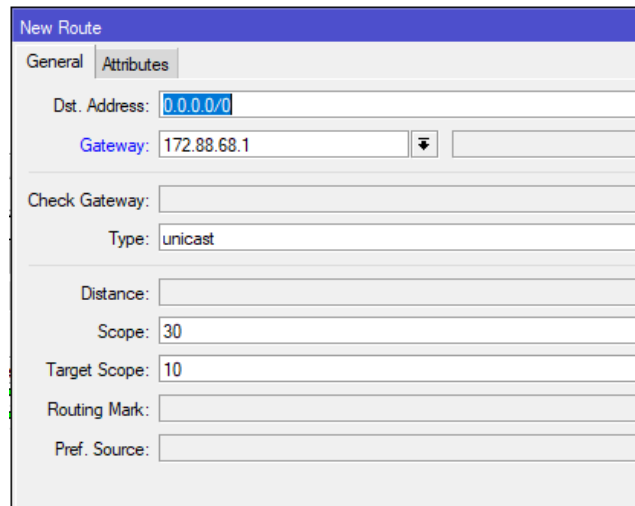


Gambar 4.7 Konfigurasi NAT *Masquerade*

Pada Gambar 4.7 *action* yang digunakan pada *firewall* NAT adalah *masquerade* ini digunakan agar pada saat mengakses internet *user* menggunakan IP *public* yang telah tersedia bukan IP *private*. Pada MikroTik inilah sering disebut dengan *Masquerade* MikroTik

Selanjutnya mengkonfigurasi *gateway* untuk konfigurasi melalui *winbox* masuk ke menu IP lalu pilih *routes* kemudian tambahkan seperti pada Gambar 4.8. Untuk konfigurasi melalui terminal atau mode CLI, berikut perintah yang digunakan.

```
[admin@MikroTik@WebProxy] > ip route add gateway=172.88.68.1
```



New Route	
General	Attributes
Dst. Address: 0.0.0.0	
Gateway: 172.88.68.1	
Check Gateway:	
Type: unicast	
Distance:	
Scope: 30	
Target Scope: 10	
Routing Mark:	
Pref. Source:	

Gambar 4.8 Konfigurasi *Gateway*

Pada Gambar 4.8 *Gateway* yang diisikan adalah IP *Gateway internet* atau IP *Public internet* jika disediakan, konfigurasi ini diperlukan agar *router* yang digunakan dapat terhubung ke internet. Pada bagian *Dst. Address* diisikan IP 0.0.0.0 agar seluruh IP dari semua *interface* menggunakan IP 172.88.68.1 sebagai IP *Gateway*.

Setelah melakukan langkah – langkah diatas saatnya untuk mengetes hasil konfigurasi. Untuk konfigurasi sementara ini seharusnya *router* sudah dapat terkoneksi ke internet. Untuk mengetes hasil konfigurasi buka terminal MikroTik kemudian ketikkan *ping google.com*. Jika hasilnya seperti pada Gambar 4.9 maka *router* sudah berhasil terkoneksi ke internet.

Terminal					
SEQ	HOST	SIZE	TTL	TIME	STATUS
0	172.217.160.14	56	52	45ms	
1	172.217.160.14	56	52	42ms	
2	172.217.160.14	56	52	80ms	
3	172.217.160.14	56	52	43ms	
4	172.217.160.14	56	52	34ms	
5	172.217.160.14	56	52	34ms	
6	172.217.160.14	56	52	74ms	
7	172.217.160.14	56	52	36ms	
8	172.217.160.14	56	52	41ms	
9	172.217.160.14	56	52	38ms	
10	172.217.160.14	56	52	115ms	
11	172.217.160.14	56	52	66ms	
12	172.217.160.14	56	52	81ms	
13	172.217.160.14	56	52	86ms	
14	172.217.160.14	56	52	41ms	
15	172.217.160.14	56	52	33ms	
16	172.217.160.14	56	52	37ms	
17	172.217.160.14	56	52	41ms	
18	172.217.160.14	56	52	60ms	
19	172.217.160.14	56	52	47ms	
sent=20 received=20 packet-loss=0% min-rtt=33ms avg-rtt=53ms max-rtt=115ms					

Gambar 4.9 Hasil *ping google.com*

Jika sudah melakukan konfigurasi dasar pada MikroTik selanjutnya adalah mengkonfigurasi *web proxy* pada MikroTik.

