Jurnal Ilmu Teknik dan Komputer
Vol. 3 No. 1 Januari 2019
P-ISSN 2548-740X
E-ISSN 2621-1491

ANALISA QOS ADMINISTRATIVE DISTANCE STATIC ROUTE PADA FAILOVER VPN IPSEC

Agus Darojat[1], Ida Nurhaida[2]

Jurusan informatika, Fakultas Ilmu komputer, Universitas Mercu Buana
Jl. Raya Meruya Selatan No. 1, Jakarta 11650, Indonesia

ABSTRACT

Sebuah jaringan komputer yang memiliki satu koneksi virtual Private virtual (VPN) tunnel sangat rentan terhadap gangguan yang disebabkan oleh beberapa hal diantaranya kualitas dari internet yang tidak stabil maupun gangguan koneksi fisik kabel dan bencana berskala besar yang menyebabkan kegagalan komunikasi dalam kasus IPsec VPN. Untuk menanggulangi masalah tersebut diperlukan solusi yaitu failover. Pendekatan failover adalah perpindahan jalur ketika komunikasi utama ke jalur kedua secara otomatis. Ketika komunikasi antara perangkat yang dihubungkan virtual Private virtual (VPN) mendeteksi kegagalan maka perangkat tersebut akan melakukan routing ulang untuk menentukan rute jalur baru. Dengan adanya metode failover VPN Ipsec ini dapat memberikan ketersediaan koneksi data center dengan kantor yang berada di area pelosok dikarenakan insfrastruktur jaringan yang kurang memadai dapat memanfaatkan jaringan internet 4G sebagai jaringan ISP untuk tunnel VPN backup.

Kata Kunci: VPN, Failover dan Backup

1. PENDAHULUAN

Virtual Private Network (VPN) adalah jaringan yang biasanya menggunakan infrastruktur telekomunikasi public Seperti *internet* untuk menyediakan akses kantor pusat atau pengguna yang tidak dikantor dengan jaringan organisasi pusat. Biasanya VPN memerlukan pengguna atau perangkat jarak jauh untuk otentiakasi dan sering mengamankan data dengan teknologi enkripsi untuk mencegah pengungkapan informasi pribadi kepada pihak yang tidak berwenang(Ravinath, Kumar, & Bhattacharya, 2013). Jaringan VPN biasanya menyertakan beberapa router menggunakan infrastruktur publik supaya berkomunikasi satu sama lain untuk membuat jaringan *wide area network* (WAN). Sebagai contoh perusahaan yang membutuhkan VPN site to site adalah perusahaan yang berkembang dengan puluhan kantor cabang. Sebuah VPN *site to site* dapat diatur antara dua router (atau perangkat yang mendukung teknologi VPN) di lokasi berbeda yang menyediakan akses ke WAN untuk tempat tersebut (Router juga disebut sebagai *endpoint* atau VPN perangkat jaringan endpoint) Ketika beberapa router menjadi bagian dari jaringan VPN yang sama, biasanya terbentuk terowongan VPN (VPN tunnel) antara masing-masing router untuk membentuk sebuah jalur jaringan(Francisco et al., 2014).

Internet Protocol Security (IPsec) adalah protokol untuk mengamankan komunikasi Internet Protocol (IP) dengan melakukan proses otentikasi dan enkripsi pada setiap *tunnel* komunikasi paket data. IPsec juga mencakup protokol untuk membangun hubungan timbal balik otentikasi antar perangkat pada awal komunikasi dan negosiasi kunci kriptografi yang akan digunakan selama sesi komunikasi(Tjahjono, Shaikh, & Ren, 2014).

Memperhatikan ketersedian VPN yang digunakan bagi setiap perusahaan yang memiliki banyak cabang maka diperlukan solusi untuk menghindari gangguan yang disebabkan oleh gagalnya *komunikasi internet service provider* (ISP) maupun

bencana berskala besar yang menyebabkan kegagalan komunikasi dalam kasus VPN. Secara umum, lebih baik untuk memperluas *wide area network* (WAN) dimana komunikasi dipulihkan dengan menggunakan metode *failover* VPN . Metode *failover* VPN yang ada dapat mengurangi kegagalan komunikasi. Dalam metode ini, VPN menyamakan informasi waktu terlebih dahulu dan ketika VPN *tunnel* yang aktif gagal, tunnel yang dalam kondisi *standbye* mengambil alih pemrosesan menjadikan *tunnel* aktif. Dengan demikian, dalam mengusulkan metode *failover* VPN yang dapat diterapkan pada VPN yang ditempatkan pada segmen IP address yang berbeda. Metode yang ada adalah *framework* yang mensinkronisasi informasi antara VPN yang aktif dan VPN *standby*. Hal ini memungkinkan komunikasi berlanjut saat *tunnel* utama gagal. Namun, metode ini tidak bisa sepenuhnya mencegah kegagalan komunikasi secara *zero* RTO (request time out) dikarenakan adanya proses initialisasi kembali jalur *tunnel* yang baru.

Secara umum, Penelitian ini memiliki pendekatan terhadap *failover* jalur komunikasi antara komputer yang dihubungkan oleh sebuah *tunnel* pada jaringan VPN. Pendekatan ini menjelaskan cara kerja mendeteksi jalur komunikasi dan kegagalan perangkat melalui pemantauan routing komunikasi pada saat terjadi kegagalan terjadi.

