ANALISIS PERFORMANSI JARINGAN IP DENGAN IPSEC VPN TUNNEL TERHADAP SERANGAN

ANALYSIS OF IP NETWORK PERFORMANCE WITH IPSEC VPN TUNNEL AGAINST ATTACK

Bimo Hadiprasetyo[1], Dr. Ir. Basuki Rahmat, M.T.[2], Dr. Doan Perdana, S.T., M.T.[3]
[1,2,3] Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
[1]**bimohdp@telkomuniversity.ac.id**, [2]**basukir@telkomuniversity.ac.id**,
[3]**doanperdana@telkomuniversity.ac.id**

Abstrak

Network security adalah suatu metodologi yang bisa digunakan untuk memberikan keamanan tambahan pada sebuah jaringan data dimana salah satu metode yang sering diimplementasikan adalah IPSec VPN Tunnel. Dalam penelitian dan penulisan skripsi ini, dibahas dan disimulasikan bagaimana pengaruh implementasi IPSec VPN Tunnel pada performansi suatu jaringan.

Hasil penelitian pada simulasi jaringan yang dipergunakan menunjukan bahwa jaringan yang mengimplementasikan IPSec VPN Tunnel memiliki nilai performansi jaringan ; throughput 3.050,441 bit/s, packet loss 0%, average one way delay 0,452 ms, dan average jitter 0,236 ms sedangkan jaringan tanpa IPSec VPN Tunnel memiliki nilai performansi jaringan ; throughput 3057,234 bit/s, packet loss 0%, average one way delay 0,448 ms, dan average jitter 0,240 ms.

Dengan demikian, didapatkan hasil bahwa implementasi IPSec VPN Tunnel mempengaruhi performansi suatu jaringan data dengan besar perubahan performansi throughput 0.22%, average one way delay 0,89%, jitter 1,67%, sedangkan nilai dari packet loss tidak mengalami perubahan.

Kata kunci: Keamanan Jaringan, VPN, QoS

Abstract

Network security is a means of giving an extra security into a network where one of the common way of doing that is by adding an IPSec VPN Tunnel into the network. This research explain and simulate the effect of using IPSec VPN Tunnel in different condition.

The result of this research shows that a network with IPSec VPN Tunnel has a throughput of 3050,441 bit/s, packet loss at 0%, average one way delay 0,452 ms, and average jitter at 0,236 ms. And for the network without IPSec VPN Tunnel has a throughput value of 3057,234 bit/s, packet loss at 0%, average one way delay at 0,448 ms, and average jitter 0,24 ms.

The result of this research shows that the implementation of IPSec VPN Tunnel does affect the performance of throughput for 0,22%, average one way delay 0,89% and jitter 1,67%, while packet loss does not show any changes in performance.Keywords: Network Security, VPN, QoS

1. Pendahuluan

Seiring dengan berkembangnya teknologi digital yang dapat digunakan secara luas oleh masyarakat sekarang ini, banyak perubahan yang terjadi pada kehidupan sehari – hari. Perubahan itu diantaranya terjadi di bidang transaksi data yang dilakukan oleh banyak pihak melalui jaringan internet. Transaksi data yang terjadi pada masa ini meliputi banyak data sensitif yang dikirimkan melalui internet. Hal ini memungkinkan terjadinya kejahatan baru, yaitu pencurian data yang dikirimkan melalui internet. Hal ini dapat terjadi pada siapapun, baik terhadap pihak individu, kelompok, maupun kepada pihak perusahaan berskala global, seperti yang baru – baru ini terjadi terhadap Facebook. Pada kejadian tersebut, ratusan ribu data akun pengguna Facebook diretas. Akibatnya, data pribadi dari akun pengguna Facebook diambil tanpa izin oleh pihak Cambridge Analytica. Data – data yang dicuri dari Facebook tersebut meliputi beberapa hal termasuk ke dalam privasi, seperti nama, jenis kelamin, asal, nomor telpon, dan alamat tempat tinggal [1].

