InComTech: Jurnal Telekomunikasi dan Komputer
vol.13, no.2, Agustus 2023, 113-124
http://publikasi.mercubuana.ac.id/index.php/Incomtech
P-ISSN: 2085-4811 E-ISSN: 2579-6089

Analisis Manajemen *Bandwidth* dan Keamanan Jaringan Menggunakan Metode *Hierarchical Token Bucket* dan *Port Knocking* Pada Router Mikrotik

Nareza Ocha Safira*, Eka Wahyudi, Fauza Khair

Teknik Telekomunikasi, Institut Teknologi Telkom Purwokerto,
Jl. Panjaitan, Jawa Tengah 53417, Indonesia
*Email Penulis Koresponden: 18101024@ittelkom-pwt.ac.id,

***Abstrak* :**
Penelitian ini membahas tentang penerapan manajemen *bandwidth* dan keamanan jaringan menggunakan metode *hierarchical token bucke*t dan *port knocking* pada *router* mikrotik. Pada penelitian ini mengambil contoh kasus penerapan yang sudah dilakukan di Perumdam Tirta Satria yang melakukan manajemen *bandwidth* dengan alokasi bandwidth dari *provider* sebesar 150Mbps. Serta penerapan kemamanan jaringan menggunakan metode port knocking yang dapat mengatur dan membatasi *user / client* dalam mengakses *server* atau koneksi *public*. Penelitian ini bertujuan untuk mengetahui seberapa efektif penerapan metode *hierarchical token bucket* dan *port knocking* pada *router* mikrotik. Pengujian dilakukan dengan mengukur *Quality of service* (QoS) menggunakan *tools* wireshark pada server jaringan setelah diterapkan nya metode tersebut. Dari hasil pengujian QoS dapat diketahui bahwa penerapan metode tersebut berhasil sangat baik dengan nilai *throughput* 73,059kbps (standart >100kbps), delay 0,007163 ms (standart <1 ms), jitter 0,000833 ms (standart <1 ms) dan packet loss 0% (standart 0%). Serta dalam pengujian *scanning port* dapat dilihat hasil bahwa *port* tersebut dalam *status filtered* yang berarti *port* tersebut hanya bisa di akses oleh koneksi yang sudah di tertukan di *router* mikrotik.

Keywords:
Hierarchical Token Bucket,
Bandwidth,
Port Knocking

Article history:
Diserahkan 19 September 2022
Direvisi 05 Juni 2023
Diterima 12 Juni 2023
Dipublikasi 15 Agustus 2023

DOI:
10.22441/incomtech.v13i2.17214

1. PENDAHULUAN

Internet pada revolusi industri 4.0 semakin berkembang pesat, yang pada akhirnya *internet* menjadi salah satu kebutuhan yang sangat penting bagi semua

kalangan seperti pada sebuah perusahaan untuk mengirim dan menerima informasi ataupun dalam pengambilan keputusan [1]. Penggunaan *router* mikrotik sangat *familiar* dalam suatu perusahaan yang menggunakan jaringan *internet*. Sehingga tidak banyak perusahaan-perusahaan tersebut kurang peduli terhadap pembagian *bandwidth* dan keamanan jaringan yang digunakan.

Untuk itu diperlukan nya manajemen *bandwidth* dengan metode *Hierarchical Token Bucket* (HTB), metode ini banyak digunakan untuk mengatasi permasalahan pada koneksi Internet, memaksimalkan penggunaan *bandwidth* sehingga semua *user* dapat menggunakan *bandwidth* secara adil dan semua *user* mendapatkan kenyamanan dan kepuasan ketika *browsing*, Penelitian ini menggunakan metode *Hierarchical Token Bucket* (HTB) yaitu salah satu metode yang dirancang untuk bisa melakukan manajemen *bandwidth* dengan baik, dimana algoritma ini menerapkan disiplin antrian yang mempunyai kelebihan dalam pembatasan trafik pada tiap *level* maupun klasifikasi, sehingga *bandwidth* yang tidak dipakai oleh *level* yang tinggi dapat digunakan atau dibagi oleh *level* yang lebih rendah [2].

