RANCANG BANGUN AUTOMATED VIRTUAL PRIVATE NETWORK MENGGUNAKAN JARINGAN SMALL OFFICE HOME OFFICE (SOHO) DI PT. SATNETCOM BALIKPAPAN

DESIGN AND IMPLEMENTATION OF AUTOMATED VIRTUAL PRIVATE NETWORK USING SMALL OFFICE HOME OFFICE (SOHO) NETWORK IN PT. SATNETCOM BALIKPAPAN

Achmad Zacky Fathoni Haque[1*], Wisnu Hera Pamungkas[2], Jamal[3]
[1]*Universitas Mulia, Balikpapan, l. Letjend. TNI. Z.A Maulani No. 9, Balikpapan*
[2]*Universitas Mulia, Balikpapan, l. Letjend. TNI. Z.A Maulani No. 9, Balikpapan*
[3]*Universitas Mulia, Balikpapan, l. Letjend. TNI. Z.A Maulani No. 9, Balikpapan*

[*]*haqproject@gmail.com*

ABSTRAK

Informasi merupakan hal yang penting dalam perusahaan sehingga distribusinya menjadi suatu kebutuhan yang diharuskan. Metode distribusi informasi dari kantor pusat ke kantor cabang menjadi hal yang harus dipikirkan. *Virtual Private Network* salah satu solusi untuk menghubungkan kantor pusat dengan kantor cabang secara *LAN*. Pembuatan *VPN* dengan *Ethernet over Internet Protocol (EoIP)* membutuhkan informasi ip address yang bersifat statik sehingga tidak bisa diimplementasikan pada ip address yang bersifat dinamis. Dengan *Automated Virtual Private Network* ini diharapkan dapat membantu perusahaan dalam distribusi data yang melewati Tunnel EoIP Protocol dimana salah satu kantor menggunakan *IP Address* publik dinamis.

Dalam pengembangan *Automated Virtual Private Network* ini penulis menggunakan tahapan-tahapan dari pengembangan PPDIOO. Sedangkan perangkat yang digunakan ialah perangkat dengan merek Mikrotik. Penulis melibatkan *Layer-2 Tunnel Protocol (L2TP), Netwatch, Bridge, VLAN* dan *Script* dalam pembuatan konfigurasi untuk merubah remote address milik EoIP secara otomatis.

Kata kunci : **EoIP, VPN, Dinamis, Statis, Mikrotik.**

ABSTRAK

Information is important in a company so that its distribution becomes a necessity. The method of information distribution from headquarter office to branch office is something that must be considered. Virtual Private Network is one of the solutions to connect the headquarter office and branch offices to be in the same LAN. Making a VPN with Ethernet over Internet Protocol (EoIP) requires static IP address information to work. So, it cannot be implemented on dynamic IP addresses. With this Automated Virtual Private Network, it is hoped to help companies in data distribution using the EoIP Tunnel Protocol where one of the office using dynamic ip address to connect to the Internet.

In the development of this Automatic Virtual Private Network, the author uses the stages of development from PPDIOO method. The author uses MikroTik devices for this research. The author involves Layer-2 Tunnel Protocol (L2TP), Netwatch, Bridge, VLAN and Script in making configuration to automatically change EoIP's remote and local addresses.

***Keywords** : EoIP , VPN , Dynamic, Static, MikroTik*

PENDAHULUAN

Network menjadi media yang berpengaruh dalam distribusi informasi, terutama dalam hal distribusi informasi jarak jauh seperti dari suatu kota ke kota lain secara real-time. Seiring dengan berkembangnya bisnis perusahaan, suatu perusahaan akan membuka kantor cabang di kota-kota lain. Kebutuhan akan distribusi informasi dari kantor pusat ke kantor cabang dan sebaliknya menjadi kebutuhan yang penting. Tim IT harus memikirkan opsi yang bisa digunakan untuk dapat melakukan distribusi informasi secara efisien dan efektif. Keamanan juga menjadi alasan yang harus di perhatikan saat menentukan suatu pilihan dalam jaringan.

PT. Satnetcom Balikpapan merupakan salah satu perusahaan Internet Service Provider berpusat di kota Balikpapan yang tengah berkembang dan memiliki beberapa kantor cabang yaitu di Jakarta, Bandung dan Sangatta. Di kantor cabang tersebut, PT. Satnetcom Balikpapan menyewa jasa internet dari perusahaan internet service provider lain dengan produk Small Office Home Office yang memberi layanan IP Public dinamis.

Untuk membuat jaringan kantor cabang dapat terhubung secara LAN dan berada pada IP Network yang sama dengan kantor pusat dibutuhkan sebuah teknologi bernama Virtual Private Network yang menggunakan tunnel protocol Ethernet over Internet Protocol (EoIP) milik Mikrotik. Namun tunnel protocol EoIP mengharuskan masing-masing router mengetahui ip address tujuan tunnelnya untuk membentuk VPN. Hal ini menjadi masalah ketika jaringan yang digunakan adalah Small Office Home Office dimana IP publicnya selalu berubah-ubah yang membuat tim IT harus memperbarui konfigurasi tersebut secara manual setiap pergantiannya.

