PERBANDINGAN RELIABILITY OPEN VPN DENGAN VPN IPSEC

Ria Rizki Panola Sari [1], Ilman Zuhri Yadi [2*], Suryayusra [3]
Fakultas Ilmu Komputer, Universitas Bina Darma
Email: riarizki366@gmail.com[1], ilmanzuhriyadi@binadarma.ac.id[2*], suryayusra@binadarma.ac.id[3]

ABSTRACT

Comparison of network devices is the ability of a tool to work properly and know the tool if it is used to build a network. Microtic Router is a tool used to build a network in real. Evaluation of the performance of a proxy-based router network, aims to find out which is more optimal for building a VPN network and which is more reliable between OVPN and IPSec. To find out how much the performance or reliability of the proxy router tool using fiber optics and comparing between OVPN and IPSec, we must therefore make a measurement and test using the RMA testing method on the VPN network. RMA parameters used are reliability, maintainability, more availability to tools such as microtic routers in this study using PRTG Monitoring Tools and getting results from measurements, knowing Reliability, Maintainability and Availability.

Keywords: Comparison of network devices, Microtic Router, Fiber Optic, OVPN, IPSec, RMA (Reliability, Maintainability, Availability

1. PENDAHULUAN

Teknologi informasi saat ini telah berkembang sangat pesat. Munculnya teknologi-teknologi baru sangat membantu dalam kegiatan bisnis suatu perusahaan. Selain didukung teknologi terbaru, kebutuhan akan informasi secara *real time*, kinerja pada suatu jaringan merupakan suatu faktor penting dalam keberhasilan bisnis suatu perusahaan. Untuk mendukung keberhasilan tersebut, maka dibutuhkannya suatu teknologi yang dapat digunakan untuk menghubungkan perangkat yang berada diluar jaringan internet agar dapat terhubung ke dalam satu jaringan dengan aman kapanpun dan dimanapun. Maka banyak perusahaan baik perusahaan besar maupun kecil berlomba-lomba untuk menerapkan teknologi yang ada.

Setiap perusahaan pastinya akan memiliki cabang-cabang perusahaan. Kantor-kantor tersebut tentu memiliki kebutuhan untuk saling berhubungan antara satu dengan yang lainnya, Perusahaan cabang biasanya masih berada dibawah kantor pusat sehingga laporan-laporan, informasi data dan kemajuan tidak terlepas dari monitoring kantor pusat. Hal ini terjadi karena hanya menggunakan email untuk mengirimkan akses data kepada kantor cabang yang dimiliki perusahaan, selain itu aktifitas *owner* yang *mobile* sering menghambat keputusan dalam menyelesaikan sebuah permasalahan.

Jika dilihat dari permasalahan yang ada, perusahaan pastilah akan membutuhkan sebuah jaringan yang menujang kegiatan perusahaan. Hal ini dapat dilakukan dengan menerapkan teknologi *Virtual Private Network (VPN)* pada jaringan.

Dari beberapa jenis VPN yang ada, pada penelitian dibandingkan antara Open VPN dan VPN IPSec sebagai objek untuk dilakukan perbandingan kehandalan perangkat dengan mengukur *reliability* keduanya dengan menggunakan *Reliability, Maintainability, Availability (RMA).* Untuk mengetahui mana yang terbaik, namun sebelum itu kita ketahui dulu apa itu definisi dari Open VPN dan VPN IPSec, akan digunakan untik membangun *Virtual Private Network* (VPN).

Dari uraian diatas, pada penelitian ini dibangun jaringan *VPN* mengunakan *OpenVPN* dan *VPN IPSec* dengan menghubungkan kantor pusat dan kantor cabang untuk mengetahui protokol mana yang lebih cocok dipilih perusahaan, dalam menentukan kecepatan data yang lebih baik, murah, dan manajemen lebih mudah. Pada penelitian ini dipilih topik yang berjudul. ***"Perbandingan Reliability Open VPN dengan VPN IPSec".***

2. METODOLOGI PENELITIAN

2.1. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah *Action Research.* Menurut Gunawan (2007) *action research* adalah kegiatan dan tindakan perbaikan sesuatu yang perencanaan, pelaksanaan dan evaluasinya digarap secara sistematik sehingga validasi dan reliabilitasnya mencapai tingkat riset. *Action*

research merupakan proses yang mencakup siklus aksi, yang mendasarkan pada refleksi umpan balik (*feedback*), bukti (*evidence)* dan evaluasi atas aksi sebelumnya dan situasi sekarang. Prosedur penelitian tindakan berupa suatu siklus yang setiap langkahnya terdiri dari lima tahap, yaitu diagnosa, perencanaan, tindakan, observasi dan refleksi.

