Progresif: Jurnal Ilmiah Komputer
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0877
p-ISSN: 0216-3284

Optimasi IPSec *Site to Site* VPN Mikrotik menggunakan Algoritme Enkripsi *Blowfish*

Ikhwanul Kurnia Rahman[1*], Dadang Iskandar Mulyana[2], Yuma Akbar[3]
Program Studi Teknik Informatika, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, Jakarta, Indonesia
Corresponding Author: ikhwanulkurnia@gmail.com

Abstract

Although data security is very important, the performance of a VPN (Virtual Private Network) must also be a concern. This paper presents how the use of encryption algorithms affects the performance of a site-to-site VPN. This research simulates a site-to-site IPsec VPN network using the EVE-NG simulator to run two point-to-point network security encryption algorithms, namely IPSec with the default encryption algorithm AES (Advanced Encryption Standard) and IPSec (Internet Protocol Security) with the Blowfish encryption algorithm to encrypt traffic. data sent over a public network. Test uploading a file of 900 Megabytes from computer 2 and computer 3 to the FTP (File Transfer Protocol) Server with a throughput of 3.51 MBps with the AES encryption algorithm; and 3.81 MBps throughput with the Blowfish encryption algorithm. Traffic does not experience problems on the network or Request Time Out (RTO) with an average ping latency of 8ms on the IPSec network with the AES encryption algorithm; and 7ms on an ipsec network that uses the Blowfish algorithm. The test results show that the Blowfish encryption algorithm has better performance in throughput and latency than using the AES encryption algorithm.
Keywords: *Virtual Private Network; Internet Protocol Security; Mikrotik; Blowfish Algorithm*

Abstrak

Meskipun keamanan data sangat penting, akan tetapi performa VPN (*Virtual Private Network*) juga harus menjadi perhatian. Paper ini menyajikan bagaimana penggunakan algoritme enkripsi mempengaruhi performa dari *site to site* VPN. Penelitian mensimulasikan jaringan *site to site IPsec* VPN menggunakan simulator EVE-NG untuk menjalankan dua algoritme enkripsi keamanan jaringan *point to point*, yaitu *IPSec* dengan algoritme enkripsi default AES (*Advanced Encryption Standard*) dan *IPSec* (*Internet Protocol Security*) dengan algoritme enkripsi *Blowfish* dalam mengenkripsi trafik data yang dikirim melalui jaringan publik. Uji *upload* file sebesar 900 *Megabyte* dari komputer 2 dan komputer 3 ke FTP (*File Transfer Protocol*) Server dengan *throughput* 3,51 MBps dengan algoritme enkripsi AES; dan *throughput* 3,81 MBps dengan algoritme enkripsi *Blowfish*. Trafik tidak mengalami kendala pada jaringan atau *Request Time Out* (RTO) dengan *latency* ping rata-rata 8ms pada jaringan IPSec algoritme enkripsi AES; dan 7ms pada jaringan ipsec yang menggunakan algoritme *Blowfish*. Hasil uji menunjukkan algoritme enkripsi *Blowfish* memiliki performa lebih baik dalam *troughput* dan *latency* dibandingkan menggunakan algoritme enkripsi AES.
Kata kunci: *Virtual Private Network; Internet Protocol Security; Mikrotik; Advanced Encryption Standard; Algoritme Blowfish*

1. Pendahuluan

Pada era moderen ini komunikasi menjadi hal yang umum terjadi dan bisa dilakukan dengan mudah bagi masyarakat umum dan bahkan perusahaan moderen. Dengan majunya perkembangan teknologi, komunikasi juga berkembang menjadi lebih moderen. Adanya perkembangan yang maju dan moderen ini memicu masalah yang lebih kompleks, seperti pembobolan jaringan komunikasi.

Berbagai upaya dilakukan dalam upaya meminimalkan risiko pembobolan data dalam sistem jaringan komunikasi, seperti penggunaan *password* [1, 2], pengamanan sistem jaringan [3, 4], enkripsi data [5, 6], dan berbagai cara lainnya. Di antara sistem-sistem pengamanan

tersebut, salah satu yang paling populer adalah sistem enkripsi. Meskipun sudah menerapkan algoritme enkripsi dalam mengamankan jalur data, jika performa sistem enkripsi tersebut buruk, maka *user* tetap merasa tidak nyaman, sehingga perlu dilakukan optimalisasi jaringan agar performa dan kecepatan menjadi lebih baik dan cepat.

IPSec *site to site* VPN memiliki beberapa pilihan algoritme enkripsi yang dapat digunakan untuk mengamankan data. Secara *default,* algoritme enkripsi yang digunakan oleh IPSec *site to site* VPN Mikrotik adalah algoritme AES. IPSec dapat berfungsi mengamankan jalur komunikasi data *end-to-end*, namun dapat berefek pada penurunan performa jaringan [7], sehingga perlu kajian kemungkinan penggunaan alternatif algoritme untuk optimasi kinerja.

Blowfish adalah algoritme kunci simetrik *cipher* blok yang telah mendapatkan tempat di dunia kriptografi, khususnya bagi masyarakat yang membutuhkan algoritme kriptografi yang cepat, kuat, dan tidak terhalang oleh lisensi. *Blowfish* dirancang dan diharapkan mempunyai kriteria perancangan yang diiginkan sebagai algoritme yang memiliki tingkat keamanan yang bervariasi. Algoritme *Blowfish* telah meluas digunakan dalam sistem enkripsi, seperti dalam [8 – 11]

Penelitian kami bertujuan menganalisa dan membandingkan algoritme enkripsi IPSec *Blowfish* dan AES, untuk memberikan kontribusi pada ilmu pengetahuan, yaitu memberikan informasi mengenai kinerja atau performa kedua algoritme tersebut sebagai Algoritme enkripsi IPSec *site to site* VPN.