Dalam membangun VPN diperlukan ip publik pada masing masing lokasi dari hubungan antar ip publik tersebut akan ada sebuah terowongan untuk jalur koneksi antar IP lokal. Sebuah metode untuk menentukan *tunnel* VPN status nya aktif dalam sebuah komunikasi jaringan. Pada jaringan IP publik pertama elemen jaringan yang berasal akan mengirim sebuah pesan IPSec kepada jaringan IP publik kedua kemudian ditanggapi untuk menerima pesan tersebut untuk mengaktifkan *tunnel*, pada jaringan IP publik kedua setelah menerima pesan IPSec kemudian mengirim balik pesan IPsec ke jaringan ip publik pertama tersebut untuk mengaktivkan tunnel. Berapa kali kegagalan tanggapan dari pengiriman pesan IPSec tersebut akan dibandingkan dengan nilai ambang batas untuk menentukan jika *tunnel* IPsec yang aktif menjadi dinonaktivkan(Chassiakos, Ph.D.(Chair), Khoo, Ph.D., & Yeh, Ph.D, 2017).

2. STUDI LITERATUR

2.1 Konsep VPN Ipsec Tunnel

Jalur data antara komputer atau perangkat pengguna dan jaringan VPN disebut sebagai sebuah terowongan Seperti terowongan fisik, jalur data hanya bisa diakses di kedua ujungnya. Enkapsulasi membuat ini mungkin terjadi. Paket IPsec melewati satu ujung terowongan yang lain dan berisi paket data yang dipertukarkan antara pengguna lokal dan *remote private* jaringan. Enkripsi paket data memastikan bahwa pihak ketiga mana yang mencegat IPsec paket tidak dapat mengakses data(Chassiakos, Ph.D.(Chair) et al., 2017).

Gambar 1. Konsep VPN IPsec tunnel

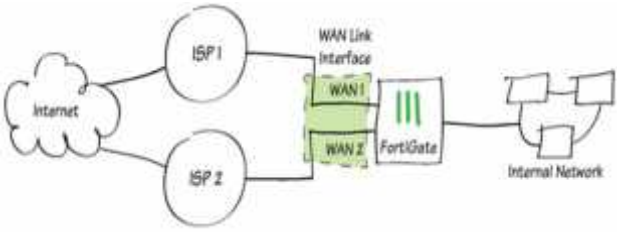
Pada gambar 1 menjelaskan sebuah sesi komunikasi yang aman antara dua komputer dengan menggunakan IPsec, maka dibutuhkan sebuah *framework* protokol yang disebut dengan ISAKMP/Oakley(Gamundani, Nambili, & Bere, 2014). *Framework* tersebut mencakup beberapa algoritma kriptografi yang telah ditentukan sebelumnya, dan juga dapat diperluas dengan menambahkan beberapa sistem kriptografi tambahan yang dibuat oleh pihak ketiga. Selama proses negosiasi dilakukan, persetujuan akan tercapai dengan metode otentikasi dan kemanan yang akan digunakan dan protokol pun akan membuat sebuah kunci yang dapat digunakan bersama (*shared key*) yang nantinya digunakan sebagi kunci enkripsi data. IPsec mendukung dua buah sesi komunikasi keamanan yakni sebagai berikut:

- Protokol *Authentication Header* (AH): Menawarkan otentikasi pengguna dan perlindungan dari beberapa serangan (umumnya serangan *man in the middle*) dan juga menyediakan fungsi otentikasi terhadap data serta integritas terhadap data. Protokol ini mengizinkan penerima untuk merasa yakin bahwa identitas pengirim adalah benar adanya dan data pun tidak dimodifikasi selama transmisi. Namun, protokol AH tidak menawarkan fungsi enkripsi terhadap data yang ditransmisikannya. Informasi AH dimasukkan ke dalam *header* paket IP yang dikirimkan dan dapat digunakan secara sendirian atau bersamaan dengan protokol Encapsulating *Security Payload*(Francisco et al., 2014).

- Protokol *Encapsulation Security Payload* (ESP): Protokol ini melakukan enkapsulasi serta enkripsi terhadap data pengguna untuk meningkatkan kerahasiaan data. ESP juga dapat memiliki skema otentikasi dan perlindungan dari beberapa serangan dan dapat digunakan secara sendirian atau bersamaan dengan Authentication Header. Sama seperti halnya AH, informasi mengenai ESP juga dimasukkan ke dalam header paket IP yang dikirimkan(Francisco et al., 2014).

2.2 Multipath Routing Algoritma

Multipath routing terjadi ketika lebih dari satu konfigurasi routing ke tujuan yang sama hadir dalam tabel *routing*. Dua metode untuk menyelesaikan beberapa rute secara manual ke tujuan yang sama adalah dengan menurunkan nilai *administrative distance* satu atau menetapkan prioritas kedua rute.
Administrative distance didasarkan pada kehandalan yang diharapkan dari rute yang diberikan. Ini ditentukan melalui kombinasi jumlah *hop* dari protokol yang digunakan(Alsaheel & Almogren, 2014).
Hop (lompatan) adalah ketika lalu lintas bergerak dari satu router ke router berikutnya. Lebih banyak lompatan dari sumber berarti lebih banyak kemungkinan titik kegagalan.



Gambar 2. Multipath route

Berikut ini seperti pada gambar 2 *multipath route* untuk mengilustrasikan cara kerja *administrative distance* dan prioritas. Jika ada dua lalu lintas rute yang dapat dilakukan antara dua tujuan dengan *administrative distance* dengan nilai 5 dan 31 (kadang-kadang tidak tersedia) dengan prioritas sama (dengan nilai 0), lalu lintas akan menggunakan rute dengan administrative distance bernilai 5. Jika karena alasan tertentu, rute yang disukai (administrative distance 5) adalah tidak tersedia, rute lain dengan nilai 31 akan digunakan sebagai cadangan.
Metode lain untuk menentukan rute terbaik adalah secara manual mengubah prioritas kedua rute yang dimaksud. Jika administrative distance dari hop berikutnya dari dua rute pada unit router adalah sama, mungkin tidak jelas rute paket mana akan mengambil. Mengkonfigurasi secara manual prioritas untuk setiap rute tersebut akan memperjelas apa yang akan digunakan *hop* berikutnya. Rute prioritas yang lebih rendah akan menjadi rute terbaik.