1. Melakukan Diagnosa (*Diagnosing)*
2. Membuat Rencana Tindakan (*Action Planning)*
3. Melakukan Tindakan (*Action Taking)*
4. Melakukan Evaluasi (*Evaluating)*
5. Pembelajaran *(Learning*)

2.2. Desain dan Perancangan

1. Melakukan Diagnosa (*Diagnosing)*

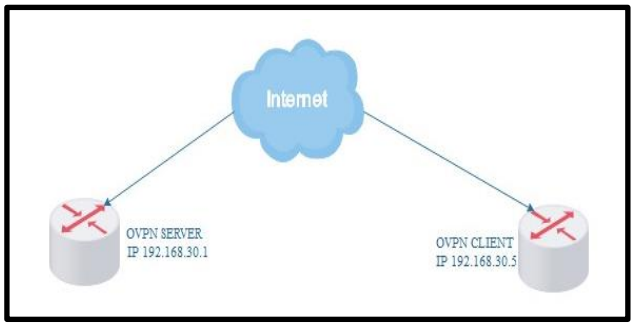
   Pada tahapan ini peneliti melakukan diagnosa dengan melakukan identifikasi terhadap kedua jenis VPN agar peneliti mendapatkan pokok permasalahan yang akan diteliti, berdasarkan data awal yang sudah didapat, VPN memiliki beberapa jenis yang umum digunakan salah satunya adalah Open VPN dan VPN IPSec.
2. Membuat Rencana Tindakan (*Action Planning)*

   Pada tahap ini peneliti meyusun rencana tindakan (*planning*) sebelum masuk ke tahap berikutnya yaitu *action taking* mengenai hal apa saja yang akan dilakukan untuk membangun jaringan VPN, baik itu Open VPN maupun VPN IPSec. Adapun tindakan yang akan dilakukan yaitu, desain perancangan topologi dan menentukan alat dan bahan apa saja yang dibutuhkan.

   - Perancangan Topologi

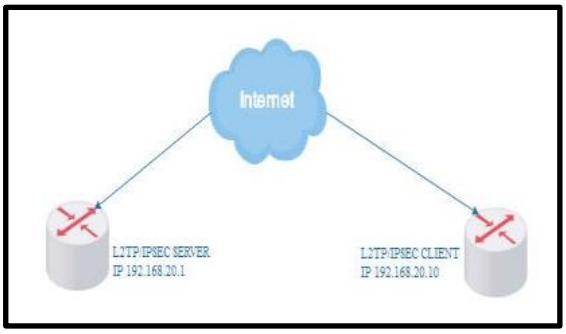
Gambar 1. Desain Topologi

Pada gambar diatas, terdapat 2 *router* yang akan berfungsi menjadi *server* dan *client* VPN dari masing-masing kantor yang terhubung melalui *Fiber Optik* dan memiliki IP Publik sendiri yang langsung terhubung ke jaringan internet. Kantor Pusat memiliki IP Publik 158.140.165.228/32 dengan *network* IP Lokal 192.168.50.0/24. Sedangkan Kantor Cabang memiliki IP Publik 103.119.60.186/32 dengan *network* IP Lokal 192.168.60.0/24.



Gambar 2. Alur pengujian OVPN

Pada gambar diatas, terdapat 2 router yang berfungsi sebagai *server* dan *client* VPN. Pada masing-masing *router* terdapat IP sendiri, *router* OVPN *server* memiliki IP 192.168.30.1 dan OVPN *client* memiliki IP 192.168.30.5. Pada jalur vpn tersebut, akan dilakukan pengukuran satu arah dari *server* ke *client* pada masing-masing VPN.