Pencurian data yang terjadi pada Facebook membuktikan bahwa pencurian data tidak memandang siapa pun dalam kejahatan tersebut. Pencurian data dapat terjadi pada siapa pun, baik pihak yang diserang menyadarinya atau tidak. Jika disadari, pihak yang diserang akan dapat melakukan pencegahan saat data tersebut sedang diambil atau diunduh oleh pihak penyerang. Tetapi pada sebagian besar kasus, pihak yang diserang tidak pernah menyadari bahwa dirinya sedang menjadi target dari pencurian data. Kasus tersebut juga menunjukan, bahwa pencurian data dapat terjadi kapanpun. Untuk itu, diperlukan sebuah sistem keamanan yang dapat melindungi data yang sedang dikirimkan, untuk memperlambat terjadinya pencurian data. Sistem keamanan ideal tersebut berupa sistem keamanan yang dapat mengenkripsi atau mengautentikasi data yang dikirimkan, sehingga pihak yang tidak ditujukan untuk dikirim data tersebut tidak dapat mengaksesnya, karena tidak memiliki kunci untuk dekripsi atau autentikasinya.

Berdasarkan hasil penelitian yang pernah dilakukan[2] tentang efek penggunaan Virtual Private Network (VPN) pada sebuah jaringan, paket data yang dikirimkan melalui jaringan tersebut tidak terlalu banyak terpengaruh

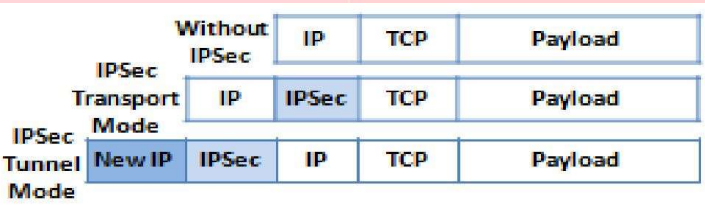
oleh serangan *blackhole* dan *rushing*. Hasil dari penelitian tersebut menunjukan nilai Quality of Service (QoS) dari jaringan tersebut. Didapat nilai *throughput* 1253.16 Kbps, *delay* 394.17 ms, dan *packet loss* 9.22% dari jaringan yang diberi tambahan keamanan dan diuji dengan serangan *blackhole*. Hasil tersebut lebih baik dibandingkan dengan jaringan yang tidak diberi keamanan tambahan. Sedangkan untuk serangan *rushing* terhadap jaringan tanpa keamanan tambahan didapat hasil QoS *throughput* 740.76 Kbps, *delay* 233.53 ms, dan *packet loss* 2.2%. Hasil ini lebih buruk dibandingkan dengan jaringan yang diberi keamanan tambahan.

Untuk itu, pada penelitian ini penulis mensimulasikan sistem keamanan tersebut terhadap serangan Denial of Service (DOS) dan *Packet Sniffing* dan kemudian mengukur performansi dari jaringan tersebut. Performansi jaringan yang akan diukur adalah *throughput*, *delay*, dan *packet loss* dari sistem yang dilengkapi dengan sistem keamanan tambahan dan tidak.

2. Konsep Dasar / Material dan Metodologi / Perancangan

2.1 *Internet Protocol Sercurity (*IPSec*)*

Internet Protocol Security adalah protokol enkripsi yang digunakan untuk menambahkan kemanan kepada jaringan yang tidak memiliki keamanan nya sendiri. Perlindungan ini diwujudkan dengan adanya *Encapsulating Security Payload* (ESP) dan *Authentication Header* (AH) [3].