Oleh karena itu, perlu dibuat sebuah network yang mampu mengatasi masalah dalam penggunaan tunnel protocol EoIP tersebut secara otomatis. Sehingga dapat membantu tim IT mengelola network mereka secara lebih praktis tanpa harus melakukan konfigurasi ulang secara manual.

1. Rancang Bangun

Rancang Bangun (desain) adalah tahap dari setelah analisis dari siklus pengembangan sistem yang merupakan pendefinisian dari kebutuhan-kebutuhan fungsional, serta menggambarkan bagaimana suatu sistem dibentuk yang dapat berupa penggambaran, perencanaan, dan pembuatan sketsa atau pengaturan dari beberapa elemen yang terpisah kedalam satu kesatuan yang utuh dan berfungsi, termasuk menyangkut mengkonfigurasi dari komponen-komponen perangkat keras dan perangkat lunak dari suatu system [2].

2. Virtual Private Network

Virtual Private Network (VPN) adalah tiruan dari sebuah fasilitas Wide Area Network (WAN) privat menggunakan fasilitas IP (termasuk Internet Publik, atau backbone IP Privat). VPN menyediakan komunikasi privat antar end user, seperti remote office dan telecommuters. Banyak organisasi menggunakan VPN untuk menghubungkan kantor, home office, rekan bisnis dan masih banyak lagi. Selain karena murah dan mudah digunakan, VPN juga digunakan karena mengutamakan keamanan. “VPN merupakan sebuah sarana untuk mengamankan dan memprivatkan pengiriman data melalui sebuah infrastruktur jaringan yang tidak aman dan dapat digunakan bersama (shared). Jaringan VPN bisa disebut aman karena semua data yang ditransmisikan melalui sebuah terowongan (tunnel) selalu dienskripsi menggunakan algoritma-algoritma tertentu, bergantung pada protokol yang digunakan [3].

3. Teknologi Tunneling

Teknologi tunneling merupakan teknologi yang bertugas untuk menangani dan menyediakan koneksi point-to-point dari sumber ke tujuannya. Disebut tunnel karena koneksi point-to-point tersebut sebenarnya terbentuk dengan melintasi jaringan umum, namun koneksi tersebut tidak mempedulikan paket-paket data milik orang lain yang sama-sama melintas jaringan umum tersebut, tetapi koneksi tersebut hanya melayani transportasi data dari pembuatnya [4].

4. Small Office Home Office (SOHO)

SOHO adalah singkatan dari ‘Small Office, Home Office’, yaitu: tren bekerja di dalam rumah. Dapat disimpulkan definisi SOHO adalah sebuah hunian, yaitu rumah atau apartemen, yang menggabungkan fungsi tempat tinggal dengan kantor sehingga didalamnya dilengkapi dengan fasilitas penunjang kantor. Konsep SOHO ini memungkinkan para pemilik dan pengguna unit apartemen untuk menggunakan unit apartemennya sebagai unit hunian ataupun sebagai unit kantor dengan izin yang legal [5].

5. Ethernet over IP (EoIP)

EoIP merupakan protocol pada Mikrotik RouterOS yang berfungsi untuk membangun sebuah Network Tunnel antar MikroTik router di atas sebuah koneksi TCP/IP [6]. EoIP merupakan protocol proprietary MikroTik [3].

6. Point-to-Point Tunnel Protocol (PPTP)

Point-to-Point Tunneling Protocol (PPTP) adalah data link protokol yang umum digunakan dalam membangun hubungan langsung antara dua node jaringan. Hal ini dapat menyediakan koneksi otentikasi, transmisi enkripsi menggunakan ECP, RFC 1968, dan kompresi [7].

7. Layer 2 Tunnel Protocol (L2TP)

Layer 2 Tunneling Protocol (L2TP) adalah sebuah standar Internet Engineering Task Force (IETF) untuk masalah protokol tunneling yang digunakan untuk melakukan enkapsulasi terhadap frame-frame protocol PPTP untuk ditransmisikan melalui jaringan TCP/IP, X.25, frame relay atau jaringan Asynchronous Transfer Mode (ATM). L2TP sering digunakan untuk membuat sebuah Virtual Private Network (VPN) yang terdapat di dalam sebuah jaringan publik, seperti Internet. Karena merupakan standar IETF, protokol ini menawarkan interoperabilitas yang sangat tinggi antar vendor komputer dan jaringan [8].

8. MikroTik Router OS

MikroTik RouterOS merupakan sistem operasi yang diperuntukkan sebagai Network Router. MikroTik routerOS sendiri adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer biasa menjadi router network yang mencakup berbagai fitur yang dibuat untuk IP Network dan jaringan wireless. Fitur-fitur tersebut diantaranya Firewall & Nat, Routing, Hotspot, Point to Point Tunneling Protocol, DNS server, DHCP server dan masih banyak lagi fitur lainnya. MikroTik routerOS merupakan sistem operasi Linux base yang diperuntukkan sebagai network router. Didesain untuk memberikan kemudahan bagi penggunanya. Administrasinya bisa dilakukan melalui Windows Application (WinBox). Selain itu instalasi dapat dilakukan pada Standard komputer PC (Personal Computer). PC yang akan dijadikan router mikrotik pun tidak memerlukan resource yang cukup besar untuk penggunaan standard, misalnya hanya sebagai gateway. Untuk keperluan beban yang besar (network yang kompleks, routing yang rumit) disarankan untuk mempertimbangkan pemilihan sumber daya PC yang memadai [4]

9. Winbox

Winbox adalah utilitas atau aplikasi yang memungkinkan administrasi Mikrotik RouterOS menggunakan GUI cepat dan sederhana [9].