Gambar 3. Alur pengujian L2TP/IPSEC

- Perangkat yang dibutuhkan

Tabel 1. Perangkat Kerja

No	Nama	Jenis	Spesifikasi
1.	Acer Personal Computer	PC	* *Prosesor Intel® Core™ i3- 2367M* * *RAM 2 GB* * *Hardisk 500 GB*
2.	HP 240 G5	Laptop	* *Prosesor Intel Core™ i3- inside* * *RAM 4 GB* * *Hardisk 500 GB*
3.	Mikrotik HAP Lite RB941	Router	**Processor 650 Mssshz* **4 port Fast Ethernet* **Build-in Wireless 2.4Ghz (802.11b/g/n)* **Antenna internal Dual-Chain 2 x 1.5dbi*
4.	Huawei Modem/ISP	ISP	**Fiber Optic* **Internet Acess UP to 50 Mbps*

- *Software* yang dibutuhkan

Ada beberapa *software* yang akan digunakan untuk mendukung penelitian ini, sebagai berikut :

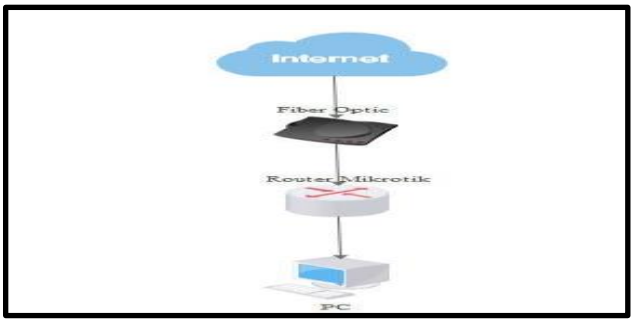
1. PRTG (*Paessler Router Traphic Grapher*) tools yang digunakan untuk membantu mengukur RMA dari tiap jaringan VPN.
2. Edraw Max tools yang digunakan untuk merancang desain topologi jaringan dalam melakukan penelitian.
3. Winbox tools yang digunakan untuk *remote access* VPN dari kantor pusat ke kantor cabang.

3. Melakukan Tindakan (*Action Taking*)

Pada tahap *action taking* peneliti melakukan konfigurasi sebelum menuju ke tahap simulasi. Berikut ini ada beberapa tindakan yang akan dilakukan pada *action taking* sebelum masuk ke tahap simulasi, sebagai berikut :

- Menghubungkan *Router* ke jaringan

Sebelum melakukan tahap konfigurasi, hal pertama yang harus dilakukan yaitu menghubungkan *router* mikrotik ke modem ISP dan juga menghubungkan ke dalam jaringan *Local Area Network* (LAN) seperti gambar dibawah ini :



Gambar 4. Rancangan Topologi

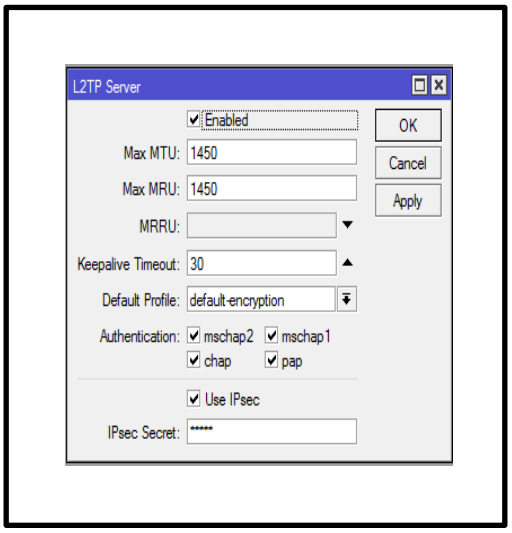
Pada gambar 2 mikrotik terhubung ke modem ISP berbasis *fiber optic* melalui port *ether1*, dan terhubung ke jaringan *Local Area Network* (LAN) melalui port *ether2* menggunakan kabel UTP.