2.3 Parameter Quality of Services (QoS)

Teori trafik yang digunakan untuk menganalisa dan merencanakan jaringan telekomunikasi yang digunakan untuk membawa masing-masing informasi akan berbeda pula(Diwi, Rumani, & Wahidah, 2014). Sebuah kualitas jaringan dapat dianalogikan sebagai berikut:

1. *Bandwidth / Throughput*, dianalogikan pipa
2. *Delay*, mempresentasikan panjang pipa
3. *Jitter*, variasi delay pada pipa
4. *Loss*, menggambarkan kebocoran pada pipa

Definisi empat kelas Kualitas Layanan TIPHON yang dapat digunakan untuk mengklasifikasikan layanan *Telecommunications and Internet Protocol Harmonization Over Networks* (TIPHON) dipengaturan *peering* dan kontrak pasokan di mana tarif yang berbeda dapat berlaku untuk berbagai tingkat kualitas atau dimana jaminan kinerja dapat diberikan(ETSI, 1999).

Tabel 1. Persentasi dan Nilai dari QOS

Nilai Indeks	Persentase (%)	Indeks
3,8 – 4	95 – 100	Sangat Memuaskan
3 – 3,79	75 – 94,75	Memuaskan
2 – 2,99	50 – 74,75	Kurang Memuaskan
1 – 1,99	25 – 49,75	Jelek

2.3.1 Throughput

Throughput adalah jumlah bit yang diterima dengan sukses perdetik melalui sebuah sistem atau media komunikasi (kemampuan sebenarnya suatu jaringan dalam melakukan pengiriman data). *Throughput* diukur setelah transmisi data (*host/client*) karena suatu sistem akan menambah delay yang disebabkan *processor limitations*, kongesti jaringan, *buffering inefficients*, *error* transmisi, *traffic loads* atau mungkin desain *hardware* yang tidak mencukupi(Diwi et al., 2014).

Tabel 2. **Kategori *Throughput***

Kategori	*Throughput (bps)*	*Indeks*
Best	100	**4**
High	75	**3**
Medium	50	**2**
Best Effort	< 25	**1**

(sumber: TIPHON)

2.3.2 Delay (Latency)

Delay adalah waktu yang dibutuhkan oleh sebuah paket data terhitung dari saat pengiriman oleh *transmitter* sampai saat diterima oleh *receiver*.

Tabel 3. Kategori Delay (Latency)

Kategori	Delay (ms)	Indeks
Best	< 150 ms	**4**
High	150 ms s/d 300 ms	**3**
Medium	300 ms s/d 450 ms	**2**
Best Effort	> 450 ms	**1**

(source : TIPHON)

2.3.3 Jitter

Jitter adalah variasi delay perbedaan selang waktu kedatangan antar paket di terminal tujuan. Untuk mengatasi jitter maka paket data yang datang dikumpulkan dulu dalam *jitter buffer* selama waktu yang telah ditentukan sampai paket dapat diterima pada sisi penerima dengan urutan yang benar. Nilai jitter yang direkomendasikan oleh ITU–T Y.1541 adalah dibawah 50 ms. *Tool* yang di gunakan yaitu IPerf.

Tabel 4. Kategoi Jitter

Kategori	Jitter (ms)	Indeks
Best	**0 ms**	**4**
High	**0 ms s/d 75 ms**	**3**
Medium	**75 ms s/d 125 ms**	**2**
Best Effort	**125 ms s/d 225 ms**	**1**

(Source : TIPHON)

2.3.4 Packet Loss

Packet loss adalah banyaknya paket yang hilang selama proses transmisi ke tujuan. Tool yang dapat digunakan yaitu IPerf atau *wireshark*, Adapun faktor yang menyebabkan packet loss diantaranya :

1. Terjadi tabrakan data atau antrian penuh
2. *Link* atau *hardware* disebabkan CRC error
3. Perubahan rute (temporary drop) atau *blackhole* route (persistent drop)
4. Interface atau router *down*

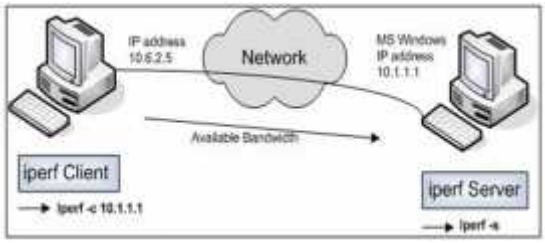
Tabel 5.Kategori Pakcet Loss

Kategori	Packet Loss (%)	Indeks
Best	**0**	**4**
High	**3**	**3**
Medium	**15**	**2**
Best Effort	**25**	**1**

(sumber : TIPHON)

2.4 Tool IPerf

IPerf adalah salah satu *tool* untuk mengukur *troughput bandwidth* dan *performance* dalam sebuah link network, sesuai pada gambar 3 Pengujian menggunakan IPerf agar dapat dilakukan pengukuran diperlukan IPerf yang terinstall *point to point*, baik disisi server maupun client. Iperf sendiri bisa digunakan untuk mengukur performance link dari sisi TCP/UDP.



Gambar 3. Pengujian menggunakan IPerf

Alat estimasi bandwidth *end-to-end* seperti IPerf meskipun cukup akurat bersifat intrusif. Pengujian dapat memperkirakan bandwidth end-to-end akurat, sementara mengkonsumsi jaringan jauh lebih sedikit bandwidth dan waktu(Hadi, n.d.)**.**

2.5 Fortigate

Fortigate adalah sebuah sistem keamanan yang dikeluarkan oleh perusahaan Fortinet. Fortinet merupakan perusahaan, penyedia layanan, dan badan pemerintah di seluruh dunia, termasuk mayoritas dari perusahaan Fortune Global 100 tahun 2009. Fortinet merupakan pemimpin pasar *untuk unified threat management* (UTM)(Documentation, 2014).
Fortigate sebagai perangkat yang menjamin keamanan jaringan secara keseluruhan sekaligus berfungsi sebagai gateway dan router bagi jaringan LAN sehingga tak dibutuhkan lagi router ataupun

perangkat tambahan *load balancing* bila ada lebih dari satu koneksi WAN.