10. IP Security Protocol (IPSec)

IPSec (singkatan dari IP Security) adalah sebuah protokol yang digunakan untuk mengamankan transmisi datagram dalam sebuah internetwork berbasis TCP/IP. IPSec diimplementasikan pada lapisan transport dalam OSI Reference Model untuk melindungi protokol IP dan protokol-protokol yang lebih tinggi dengan menggunakan beberapa kebijakan keamanan yang dapat dikonfigurasikan untuk memenuhi kebutuhan keamanan pengguna, atau jaringan [10].

METODOLOGI

1. Wawancara

Metode yang digunakan secara langsung untuk mendapatkan data adalah metode wawancara.

Hasil dari wawancara ini berguna untuk mendukung bahasan penelitian ini dalam hal melakukan perancangan dan membangun Automated Virtual Private Network yang dapat menghasilkan rancangan jaringan.

2. Observasi

Proses observasi didasarkan pada pengamatan langsung dan mencatat perilaku atau kejadian seperti keadaan yang sebenarnya.

Pada metode pengamatan (observasi), ini dilakukan peninjauan dan penelitian langsung di lapangan untuk memperoleh dan mengumpulkan data-data yang berhubungan seperti konfigurasi, pengetesan, analisa konfigurasi dan mencari tahu apa kebutuhan yang harus di konfigurasi kembali.

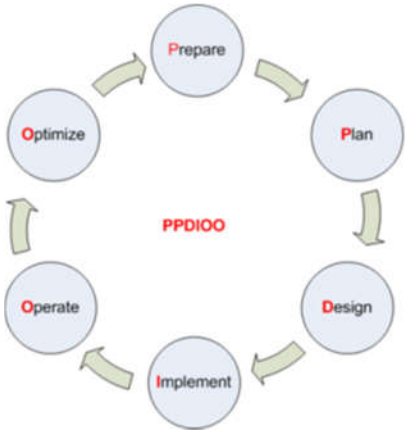
3. Studi Literatur

Penulis mendapatkan informasi atau data dari berbagai sumber bacaan jurnal atau hasil penelitian sebelumnya yang relevan dengan topik pembahasan dari penelitian. Selain itu penulis juga mengumpulkan data dari situs-situs internet yang berhubungan dengan topik pembahasan dari penelitian.

4. Kebutuhan Sistem
   a) Router Mikrotik RB951/750
   b) Notebook
   c) Sistem Operasi Windows 7.
   d) WinBox
   e) Mikrotik RouterOS
   f) Putty

5. Perancangan Jaringan

Perancangan jaringan dengan model Prepare, Plan, Design, Implement, Operate and Optimize (PPDIOO).



Gambar 1. Metode perancangan jaringan model PPDIOO

6. Permodelan Konfigurasi

Proses permodelan konfigurasi didasarkan pada bagaimana sebuah skema dari konfigurasi akan berjalan agar penelitian ini dapat terlaksana dengan baik.

7. Implementasi

Pada tahapan ini dilakukan perancangan dan konfigurasi pada router yang berada di kantor pusat serta kantor cabang sesuai dengan analisis dan perancangan sistem.

Adapun langkah-langkah yang dilakukan yaitu sebagai berikut :

1) Interface Router dan Host
2) Konfigurasi EoIP Tunnel
3) Konfigurasi PPP Server dan L2TP-Client
4) Konfigurasi Script

8. Pengujian

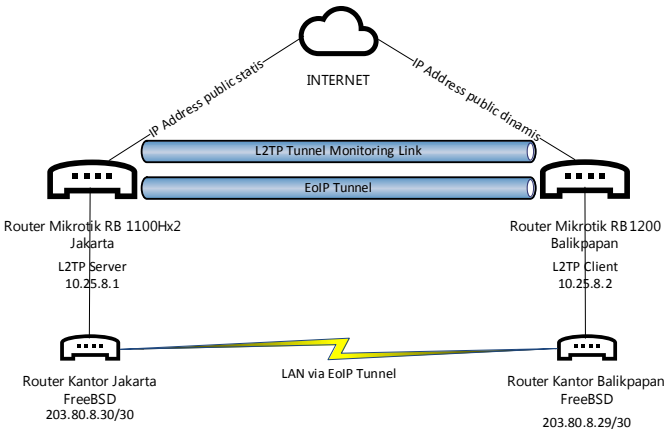
Pada tahap ini dilakukan pengujian pada sistem yang telah dibuat apakah telah memenuhi kebutuhan atau tidak dengan detail sebagai berikut :

1) Pengujian Kinerja Script dalam Konfigurasi Otomatis.
2) Pengaruh L2TP Sebagai Monitor Link Dalam Kualitas Delivery.
3) Pengujian Waktu Downtime Saat Terjadi Perubahan IP Public Dynamic.
4) Pengecekan Keamanan Transfer Data Menggunakan Packet Sniffer.