Saat ini keamanan telah menjadi hal yang sangat penting, terutama dalam bidang Teknologi Informasi. Statistik tingkat eksploitasi keamanan terhadap banyak *server* dan jaringan makin hari semakin meningkat. Bahkan seseorang yang tidak memiliki pengetahuan yang cukup dalam masalah keamanan jaringan dapat melakukan penetrasi terhadap sebuah sistem jaringan dengan hanya men-*download exploit* untuk sistem yang diserangnya dan kemudian menggunakannya untuk kepentingan sendiri. Salah satu upaya mengamankan sebuah *server* adalah dengan menggunakan *firewall*, tetapi saat ini *firewall* masih memiliki kelemahan. Sehingga dicari solusi terbaik agar dapat mengakses *service* tertentu walaupun *port* tersebut tertutup [3].

2. METODE

2.1. Studi Literatur

Metode yang dilakukan dari beberapa jurnal yang digunakan sebagai acuan. Penelitian yang dilakukan oleh Rizka dkk menggunakan metode *sniffing* dan *port knocking*. Penelitian ini dilakukan pengujian serangan terhadap jaringan dengan menggunakan zenmap dan wireshark [1]. Penelitian kedua oleh ketut dkk menggunakan metode *Hierarchical Token Bucket* pada layanan *Hotspot*. Hasil penelitian ini yaitu pengujian kondisi *maximum user* dan *minimum user parameter packet loss* [2]. Penelitian ketiga oleh Christian dkk dengan menggunakan metode *port knocking* dan *action tarpit* pada *router* mikrotik. *Port Knocking* adalah metode yang dilakukan untuk membuka akses ke *port* tertentu yang telah di*block* oleh *firewall* pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Hasil dari pengujian ini yaitu metode *port knocking* dapat meminimalisir terjadinya penyusupan yang tidak mempunyai hak akses dan membantu *administrator* dalam menjaga akses keamanan *port* autentikasi [3].

2.2. Alat Dan Bahan (Hardware Dan Software)

Penelitian ini menggunakan beberapa alat dan bahan ditunjukkan pada Tabel 1 dan tabel 2

Tabel 1. Perangkat Keras *(Hardware)*

PERANGKAT KERAS *(HARDWARE)*
Kabel UTP Cat 6 AMP
Switch dan *Hub D-Link*
Routerboard Mikrotik RB750
PC Server HP Proliant Gen9
Laptop Core i3 sebanyak 5 unit
Access Point D-Link

Tabel 2. Perangkat Lunak *(Software)*

PERANGKAT LUNAK *(SOFTWARE)*
Winbox
Mikrotik OS
Windows Operating System
Wireshark

2.3 Parameter Penelitian

Berdasarkan standar TIPHON dalam pengukuran Analisis *Quality of Service* (QoS) sebuah jaringan menggunakan empat *parameter*, diantaranya adalah *Delay*, *Jitter*, *Throughput* dan *Packet Loss*.

Delay adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal hingga ke tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama [4].

Persamaan Perhitungan *delay*:

$$Delay = \frac{Total\ delay(ms)}{Total\ paket\ yang\ diterima} \quad (1)$$

Tabel 3. *Delay*

Kategori	**Besar *Delay***	**Indeks**
Sangat Bagus	< 150 ms	4
Bagus	150 – 300 ms	3
Sedang	300 – 400 ms	2
Buruk	< 450 ms	1

Jitter didefinisikan sebagaai variasi *delay* yang diakibatkan oleh panjang *queue* dalam suatu pengolahan *data* dan *reassemble* paket-paket data di akhir pengiriman akibat kegagalan sebelumnya [5].