3. METHODOLOGI

Metodologi ini akan menerangkan mengenai cara dan langkah-langkah yang akan dilakukan pada penelitian untuk membangun *failover* VPN IPsec *tunnel* dengan menggunakan tiga jalur Internet service provider yang memiliki masing masing satu tunnel sehingga akan saling menjaga intekoneksi VPN agar tetap terhubung.

Gambar 4. Diagram Metodologi yang Diusulkan

3.1 Analysis Requirement

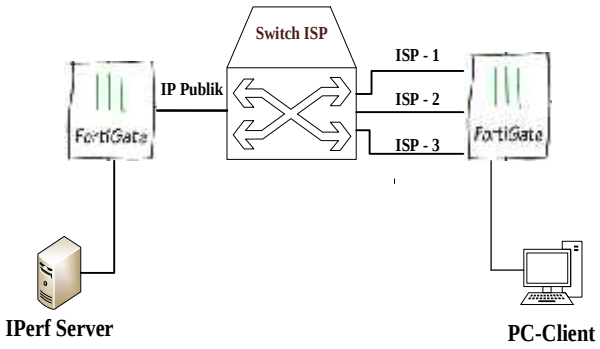
Pada tahap ini penulis melakukan analisa semua kebutuhan elemen dan kebutuhan sistem baru seperti pada tabel 1 yang akan dibangun meliputi kebutuhan perangkat lunak (*software*) dan kebutuhan perangkat keras (*hardware*).

Tabel 6. Kebutuhan hardware dan software

Hardware	**Spesifikasi**
Laptop	Intel Core i3@ 1.80Ghz dan RAM 4Gb
PC Desktop	Intel dualcore @ 1.80Ghz dan RAM 4Gb
Fortigate 101E	FortiOS 5.6.3
Fortigate 50E	FortiOS 5.6.3
Switch L3	Cisco Catalyst 3560
Software	**Versi**
windows	Windows 7 /10
Command Prompt	Microsoft Windows
Iperf	For Windows 64 bits

3.2 Desain Simulasi Topologi

Pada penelitian ini untuk dapat menganalisa tingkah laku dari proses *failover* VPN IPsec *tunnel* memerlukan sebuah IP (internet protocol) Publik yang merupakan IP yang bisa diakses langsung oleh internet. Dengan menggunakan Switch L3 dapat dirancang sebagai interkoneksi antar IP publik sehingga switch L3 dianalogikan sebagai *internet service provider* (ISP).



Gambar 5. Design Topologi Simulasi

Pada skema gambar 5 topologi simulasi terdapat tiga perangkat sebagai instrumen untuk membangun system VPN IPsec tunnel dimana fortigate yang terhubung dengan Server sebagai *fortigate server* dan *fortigate* yang terhubung dengan PC *client* sebagai fortigate *client* sedangkan Switch ISP sebagai pendistribusi IP publik sehingga fortigate client dan fortigate server dapat berkomunikasi untuk membentuk sebuah *tunnel*, switch L3 ini mendistribusikan empat IP Publik diantaranya satu IP publik untuk Fortigate server dan tiga IP Publik untuk Fortigate client dimana penggunaan IP publik ini untuk backup link sehingga nantinya jalur data akan berpindah secara otomatis jika terjadi gangguan pada ISP utama, setelah tunnel terbentuk maka pc client dapat terhubung ke server lewat VPN IPSec *tunnel*.

Tabel 7. IP Addressing Fortigate

Fortigate client		
Interface wan1 (ISP-1)	220.10.180.2 /28	
Interface wan2 (ISP-2)	220.20.180.2 /28	
Interface wan3 (ISP-3)	220.30.180.2 / 28	
Interface Lan	172.20.18.1 /24	
Fortigate Server		
Interface wan1 (IP Publik)	116.150.100.2 /28	
Interface Lan	10.10.10.1 /24	