HASIL DAN PEMBAHASAN

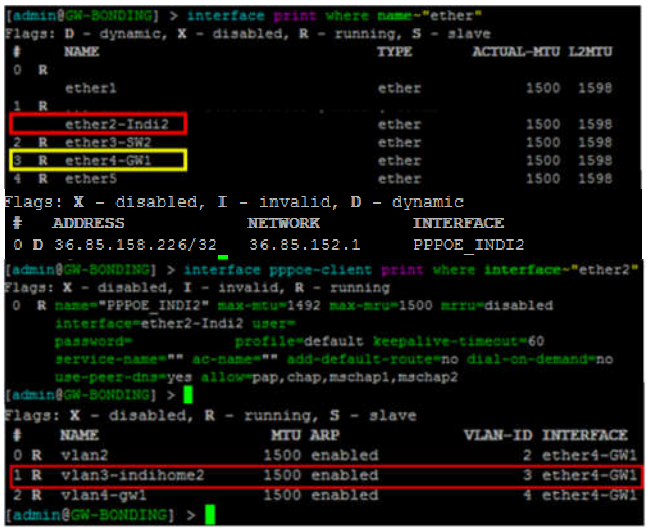
1. Perancangan Virtual Private Network

Dalam perancangan jaringan ini, topologi Virtual Private Network yang diajukan sebagai berikut :

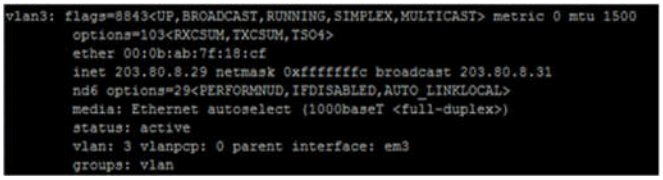


Gambar 2. Topologi Virtual Private Network dengan EoIP Tunnel

2. Konfigurasi Balikpapan



Gambar 3. Konfigurasi Router Balikpapan



Gambar 4. Konfigurasi *Host* Balikpapan

```
[admin@GW-BONDING] > ip address print where interface~"automatedvpn-monitoring"
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0 D 10.25.8.2/32       10.25.8.1       automatedvpn-monitoring
[admin@GW-BONDING] > interface l2tp-client add name=automatedvpn-monitoring
user=automatedvpn password=automatedvpn connect-to=103.28.74.133 add-default
-route=no disabled=no keepalive-timeout=2
```

Gambar 5. Konfigurasi Bridge Router Balikpapan

```
[admin@GW-BONDING] > interface bridge add name=bridge-indihome
[admin@GW-BONDING] > interface bridge port add interface=eoip-balikpapan-jakarta
bridge=bridge-indihome
[admin@GW-BONDING] > interface bridge port add interface=vlan3-indihome2 bridge=b
ridge-indihome
[admin@GW-BONDING] >
```

Gambar 6. Konfigurasi L2TP Router Balikpapan

```
[admin@GW-BONDING] > interface eoip add name=eoip-balikpapan-jakarta remote-
address=103.28.74.133 local-address=36.83.55.80 tunnel-id=2607 ipsec-secret=
asdlkj123098 allow-fast-path=no
```

Gambar 7. Konfigurasi EoIP Tunnel Router Balikpapan

3. Konfigurasi Jakarta

```
 1  R  ether2-IDC                          ether            1500  1598
 2  R  ether3-APJII                        ether            1500  1598
 3  R  ether4-Backbone                     ether            1500  1598
 4  R  ether5-GW1-MAIN                     ether            1500  1598
 6 X   VLAN170-OpenIXP       1500 enabled              170 ether4-Backbone
 7 R   vlan4                 1500 enabled                4 ether4-Backbone
 8 R   vlan5-Indihome        1500 enabled                5 ether4-Backbone
[zacky@GW1-JKT-BACKUP] > ip address print where interface~"ether3-APJII"
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   103.28.74.133/23   103.28.74.0     ether3-APJII
[zacky@GW1-JKT-BACKUP] >
```

Gambar 8. Konfigurasi Router Jakarta

```
vlan5: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=3<RXCSUM,TXCSUM>
        ether 00:0b:ab:56:36:e0
        inet 203.80.8.30 netmask 0xfffffffc broadcast 203.80.8.31
        media: Ethernet autoselect (1000baseTX <full-duplex>)
        status: active
        vlan: 5 parent interface: em0
```

Gambar 9. Konfigurasi Host Jakarta

```
[zacky@GW1-JKT-BACKUP] > interface bridge add name=bridge-indihome
[zacky@GW1-JKT-BACKUP] > interface bridge port add interface=eoip-jakarta-balikpapan bridge=bridge-indihome
[zacky@GW1-JKT-BACKUP] > interface bridge port add interface=vlan5-Indihome bridge=bridge-indihome
```

Gambar 10. Konfigurasi Bridge Router Jakarta

```
[zacky@GW1-JKT-BACKUP] > interface l2tp-server server set enabled=yes

[zacky@GW1-JKT-BACKUP] > ppp secret add name=automatedvpn password=automatedvpn
 local-address=10.25.8.1 remote-address=10.25.8.2
```