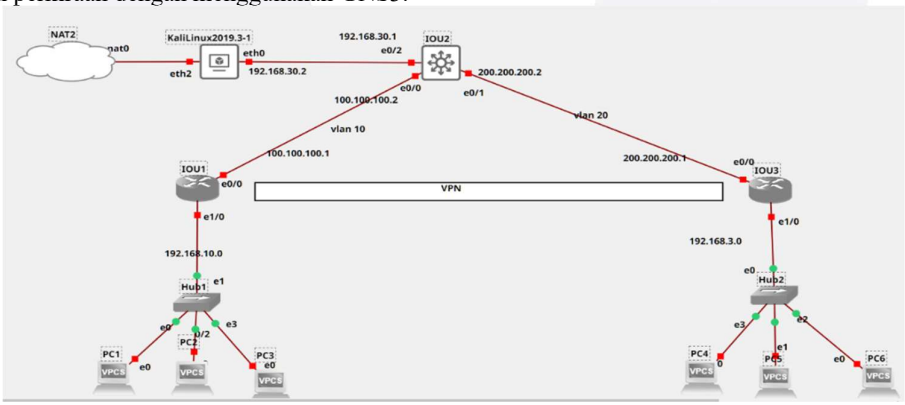
Gambar 1 Arsitektur data dengan VPN[4].

IPSec memiliki dua tipe, *Transport Mode* dan *Tunnel Mode*.

1. *Transport Mode*
   Dalam *transport mode*, paket yang dikirimkan masih menggunakan IP asli hanya saja diberikan tambahan IPSec di dalamnya.
2. *Tunnel Mode*
   Dalam *tunneling mode*, IP asli akan diberikan IP baru yang memiliki AH nya sendiri. Sehingga seluruh paket data akan dienkripsi

2.2 Desain Model Simulasi Jaringan

Model simulasi jaringan ini dirancang untuk meniru jaringan internet kampus Telkom University berdasarkan perkiraan dengan menggunakan GNS3.



Gambar 2 Model Simulasi Jaringan.

Pada model simulasi jaringan ini, IOU2 berperan sebagai ISP atau router utama dari Telkom University yang menghubungkan client ke internet. IOU1 dan IOU3 berperan sebagai router yang digunakan sebagai access point dari client yang ingin menggunakan internet melalui jaringan internet Telkom University.

2.3 Parameter Kinerja Sistem

Untuk mengetahui apakah performa sistem dapat diterima atau tidak, maka diperlukan standar pengukuran yang dapat dibandingkan dengan hasil simulasi yang didapat. Standar ini diambil dari beberapa poin *Quality of Service* (QoS), parameter tersebut adalah *throughput*, *packet* loss, *delay* dan *jitter*. Untuk penerapan standar yang digunakan adalah mengikuti standar dari ETSI-TIPHON[23]. Untuk standar yang digunakan dapat

dilihat pada tabel 1. Sedangkan untuk indeks jaringan dapat dilihat pada tabel 2.

Tabel 1 Standar QoS Jaringan.

Kategori QoS	Throughput (bit/s)	Packet Loss (%)	Delay (ms)	Jitter (ms)	Nilai Indeks
Sangat Bagus	100	0	<150	<150	4
Bagus	75	3	150 s/d 300	150 s/d 300	3
Sedang	50	15	300 s/d 450	300 s/d 450	2
Buruk	<25	>25	>450	>450	1

Tabel 2 Indeks QoS Jaringan

Nilai	Indeks
3,8 – 4	Sangat Memuaskan
3 – 3,79	Memuaskan
2 – 2,99	Kurang Memuaskan
1 – 1,99	Buruk

A. Throughput

Throughput adalah pengukuran kecepatan transfer data dalam ukuran *bit/s*, nilai ini dapat dihitung dengan menggunakan rumus (1)[8].

$$Throughput = \frac{Paket\ data\ diterima}{Lama\ pengamatan} \qquad (1)$$

B. Packet Loss

Packet loss terjadi ketika paket data yang dikirim gagal diterima atau terkirim ke penerima. Nilai packet loss adalah perbandingan antara data yang diterima dan jumlah data yang dikirimkan dalam persen, dan rumus nya dapat dilihat pada rumus (2)[9][10][11].

$$\text{Packet Loss} = \frac{packet\ drop}{packet\ sent} \text{ x } 100\% \qquad (2)$$

C. Delay

Delay adalah pengukuran waktu yang diperlukan oleh paket data untuk mencapai tujuan atau kembali ke pengirim. Jika waktu yang diukur adalah waktu kembali ke pengirim maka disebut *Round Trip Time* (RTT), jika waktu yang diukur adalah waktu sampai ke tujuan maka disebut *One Way Delay* (OWD). Nilai dari OWD dapat diukur dengan rumus (3), sedangkan waktu RTT adalah dua kali dari OWD[16].