4.3.3. Konfigurasi *Web Proxy* Pada MikroTik

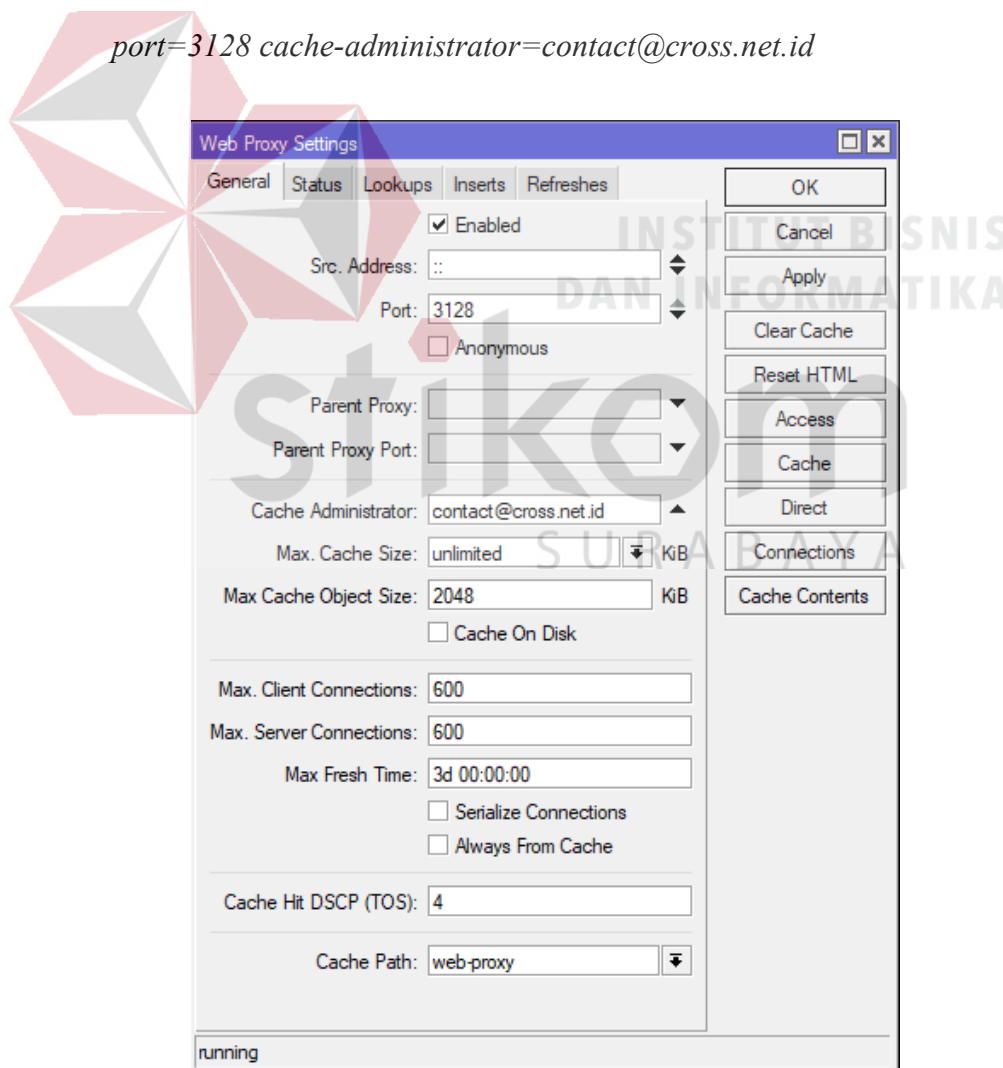
Pada konfigurasi *web proxy* ini nantinya *web – web* yang digunakan untuk pengetesan adalah *web – web social media* dimana pada kantor Cross Network Indonesia tidak diperbolehkan diakses ketika jam kerja.

Perlu diperhatikan untuk *web proxy* pada MikroTik ketika diaktifkan, *web proxy* akan menjalankan *filtering* dan *caching* sekaligus. Untuk *filtering* digunakan untuk membatasi konten – konten yang diakses ataupun *web – web* yang nantinya akan diblokir. Sedangkan *caching* digunakan menyimpan *web* konten dari internet ke *storage* MikroTik. Pada umumnya *storage* yang dimiliki MikroTik tidaklah besar sehingga membutuhkan

storage external, untuk hal seperti ini nantinya juga akan menambah biaya untuk keperluan *storage external*.

Maka dari itu untuk keperluan *project* pada *web proxy* akan dikonfigurasi khusus untuk *filtering* sedangkan penggunaan *caching* tidak digunakan. Untuk awal konfigurasi *web proxy* masuk ke menu IP lalu pilih *web proxy*. Untuk konfigurasi melalui terminal atau mode CLI, berikut perintah yang digunakan.

```
[admin@MikroTik@WebProxy] > ip proxy set enabled=yes
port=3128 cache-administrator=contact@cross.net.id
```

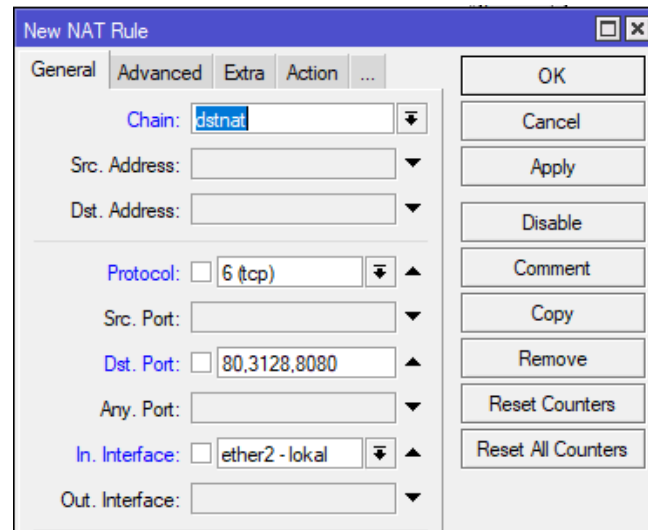
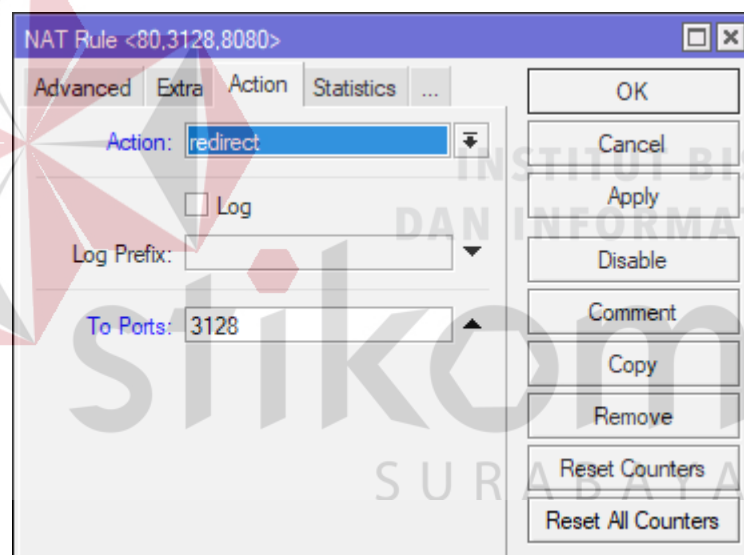


Gambar 4.10 Konfigurasi *Web Proxy*

Dari Gambar 4.10 untuk konfigurasi awal, centang pada bagian *enabled* dan kemudian isikan port *proxy*. Umumnya port *proxy* yang sering digunakan adalah 3128. Pada bagian *cache administrator* isikan *email support* yang digunakan untuk mengatasi *web proxy*.