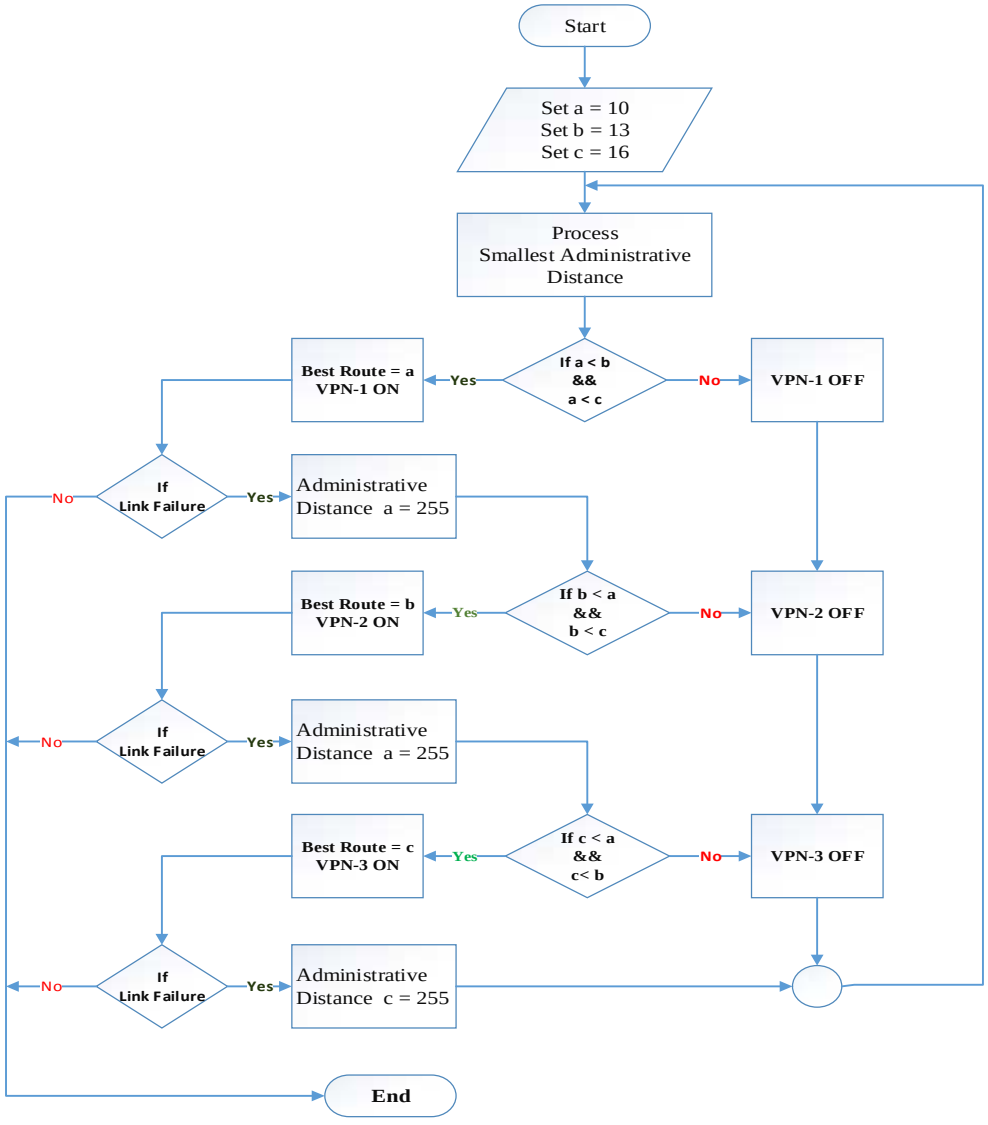
Tabel 8. IP Addressing switch dan PC

PC	
PC client	10.10.10.2 /24
Gateway pc client	10.10.10.1 /24
PC sever	172.20.18.2 /24
Gateway PC server	172.20.18.1 /24

Switch L3	
Port 1	116.150.100.1 /28
Port 1/0/17	220.10.180.1 /28
Port 1/0/18	220.20.180.1 /28
Port 1/0/19	220.30.180.1 / 28

Pada tabel 7 IP addressing Fortigate merupakan IP address yang dikonfigurasi kedalam perangkat untuk berkomunikasi yang akan ditumpangi sebuah tunnel. *fortigate client* akan mendaftarkan IP address *fortigate* server dan sebaliknya fortigate server akan mendaftarkan IP address *client* sehingga saling bertukar informasi dan mengidentifikasi satu sama lain.

Pada tabel 8 IP address switch dan PC terdapat Switch L3 yang mengatur jalur dari IP *fortigate* sehingga menyerupai IP internet dan IP address PC merupakan jaringan local yang tidak tidak dapat terhubung ke PC yang lain sebelum *tunnel* terbentuk. Setelah merencanakan topologi simulasi dilanjutkan dengan konfigurasi menerapkan algoritma *administrative distance* untuk menentukan prioritas jalur data *primary* dan *secondary*.



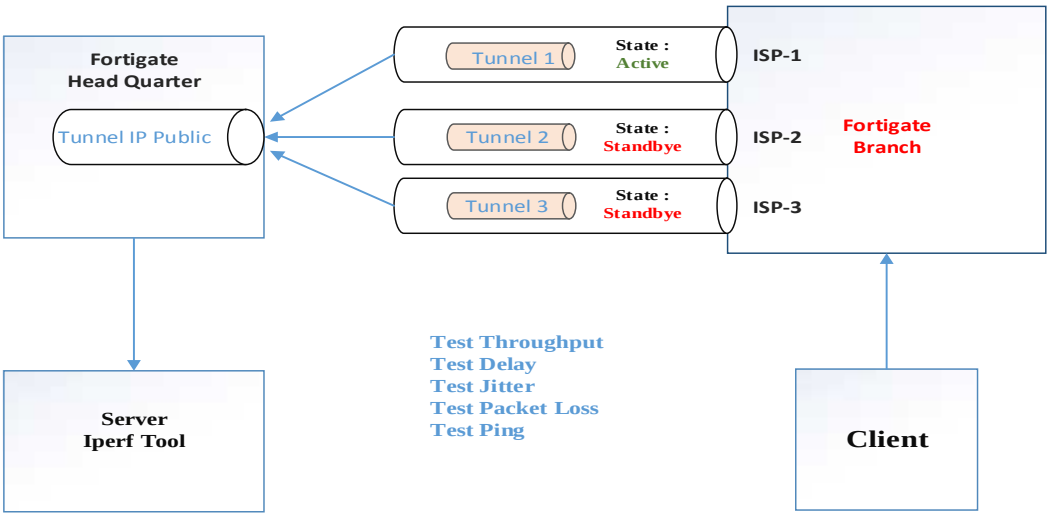
Gambar 6. Algoritma administrative distance untuk *failover*

Menentukan sebuah prioritas jalur VPN Ipsec tunnel pada perangkat Fortigate client nilai dari *administrative distance*-nya dikonfigurasi secara terurut sesuai pada gambar 6 Algoritma *administrative distance* untuk *failover* sehingga menghasilkan tiga jalur VPN IPsec tersebut menjadi

VPN-1 (aktiv), VPN-2 *(standbye)* dan VPN-3 *(standbye)*. Pada *Fortigate client* memiliki tiga *static route* dengan nilai *administrative distance*-nya berbeda. Fortigate akan melakukan pengecekan pada daftar routing untuk mencari *best route* dengan memilih nilai administrative distance terkecil dari tiga static route tersebut sebagai best route, Fortigate client memiliki tiga *static route* yang sudah dikonfigurasi untuk VPN IPsec tunnel pertama (VPN-1) nilai *administrative distance*-nya 10, VPN IPsec *tunnel* kedua (VPN-2) nilai *administrative distance*-nya 13 dan VPN IPsec tunnel ketiga (VPN-3) nilai administrative distance-nya 16 Sehingga hasilnya VPN-1 sebagai prioritas pertama, VPN-2 sebagai prioritas kedua dan VPN-2 sebagai prioritas ketiga. Algoritma routing tersebut dibuat seperti algortima *Selection* dimana nilai *administrative distance* paling kecil akan menjadi prioritas utama sehingga dapat membuat VPN IPsec tunnel bersifat *Auto connect* (terhubung secara otomatis).