$$\text{OWD} = \frac{Packet\ Length}{Link\ Bandwidth} \qquad (3)$$

D. Jitter

Jitter adalah pengukuran perubahan nilai *delay* dari paket data yang diterima. Jika dalam kondisi ideal, paket data yang dikirimkan akan tiba dengan jarak waktu yang sama. Nilai jitter dapat berubah karena adanya *congestion* di dalam jaringan. Nilai jitter dapat dihitung dengan rumus (4)[20].

$$\text{Jitter} = \frac{Total\ variasi\ delay}{Total\ paket\ yang\ diterima} \text{ x } 100\% \qquad (4)$$

3. Pengujian dan Analisis

3.1 Pengujian Performansi

Pada pengujian ini dilakukan untuk menguji performansi sistem dapat berkerja dengan baik dalam kondisi yang sudah ditetapkan.

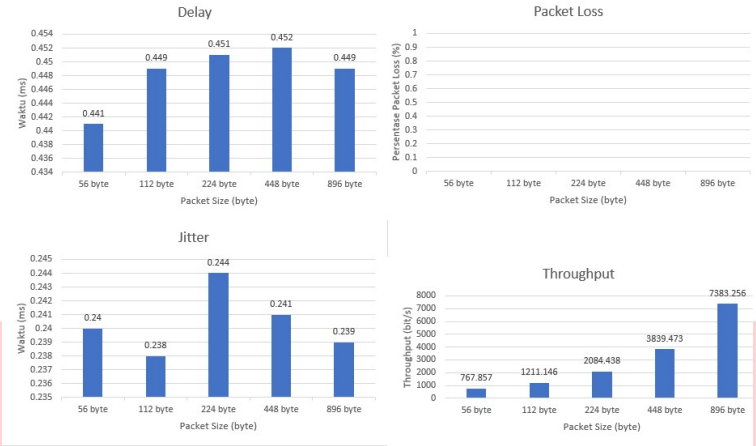
3.1.1 Pengujian Performansi Jaringan tanpa VPN

Pengujian ini akan mengukur performansi jaringan dengan kondisi berikut:

1. Simulasi jaringan yang dibuat tanpa menggunakan VPN.
2. Tipe serangan yang digunakan adalah DoS dan MAC Overflow.

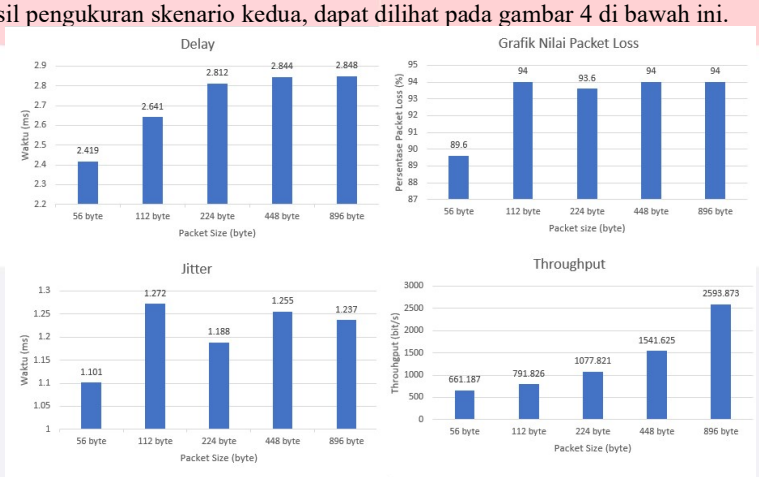
Dengan kondisi di atas, maka penulis dapat melakukan pengujian untuk mendapatkan tiga hasil dari tiga skenario. Skenario pertama adalah untuk mengukur performansi jaringan dalam kondisi normal tanpa ada gangguan dari manapun. Skenario kedua adalah untuk mengukur performansi jaringan dalam kondisi diserang oleh MAC Overflow. Skenario ketiga adalah untuk mengukur performansi jaringan dalam kondisi diserang oleh DoS.