Selanjutnya melakukan konfigurasi *transparent web proxy*, ini diperlukan, karena jika tidak dilakukan konfigurasi nantinya setiap *user* yang terhubung ke *router* dan akan melakukan akses internet *user* tersebut harus melakukan konfigurasi manual pada setiap *browser* agar menggunakan port *proxy*. Tentu sangat merepotkan jika *user* yang mengakses sangat banyak. Maka dari itu diperlukan *transparent web proxy* agar setiap *user* yang mengakses internet atau melakukan *request* akan dipaksa atau dialihkan ke port *web proxy*. Untuk konfigurasi *transparent web proxy*, pada MikroTik masuk menu IP lalu pilih *firewall* lalu pilih tab NAT. Untuk konfigurasi melalui terminal atau mode CLI, berikut perintah yang digunakan.

```
[admin@MikroTik@WebProxy] > ip firewall nat add chain=dstnat
protocol=tcp dst-port=80,3128,8080 in-interface="ether2 - lokal"
action=redirect to-ports=3128
```

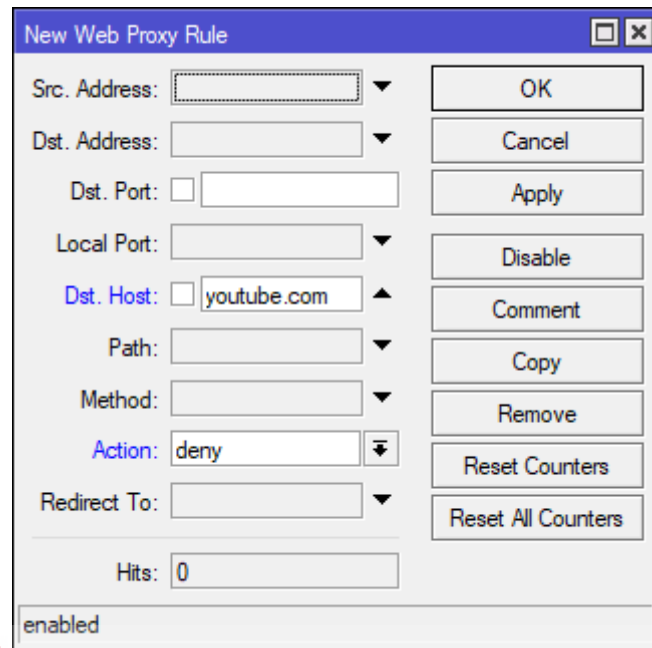
Gambar 4.11 Konfigurasi *Transparent Web Proxy* (1)Gambar 4.12 Konfigurasi *Transparent Web Proxy* (2)

Dari Gambar 4.11 dan Gambar 4.12 dapat dilihat konfigurasi *transparent web proxy*. Pada Gambar 4.11 bagian *chain* diisi dengan *dstnat*, *chain* ini sendiri berfungsi untuk menentukan jenis *traffic* yang akan diolah, dan *chain* yang digunakan adalah *dstnat*, *dstnat* sendiri digunakan untuk mengubah alamat tujuan pada sebuah paket data dan untuk membuat host

dalam jaringan lokal dapat diakses dari luar jaringan atau internet dengan cara NAT akan mengganti alamat IP tujuan paket dengan alamat IP local. Kemudian pada bagian *protocol* diisikan *6(tcp)*, ini berarti protokol yang digunakan selama pengolahan *traffic* dan paket adalah *tcp*, selain protokol tersebut *traffic* dan paket tidak diolah. Kemudian pada bagian *dst. port* digunakan untuk mengecek apakah *user* mengakses *port* sesuai dengan yang ditentukan. Dan pada bagian *In interface* digunakan untuk mengecek apakah *traffic* berada pada *interface* yang telah ditentukan. Kemudian pada *tab action*, pada bagian *action* diisikan *redirect* ini digunakan untuk mengarahkan atau mengubah *port* menuju *port* pada *To Ports* yaitu *port 3128*

Selanjutnya, masukan seluruh *web* yang akan diblok. Sebagai contoh untuk pengetesan maka masukan salah satu *web* terlebih dulu. Nantinya *web* – *web* yang akan dimasukan ke dalam *list* dan diblok akan menjadi *web blacklist* yang akan diblokir akses nya. Untuk menambahkan masuk ke menu IP lalu pilih *Web Proxy* kemudian cari *Access*. Untuk konfigurasi melalui terminal atau mode CLI, berikut perintah yang digunakan.

```
[admin@MikroTik@WebProxy] > ip proxy access add dst-  
host="youtube.com" action=deny comment="youtube"
```