2. Tinjauan Pustaka

Penggunaan IPSec yang berfungsi sebagai pengaman jalur komunikasi data end-to-end pada penelitian [12]berefek pada penurunan performa, sehingga perlu dilakukan analisa performa IPSec protokol dengan menggunakan IPv4 dan IPv6. Perkembangan komunikasi pertukaran data mengarah pada komunikasi terpusat. Penggunaan jaringan yang tersedia pada penelitian [13] memungkinkan adanya penyadapan. Pengujian dilakukan dengan membandingkan VPN PPTP dan VPN L2TP/IPSec. Penggunaan internet yang tinggi membutuhkan sistem keamanan yang tinggi juga, sehingga di penelitian [14] menguji kemampuan VPN Tunnel yakni GRE dan IPSec. Hasilnya IPSec lebih unggul dengan memberikan fitur enkripsi.

Pada penelitian [15] dilakukan pengujian terhadap keamanan jaringan dengan menggunakan s*trongswan dataplane* yang dapat meningkatkan performa *troughput* jaringan IPSec. Pengujian di penelitian [16] membandingkan antara jaringan VPN dengan non VPN. Hasilnya jaringan yang menggunakan VPN memiliki kualitas bagus daripada non VPN dan menunjukkan VPN dapaat mencegah serangan MITM. VPN juga dapat rentan terhadap kualitas internet yang buruk, maka di penelitian [17] dilakukan pengujian menggunakan failover dengan algoritme administrative distance routing. Pengujian ini membuktikan pada sebuah *failover* dapat dibangun sesuai dengan prioritas jalur *routing*.

Penelitian [18] bertujuan untuk membuat jaringan privat dengan mementingkan aspek *security* dan pendistribusian IP *public* dengan menggunakan algoritme *routing* dan dihasilkan EoIP *Tunnel over* IPSec dapat digunakan untuk menghubungkan antar kantor cabang. Pengujian di PT PPA dan PT Penas pada penelitian [19] bertujuan untuk menguji jaringan VPN pada lokasi tersebut. Dari penelitian ini didapatkan hasil VPN IPSec dapat menyediakan jaringan yang aman dan cepat untuk pertukaran data di jaringan publik.

Penerapan QoS pada aplikasi realtime seperti VoIP di jaringan VPN dapat mempengaruhi operasi IPSec dan kinerja aplikasi jaringan pada penelitian [20]. Pengujian QoS pada VPN juga dilakukan pada penelitian [21], penelitian ini menguji terhadap performa VPN PPTP, L2TP, SSTP, dan IPSec. Hasil pengujian membuktikan bahwa IPSec memiliki hasil yang baik di sektor *download, delay, packet loss*, dan *troughput*.

Penelitian [22] membahas DMVPN yang mewajibkan menggunakan IPPSec, untuk menganalisa performa dari DMVPN + IPSec. Hasilnya troughput berkurang.Penelitian [23] dilakukan untuk pengamanan pada koneksi Voip menggunakan IPSec. Di penelitian [24] dibutuhkan mekanisme untuk mengakses jaringan lokal dari luar kantor sehingga dilakukan pengujian VPN yang menjadi solusi untuk permasalahan tersebut. Internet memungkinkan user untuk terhubung kemanapun dan kapanpun, maka dari itu keamanan data sangat diperlukan untuk mencegah terjadinya serangan *hacking*. IPSec terbukti menjadi solusi terbaik untuk mengamankan *network layer* pada penelitian [25].

Pada penelitian [26] hampir sama seperti penelitian [12], hanya diperlukan analisa untuk IPv6, pengujian ini menerapkan IPSec sebagai salah satu faktor yang memberikan dampak penurunan *troughput*. Analisa performa pada jaringan MPLS pada penelitian [27] menerapkan IPSec pada jaringan MPLS memberikan dampak pada troughput namun masih bisa diterima. Dalam penelitian [28] dilakukan untuk mencari cara agar kinerja troughput IPSec bisa meningkat, dan ditemukan hasil dengan menggunakan *multicore* dalam memproses IPSec.

Pada penelitian [13] menggunakan komunikasi terpusat dan penelitian [29] komunikasi data berkembang mengarah ke sentralisasi komunikasi seperti intranet, untuk sekuritas komunikasi data memanfaatkan VPN IPSec. Hasilnya dikonfirmasi bahwa menggunakan VPN IPSec dapat menghubungkan kantor cabang dengan kantor pusat.

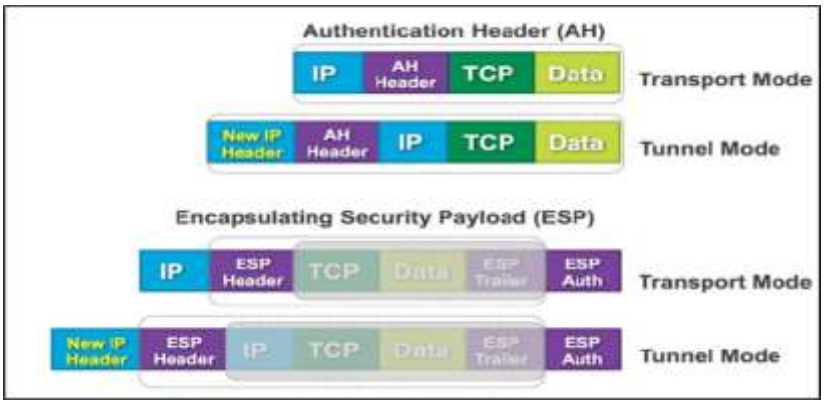
Analisis perbandingan kinerja antara SSTP dan L2TP dengan metode QoS seperti penelitian [30], VPN membuat jaringan lambat setelah analisa L2TP + IPSec lebih baik dari SSTP. Implementasi VPN di Mikrotik seperti pada penelitian [31] guna untuk mempermudah pertukaran data ternyata memberikan dampak positif sehingga penggunaan VPN bermanfaat.