Untuk hasil pengukuran dari skenario pertama dapat dilihat pada gambar 3 di bawah ini.



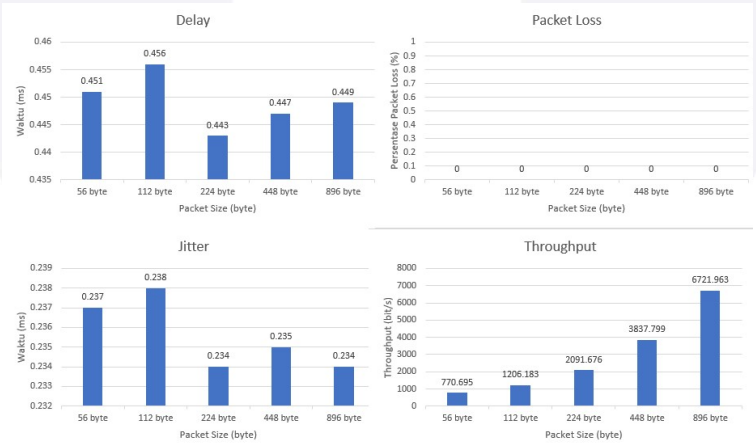
Gambar 3 Hasil pengukuran performansi jaringan normal.

Untuk hasil pengukuran skenario kedua, dapat dilihat pada gambar 4 di bawah ini.



Gambar 4 Hasil pengukuran performansi jaringan normal setelah MAC Overflow.

Untuk hasil pengukuran skenario ketiga, dapat dilihat pada gambar 5 di bawah ini.



Gambar 5 Hasil pengukuran performansi jaringan normal setelah DoS.

Pada gambar 3, performansi dari jaringan normal semua nilai QoS nya dapat dikategorika ke sangat bagus. Performansi dari jaringan tersebut dapat digunakan sebagai data kontrol untuk dibandingkan dengan semua hasil berikutnya. Gambar 4 menunjukan performansi dari jaringan normal setelah diserang dengan MAC Overflow. Berdasarkan data yang didapat dapat dilihat bahwa terjadi penurunan nilai QoS dengan penurunan nilai *packet loss* yang sangat besar, sedangkan untuk nilai *delay* dan *jitter* hanya mengalami sedikit penurunan. Gambar 5 menunjukan nilai performansi jaringan normal setelah diserang dengan DoS. Berdasarkan data tersebut dapat dilihat bahwa nilai QoS dari skenario ketiga tidak banyak berubah dibandingkan dengan data kontrol.

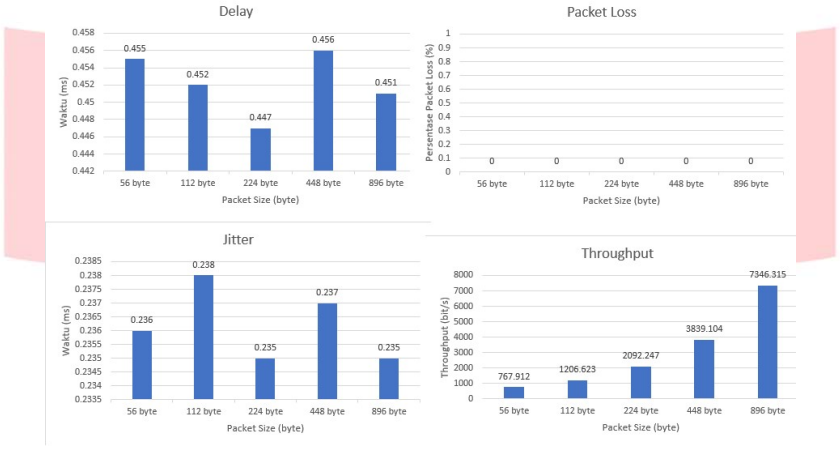
3.1.2 Pengujian Performansi Jaringan dengan VPN

Pengujian ini akan mengukur performansi jaringan dengan kondisi berikut:

1. Simulasi jaringan yang dibuat dengan menggunakan VPN *tunnel mode*.
2. Tipe serangan yang digunakan adalah DoS dan MAC Overflow.