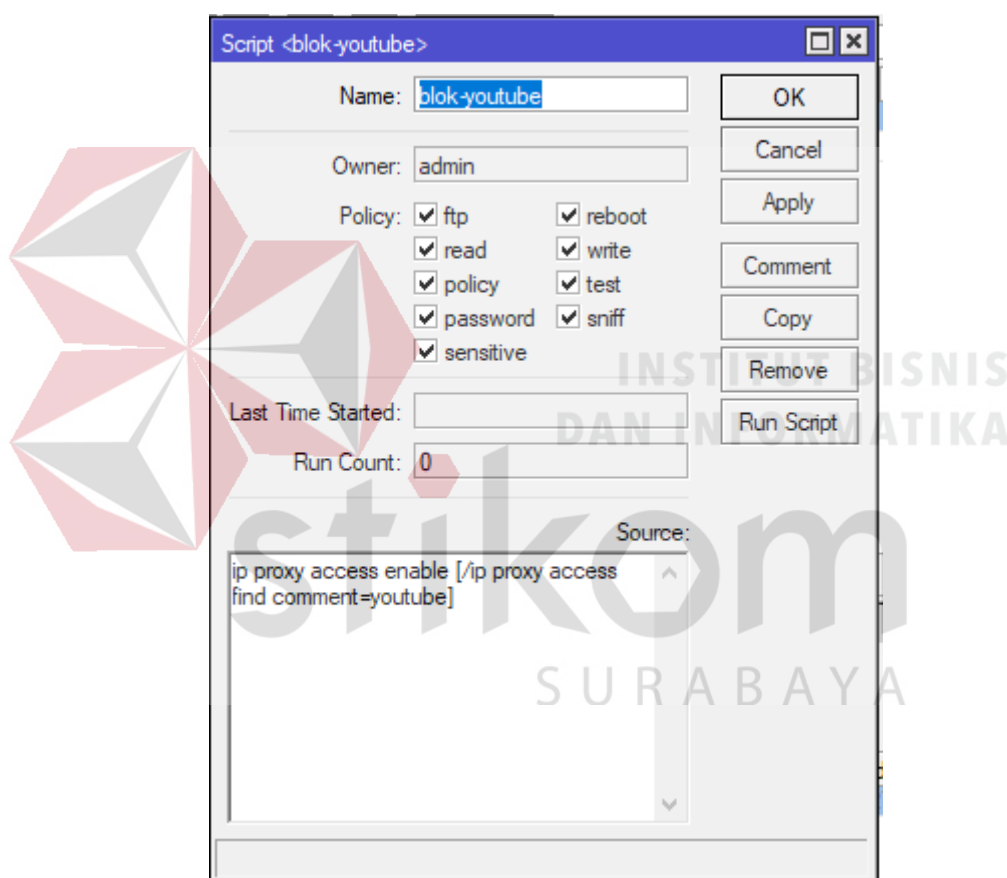
Gambar 4.13 *Blacklist web* yang diblokir

Dari Gambar 4.13 konfigurasi untuk mengaktifkan *blacklist web* yang akan diblokir. Pada bagian *Dst. Host* isikan *website* yang akan diblokir dan pada *action* pilih *deny* yang nantinya berfungsi untuk menolak akses *website* tersebut ketika ada *user* yang *request* untuk mengakses *website*.

Karena pemblokiran *web* ini bersifat tidak selamanya dengan begitu dibutuhkan penjadwalan untuk memblokir *web – web* yang telah didaftarkan ke dalam *blacklist web*. Pada pengerjaan *project* ini *web – web* didalam *blacklist web* akan diblokir selama waktu jam kerja dan akan dibuka setelah jam kerja. Untuk mengaktifkan buka menu *system* lalu pilih *scripts*. Untuk konfigurasi melalui terminal atau mode CLI, berikut perintah yang digunakan.

```
[admin@MikroTik@WebProxy] > system script add name="blok-  
youtube" source="ip proxy access enable [/ip proxy access find  
comment=youtube]"
```

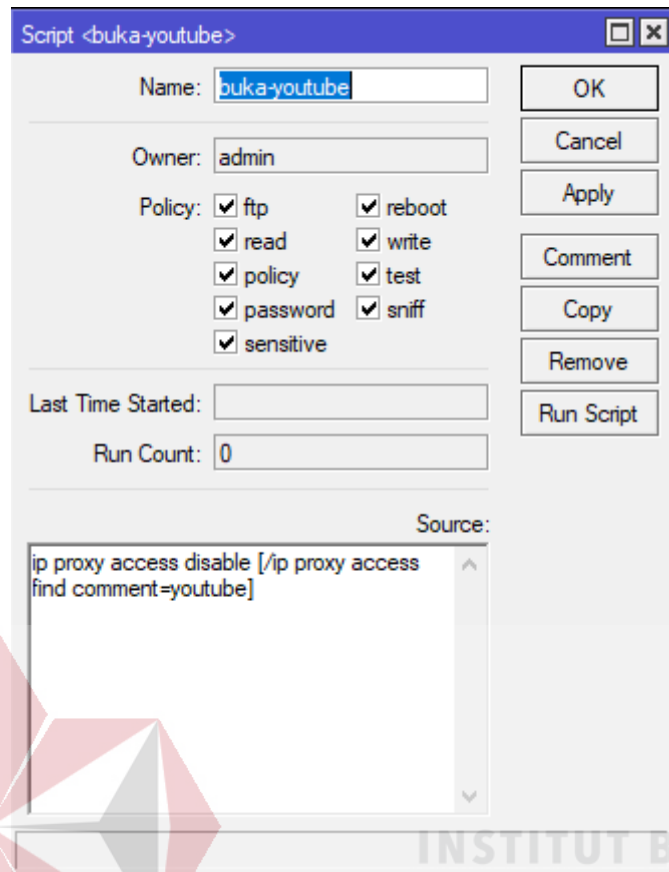
```
[admin@MikroTik@WebProxy] > system script add name="buka-  
youtube" source="ip proxy access disable [/ip proxy access find  
comment=youtube]"
```



Gambar 4.14 Script untuk mengaktifkan web proxy

Dari Gambar 4.14 konfigurasi digunakan untuk mengaktifkan script blok-youtube. Pada bagian *source* isikan script berikut

```
ip proxy access enable [/ip proxy access find comment=youtube]
```



Gambar 4.15 Script untuk menonaktifkan *web proxy*

Dari Gambar 4.15 konfigurasi digunakan untuk mengaktifkan *script* buka-youtube. Pada bagian *source* isikan *script* berikut

ip proxy access disable [/ip proxy access find comment=youtube]

Setelah itu buat penjadwalan waktu. Buka menu *system* lalu pilih *scheduler*. Untuk konfigurasi melalui terminal atau mode CLI, berikut perintah yang digunakan.

```
[admin@MikroTik@WebProxy] > system scheduler add
name="jadwal-blok-youtube" start-time=08:00:00 interval=24:00:00 on-
event=blok-youtube
```

```
[admin@MikroTik@WebProxy] > system scheduler add
name="jadwal-buka-youtube" start-time=17:00:00 interval=24:00:00 on-
event=buka-youtube
```