Penelitian kami menganalisis kinerja algoritme enkripsi IPSec *Blowfish* sebagai alternatif untuk mengoptimalkan IPSec *Site to Site* VPN Mikrotik yang dapat menurunkan performa jaringan, walau dapat membuat koneksi jaringan yang aman.

3. Metodologi

3.1 Topologi Jaringan

IPSec menggunakan dua protokol untuk menyediakan layanan keamanan lalulintas yaitu *Authentication Header* (AH) *and Encapsulating Security Payload* (ESP). Implementasi IPSec harus mendukung ESP dan juga AH. Protokol AH menyediakan integritas hubungan, authentifikasi data asal dan layanan anti jawaban.



Gambar 1. Topologi Jaringan

Berdasarkan fungsinya di dalam IPSec terdapat 2 protokol yakni *Authentication Header* (AH) yang menyediakan layanan *authentication, integrity, replay protection* pengamanan pada *header* IP, namun tidak menyediakan layanan *confidentally*. Selanjutnya, *Encapsulating Security Payload* (ESP), menyediakan layanan *Authentication, integrity, replays protection* dan *confidentiality* terhadap data (ESP melakukan pengamanan data terhadap segala sesuatu dalam paket data setelah *header*).

3.2 Alur Implementasi

Adapun pembahasan umum dari alur implementasi topologi jaringan diatas adalah sebagai berikut:

1. Tahapan dimulai dengan perancangan prototype topologi jaringan *point to point* mulai dari kebutuhan perangkat *network*, IP *Address* dan koneksi ke internet.
2. Konfigurasi IPSec pada perangkat dan algoritme enkripsi
3. Menjalankan simulator menggunakan EVE-NG yakni aplikasi untuk menjalankan berbagai software atau *firmware* jaringan untuk perangkat jaringan salah satunya yang akan digunakan peneliti Windows dan *Router Mikrotik*.
4. Selanjutnya dilakukan uji konektivitas, yakni uji ping antar *router* dan uji koneksi internet dari *client*.

5. Setelah koneksi berhasil, maka dilakukan pengujian kualitas.
6. Setelah dilakukan pengujian, kemudian dilakukan analisa data dan penulisan laporan.

3.3 Skema Pengujian

Untuk melakukan pengujian implementasi VPN akan dilakukan dengan beberapa skema. Adapun 3 skema yang akan dilakukan adalah sebagai berikut:

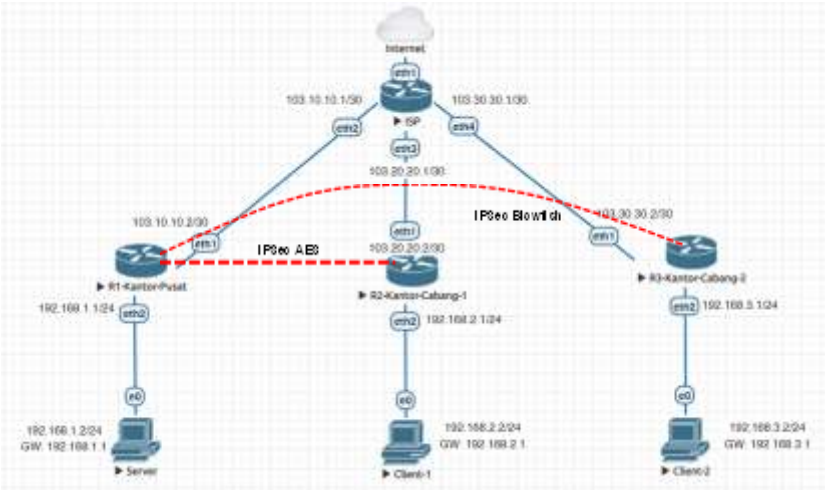
1. Skema 1, pengujian dan pengukuran parameter *packetloss* dan ketersediaan jaringan dikondisi normal.
2. Skema 2, pengujian dan pengukuran parameter *packetloss* dan ketersediaan jaringan ketika terjadi gangguan di *router* utama atau jalur utama. Ketika router/jalur utama mati, *traffic* akan ditangani oleh *router backup.*
3. Skema 3, pengujian dan pengukuran parameter packetloss dan ketersediaan jaringan ketika *router*/jalur utama kembali aktif.

Setelah melakukan pengujian di ketiga skema tersebut, selanjutnya akan dipaparkan hasil ketersediaan jaringan dengan cara membandingkan paket yang dikirim dengan banyak paket *loss* yang terjadi.

4. Hasil dan Pembahasan

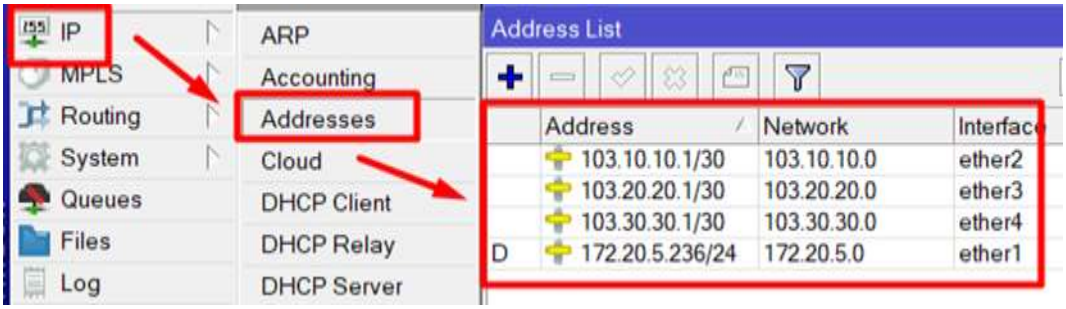
4.1 Verifikasi Konfigurasi awal

Konfigurasi *Router* ISP menggunakan aplikasi *winbox*, dimana *Router* ISP menyediakan layanan internet yang memberikan IP publik.