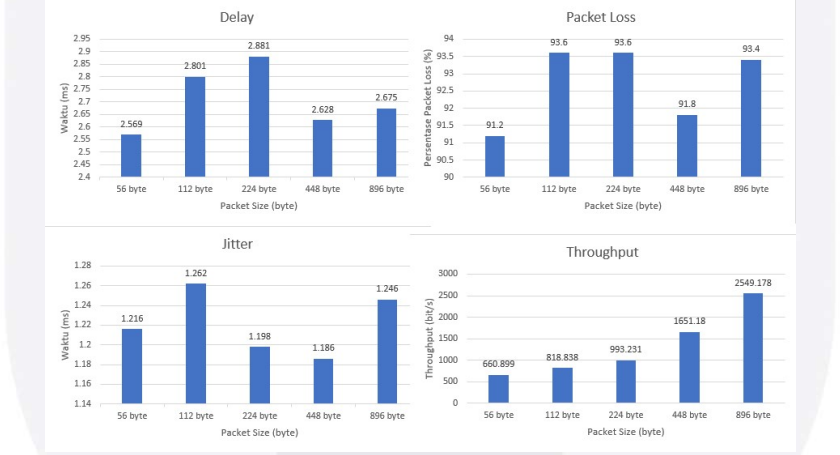
Dengan kondisi di atas, maka penulis dapat melakukan pengujian untuk mendapatkan tiga hasil dari tiga skenario. Skenario pertama adalah untuk mengukur performansi jaringan dalam kondisi normal tanpa ada gangguan dari manapun. Skenario kedua adalah untuk mengukur performansi jaringan dalam kondisi diserang oleh MAC Overflow. Skenario ketiga adalah untuk mengukur performansi jaringan dalam kondisi diserang oleh DoS.

Untuk hasil pengukuran dari skenario pertama dapat dilihat pada gambar 6 di bawah ini.



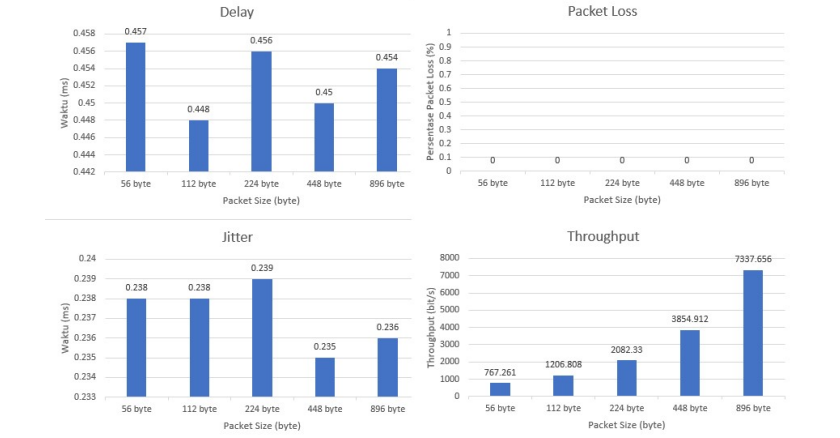
Gambar 6 Hasil pengukuran performansi jaringan dengan VPN.

Untuk hasil pengukuran dari skenario kedua dapat dilihat pada gambar 7 di bawah ini.



Gambar 7 Hasil pengukuran performansi jaringan dengan VPN setelah MAC Overflow.

Untuk hasil pengukuran dari skenario ketiga dapat dilihat pada gambar 8 di bawah ini.



Gambar 8 Hasil pengukuran performansi jaringan dengan VPN setelah DoS.

Berdasarkan gambar 6, nilai performansi dari jaringan yang diberikan VPN tidak banyak berubah jika dibandingkan dengan data kontrol. Hal ini menunjukan penggunaan VPN lebih baik diterapkan agar jaringan lebih aman tanpa mempengaruhi nilai QoS dari jaringan tersebut. Gambar 7 merupakan hasil performansi dari jaringan VPN setelah diserang dengan MAC Overflow. Berdasarkan gambar tersebut dapat dilihat bahwa nilai performansi sedikit lebih membaik dibandingkan jaringan tanpa VPN meskipun nilai dari *packet loss* tetap sangat tinggi. Sedangkan gambar 8 menunjukan VPN mempengaruhi nilai QoS dari jaringan yang diserang dengan DoS meskipun tidak terlalu banyak.