New Schedule

Name:

Start Date:

Start Time:

Interval:

On Event:

Owner:

Policy: ☒ ftp ☒ reboot ☒ read ☒ write ☒ policy ☒ test ☒ password ☒ sniff ☒ sensitive

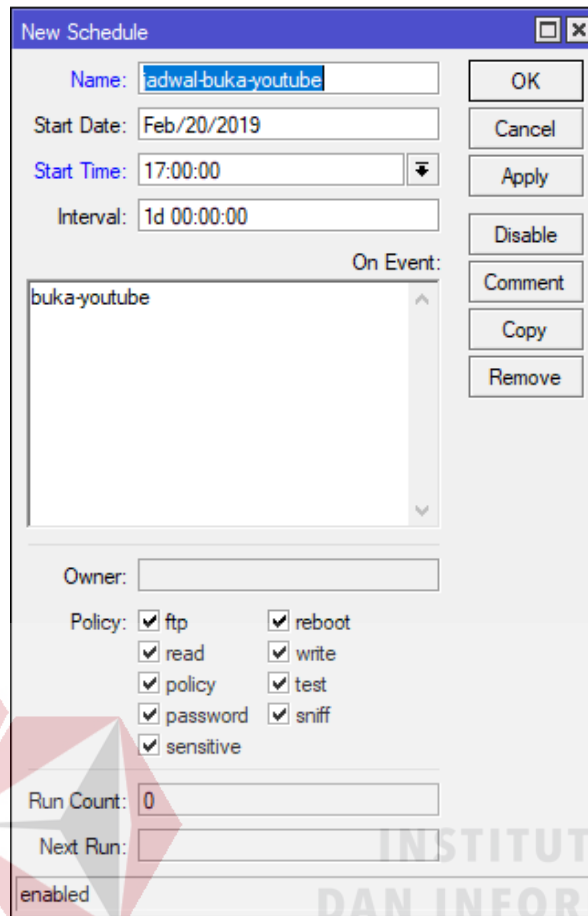
Run Count:

Next Run:

☒ enabled

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

Gambar 4.16 Penjadwalan untuk *script* blok-youtube



New Schedule

Name:

Start Date:

Start Time:

Interval:

On Event:

Owner:

Policy: ☒ ftp ☒ reboot
☒ read ☒ write
☒ policy ☒ test
☒ password ☒ sniff
☒ sensitive

Run Count:

Next Run:

☒ enabled

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

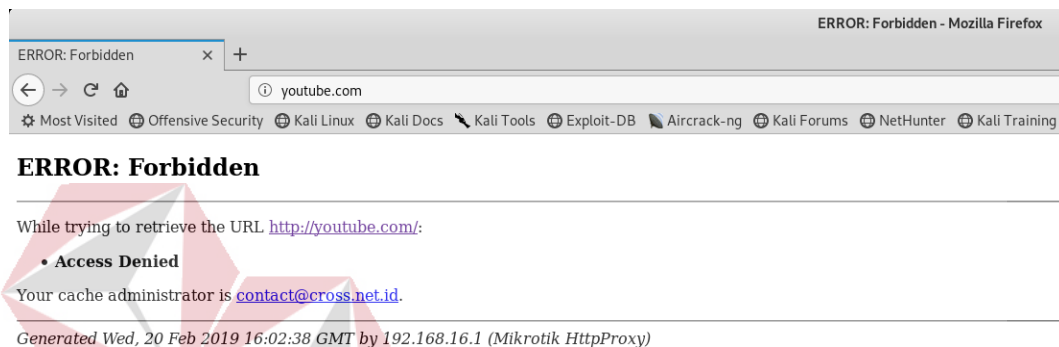
Gambar 4.17 Penjadwalan untuk *script* buka-youtube

Pada Gambar 4.16 dan Gambar 4.17 konfigurasi untuk mengatur kapan *script* yang telah dibuat sebelumnya dijalankan, pada bagian *start time* isikan pada jam berapa *script* akan dijalankan dan pada bagian *interval* isikan berapa lama waktu yang diperlukan untuk menjalankan *script*. Setelah itu pada bagian *on event* isikan nama *script* yang telah dibuat.

4.4. Hasil dan Pembahasan

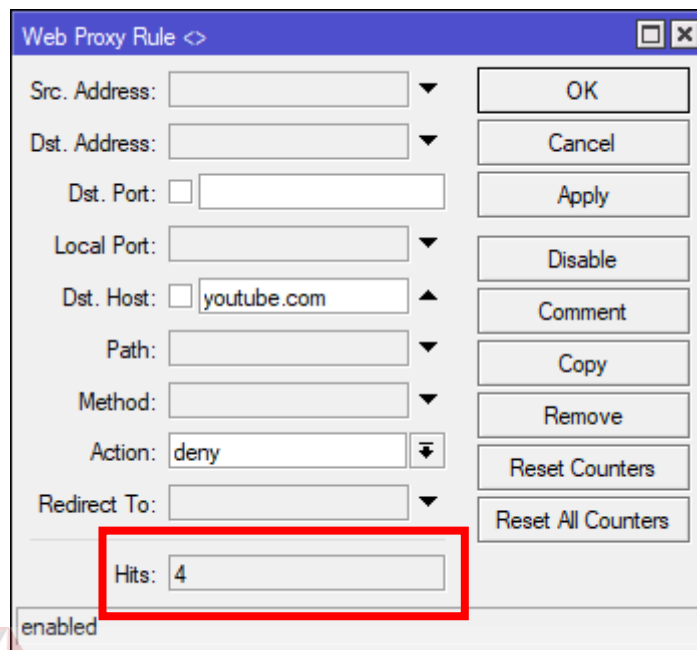
- Tampilan situs *web* yang telah berhasil terblokir oleh *web proxy*

Setelah melakukan seluruh konfigurasi pada *web proxy* tahap selanjutnya adalah pengujian. Pengetesan bisa dilakukan langsung pada *device client* yang terhubung ke *router* atau terhubung ke jaringan *router* tersebut.