3.3 Skenario Pengukuran

Pada tahap ini terdapat beberapa skenario pengujian untuk memastikan *failover* berjalan dengan benar dan
mencari data-data parameter *Quality of Serviced* dengan menggunakan *tool* IPerf.



Gambar 7. Skenario pengujian.

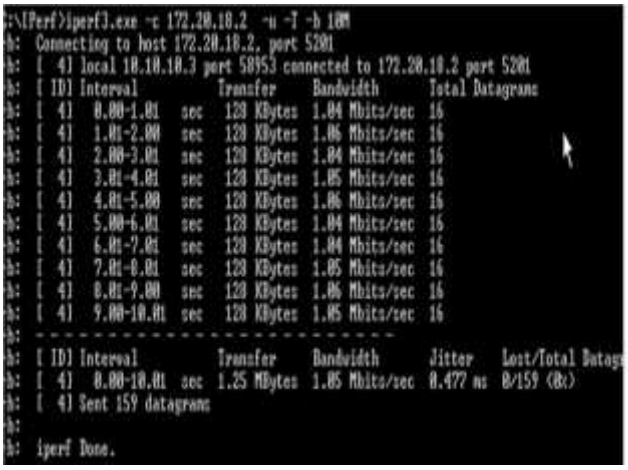
Pengujian dilakukan sesuai gambar 7 skenario pengujian dengan *tool IPerf* yang digunakan sebagai pengukuran QOS pada udp/tcp parameter pada failover parameter Qos yang diperhatikan yaitu nilai *packet loss* yang sesuai dengan harapan standart THIPON. Skenario pengujian dilakukan selama 60 detik dengan *buffer size* 10Mb dan Pengujian juga dilakukan uji coba sebanyak lima kali untuk mendapatkan banyak data. Beberapa pengujian dibagi lagi menjadi skenario sebelum *failover* dan setelah kondisi *link* utama kembali pulih (*connection recovered*) sehinga mendapatkan perbandingan data yang akurat. Langkah-langkah yang perlu dilakukan untuk Pengukuran sebagai berikut :

1. Pada PC *Server* (*receiver*) hidupkan IPerf sebagai server dengan cara buka *command prompt* kemudian ketik **iperf3.exe –s**

Gambar 8. IPerf sebagai server

Pada gambar 8 IPerf sebagai server menunjukan sudah *running* dan siap untuk menerima perintah tes dari *client* .

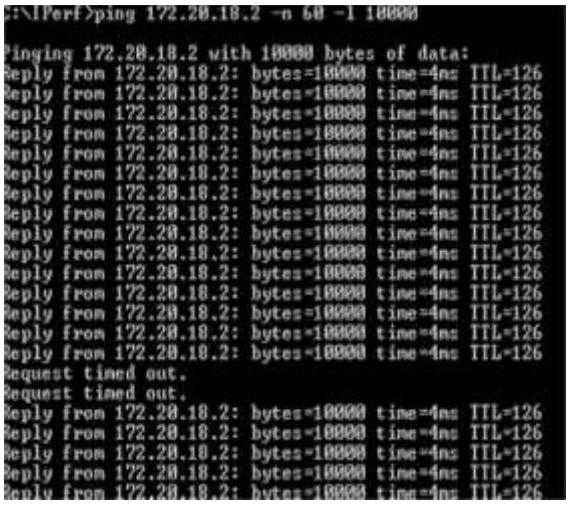
2. Pada PC *Client* (*sender*) hidupkan IPerf sebagai server dengan cara buka *command prompt* kemudian ketik **iperf3.exe -c 172.20.18.2 -t 60 -u -T -b 10M**



Gambar 9. IPerf mengirim perintah tes

Pada gambar 9 IPerf mengirim perintah tes udp/tcp dengan *buffer size* 10Mb selama 60 detik akan menunjukan informasi *transfer rate*, *bandwidth*, *Jitter* dan *packet loss*.

3. Pengujian tes ping dengan membuka command prompt Pada PC *Client* kemudian ketik **ping 172.20.18.2 -n 60 -l 10000**



Gambar 10. Pengujian Ping

Untuk mendapatkan informasi *latency* perlu dilakukan sesuai dengan gambar 10. pengujian ping yang menunjukan informasi **request time out** (Koneksi terputus) dan **reply from 172.20.18.2** (jaringan terhubung dengan server). Hal ini menandakan terjadi *failover*.

Pada uji coba pengukuran dengan skenario sebagai berikut:

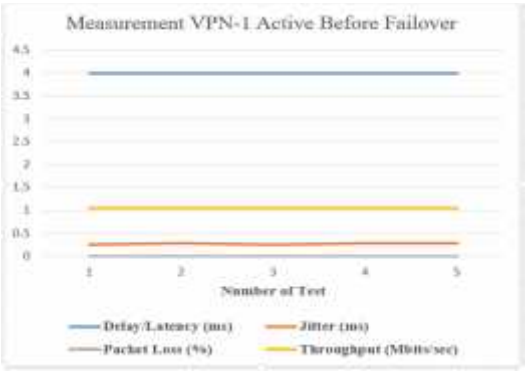
1. Pengujian Link VPN-1 ON Sebelum Failover
2. Pengujian Failover VPN-2 Aktif
3. Pengujian Failover VPN-3 Aktif
4. Pengujian Link ISP-2 Terhubung kembali VPN-2 Aktif
5. Pengujian Link ISP-1 Terhubung kembali VPN-1 Aktif

4. HASIL DAN DISKUSI

Kinerja *failover* telah diuji dengan beberapa skenario dengan melakukan langkah-langkah pada skenario pengukuran.