Melakukan konfigurasi dasar pada mikrotik

Setelah selesai menghubungkan *router* mikrotik ke jaringan, selanjutnya melakukan konfigurasi dasar pada *router* mikrotik agar dapat terhubung ke jaringan *Local Area* Network (LAN) maupun *Wide Area* Network (WAN). Untuk melihat semua konfigurasi secara detail, peneliti akan menyusun semua tahapan konfigurasi dasar pada mikrotik secara lengkap akan dimasukan ke dalam lampiran di akhir penelitian ini.

- Melakukan konfigurasi VPN

Pada tahapan konfigurasi VPN dimana dilakukan konfigurasi pada *router* mikrotik dalam membentuk sebuah jaringan *Virtual Private Network* (VPN) dan akan menghubungkan jaringan antara kantor pusat dan kantor cabang.



Gambar 5. *Server VPN*

Untuk melihat konfigurasi VPN lebih detail, peneliti menyusun semua tahapan - tahapan konfigurasi VPN pada *router* mikrotik secara lengkap dimasukan ke dalam lampiran diakhir penelitian ini.

- Evaluasi (Evaluating)

Setelah jaringan VPN selesai dan berhasil dikonfigurasi, dan *client* VPN sudah bisa mengakses jaringan VPN ke *server*, maka langkah yang selanjutnya masuk ke tahap evaluasi, dengan melakukan pengukuran RMA terhadap jaringan VPN menggunakan *software* PRTG *Network Monitor*. Hasil dari pada pengukuran ini akan dibahas pada bab 4.

- Pembelajaran (*Learning)*

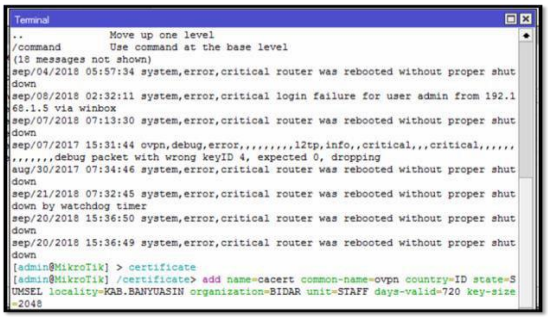
Pada tahap ini merupakan akhir dari penelitian ini, yang mana akan dilakukan perbandingan hasil pada bab 4, setelah dilakukannya pengukuran selama 6 hari berdasarkan parameter yang ada pada RMA. Di dalam tahap perbandingan akan disajikan dalam bentuk tabel perbandingan, dimana akan terlihat dalam sisi kekurangan dan kelebihan dari kedua jenis VPN.

3. HASIL DAN PEMBAHASAN

Setelah bab sebelumnya peneliti melakukan *diagnosing* dan *action planning* maka pada bab ini akan membahas tiga tahapan selanjutnya yaitu *action taking*, *evaluating*. Pada tahap *action taking*, peneliti melakukan konfigurasi VPN. Dengan menggunakan metode pengujian RMA, pengujian ini berguna untuk mengukur Keandalan (*Reliability*), Kemudahan Pemeliharaan (*Maintainability*), dan Ketahanan Alat (*Availability).*

1. Konfigurasi OVPN di *Router Mikrotik*
   - OVPN *Server*

   Tahap pertama yang dilakukan pada konfigurasi OVPN di *router mikrotik* yaitu membuat sertifikat CA di terminal winbox seperti yang dilihat pada gambar 6, dimana ada beberapa perintah yang dimasukan seperti *add name*=cacert, *common-name*=ovpn, *country*=ID,*state*=SUMSEL,*locality*=KAB.BANSIN,*organization*=BIDAR,*unit*=STAFF,*day valid*=720,*key-size*=2048.

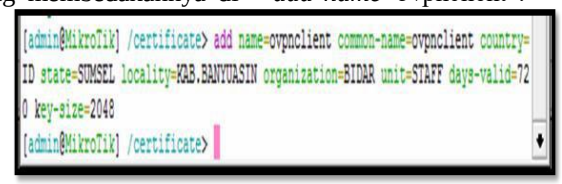


Gambar 6. Sertifikat CA

Membuat sertifikat OVPN *Server* seperti Gambar 7 dibawah ini. Bisa dilihat ada beberapa perintah yang sama seperti membuat sertifikat CA hanya yang membedakannya di "*add name*=ovpnserver".