Gambar 4.18 Pengujian *web proxy*

Pada gambar diatas dilakukan pengujian terhadap *website youtube.com* dimana *website youtube.com* telah dimasukkan kedalam *blacklist web* dan dari hasil ketika *website* diakses maka akan muncul *denied webpage* dari *web proxy*.



Gambar 4.19 Jumlah *counter* pada *hits* yang terus bertambah

Jika ingin memastikan berapa banyak *user* yang mengakses, bisa dilakukan pengecekan di dalam *router* pada bagian *web proxy* untuk melihat jumlah berapa kali *website* yang diblokir diakses oleh *user*. Pada gambar diatas dapat dilihat pada bagian *hits* tersebut sekarang jumlahnya menjadi 4, dan jumlah pada *hits* tersebut akan terus bertambah apabila terdapat *user* yang mencoba untuk mengakses *website* tersebut.

- **Penjadwalan waktu akses *social media***

Pada konfigurasi sebelumnya telah dibuat penjadwalan waktu akses untuk *website social media*. Adapun waktu penjadwalan pada jam kerja (08:00 – 17:00 WIB) akses *website social media* dimatikan dan pada diluar jam kerja akses dibuka kembali. Beberapa situs yang berhasil diblokir pada saat jam kerja oleh *web proxy* bisa dilihat pada table dibawah.

Tabel 4.3 Hasil penjadwalan waktu akses *social media*

Content	Waktu	
	08:00 - 17:00 WIB	17:01 - 07:59 WIB
Social Media		
Instagram	Akses Ditolak	Akses Diijinkan
Twitter	Akses Ditolak	Akses Diijinkan
Facebook	Akses Ditolak	Akses Diijinkan
YouTube	Akses Ditolak	Akses Diijinkan
Pinterest	Akses Ditolak	Akses Diijinkan

- **Penggunaan CPU**

Untuk penggunaan CPU pada *web proxy* MikroTik bisa dibilang *resource* yang digunakan besar. Apabila *hardware* yang digunakan tidak mendukung bukan tidak mungkin *hardware* tersebut bisa cepat panas pada saat pemakaian, karena pada saat penggunaan *router* akan dinyalakan terus menerus hingga waktu *maintenance* yang ditentukan. Maka dari itu sangat direkomendasikan mencari *hardware router* MikroTik yang mendukung untuk penggunaan fitur *web proxy* misal seperti RB951G. Pada *project* ini penulis menggunakan RB433 dimana dari segi *hardware* masih mendukung untuk penggunaan fitur *web proxy* namun *hardware* akan mendapatkan masalah apabila dinyalakan secara terus menerus.

- **Perbandingan dengan menggunakan *firewall***

Ketika *web proxy* digunakan sebagai *filtering* maka fitur ini lebih terasa penggunaannya daripada menggunakan *firewall* MikroTik dengan maksud apabila *web proxy* diaktifkan dan ingin memblokir suatu *web* maka terdapat *denied page* dari *web proxy* yang akan tampil dengan begitu *user* dapat

mengetahui apabila *website* tersebut benar adanya jika diblokir. Berbeda dengan *web proxy*, ketika ingin menggunakan fitur *firewall* dan mengaktifkan fitur *firewall* sebagai *filtering website* maka harus menambahkan *rule* dan *rule* yang ditambahkan pun juga tidak sedikit. Dan seorang *user* tidak dapat mengetahui dengan pasti apakah *website* tersebut diblokir atau *down* dari *server*-nya.

Namun disisi lain untuk penggunaan *resource*, *web proxy* memang membutuhkan *resource hardware* yang besar sedangkan penggunaan fitur *firewall* sebagai *filtering* membutuhkan *resource* yang sedikit. Itulah sebabnya terdapat berbagai cara untuk melakukan *filtering website content* pada MikroTik dengan berbagai macam kelebihan dan kekurangan.



Gambar 4.20 Hasil *filtering website* menggunakan *firewall*

Pada jaringan PT. Cross Network Indonesia khususnya kantor menggunakan fitur *firewall* sebagai *filtering website*. Dan pada gambar diatas

dapat dilihat bagaimana tampilan ketika *website youtube.com* diblokir menggunakan *firewall*.

- **Masalah MikroTik tidak dapat memblokir koneksi HTTPS**

Kelemahan *web proxy* yang masih tidak dapat dihindari adalah ketika *web proxy* mengharuskan memblokir koneksi *website* yang menggunakan *protocol secure* seperti HTTPS sekalipun *website* tersebut sudah dimasukan kedalam *blacklist website*, *website* tersebut masih dapat diakses. Ini dikarenakan *website* yang menggunakan *protocol secure* HTTPS memiliki enkripsi sendiri didalam *website* tersebut dan ketika mengakses *website* yang menggunakan HTTPS maka secara otomatis *url* yang dikirimkan akan dienkripsi dan dimana oleh *web proxy* enkripsi tersebut tidak dapat dibaca sehingga ketika *web proxy* membaca *web* yang menggunakan HTTPS maka *web proxy* akan melakukan *by-pass*.