4. Kesimpulan

Berdasarkan hasil dari simulasi yang dilakukan, didapatkan beberapa hasil diantaranya:

1) Jaringan normal dengan dan tanpa VPN memiliki nilai QoS yang hampir sama. Hal ini menunjukan bahwa penggunaan VPN tidak mengurangi performansi dari jaringan tersebut. Nilai rata – rata dari performansi tersebut untuk jaringan tanpa VPN adalah throughput 3057,234 bit/s, packet loss 0%, delay 0,448 ms, dan jitter 0,240 ms. Sedangkan untuk jaringan dengan VPN memiliki rata – rata nilai performansi throughput 3050,441 bit/s, packet loss 0%, delay 0,452 ms, dan jitter rata – rata 0,236 ms.
2) MAC Overflow merupakan tipe serangan yang kurang efektif untuk memperlambat jaringan, karena pada saat ini beberapa tipe perangkat sudah dilengkapi untuk mencegah adanya serangan tipe ini. Tetapi untuk jaringan yang tidak memiliki perangkat yang dapat mencegah serangan ini, akibat dari serangan ini dapat terlihat dari nilai QoS nya. Untuk jaringan tanpa VPN memiliki rata – rata nilai throughput 1333,266 bit/s, packet loss 93.04 %, delay 2,718 ms, dan jitter 1,210 ms. Sedangkan untuk jaringan dengan VPN rata – rata nilai throughput 1334,665 bit/s, packet loss 98,72%, delay 2,71 ms, dan jitter 1,222 msBerdasarkan uji kualitas layanan (QoS) dengan tolok ukur menggunakan standard TIPHON, menunjukkan bahwa sistem yang dirancang dan di ujicoba pada 5 tempat menghasilkan nilai dengan rata-rata *bandwidth* 8.692 Mbps, *throughput* 99.82%, rata-rata *delay* 27.121 ms, dan rata-rata *packet loss* sebesar 0.2%.
3) DoS Attack yang dilakukan kepada IOU target kurang efektif untuk memperlambat performansi jaringan dikarenakan network resource dari IOU target lebih banyak dari paket data yang dikirimkan. Akan tetapi jika serangan dilancarkan kepada PC, maka PC tersebut akan crash dan harus di reboot agar dapat digunakan kembali. Nilai QoS rata – rata dari jaringan tanpa VPN adalah throughput 2925,717 bit/s, packet loss 0%, delay 0,449 ms, dan jitter 0,235 ms. Sedangkan untuk jaringan yang menggunakan VPN didapatkan nilai rata – rata QoS untuk throughput 3049,793 bit/s, packet loss 0%, delay 0,453 ms, dan jitter 0,237 ms.

5. Daftar Pustaka:

[1] M. Isaac and S. Frenkel, “Facebook Security Breach Exposes Accounts of 50 Million Users,” *28 September*, 2018. [Online]. Available: https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html. [Accessed: 23-Oct-2018].

[2] F. M. Ridwan, L. V. Yovita, and D. Perdana, “IPSEC VPN TUNNEL SEBAGAI ALTERNATIF KEAMANAN KONEKTIVITAS ANTAR NETWORK IPSEC VPN TUNNEL AS AN ALTERNATIVE SECURITY NETWORK CONNECTIVITY BETWEEN NETWORK,” vol. 1, no. 1, pp. 1–8, 2017.

[3] Y. Li and J. Mao, “SDN-based access authentication and automatic configuration for IPSec,” *SDN-based Access Authentication Autom. Config. IPSec*, pp. 1–4, 2015.