Persamaan Perhitungan *jitter*:

$$Jitter = \frac{Total\ variasi\ delay}{Total\ paket\ diterima} \quad (2)$$

Tabel 4. *Jitter*

Kategori	**Besar *Jitter***	**Indeks**
Sangat Bagus	0 ms	4
Bagus	0 – 75 ms	3
Sedang	75 – 125 ms	2
Buruk	125 - 225 ms	1

Throughput yaitu kecepatan (*rate*) *transfer* data efektif, yang diukur dalam *bps*. *Throughput* merupakan jumlah total kedatangan paket yang sukses yang diamati pada tujuan selama *interval* waktu tertentu dibagi oleh durasi *interval* waktu tersebut [7]. Parameter Persamaan *Throughput*:

$$Throughput = \frac{Paket\ data\ diterima(bytes)}{Lama\ pengiriman(sec)} \quad (3)$$

Tabel 5. *Throughput*

Kategori	Besar *Throughput*	Indeks
Sangat Bagus	100 %	4
Bagus	75 %	3
Sedang	50 %	2
Buruk	< 25%	1

Packet loss merupakan suatu *parameter* yang menggambarkan kondisi yang menunjukan jumlah total paket yang hilang[9]. Parameter Persamaan *Packet loss*:

$$Packet\ Loss = \frac{(Paket\ data\ dikirim - Paket\ data\ diterima)x100\%}{Paket\ data\ yang\ dikirim} \quad (4)$$

Tabel 6. *Packet Loss*

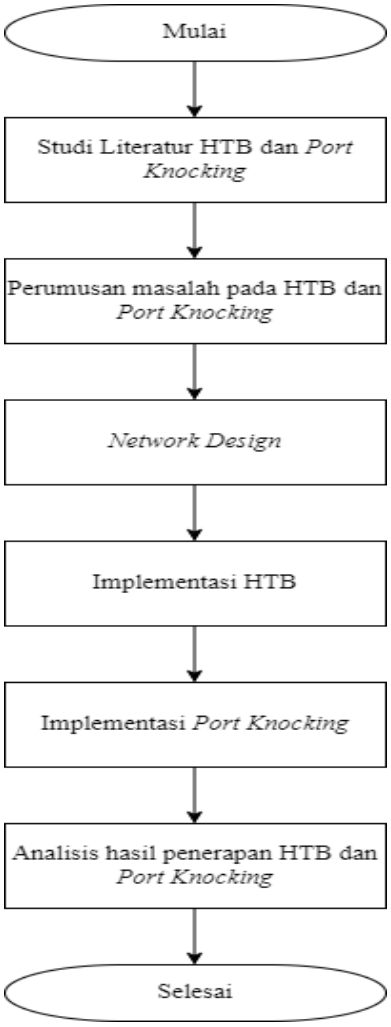
Kategori	Besar *Packet Loss*	Indeks
Sangat Bagus	0 %	4
Bagus	3 %	3
Sedang	15 %	2
Buruk	25 %	1

2.4. Alur Penelitian

Adapun alur penelitian terdiri dari beberapa tahap seperti yang ditunjukkan oleh Gambar 1 agar mendapatkan hasil yang diinginkan.

Pada Gambar 1 merupakan penjelasan yang sesuai dengan diagram alir penelitian, penelitian ini dilakukan dengan beberapa tahapan proses pengerjaan yaitu dari identifikasi masalah: melakukan beberapa identifikasi beberapa masalah dengan penelitian yaitu bagaimana melakukan manajemen *bandwidth* dan kemanan jaringan. Studi literatur: melakukan studi literatur yang berkaitan dengan penelitian yaitu dengan pencarian informasi topik yang berhubungan dengan penelitian manajemen *bandwidth* dan keamanan jaringan yang didapatkan dari jurnal, buku, dan *internet*. Selanjutnya analisis: melakukan analisis dari studi literatur yang telah dilakukan sehingga dapat mengetahui penelitian yang akan dilakukan. Desain: membuat konfigurasi atau perancangan jaringan sesuai dengan penelitian yang dilakukan dan nanti pada saat *maintenance* mudah dilakukan. Implementasi: tahap implementasi merupakan tahap paling penting dimana tahap ini menentukan berhasil tidaknya perancangan jaringan yang sudah dibuat sebelumnya. Menganalisis hasil: Analisa ini dilakukan untuk mengetahui tingkat kinerja dari sisi