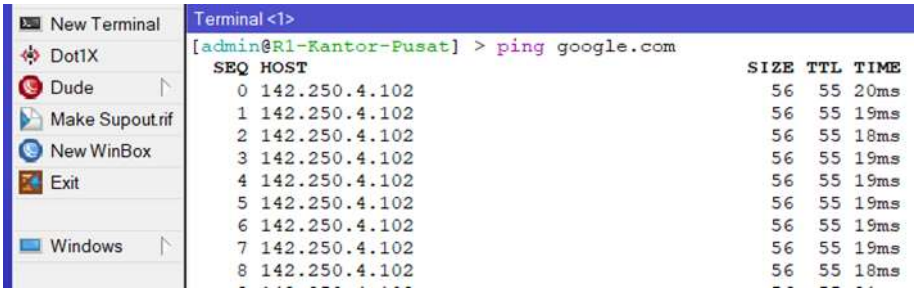
Gambar 2. Prototype Jaringan *Testing*

Kemudian IP Address dikonfigurasi pada masing-masing *interface Router* ISP, pada menu IP → *Address* menampilkan seluruh alamat IP yang ada pada *interface router*.



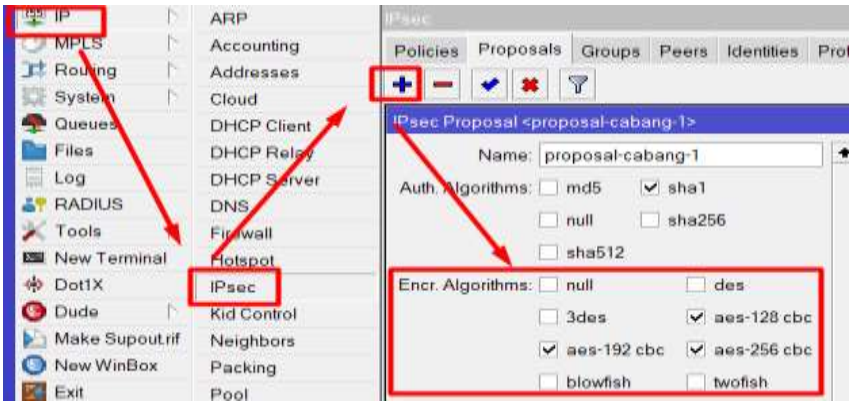
Gambar 3. IPv4 *Router* ISP

Konfigurasi router kantor pusat, dari IP Publik yang digunakan untuk terhubung dengan internet, lalu konfigurasi VPN IPSec untuk terhubung ke *router* cabang. Setelah dikonfigurasi dilakukan pengecekan koneksi internet pada R1-Kantor Pusat dengan menggunakan terminal lalu *ping test* ke google.com



Gambar 4. *Ping Test* ke Laman *Google*

Konfigurasi selanjutnya yakni algoritme enkripsi untuk peering ke *router* kantor pusat menggunakan algoritme default AES.



Gambar 5. Konfigurasi *Router* Kantor Pusat

4.2 Pengujian Skema 1

Skema pengujian 1 adalah analisa trafik menggunakan *Wireshark*, terlihat pada gambar terdeteksi trafik komunikasi yang terbentuk antara *Router* Pusat (R1-Kantor-Pusat) dengan alamat IP sumber 103.10.10.2 dengan tujuan *Router* Cabang (R1-Kantor-Cabang) dengan alamat IP Publik 103.20.20.2 dimana VPN IPSec menggunakan protokol ESP untuk mengenkripsi komunikasi.

```
[admin@R1-Kantor-Pusat] > ping 192.168.2.1 src-address=192.168.1.1 count=20
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.2.1                                56  64 2ms
    1 192.168.2.1                                56  64 2ms
    2 192.168.2.1                                56  64 2ms
    3 192.168.2.1                                56  64 1ms
    4 192.168.2.1                                56  64 2ms
    5 192.168.2.1                                56  64 2ms
    6 192.168.2.1                                56  64 2ms
    7 192.168.2.1                                56  64 2ms
    8 192.168.2.1                                56  64 2ms
    9 192.168.2.1                                56  64 2ms
   10 192.168.2.1                                56  64 2ms
   11 192.168.2.1                                56  64 2ms
   12 192.168.2.1                                56  64 2ms
   13 192.168.2.1                                56  64 2ms
   14 192.168.2.1                                56  64 2ms
   15 192.168.2.1                                56  64 2ms
   16 192.168.2.1                                56  64 1ms
   17 192.168.2.1                                56  64 2ms
   18 192.168.2.1                                56  64 1ms
   19 192.168.2.1                                56  64 2ms
    sent=20 received=20 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=2ms
```