4.1 Pengujian Link VPN-1 Aktif Sebelum Failover

Pengujian dilakukan pada gambar 6. Pengujian sebelum *failover* menunjukan hasil saat kondisi ISP-1 terhubung dengan status VPN-1 ON, VPN-2 OFF dan VPN-3 OFF.

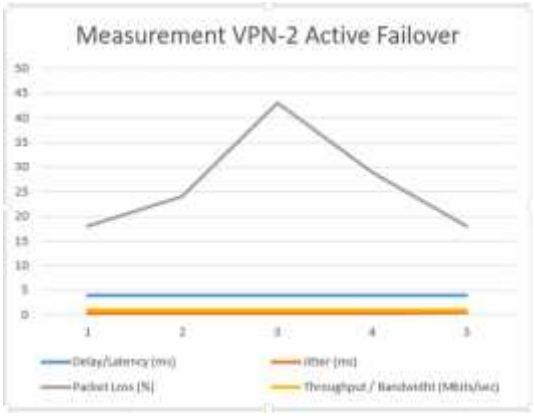


Grafik 1. Hasil Pengujian Sebelum *Failover*

Pada grafik 1. Hasil Pengujian sebelum failover menunjukan nilai dari Paramater QOS yang stabil dengan melakukan lima kali melakukan langkah langkah pengujian.

4.2 Pengujian Failover VPN-2 Aktif

Pengujian dilakukan pada saat kondisi ISP-1 terputus dengan status VPN-1 OFF, VPN-2 ON dan VPN-3 OFF.

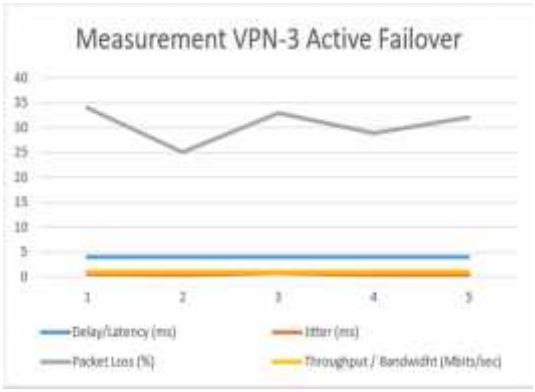


Grafik 2. Hasil Pengujian Failover VPN-2 Aktif

Pada grafik 2 hasil pengujian failover VPN-2 aktif menunjukan ada kenaikan *packet loss* dengan nilai tertinggi 40% lebih sehingga ini masuk kategori jelek.

4.3 Pengujian Failover VPN-3 Aktif

Pengujian dilakukan pada saat kondisi ISP-1 dan ISP-2 terputus dengan status VPN-1 OFF, VPN-2 OFF dan VPN-3 ON.

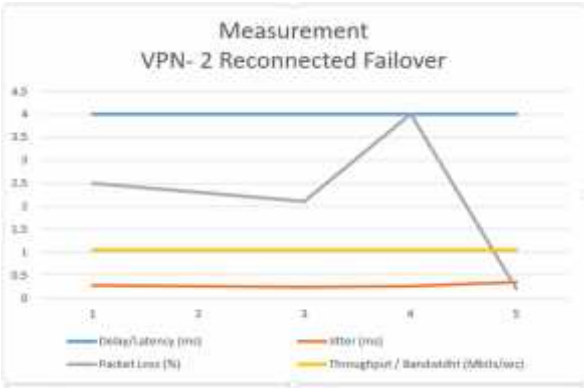


Grafik 3. Hasil Pengujian Failover VPN-3 ON

Pada grafik 3 hasil pengujian *failover* VPN-3 ON menunjukan nilai *packet loss* tertinggi 35% sehingga masih masuk kategori *best effort* atau jelek.

4.4 Pengujian Link ISP-2 (Reconnected) VPN-2 Aktif

Pengujian dilakukan pada saat kondisi ISP-2 terhubung kembali dan ISP-1 masih terputus dengan status VPN-1 OFF, VPN-2 ON dan VPN-3 OFF.

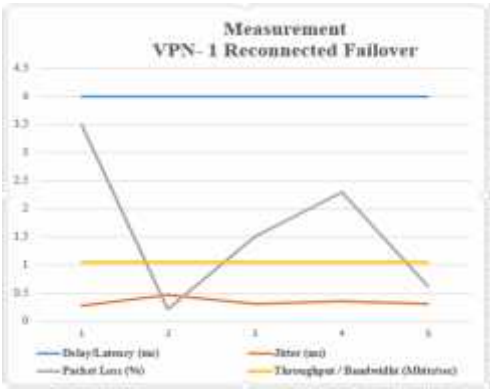


Grafik 4. Hasil pengujian Reconnected VPN-2

Pada grafik 4 Hasil pengujian Reconnected VPN-2 menunjukan nilai packet loss tertinggi 4 % yang mengindikasikan berada dalam kategori cukup bagus.

4.5 Pengujian Link ISP-1 (Reconnected) VPN-1 Aktif

Pengujian dilakukan pada saat kondisi ISP-1 dan ISP-2 terhubung kembali kembali (*connection recovered*) dan ISP-1 dengan status VPN-1 OFF, VPN-2 ON dan VPN-3 OFF.