Gambar 11. Konfigurasi L2TP Router Jakarta

```
[zacky@GW1-JKT-BACKUP] > interface eoip add name=eoip-jakarta-balikpapan
 remote-address=36.83.55.80 local-address=103.28.74.133 tunnel-id=2607 i
psec-secret=asdlkj123098 allow-fast-path=no
```

Gambar 12. Konfigurasi EoIP Router Jakarta

4. Konfigurasi Script Balikpapan

Pada script yang berada di router Balikpapan dengan nama local-add-eoip dengan policy read, reboot, write dan test , ada 3 variable yang dibuat. Variable pertama yaitu "ipaddpppoe2" yang nilainya mengambil informasi dari IP Address yang berada pada interface "PPPOE_INDI2". Kemudian Variable kedua yaitu "ipadd" yang nilainya mengambil informasi dari variable "ipaddpppoe2" dengan menghilangkan nilai "/" dan setelahnya. Sebagai contoh, jika nilai variable "ipaddpppoe2" adalah "203.80.8.30/30", maka nilai dari variable "ipadd" adalah "203.80.8.30". Pada Variable ketiga yaitu "eoipbpp", mengambil informasi local-address yang berada pada Interface EoIP dengan nama interface "eoip-balikpapan-jakarta".

Setelah variable "eoipbpp" dan "ipadd" memiliki nilai, kemudian kedua variable dibandingkan apakah nilainya sama atau tidak ($eoipbpp!=$ipadd). Dengan menggunakan "if - else", maka akan ada 2 aksi yang dibuat.

Jika tidak sama, maka :

/interface eoip disable [find name="eoip-balikpapan-jakarta"];

Interface eoip dengan nama interface "eoip-balikpapan-jakarta" akan didisable

/interface eoip set [find name="eoip-balikpapan-jakarta"] local-address="$ipadd";

Local-address pada interface eoip dengan nama "eoip-balikpapan-jakarta" akan dirubah sesuai dengan nilai dari variable "ipadd".

/ip ipsec policy remove [find comment="eoip-balikpapan-jakarta"];

Ipsec policy dengan comment "eoip-balikpapan-jakarta" akan diremove.

/ip ipsec remote-peers kill-connections;

Seluruh koneksi remote-peers ipsec akan dikill atau hapus.

:log info "IP Public indihome router Balikpapan berubah menjadi $ipadd";
:log info "Link EoIP Jakarta Balikpapan telah kembali up";

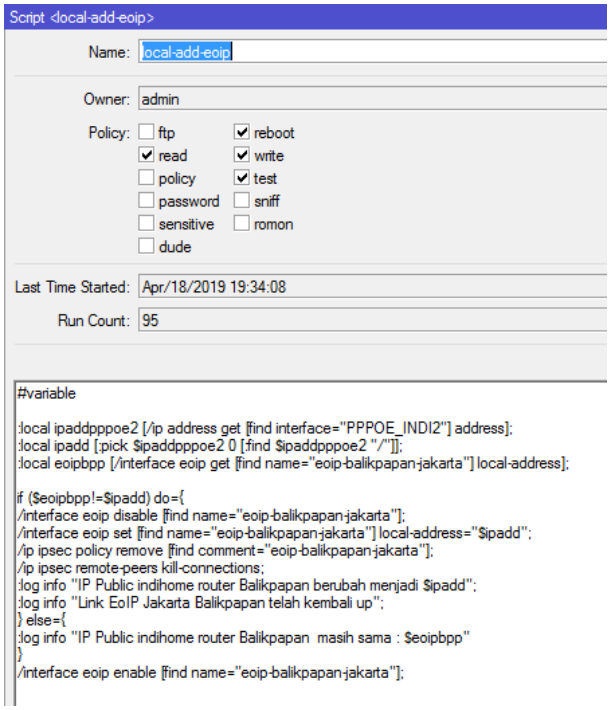
Diberikan informasi yang nantinya akan muncul kedalam log sesuai dengan teks yang sudah dibuat seperti diatas.

Jika sama, maka :

:log info "IP Public indihome router Balikpapan masih sama : $eoipbpp"

Diberikan informasi yang nantinya akan muncul kedalam log sesuai dengan teks yang sudah dibuat seperti diatas bahwa IP Address Public router Balikpapan masih sama seperti yang ada pada konfigurasi local-address EoIP.

Kemudian diluar dari "if –else", script ini diakhiri dengan melakukan "enable" terhadap interface EoIP dengan nama interface "eoip-balikpapan-jakarta".