Gambar 6 Test Ping *Router* Pusat ke *Router* Cabang

4.3 Skema Pengujian 2

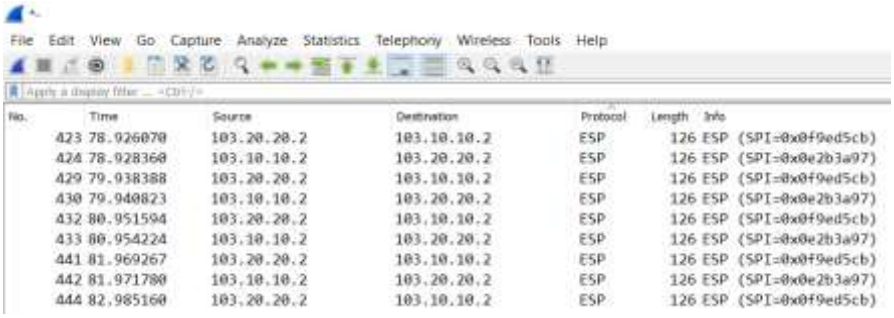
Pengujian ping dari *Router* di kantor pusat ke *Router* kantor cabang dengan alamat ip sumber 192.168.1.1 dengan ip tujuan 192.168.2.1 menggunakan pengulangan sebanyak 20 ping, hasil sukses 100 persen tanpa ada time *out* dengan nilai delay minimal 1 ms, rata-rata 1 ms dan maksimal 2 ms.

```
[admin@R2-Kantor-Cabang] > ping 192.168.1.1 src-address=192.168.2.1 count=20
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.1.1                                56  64 1ms
    1 192.168.1.1                                56  64 1ms
    2 192.168.1.1                                56  64 2ms
    3 192.168.1.1                                56  64 2ms
    4 192.168.1.1                                56  64 2ms
    5 192.168.1.1                                56  64 2ms
    6 192.168.1.1                                56  64 2ms
    7 192.168.1.1                                56  64 2ms
    8 192.168.1.1                                56  64 2ms
    9 192.168.1.1                                56  64 2ms
   10 192.168.1.1                                56  64 2ms
   11 192.168.1.1                                56  64 2ms
   12 192.168.1.1                                56  64 2ms
   13 192.168.1.1                                56  64 2ms
   14 192.168.1.1                                56  64 2ms
   15 192.168.1.1                                56  64 1ms
   16 192.168.1.1                                56  64 2ms
   17 192.168.1.1                                56  64 2ms
   18 192.168.1.1                                56  64 2ms
   19 192.168.1.1                                56  64 2ms
    sent=20 received=20 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=2ms
```

Gambar 7 Test Ping *Router* Cabang ke *Router* Pusat

4.4 Hasil Akhir Pengujian

Hasil dari uji coba penelitian dilakukan untuk mengetahui proses terbentuknya sinkronisasi antar router pusat dengan router cabang menggunakan IPSec, selanjutnya akan dilakukan *trace, ping,* unduh dan unggah data melalui FTP dari PC 2 ke PC 1 (FTP Server) lainnya. Secara topologi dari *router* pusat ke router cabang melewati *Router* ISP dan memiliki 2 hop untuk mencapai PC 1 (FTP – *Server*), karena penelitian ini mengimplementasikan VPN IPSec dan GRE maka antar router pusat dan *router* cabang terhubung dengan hanya 1 hop melewati *tunnel.* Gambar berikut dibawah ini proses enkripsi dari masing-masing aturan IPSec.



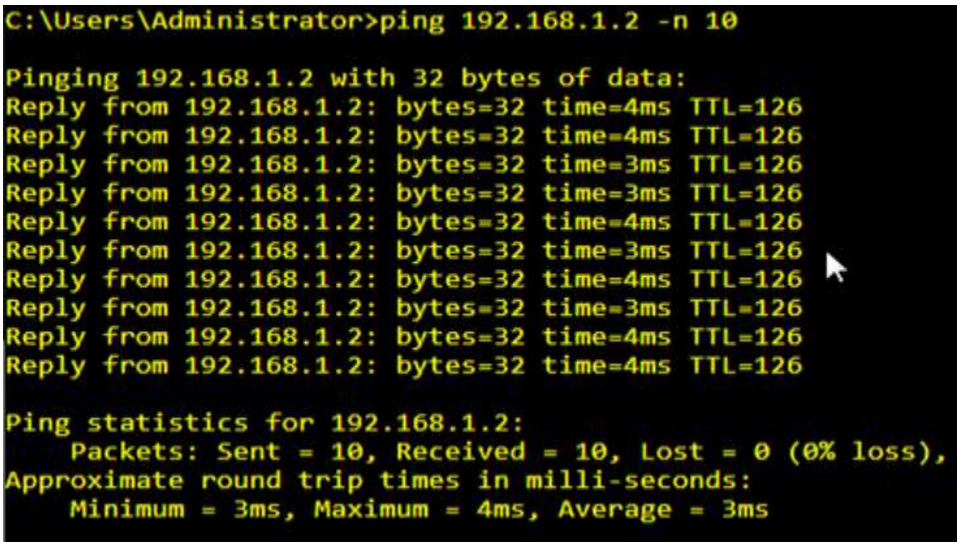
Gambar 8 IPSec *Tunnel Encryptions*

Pengujian ping dari *Router* (Gambar 9) di kantor cabang ke *Router* kantor pusat dengan alamat IP sumber 192.168.2.1 dengan IP tujuan 192.168.1.1 menggunakan pengulangan sebanyak 20 ping, Hasil sukses 100 persen tanpa ada *time out* dengan nilai delay minimal 1 ms, rata-rata 1 ms dan maksimal 2 ms.

```
C:\Users\Administrator>tracert -d 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops

  1     1 ms    <1 ms    <1 ms  192.168.2.1
  2     *        *        *     Request timed out.
  3     5 ms     3 ms     4 ms  192.168.1.2

Trace complete.
```