- **Pemblokiran berdasarkan kategori tertentu**

Tabel 4.4 Tabel hasil pengujian (1)

Content	Pemblokiran Tipe File	
	Proxy	Non-Proxy
File Type(s)		
mp4	Akses Ditolak	Akses Diijinkan
mp3	Akses Ditolak	Akses Diijinkan
mkv	Akses Ditolak	Akses Diijinkan
jpg	Akses Diijinkan	Akses Diijinkan
pdf	Akses Diijinkan	Akses Diijinkan

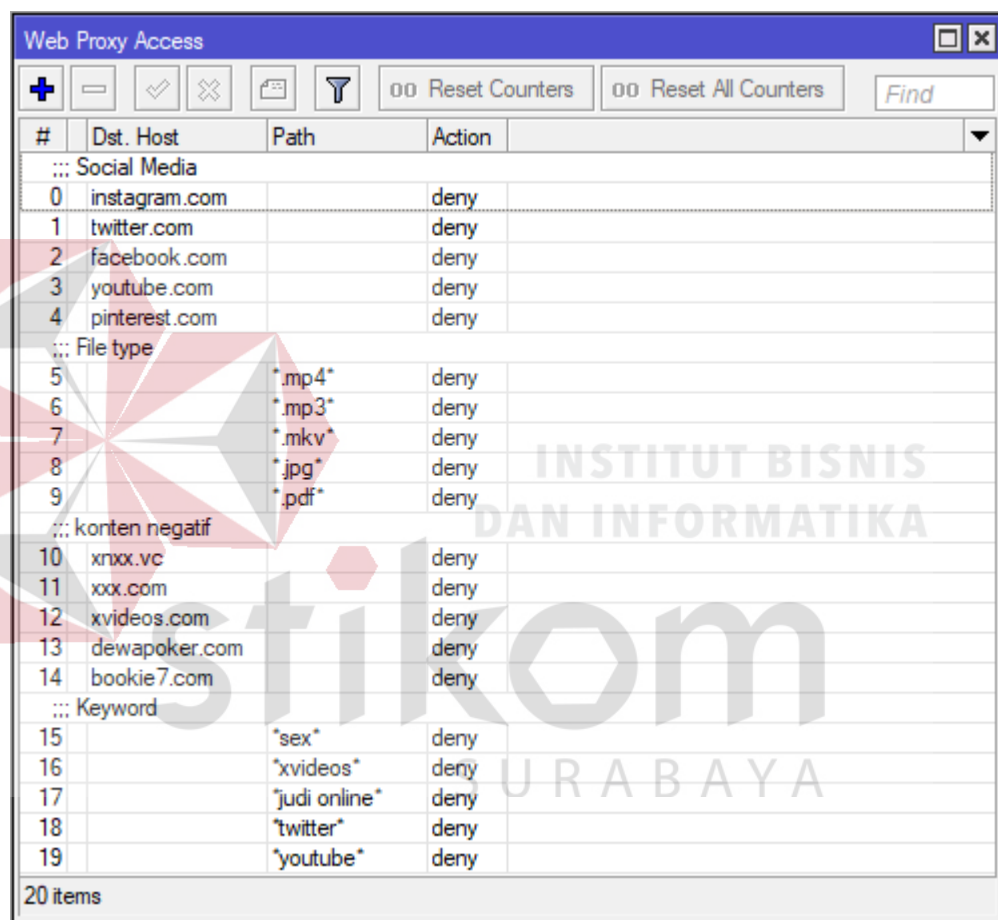
Tabel 4.5 Tabel hasil pengujian (2)

Content	Pemblokiran Konten Negatif	
	Proxy	Non-Proxy
Negative Content		
xnxx.vc	Akses Ditolak	Akses Diijinkan
xvideos.com	Akses Diijinkan	Akses Diijinkan
xxx.com	Akses Diijinkan	Akses Diijinkan
dewapoker.com	Akses Ditolak	Akses Diijinkan
bookie7.com	Akses Ditolak	Akses Diijinkan
Content	Pemblokiran Keyword	
	Proxy	Non-Proxy
Keyword		
Sex	Akses Ditolak	Akses Diijinkan
xvideos	Akses Ditolak	Akses Diijinkan
Judi Online	Akses Ditolak	Akses Diijinkan
Twitter	Akses Ditolak	Akses Diijinkan
Youtube	Akses Ditolak	Akses Diijinkan

Pada Tabel 4.4 dan Tabel 4.5 dapat dilihat *list* hasil pengujian dengan menggunakan beberapa *website* dan konten negatif. Pada bagian pemblokiran tipe file dilakukan dengan melakukan *download file* dengan menggunakan tipe file yang telah ditentukan hasilnya pada saat melakukan *download file mp4, mp3, dan mkv*, *web proxy* telah aktif dan berhasil melakukan blok koneksi. Namun pada saat melakukan *download file* dengan tipe file *jpg* dan *pdf*, *web proxy* tidak dapat melakukan pemblokiran ini dikarenakan *website* yang bersangkutan menggunakan koneksi *secure* atau HTTPS dimana *web proxy* tidak dapat melakukan *drop* koneksi.

Pada bagian permblokiran konten negatif terdapat beberapa *website* yang tidak bisa diblokir, sama seperti penjelasan sebelumnya ini dikarenakan *website* menggunakan koneksi *secure* atau HTTPS. Sedangkan pada bagian pemblokiran

keyword semua *keyword* yang telah dimasukkan ke dalam *blacklist* berhasil di blokir. Pemblokiran ini akan berhasil apabila pencarian kata atau *keyword* ini tidak dilakukan dengan menggunakan *search engine* (seperti *Google*, *Yahoo*, dan lain – lain). Pada Gambar 4.21 menunjukkan hasil *update* untuk seluruh *blacklist* yang digunakan untuk pengujian



#	Dst. Host	Path	Action
... Social Media			
0	instagram.com		deny
1	twitter.com		deny
2	facebook.com		deny
3	youtube.com		deny
4	pinterest.com		deny
... File type			
5		*.mp4*	deny
6		*.mp3*	deny
7		*.mkv*	deny
8		*.jpg*	deny
9		*.pdf*	deny
... konten negatif			
10	xnxx.vc		deny
11	xxx.com		deny
12	xvideos.com		deny
13	dewapoker.com		deny
14	bookie7.com		deny
... Keyword			
15		*sex*	deny
16		*xvideos*	deny
17		*judi online*	deny
18		*twitter*	deny
19		*youtube*	deny

20 items

Gambar 4.21 *Update blacklist web proxy*

BAB V

PENUTUP

Pada *project* ini telah dibuat sebuah *web proxy* yang menggunakan MikroTik yang diterapkan pada jaringan PT. Cross Network Indonesia. Dari hasil pengujian pada beberapa *website* dan konten negatif di internet masih terdapat beberapa konten yang masih belum bisa diblokir oleh MikroTik salah satunya adalah karena *web proxy* MikroTik tidak dapat memblokir koneksi HTTPS. Dari *project* yang telah dibuat ini tingkat keberhasilan pada *project* bisa mencapai 100% apabila *web proxy* memblokir *blacklist website* yang berasal dari ketikan melalui *url* dan bukan dari mesin pencarian atau *search engine* (seperti *Google*, *Yahoo*, dan lain – lain). Dan pada *project* ini sebagian besar sudah memenuhi harapan dimana *web proxy* dapat memblokir konten – konten negatif yang berada pada internet.