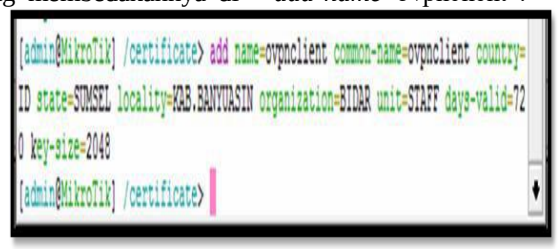
Gambar 7. Sertifikat OVPN *Server*

Membuat sertifikat OVPN *Client* seperti Gambar 9 dibawah ini. Ada beberapa perintah yang sudah dimasukan ke dalam konfigurasi tersebut hampir sama dengan perintah membuat sertifikat OVPN *Server* hanya yang membedakannya di " *add name*=ovpnclient".



Gambar 8. Sertifikat OVPN *Server*

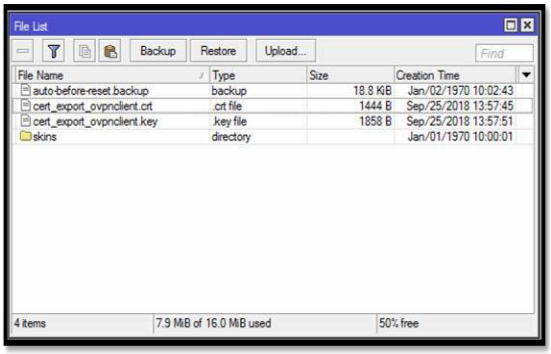
Membuat sertifikat OVPN *Client* seperti Gambar 9 dibawah ini. Ada beberapa perintah yang sudah dimasukan ke dalam konfigurasi tersebut hampir sama dengan perintah membuat sertifikat OVPN *Server* hanya yang membedakannya di " *add name*=ovpnclient".



Gambar 9. Sertifikat OVPN *Client*

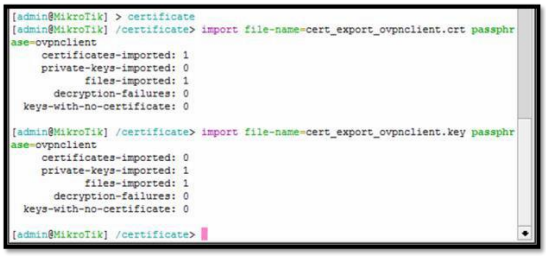
- OVPN Client

Selanjutnya masuk pada tahap konfigurasi OVPN *Client*, *upload* dua buah *file* Sertifikat yang bererktensi ovpnclient.*crt* dan ovpnclient.*key* seperti gambar dibawah ini.



Gambar 10. OVPN *Client*

Menjalankan perintah *import* Sertifikat *Client* mulai dari Sertifikat ovpnclient.*crt* dan ovpnclient.*key*.

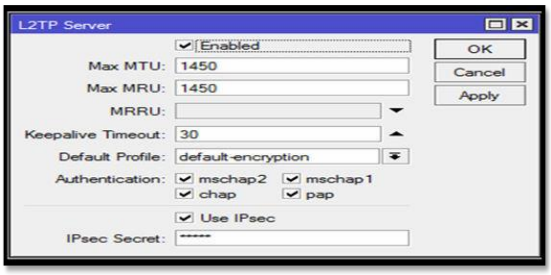


Gambar 11. Perintah *Import* sertifikat *client*

2. Konfigurasi L2TP/IPSEC di Router Mikrotik

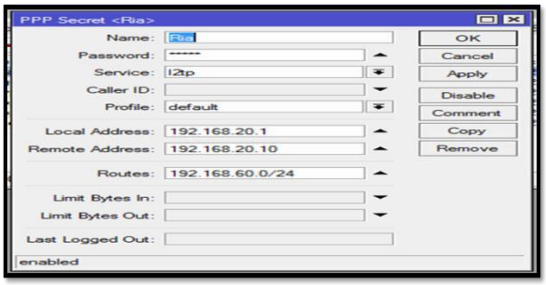
- L2TP/IPSEC *Server*

Mengaktifkan L2TP/IPSEC *Server* pada *Router Mikrotik* dengan mencentang *Enabled* lalu klik *Apply* OK. Semua konfigurasi yang sudah di *setting* pada *Router Mikrotik* akan tersimpan.