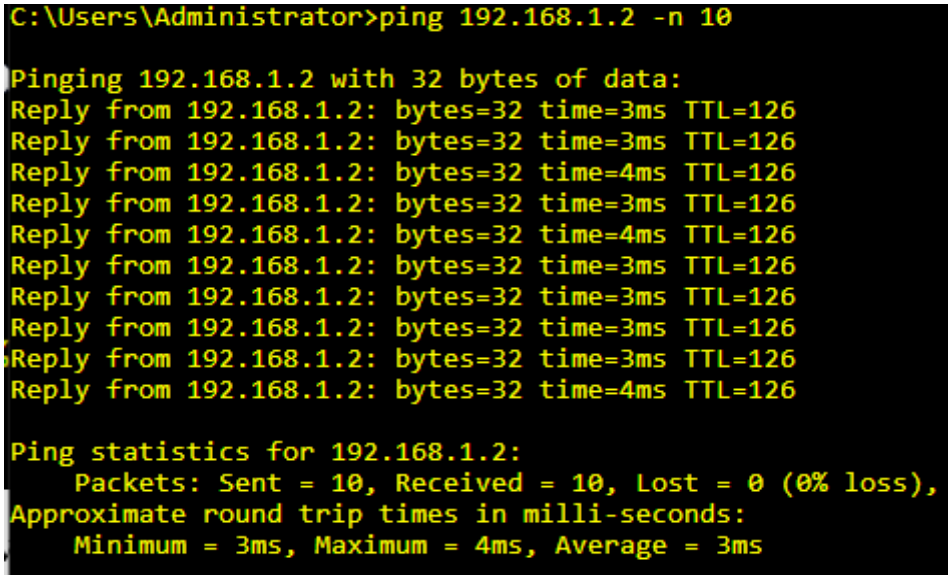
Gambar 9. Hasil *Tracert* Komputer Cabang

Dapat terlihat dari hasil *trace* dari komputer cabang ke server FTP di kantor pusat (Gambar 10) dengan alamat ip 192.168.1.2, pada hop pertama adalah IP *gateway* yang ada di *router* milik komputer cabang dan hop kedua adalah *router* pusat tapi disni tidak terlihat alamat IP berapa yang digunakan karena secara default IPSec tidak mengirimkan balik pesan *trace* yang dikirim oleh komputer 2 dan pada hop ke 3 adalah ip tujuan server FTP. Jadi dapat disimpulkan dari komputer 2 seperti tidak melewati *router* ISP itu dikarenakan tunnel yang terbentuk antar router pusat dengan *router* cabang.



Gambar 10. Hasil Ping Komputer Kantor Cabang Ke Komputer Server FTP (Pusat)

Dari hasil ping tanpa beban dari komputer di kantor cabang 1 ke server FTP yang ada di kantor pusat (Gambar 11), dapat terlihat berjalan normal dengan rata-rata 3 ms tanpa ada *request time out* (RTO).



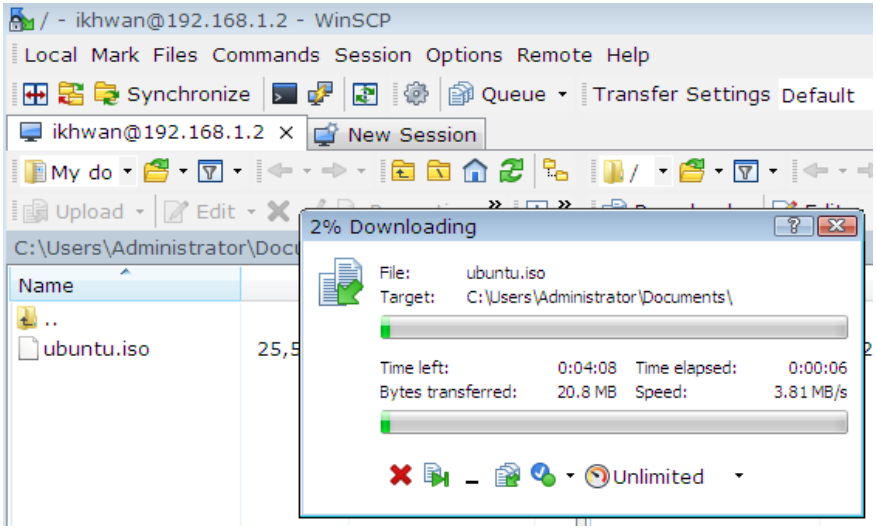
Gambar 111. Hasil Ping Komputer Kantor Cabang 1 Ke Server FTP

Dari hasil ping tanpa beban dari komputer di kantor cabang 2 ke server FTP yang ada di kantor pusat (Gambar 12), dapat terlihat berjalan normal dengan rata-rata 3 ms tanpa ada *Request Time Out* (RTO). Pengujian ping tanpa beban paket default (32byte) tidak terlihat adanya perbedaan antara menggunakan Algoritme enkripsi AES dan *Blowfish*.

```
C:\Users\Administrator>ping 192.168.1.2 -l 10000 -n 10

Pinging 192.168.1.2 with 10000 bytes of data:
Reply from 192.168.1.2: bytes=10000 time=8ms TTL=126
Reply from 192.168.1.2: bytes=10000 time=9ms TTL=126
Reply from 192.168.1.2: bytes=10000 time=8ms TTL=126
Reply from 192.168.1.2: bytes=10000 time=8ms TTL=126
Reply from 192.168.1.2: bytes=10000 time=9ms TTL=126
Reply from 192.168.1.2: bytes=10000 time=8ms TTL=126
Reply from 192.168.1.2: bytes=10000 time=7ms TTL=126
Reply from 192.168.1.2: bytes=10000 time=8ms TTL=126
Reply from 192.168.1.2: bytes=10000 time=7ms TTL=126
Reply from 192.168.1.2: bytes=10000 time=9ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 9ms, Average = 8ms
```

Gambar 122. Hasil Ping Komputer Kantor Cabang 2 Ke Server FTP

Gambar 13. FTP *Upload* File Komputer 2



Gambar 13. FTP Upload file *K*omputer 3

Pada pengujian *download* file sebesar 900 *Megabyte* terlihat pada gambar dari komputer 2 dan komputer 3 dari FTP *Server* dengan *througphut* 3,51 MBps pada komputer 2 dan 3,81 Mbps trafik masih normal dengan ping menggunakan beban 10000byte atau 10KB rata-rata 8ms untuk komputer 2 dan 7ms untuk komputer 3 selama proses *upload* file tidak mengalami kendala pada jaringan atau *request time out* (RTO).