5.1. Kesimpulan

Kesimpulan yang diperoleh dalam Membangun *web proxy* pada jaringan PT. Cross Network Indonesia menggunakan MikroTik adalah sebagai berikut :

1. Konfigurasi dan perancangan *web proxy* dilakukan di dalam router MikroTik.
2. Pada *project* ini *web proxy* telah berhasil dibuat dengan menggunakan MikroTik dan dengan cara yang telah dijelaskan pada bagian perancangan.
3. Menggunakan topologi jaringan yang sudah ada milik PT. Cross Network Indonesia.
4. Sistem pemblokiran untuk situs – situs *web* yang tidak diinginkan telah berhasil.

5. Untuk *web* yang menggunakan *protocol secure* seperti HTTPS masih belum bisa sepenuhnya terblokir.
6. *Web Proxy* berhasil mengatur waktu untuk penggunaan *web social media* pada jam kerja.
7. Kinerja *resource* pada *hardware router* MikroTik yang digunakan meningkat ketika mengaktifkan *web proxy*.
8. Perbandingan pemblokiran *website* dengan menggunakan *web proxy* dan *firewall* memiliki kelebihan dan kekurangan masing – masing.
9. Ketika *web proxy* diaktifkan dan telah berhasil memblokir suatu *website* maka akan tampil *denied page* dan *web proxy* MikroTik akan melakukan *counter*.
10. Beberapa konten – konten negatif yang digunakan pada *project* ini masih belum semua bisa diblokir

5.2. Saran

Adapun saran yang penulis ingin sampaikan adalah :

1. Sering melakukan pengecekan atau *maintenance* terhadap *router* baik dari konfigurasi maupun *hardware* karena mengingat *resource* yang digunakan untuk mengaktifkan *web proxy* besar
2. Untuk mendapatkan hasil maksimal agar *web – web* yang diblokir dapat sepenuhnya bisa terblokir terutama untuk *web* yang menggunakan *protocol secure* HTTPS bisa mengombinasikan *web proxy* dengan *firewall* pada MikroTik atau dengan metode yang lain.
3. Untuk mengurangi penggunaan *bandwidth* yang besar fitur *caching web proxy* pada MikroTik sangat memungkinkan untuk digunakan

DAFTAR PUSTAKA

- Arjuni, S. (2010). *Perancangan dan Implementasi Proxy server dan Manajemen Bandwidth Menggunakan Linux Ubuntu Server. (Studi Kasus di Kantor Manajemen PT.Wisma Bumiputera Bandung). Tugas Akhir*. Institut Teknologi Bandung: Bandung: Tidak diterbitkan.
- Cisco Systems, Inc. (2019). *Cisco RV042 Dual WAN VPN Router*. Retrieved from Cisco: <https://www.cisco.com/c/en/us/products/routers/rv042-dual-wan-vpn-router/index.html>
- DTC netconnect. (2019). *MACAM-MACAM JARINGAN KOMPUTER*. Retrieved from dtcnetconnect: <http://www.dtcnetconnect.com/AMP/index.php/blogs/315-macam-macam-jaringan-komputer>
- Edu, T. (2017, December 15). *TCP/IP, Basics of TCP/IP and OSI Model*. Retrieved from Medium: <https://medium.com/@tuplesedu/tcp-ip-6a2455ab9fa6>
- Husaini. (2008). *Implementasi PC Router, DNS Server, Active Directori dan Proxy Server Menggunakan Windows Server 2003 untuk Pengembangan Jaringan Komputer, Skripsi, Ilmu Komputer, Universitas Gadjah Mada, Yogyakarta*.
- jaringankomputer.org. (2019). *Jaringan Dasar Dan Konsep Dasar-Dasar Jaringan*. Retrieved from Jaringan Komputer: <https://jaringankomputer.org/jaringan-dasar-dan-konsep-dasar-dasar-jaringan/>

Maxmanroe. (2019). *Pengertian Proxy Server Router*. Retrieved from Maxmanroe.com: <https://www.maxmanroe.com>

MikroTik, inc. (n.d.). *RB951G-2HnD*. Retrieved from MikroTik: <https://mikrotik.com/product/RB951G-2HnD#fndtn-gallery>

PT Cross Network Indonesia. (2018). *Company Profile*. Surabaya.

Purbo, O. W. (2000). *Linux Untuk Warung Internet*. Jakarta: Elex Media Komputindo.

Riadi, I. (2011). Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik. *JUSI Vol. 1, No.1* .

Staff of Linux Journal. (2004). Linux Journal Issue 126 October 2004. *Build Your Own Router, SSC, Inc.*

Tanautama, L. (1996). *Jaringan Komputer*. Jakarta: Elex Media Komputindo.

Taringaan, A. (2009). *Bikin Gateway Murah Pakai Mikrotik*. Yogyakarta: Penerbit Ilmu Komputer.

wikipedia. (2019). *internet*. Retrieved from wikipedia ensiklopedia bebas: <https://id.wikipedia.org/wiki/Internet>

Wulandari, R. (2016). ANALISIS QoS (QUALITY OF SERVICE) PADA JARINGAN INTERNET (STUDI KASUS : UPT LOKA UJI TEKNIK PENAMBANGAN JAMPANG KULON LIPI). *Jurnal Teknik Informatika dan Sistem Informasi Volume 2 Nomor 2 Agustus 2016* .