Gambar 13. Konfigurasi Script router Balikpapan

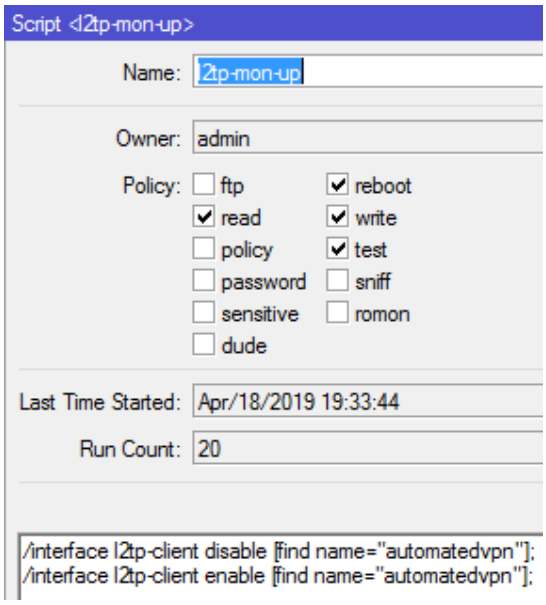
Pada router Balikpapan, ditambahkan konfigurasi script dengan policy read, reboot, write dan test untuk disable dan enable interface l2tp-client yang digunakan sebagai monitoring link dengan nama "l2tp-mon-up".

/interface l2tp-client disable [find name="automatedvpn"];

Interface l2tp-client dengan nama "automatedvpn" akan di disable

/interface l2tp-client enable [find name="automatedvpn"];

Interface l2tp-client dengan nama "automatedvpn" akan di enable.



Gambar 14. Konfigurasi script 2 router Balikpapan

Kemudian ditambahkan konfigurasi netwatch pada router Balikpapan.

```
[admin@GW-BONDING] > tool netwatch print detail where host~"10.25.8.1"
Flags: X - disabled
 0   ;;; eoip-jakarta
     host=10.25.8.1 timeout=1s interval=2s since=apr/16/2019 23:51:18
     status=up up-script=local-add-eoip down-script=l2tp-mon-up
[admin@GW-BONDING] >
```

Gambar 15. Konfigurasi Netwatch router Balikpapan

5. Konfigurasi Script Jakarta

Pembuatan konfigurasi disertai script dengan nama "automatedvpn" dibawah bertujuan untuk melakukan perubahan ip address pada remote address dari tunnel EoIP dengan menggunakan informasi caller id dari active user PPP milik user yang terhubung melalui Layer-2 Tunnel Protocol. Adapun policy yang di perbolehkan hanya read, reboot, write dan test.

Pada script yang berada di router Jakarta, ada 2 variable yang dibuat. Variable pertama yaitu "calleridbpp" yang nilainya mengambil informasi caller-id yang berada pada PPP Active dngan username "automatedvpn". Kemudian Variable kedua yaitu "eoipjkt" yang nilainya mengambil informasi remote-address yang berada pada Interface EoIP dengan nama interface "eoip-jakarta-balikpapan".

Setelah kedua variable memiliki nilai, kemudian kedua variable calleridbpp dan eoipjkt dibandingkan apakah nilainya sama atau tidak ($calleridbpp!=$eoipjkt). Dengan menggunakan "if - else", maka akan ada 2 aksi yang dibuat.

Jika tidak sama, maka :

/interface eoip disable [find name="eoip-jakarta-balikpapan"];

interface eoip dengan nama interface "eoip-jakarta-balikpapan" akan didisable

/ip ipsec policy remove [find comment="eoip-jakarta-balikpapan"];

Ipsec policy dengan comment "eoip-jakarta-balikpapan" akan diremove

/ip ipsec remote-peers kill-connections;

Seluruh koneksi remote-peers ipsec akan dikill atau hapus.

/interface eoip set [find name="eoip-jakarta-balikpapan"] remote- address=$calleridbpp;

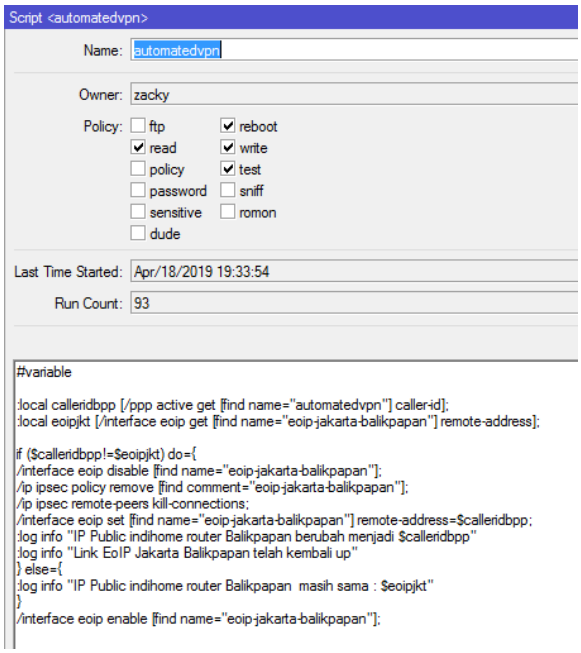
Remote-address pada interface eoip dengan nama "eoip-jakarta-balikpapan" akan dirubah sesuai dengan nilai dari variable "calleridbpp".

:log info "IP Public indihome router Balikpapan berubah menjadi $calleridbpp"
:log info "Link EoIP Jakarta Balikpapan telah kembali up"

Diberikan informasi yang nantinya akan muncul kedalam log sesuai dengan teks yang sudah dibuat seperti diatas.