Berdasarkan hasil pengujian kinerja kedua algoritme (AES dan Blowfish) bahwa optimasi jaringan *point to point* VPN IPSec menggunakan Algoritme enkripsi AES dan *Blowfish* ini pada prinsipnya dapat dibangun dengan baik dan komunikasi pertukaran data antar pusat dan cabang berjalan dengan lancar melalui dua metode yang berbeda. Namun demikian, hasil uji juga menunjukkan Algoritme enkripsi *Blowfish* memiliki performa lebih baik dalam hal *troughput* dan *latency.* Temuan hasil pengujian ini menguatkan penelitian [32] bahwa Algoritme *Blowfish* memiliki performa yang baik dalam sistem kriptografi.

5. Simpulan

Optimasi jaringan point to point VPN IPSec menggunakan Algoritme enkripsi AES dan *Blowfish* ini dapat dibangun dengan baik dan komunikasi pertukaran data antar pusat dan cabang berjalan dengan lancar melalui dua metode yang berbeda. Algoritme enkripsi *Blowfish* memiliki performa lebih baik dalam hal *troughput* dan *latency* dibandingkan menggunakan algoritme enkripsi AES. Meskipun lebih baik, penelitian selanjutnya dapat menguji penggunaan algoritme enkripsi lainnya seperti *Twofish*, *Camelia*, *Des*, dan *3des*.

Daftar Referensi

[1] M. Syarif, & W. Wijanarto, "Deteksi Kedipan Mata Dengan Haar Cascade Classifier Dan Contour Untuk Password Login Sistem". *Techno. com*, vol. 14, no. 4, pp. 242-249, 2015.

[2] A. Prayogo, & M.A. Rony, "Implementasi One Time Password pada Sistem Login dengan Algoritme SHA-256 dan DES pada Aplikasi EO Blucampus Berbasis Client Server". *SKANIKA*, vol. 1, no. 2, pp. 448-454, 2018.

[3] P. Riska, P. Sugiartawan, & I. Wiratama, "Sistem keamanan jaringan komputer dan data dengan menggunakan metode port knocking". *Jurnal Sistem Informasi dan Komputer Terapan Indonesia (JSIKTI)*, vol. 1, no. 2, pp. *1*53-64, 2018.

[4] H.F. Putra, W. Wirawan, & O. Penangsang, "Penerapan blockchain dan kriptografi untuk keamanan data pada jaringan smart grid. *Jurnal Teknik ITS*, vol. 8, no. 1, pp. A11-A16, 2019.

[5] M. Fadlan, "Pengamanan Data melalui Model Super Enkripsi Autokey Cipher dan Transposisi Kolom". *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 5, no. 6, pp. 1113-1119, 2021.

[6] Y.P. Putra, T. Mufizar, & E. Alfiyani, "Implementasi Super Enkripsi Aes Dan Rsa Pada Pengamanan Data Rekam Medis Pasien". *Jurnal VOI (Voice of Informatics)*, vol. 11, no. 2, pp. 37-46, 2022.

[7] P. Thiruvasagam, & K.J. George, "IPSec: Performance Analysis in IPv4 and IPv6". *Journal of ICT Standardization*, vol. 7, no. 1, pp. 59-76, 2019.

[8] Y.P. Astuti, E.H. Rachmawanto, & C.A. Sari, "Optimasi Enkripsi Password Menggunakan Algoritme Blowfish. *Techno. Com*, vol. 15, no. 1, pp. 15-21, 2016.

[9] S. Wardoyo, Z. Imanullah, & R. Fahrizal, "Enkripsi dan Dekripsi File dengan Algoritme Blowfish pada Perangkat Mobile Berbasis Android". *Jurnal Nasional Teknik Elektro*, vol. 5, no. 1, pp. 36-44, 2016.

[10] H.G. Simanullang, & A.P. Silalahi, "Algoritme blowfish untuk meningkatkan keamanan database MySQL". *METHODIKA: Jurnal Teknik Informatika dan Sistem Informasi*, vol. 4, no. 1, pp. 10-14, 2018.

[11] F. Riza, N. Sridewi, A.M. Husein, & M.K. Harahap, "Analisa Frekuensi Hasil Enkripsi Pada Algoritme Kriptografi Blowfish Terhadap Keamanan Informasi". *JURNAL TEKNOLOGI DAN ILMU KOMPUTER PRIMA (JUTIKOMP)*, vol. 1, no. 1, pp. 11-15, 20218.

[12] G. Wang, Y. Sun, Q. He, G. Xin, and B. Wang, "A content auditing method of IPsec VPN," Proc. - 2018 IEEE 3rd Int. Conf. Data Sci. Cyberspace, DSC 2018, pp. 634–639, 2018, doi: 10.1109/DSC.2018.00101.

[13] Y. Shen, Q. F. Zhang, L. Di Ping, Y. F. Wang, and W. J. Li, "A multi-tunnel VPN concurrent system for new generation network based on user space," Proc. 11th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. - 11th IEEE Int. Conf. Ubiquitous Comput. Commun. IUCC-2012, pp. 1334–1341, 2012, doi: 10.1109/TrustCom.2012.41.