Grafik 5. Hasil pengujian Reconnected VPN-1

Pada grafik 5 Hasil pengujian Reconnected VPN-1 menunjukan nilai *packet loss* tertinggi 3.5 % yang mengindikasikan berada dalam kategori cukup bagus.

4.6 Hasil Pengujian

Memperhatikan hasil pengujian-pengujian yang sudah dilakukan dan menghitung rata-rata nilai yang didapat serta mengacu pada standar angka THIPON sebagai perbandingan Quality of Service. Untuk membandingkan kualitas *failover* diambil nilai pada

saat terjadi failover perpindahan jalur VPN prioritas tinggi ke jalur VPN prioritas rendah dan pada saat terjadi failover perpindahan dari jalur VPN prioritas rendah ke jalur VPN prioritas tinggi (***reconnected***).

Tabel 9. Perbandingan Hasil Pengujian

Pengujian Link Failover			
Parameter QOS	**Pengukuran 60 detik**	**Indexs**	**Kategori**
Delay/Latency (ms)	4	4	
Jitter (ms)	0.25	4	
Packet Loss (%)	43	1	**Jelek**
Throughput (Mbits/sec)	1.05	4	
Average Informasi Indexs		**3.25**	**Memuaskan**
Pengujian Link Failover Reconnected			
Parameter QOS	**Pengukuran 60 detik**	**Indexs**	**Kategori**
Delay/Latency (ms)	4	4	
Jitter (ms)	0.281	4	
Packet Loss (%)	3.5	3	**Bagus**
Throughput (Mbits/sec)	1.05	4	
Average Informasi Indexs		**3.75**	**Memuaskan**

Pada tabel 9 Perbandingan hasil pengujian menunjukan ada perbedaan nilai *packet loss* yang signifikan pada saat pengujian *link failover* dengan kondisi perpindahan VPN tunnel primary (VPN-1) ke VPN *tunnel secondary* (VPN-2) dengan hasil QoS yang jelek. Pada saat pengujian link *Failover Reconnected* dengan kondisi perpindahan VPN tunnel *secondary* (VPN-2) ke VPN tunnel *primary* dengan hasil kualitas *Packet loss* yang bagus.

5. KESIMPULAN

Dengan menggunakan algoritma *administrative distance routing* pada sebuah *failover* dapat dibangun sesuai dengan prioritas jalur routing. Kombinasi tiga ISP dapat dibangun sebagai *failover* VPN IPsec *tunnel* dimana dapat membantu ketersedian koneksi antar jaringan *private*. *Administrative distance* dapat membuat *failover* lebih banyak lagi karena sebenarnya tinggal mengatur nilai terkecil agar dapat menentukan prioritas jalur yang di dilewati data. Pada hasil pengujian *Qos* dapat diambil kesimpulan sebagai berikut :

1. Pengukuran parameter-parameter QoS yang digunakan yaitu *delay/latency*, *jitter*, *packet loss* dan *throughput* dengan menggunakan aplikasi IPerf sebagai *tool* pengukuran.
2. Dari hasil pengukuran QoS terdapat hasil yang jelek saat terjadi *failover* parameter *packet loss* menunjukan hasil dengan kategori jelek.
3. Hasil pengukuran QoS yang menunjukan hasil bagus ketika pemulihan jaringan (*reconnected*) dimana perpindahan dari VPN tunnel dengan prioritas rendah ke VPN tunnel prioritas tinggi.
4. Hasil pengujian *packet loss* yang jelek dapat mempengaruhi kegagalan proses pengiriman file dan untuk mendukukung pengiriman file diperlukan *packet loss* yang rendah(Pardila & Alaydrus, 2015).

DAFTAR PUSTAKA

Alsaheel, A. A., & Almogren, A. S. (2014). A Powerful IPSec Multi-Tunnels Architecture. *Journal of Advances in Computer Networks*, *2*(4), 274–278.

Chassiakos, Ph.D.(Chair), A., Khoo, Ph.D., I.-H., & Yeh, Ph.D, H.-G. (2017). Connectivity Between Two Distant Sites with Automatic Failover To IPsec., (May).

Diwi, A. I., Rumani, R. M., & Wahidah, I. (2014). Analisis Kualitas Layanan Video Live Streaming pada Jaringan Lokal Universitas Telkom. *Buletin Pos Dan Telekomunikasi*, *12*(3), 207–216.

Documentation, F. T. (2014). FortiOS ™ Handbook Advanced Routing, 18–24.

ETSI. (1999). Telecommunication and Internet Protocol Harmonization Over Network (TIPHON); General Aspects of Quality of Service (Qos). *Etsi*, *2.1.1*, 1–37.

Francisco, S., Bicket, J., Francisco, S., Delegard, J. J., Francisco, S., Frey, C. A., … Jose, S. (2014). System And Method For Managing Site-to-Site VPNs Of A Cloud Managed Network., *2*(12).

Gamundani, A. M., Nambili, J. N., & Bere, M. (2014). A VPN Security Solution for Connectivity over Insecure Network Channels: A novel study. *SSRG International Journal of Computer Science and Engineering*, *1*(September), 1–8.

Hadi, M. Z. E. N. S. (n.d.). PENGUKURAN QoS (Quality of Service) pada STREAMING SERVER, 1–14.

Pardila, M. E., & Alaydrus, M. (2015). Studi Analisa Transfer Rate Multiprotocol Label Switching (Mpls) Pada Media Akses Wireless Dan Wirelinedi Pt. Bank Commonwealth (Ptbc). *Teknologi Elektro, Universitas Mercu Buana*, *6*(2).

Ravinath, Y., Kumar, S., & Bhattacharya, A. (2013). Backup Virtual Private Networks in Banks, *2*(5), 4–5.

Tjahjono, D., Shaikh, R., & Ren, W. (2014). Establishing An IPsec VPN, *2*(12).