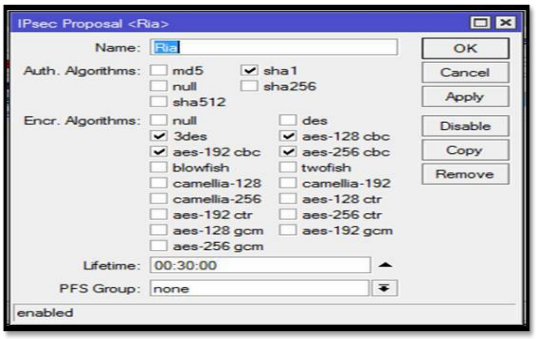
Gambar 12. L2TP/IPSEC *Server*

Membuat *user* yang akan digunakan saat autentifikasi, dengan *Local Address* 192.168.20.1 dan *Remote Address* 192.168.20.10 lalu klik *Apply* OK.



Gambar 13. L2TP/IPSEC *Secret*

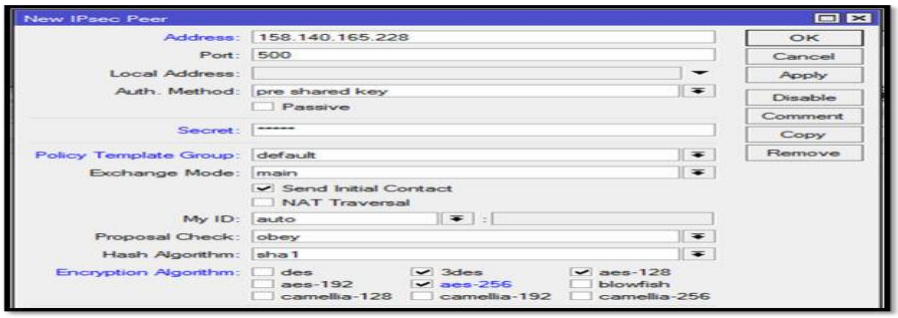
Pada tahap ini mengatur IPSec Proposal lalu klik Apply OK, maka semua konfigurasi akan tersimpan dan bisa melanjutkan untuk tahap selanjutnya. Bisa dilihat pada Gambar dibawah ini IPSec Proposal.



Gambar 14. IPsec Proposal

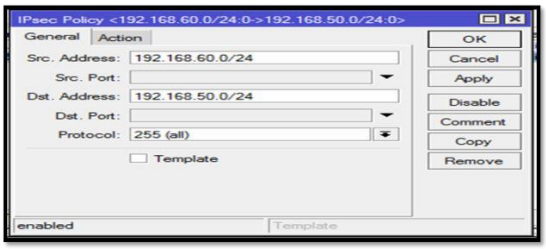
- L2TP/IPSEC *Client*

Untuk tahap selanjutnya masuk dalam konfigurasi L2TP/IPSEC *Client* pada tahap ini mengatur IPSec *peer* sama seperti L2TP/IPSEC *Server* hanya yang membedakannya jika *server* maka IP tujuannya ke *client* apabila *client* maka IP tujuannya ke *server*. Jadi, kantor cabang mengatur IPSec *Peer* dengan memasukan IP Public Kantor Pusat 158.140.165.228.



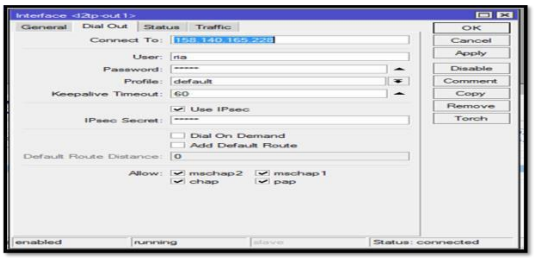
Gambar 15. IPSec *Peer Client*

Mengatur IP *Policy* dengan memasukan IP lokal kantor cabang 192.168.60.0/24 pada src dan IP lokal kantor pusat 192.168.50.0/24 pada dst. Bisa dilihat seperti Gambar dibawah ini IP tujuannya ke kantor pusat.