Jika sama, maka :

:log info "IP Public indihome router Balikpapan masih sama : $eoipjkt"

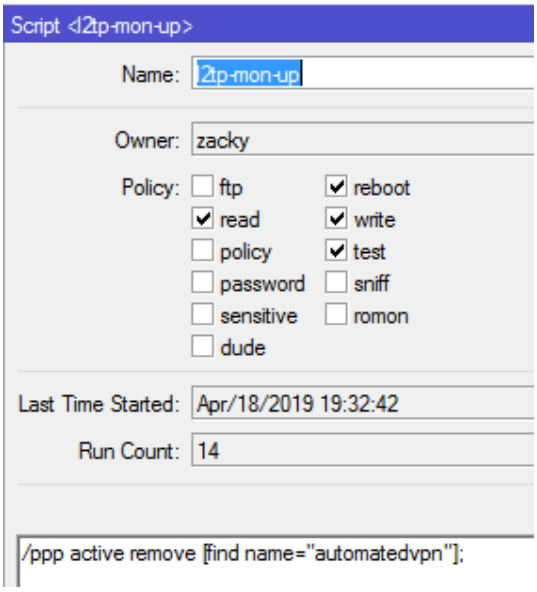


Gambar 16. Konfigurasi Script router Jakarta

Diberikan informasi yang nantinya akan muncul kedalam log sesuai dengan teks yang sudah dibuat seperti diatas bahwa IP Address Public router Balikpapan masih sama seperti yang ada pada konfigurasi remote-address EoIP.

Kemudian diluar dari "if", script ini diakhiri dengan melakukan "enable" terhadap interface EoIP dengan nama interface "eoip-jakarta-balikpapan".

Pada router Jakarta, ditambahkan konfigurasi script dengan nama "l2tp-mon-up" dengan policy read, reboot, write dan test untuk menghapus user yang active pada l2tp-server seperti gambar 17.



Gambar 17. Konfigurasi Script 2 router Jakarta

/ppp active remove [find name="automatedvpn"];

Menghapus user yang aktif pada PPP active dari L2TP yang menggunakan username "automatedvpn".

Kemudian ditambahkan konfigurasi netwatch pada router Jakarta seperti gambar 18.

Gambar 18. Konfigurasi Netwatch router Jakarta

6. Pengujian

6.1. Pengujian Kinerja Script dalam Konfigurasi Otomatis

Dari 3 (tiga) kali pengujian yang dilakukan terhadap script, perubahan konfigurasi pada Virtual Private Network berjalan dengan baik dimana konfigurasi remote address maupun local address pada tunnel EoIP baik di lokasi kantor Balikpapan dan kantor Jakarta berubah mengikuti IP address yang didapat dari indihome.

6.2. Pengaruh L2TP Sebagai Monitor Link Dalam Kualitas Delivery

Dari 3 (tiga) kali pengetesan yang dilakukan baik menggunakan Monitoring Link maupun tidak, berikut hasil yang didapatkan :

Tabel 1. Hasil Ping Test dengan Monitoring Link Menyala

Packet Size (Bytes)	Minimum	Rata-rata	Maksimum
64	29.01	30.046	33.032
800	27.984	28.788	34.05
1600	28.027	29.473	33.096

Tabel 2. Hasil Ping Test Tanpa Monitoring Link

Packet Size (Bytes)	Minimum	Rata-rata	Maksimum
64	29.022	30.670	34.184
800	28.003	29.312	32.01
1600	28.526	29.843	34.027

Berdasarkan hasil tersebut, dapat disimpulkan bahwa ada atau tidaknya L2TP Tunnel sebagai monitoring link tidak berpengaruh terhadap latency dari Automated Virtual Private Network yang menggunakan Ethernet over Internet Protocol.

Kemudian pengetesan dilanjutkan dengan tindakan upload maupun download dari kantor Balikpapan ke Jakarta serta sebaliknya pada saat monitor link menyala dan tidak. Hasilnya, Delivery bandwidth saat monitor link menyala maupun saat monitor link mati tetap dapat mencapai maksimum 10 Mbps sesuai dengan layanan yang disewa kepada jasa penyedia internet baik pada aktifitas upload maupun download.

Berdasarkan hasil tersebut, dapat dinyatakan saat menggunakan monitoring link maupun tidak menggunakan monitoring link, kualitas link Virtual Private Network secara bandwidth tidak mengalami perubahan 'dan tidak terpengaruh dengan adanya monitor link yang menggunakan Layer-2 Tunnel Protocol.

6.3. Pengujian Waktu Downtime Saat Terjadi Perubahan IP Public Dynamic

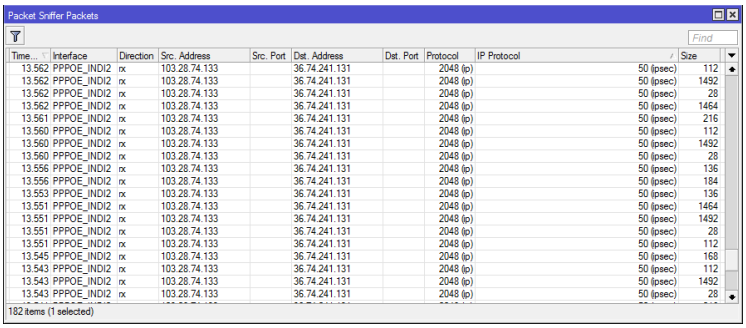
Tabel 3. Hasil Pengujian Waktu Proses Perubahan IP

Pengujian	Down	Durasi	Keterangan
1	2 detik	26 detik	Berhasil
2	3 detik	24 detik	Berhasil
3	3 detik	25 detik	Berhasil

Berdasarkan hasil dari ketiga pengujian diatas maka dapat dihasilkan kesimpulan bahwa proses berjalannya script dalam mengubah konfigurasi pada tunnel EoIP sejak IP Address publik di router Balikpapan berubah memakan waktu downtime paling lama detik. Proses keseluruhan memakan waktu 24 sampai 26 detik.