manajemen *bandwidth* dan keamanan jaringan yang telah dilakukan apakah metode yang diterapkan sudah berjalan dengan baik.

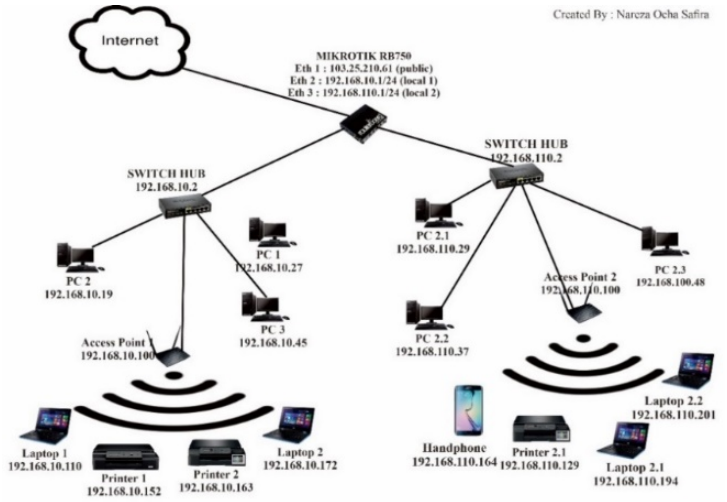


Gambar 1. Diagram Alir

2.5. Skenario Penelitian

Topologi jaringan yang digunakan merupakan jenis topologi *star extend*. *Access point* yang berfungsi sebagai *hotspot*, kabel *UTP* sebagai media transmisi yang menghubungkan seluruh komputer ke jaringan, *Hub* berfungsi juga sebagai *media internet* bagi pengguna *LAN* dan penghubung antara *server* ke jaringan. Berikut adalah analogi desain jaringan atau *network diagram* yang dapat ditunjukkan pada Gambar 2.

Penelitian ini mengambil contoh penggunaan *Routerboard* Mikrotik *RB750* menjelaskan analogi perancangan jaringan. *Routerboard* Mikrotik bertindak sebagai pembagi koneksi ke jaringan LAN dan jaringan WLAN. Dalam tahap ini yang dilakukan adalah merancang desain topologi jaringan komputer, baik topologi fisik maupun topologi logis sesuai dengan ketersediaan teknologi yang ada. Penelitian ini melakukan desain terhadap sistem yang akan dibangun dengan tujuan memaksimalkan penggunaan *bandwidth* yang ada.