Gambar 16. IPSec *Policy client*

Tahap yang terakhir kita cek status yang ada pada L2TP *client*, klik *Interface>interface-l2tp out* dengan *connect* ke IP Publik kantor pusat 158.140.165.228. Jika berhasil terhubung maka akan ada status *connected* seperti gambar dibawah.



Gambar 17. *Interface client*

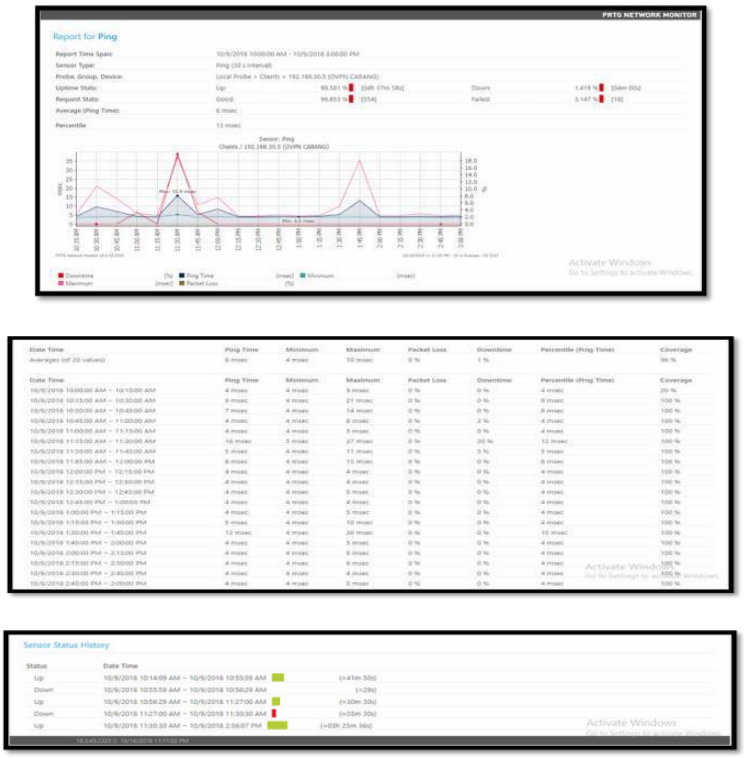
HASIL PENGUJIAN RMA

Di dalam metode RMA ada tiga karakteristik pada sistem yang berhubungan dengan operasionalnya. *Reliability, Maintainability, Availability (RMA)* adalah salah satu tinjauan yang sangat penting untuk memastikan apakah sistem berada pada kondisi yang diinginkan seperti performa, batasan waktu, untuk mengetahui kehandalan alat dan kualitas layanan pada *Router Mikrotik*.

Pada tahapan ini hasil pengukuran menggunakan alat *Router Mikrotik* dengan riset B sendiri berlokasi di lab yang menggunakan *Fiber Optic* dan menggunakan tools PRTG *Network Monitor* dengan monitoring *Router Mikrotik* dari Kantor Pusat ke Kantor Cabang.

3.1. Hasil Pengukuran PRTG *Network Monitor* OVPN pada *router* Kantor Cabang

Hasil pengukuran OVPN pada tanggal 9 Oktober 2018. Dari kantor pusat ke kantor cabang pada pukul 10.00-3.00 menggunakan PRTG *Network Monitor* di lab riset B



Gambar 18. Tampilan Hasil PRTG *Network Monitor* OVPN hari pertama pada *router* Kantor Cabang

Dari gambar datas dapat dilihat dari *router* kantor pusat ke *router* kantor cabang sangat baik karena jarak antara *router* pusat ke *router* cabang tidak berjauhan kurang lebih 300 Meter, tetapi ada gangguan terjadi padamnya listrik dan mengakibatkan *downtime* dari jam 11:27:00-11:30:30, *uptime* selama 4h37menit58second dan nilai *downtime* sekitar 2% .