6.4. Pengecekan Keamanan Transfer Data Menggunakan Packet Sniffer

Berdasarkan hasil pengecekan dengan menggunakan tool Packet Sniffer milik MikroTik pada interface PPPOE_INDI2 yang berada di router Balikpapan, terlihat koneksi dari router Jakarta “103.28.74.133” ke router Balikpapan “36.74.241.131” di enkripsi menggunakan IPSec.



Gambar 19. Hasil pengecekan keamanan menggunakan Packet Sniffer

KESIMPULAN

Kesimpulan yang bisa diambil dari penelitian rancang bangun ini dimana telah dikembangkan Virtual Private Network di PT. Satnetcom Balikpapan untuk menghubungkan kantor pusat dan kantor cabang secara LAN. Pada penelitian ini juga telah dikembangkan Automated Virtual Private Network di PT. Satnetcom Balikpapan yang memudahkan tim IT di perusahaan dalam distribusi informasi dan pengelolaan jaringan. Automated Virtual Private dalam pengaplikasiannya dapat digunakan pada jaringan berjenis Small Office Home Office dengan IP Address publik yang berubah-ubah.

SARAN

Dalam penelitian ini penulis menyadari masih ada banyak kekurangan dari hasil penelitian yang dilakukan, oleh karena itu kritik dan saran yang membangun dapat membantu dalam mencapai kesempurnaan dari penelitian ini. Saran yang dapat diberikan dalam kelanjutan penelitian ini yaitu meminimalisir waktu link mati ketika terjadi perubahan IP Address dengan menemukan mekanisme baru yang dapat membantu link ini dapat dengan cepat beradaptasi dengan perubahan IP Address dibanding dengan yang penulis buat. Penelitian ini mengharuskan di satu sisi memiliki IP Address publik statik. Penelitian ini dapat ditingkatkan dimana di dua sisi menggunakan IP Address publik dinamis.

UCAPAN TERIMA KASIH

Terima kasih kepada bapak pembimbing terbaik Bapak Wisnu Hera Pamungkas, S. Tp., M. Eng. dan Bapak Jamal, S. Kom., M. Kom. yang telah memberikan ilmu, kritik, masukan dan saran selama proses pembuatan karya tulis ini sehingga karya tulis ini dapat terselesaikan dengan baik.

Terima kasih kepada kedua orang tua yang telah memberikan dukungan selama proses pembuatan karya tulis ini.

Terimakasih juga kepada rekan-rekan se-angkatan alumni Universitas Mulia tahun 2019 yang telah bersama-sama berjuang melewati masa-masa senang dan susah selama perkuliahan berjalan.

DAFTAR PUSTAKA

[1] Komputer, Wahana., 2004, Kamus Istilah Internet, Edisi II. Yogyakarta:Andi.

[2] Jogiyanto, H.M., 2005, Analisa dan Desain Sistem Informasi: Pendekatan. Terstruktur Teori dan Praktik Aplikasi Bisnis, ANDI, Yogyakarta.

[3] B. Widodo, "Analisis Quality of Service pemanfaatan Ethernet Over IP (EoIP) Tunnel di Mikrotik RouterOS dengan Routing Protocol OSPF", INISTA, vol. 1, no. 1, September 2018.

[4] Hermawan, Rian Heri dan Bobi Kurniawan, "Implementasi Ethernet Over IP (EoIP) Tunnel Mikrotik RouterOS Pada Layanan Voice over IP (VoIP) Di PT Akurasi Kuatmega", Jurnal Ilmiah Komputer dan Informatika, Volume 5 Nomor 1, Maret 2016.

[5] Akmal, Imelda. 2010. SOHO (Small Office Home Office). Gramedia Pustaka Utama:Jakarta.

[6] Mubarok, Dzaki. (2016). Implementasi EoIP over VPN di jaringan berbasis dynamic IP.

[7] Ikhwan, S., & Amalina, A. (2017). "Analisis Jaringan VPN Menggunakan PPTP dan L2TP". JURNAL INFOTEL, vol. 9 no. 3, Agustus 2017.

[8] Handriyanto, D. F. 2009. Kajian Penggunaan Mikrotik RouterOs™ Sebagai Router Pada Jaringan Komputer. Kajian Penggunaan Mikrotik Router Os Sebagai Router Pada Jaringan Komputer. UNIVERSITAS SRIWIJAYA, 2009

[9] Athailah. 2013. Mikrotik Untuk Pemula. Jakarta: Mediakita.

[10] Hasibuan, Tiffany Ezrawati, IP Security, Online pada https://ilmuti.org/2014/04/19/ip-security/, diakses tanggal 15 April 2019.