[4] L. Djeddai and R. K. Liu, “IPSecOPEP: IPSec Over PEPs Architecture, For Secure And Optimized Communications Over Satellite Links,” *Proc. IEEE Int. Conf. Softw. Eng. Serv. Sci. ICSESS*, pp. 264–268, 2016.

[5] D. Fang, P. Zeng, and W. Yang, “Attacking the IPSec Standards When Applied to IPv6 in Confidentiality-only ESP Tunnel Mode,” *Int. Conf. Adv. Commun. Technol. ICACT*, pp. 401–405, 2014.

[6] A. Shiranzaei and R. Z. Khan, “Internet Protocol Versions – A Review,” *Proc. 9th INDIACom; INDIACom-2015*, vol. 202002, pp. 397–401, 2015.

[7] A. Alshalan, S. Pisharody, and D. Huang, “A Survey of Mobile VPN Technologies,” *IEEE Commun. Surv. Tutorials*, vol. 18, no. 2, pp. 1177–1196, 2016.

[8] M. Guowang, Z. Jens, S. K-W, and S. Ben, "Fundamentals of Mobile Data Data Networks," Cambridge University Press, ISBN 1107143217, 2016.

[9] S. David C., S. Aaron, P. Christian, “Wireless Reliability: Rethinking 802.11 Packet Loss,” Department of Computer Science and Engineering, University of Notre Dame, 2007.

[10] T. Ye, X. Kai, A. Nirwan, “TCP in Wireless Environments: Problems and Solutions,” *IEEE Radio Communications*, 2005.

[11] Kurose, J.F. & Ross, K.W. (2010). Computer Networking: A Top-Down Approach. New York: Addison-Wesley. p. 36.

[12] L. Hu, and D. Evans, “Using Directional Antenna to Prevent Wormhole Attacks,” 14 Proceedings of the 11th Network and Distributed System Security Symposium, 2003.

[13] Y.-C. Hu, A. Perrig, “A Survey of Secure Wireless Ad Hoc Routing,” Security and Privacy Magazine,

IEEE, Vol. 2, Issue 3, pp. 28-39, May 2004.
[14] S. Raj, K. R. A., "Wormhole Attack in Wireless Sensor Network," International Journal of Computer Networks and Communications Security, Vol. 1, Issue 1, pp. 22-26, January 2014.
[15] L. Lazos, and R. Poovendran, "Serloc: Secure Range-Independent Localization for Wireless Sensor Networks," Proceedings of the ACM Workshop on Wireless Security, pp. 21-30, October 2004
[16] A. Abdel Rahman, M. Ashraf, V. Paul, "Accurate One-Way Delay Estimation with Reduced Client-Trustworthiness," IEEE Communications Letters, pp. 735-738, May 2015.
[17] "Understanding Denial-of-Service Attacks," US-CERT., 6 February 2013.
[18] "What is a DDoS Attack," https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. [Accessed: 16-Aug-2019].
[19] "E.800: Terms and definitions related to quality of service and network performance including dependability". ITU-T Recommendation. August 1994. Retrieved January 14, 2020. Updated September 2008 as Definitions of terms related to quality of service
[20] "Understanding Jitter in Packet Voice Networks", February 2, 2006. Available: https://www.cisco.com/c/en/us/support/docs/voice/voice-quality/18902-jitter-packet-voice.html. [Accessed: 7-Jan-2020].
[21] "VLAN Security White Paper: Cisco Catalyst 6500 Series Switches". Cisco Systems. 2002.
[22] "What is MAC flooding attack and How to prevent MAC flooding attack," Available: http://www.omnisecu.com/ccna-security/what-is-mac-flooding-attack-how-to-prevent-mac-flooding-attack.php. [Accessed: 7-Jan-2020].
[23] European Telecommunication Standards Institute, "Telecommunication and Internet Protocol Over Networks (TIPHON); General aspects of Quality of Service (QoS)", TR 101 329, V2.1.1, (1999-06).
[24] R. Hinden; S. Deering (February 2006). IP Version 6 Addressing Architecture. Network Working Group. doi:10.17487/RFC4291. RFC 4291. Updated by: RFC 5952, RFC 6052, RFC 7136, RFC 7346, RFC 7371, RFC 8064.