3.2. Hasil Pengukuran PRTG *Network Monitor* L2TP/IPSEC pada *router* Kantor Cabang

Hasil pengukuran L2TP/IPSEC pada tanggal 13 Oktober 2018. Dari kantor pusat ke Kantor Cabang pada pukul 09.00 – 3.00 menggunakan PRTG *Network Monitor* di lab riset B.

Gambar 19. Tampilan Hasil PRTG *Network Monitor* L2TP/IPSEC hari pertama pada *router* Kantor Cabang

Dari gambar datas dapat dilihat dari *router* kantor pusat ke *router* kantor cabang cukup baik karena jarak antara *router* pusat ke *router* cabang cukup jauh kurang lebih 400 Meter, mengakibatkan nilai *downtime* menurun karena gangguan pada koneksi internet yang tidak stabil *router* mengalami *downtime* dari jam 2:13:32 – 3:00:00, *uptime* selama 5h01menit10second dan penurunan nilai downtime 2%.

4. KESIMPULAN

Setelah diuraikan dari bab-bab sebelumnya, kesimpulan yang dapat di ambil dari penelitian ini yaitu :

1. Tingkat kinerja yang lebih baik apabila IPSec berjalan pada L2TP dibandingkan dengan OVPN diharuskan *router* harus terkoneksi secara *point-to-point* dan tidak bisa dimasuki oleh jaringan lain hanya bisa kedua *router* tersebut yang telah dilakukan secara *point-to-point* dari sisi *client* maupun *server*.
2. Perbedaan antara tempat, waktu, dan jarak tidak mempengaruhi kestabilan karena jaringan VPN dapat remote access asalkan tekoneksi ke jaringan internet.
3. Apabila router mikrotik berada pada belakang NAT dengan kata lain mikrotik memperoleh IP Dinamis pada ether1 akan membuat autentifikasi pada IPSec menjadi error, atau mengalami kegagalan dalam autentifikasi.
4. Kegagalan ataupun *downtime* menggunakan perangkat jaringan *router mikrotik* disebabkan koneksi yang tidak stabil, mengakibatkan paket data yang dikirim banyak yang hilang.

DAFTAR UJUKAN

[1] Fronita Mona, Saputra Eki, dan Romadhon Husnu. 2016, *Analisis Kualitas Layanan Jaringan Internet Menggunakan Metode RMA* (*Realibility, Maintainability and Availability*) dan QOS (*Quality Of Service)*. Jurnal Rekayasa Dan Manajemen Sistem Informasi , Vol 2, No 2, Agustus 2016 e-ISSN 2502-8995 ISSN 2460-8181.

[2] Firmansyah Fikri dan Badrul Mohammad 2015, Penerapan Metode Open VPN-*Acces Server* sebagai Rancangan Jaringan *Wide Area Network.* Jurnal Techno Nusa Mandiri Vol.XII No.1, Maret 2015.

[3] http://www.pengertianku.net/2016/02/pengerti an-wan-dan-fungsinya-secara- ringkas.html

[4] Musajid, A dkk. 2017 *Virtual Private Network (VPN)* dan *Mikrotik.* Diakses dari http://blog.pessoft.com/2016/05/29/mi krotik-ipsec-tunnel-with-dns-and-nat/. Tanggal 15 Maret 2018.

[5] Oktivasari, Prihatin dan Utomo Budhi Andri. 2016, Analisa *Virtual Private Network OpenVPN* dan *Point to Point Tunneling Protocol*. Diakses dari http://jurnal.kominfo.go.id/index.php/j pkop/article/download/658/489. Tanggal 21 Januari 2018.

[6] Romadhon, Pearl Pratama. 2014. *Analisis kinerja jaringan LAN menggunakan metode QoS dan RMA pada PT Pertamina EP Uber Ramba (Persero*), Fakultas Ilmu Komputer Universitas Bina Darma : Palembang Speaks, Scott. *Reliability and MTBF Overview. Vicor Reliability Engineering*

[7] Yanto. 2013. *Analisis QoS (Quality of Service) Pada Jaringan Internet (Studi Kasus :Fakultas Teknik Universitas TanjungPura).* http://jurnal.untan.ac.id/index.php/justi n/article/view/880. Jurnal Untan. Vol 1 No 1.2013: Tanjung Pura