[14] 一种 vpn 网关支持数万连接，还有软硬件 vpn 网关实例, "Public Review for A Scalable VPN Gateway for Multi-Tenant Cloud Services Public review written by A Scalable VPN Gateway for Multi-Tenant Cloud Services," vol. 48, no. 1, pp. 49–55.

[15] I. Aouini, L. Ben Azzouz, and L. A. Saidane, “A secure neighborhood area network using IPsec,” 2016 Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2016, pp. 102–107, 2016, doi: 10.1109/IWCMC.2016.7577041.
[16] M. Salhi, M. Sliti, and N. Boudriga, “All-optical VPN platform and authentication for VLC-based networks,” 13th HONET-ICT Int. Symp. Smart MicroGrids Sustain. Energy Sources Enabled by Photonics IoT Sensors, HONET-ICT 2016, pp. 29–34, 2016, doi: 10.1109/HONET.2016.7753445.
[17] M. Rao, J. Coleman, and T. Newe, “An FPGA based reconfigurable IPSec ESP core suitable for IoT applications,” Proc. Int. Conf. Sens. Technol. ICST, pp. 1–5, 2016, doi: 10.1109/ICSensT.2016.7796269.
[18] M. Rao, J. Coleman, and T. Newe, “An FPGA based reconfigurable IPSec ESP core suitable for IoT applications,” Proc. Int. Conf. Sens. Technol. ICST, pp. 1–5, 2016, doi: 10.1109/ICSensT.2016.7796269.
[19] S. Ikhwan and A. Amalina, “Analisis Jaringan VPN Menggunakan PPTP dan L2TP (Studi Kasus: Dinhubkominfo Kabupaten Banyumas),” J. Infotel, vol. 9, no. 3, pp. 265–270, 2017.
[20] M. Iqbal and G. Y. Noviantoro, “ANALISIS PERBANDINGAN PERFORMA VPN IPSEC DAN ZRTP PADA VoIP,” Snrik 2016, vol. 1, no. Snrik, pp. 166–171, 2016.
[21] A. Darojat and I. Nurhaida, “Analisa Qos Administrative Distance Static Route Pada Failover Vpn Ipsec,” J. Ilmu Tek. dan Komput., vol. 3, no. 1, p. 11, 2019, doi: 10.22441/jitkom.2020.v3.i1.002
[22] D. F. Jaya Patih, “Analisa Perancangan Server Voip (Voice Internet Protocol) Dengan Opensource Asterisk Dan Vpn (Virtual Private Network) Sebagai Pengaman Jaringan Antar Client,” J. Inform. dan Tek. Elektro Terap., vol. 1, no. 1, pp. 42–48, 2012, doi: 10.23960/jitet.v1i1.23.
[23] A. Amarudin and S. D. Riskiono, “Analisis Dan Desain Jalur Transmisi Jaringan Alternatif Menggunakan Virtual Private Network (Vpn),” J. Teknoinfo, vol. 13, no. 2, p. 100, 2019, doi: 10.33365/jti.v13i2.309..
[24] A. Alsa’deh, C. Meinel, F. Westphal, M. Gawron, and B. Groneberg, “CGA integration into IPsec/IKEv2 authentication,” SIN 2013 - Proc. 6th Int. Conf. Secur. Inf. Networks, pp. 326–330, 2013, doi: 10.1145/2523514.2527097.
[25] J. Hua, F. Jinpo, Z. Gang, and H. Ronglei, “Design and implementation of integrated access VPN gateway,” ACM Int. Conf. Proceeding Ser., no. 7, pp. 128–132, 2019, doi: 10.1145/3371676.3371681.
[26] I. Coonjah, P. C. Catherine, and K. M. S. Soyjaudah, “Design and Implementation of UDP Tunneling-based on OpenSSH VPN,” *Proc. - IEEE 2018 Int. Conf. Adv. Comput. Commun. Control Networking, ICACCCN 2018*, no. 1, pp. 640–645, 2018, doi: 10.1109/ICACCCN.2018.8748849.
[27] H. Gunleifsen, T. Kemmerich, and V. Gkioulos, “Dynamic setup of IPsec VPNs in service function chaining,” Comput. Networks, vol. 160, pp. 77–91, 2019, doi: 10.1016/j.comnet.2019.05.015.
[28] A. Sushma and T. Sanguankotchakorn, “Implementation of IPsec VPN with SIP Softphones using GNS3,” *ACM Int. Conf. Proceeding Ser.*, pp. 152–156, 2018, doi: 10.1145/3301326.3301333.
[29] K. Rantos, A. Papanikolaou, and C. Manifavas, “IPsec over IEEE 802.15.4 for low power and lossy networks,” MobiWac 2013 - Proc. 11th ACM Int. Symp. Mobil. Manag. Wirel. Access, Co-located with ACM MSWiM 2013, pp. 59–63, 2013, doi: 10.1145/2508222.2508240.
[30] D. Migault, D. Palomares, T. Guggemos, A. Wailly, M. Laurent, and J. P. Wary, “Recommendations for IPsec configuration on homenet and M2M devices,” Q2SWinet 2015 - Proc. 11th ACM Symp. QoS Secur. Wirel. Mob. Networks, pp. 9–17, 2015, doi: 10.1145/2815317.2815323.
[31] Z. Luo, G. Yu, H. Qi, and Y. Liu, “Research of A VPN secure networking model,” Proc. 2013 2nd Int. Conf. Meas. Inf. Control. ICMIC 2013, vol. 1, pp. 567–569, 2013, doi: 10.1109/MIC.2013.6758028.
[32] M. Muhathir, “Perbandingan Algoritme Blowfish Dan Twofish Untuk Kriptografi File Gambar”. *Journal of Informatics and Telecommunication Engineering*, vol. 2, no. 1, pp. 23-30, 20218.