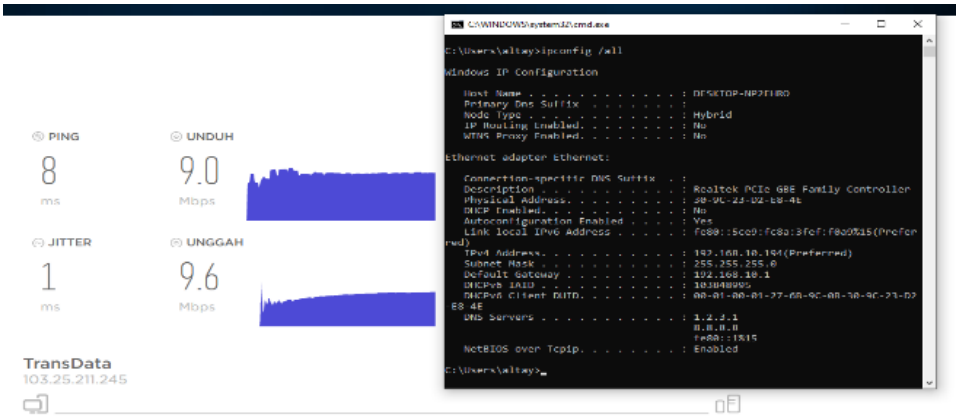
Gambar 2. *Network* diagram

Pada desain jaringan penelitian ini melakukan perancangan sebuah *router* mikrotik untuk diletakkan diantara *access point* dan *switch* utama yang difungsikan sebagai *gateway, firewall*, dan *bandwidth controller*.

3. HASIL DAN PEMBAHASAN

3.1. Hasil Penerapan HTB

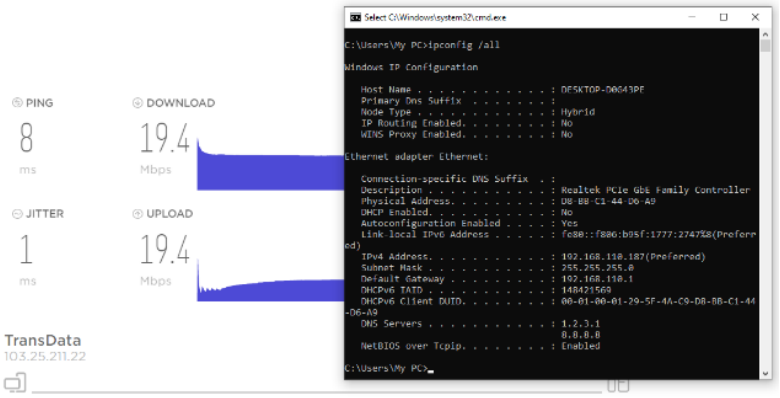
Pengujian dilakukan dengan cara mengukur *bandwidth* antara *upload* dan *download* menggunakan aplikasi *web* dari *Internet Speed Test "https://speedtest.cbn.id/"*. Pengukuran dilakukan secara *random* pada setiap *child* di *parent queue* yang terhubung ke jaringan Mikrotik. Pengujian pertama dilakukan pada *user / client* dengan *IP Address* 192.168.10.194 yang terhubung dengan *parent queue* Klas 10 ditunjukkan pada Gambar 3.



Gambar 3.Pengujian *upload* dan *download bandwidth* klas 10.

Berdasarkan hasil tersebut dapat dipastikan bahwa penerapan metode *Hierarchical Token Bucket* pada Klas *IP Address* 192.168.10.0/24 sudah berjalan dengan baik. Karena dapat dilihat hasil pengujian untuk *bandwidth download* pada *client* dengan *IP address* 192.168.10.194 adalah *download* sebesar 9.0*Mbps* dan *upload* sebesar 9.6*Mbps*.

Pengujian *bandwidth* kedua dilakukan pada *user / client* yang terhubung dengan *parent queue* Klas 110 dengan *IP Address* 192.168.110.187 yang hasilnya dapat dilihat pada Gambar 4.



Gambar 4.Pengujian *upload* dan *download bandwidth* klas 110

Berdasarkan Gambar 4. dapat disimpulkan bahwa pengujian yang dilakukan di klas 110 dengan *IP Address* 192.168.110.187 menghasilkan kecepatan *download* sebesar 19.4*Mbps* dan *upload* 19.4*Mbps*. Hal ini dapat dipastikan bahwa penerapan metode *Hierarchical Token Bucket* pada Klas *IP Address* 192.168.110.0/24 sudah berjalan dengan baik. Selain itu pengecekan apakah penerapan metode *Hierarchical Token Bucket* juga dapat dilakukan di Mikrotik dengan menggunakan *menu* ***Torch*** yang merupakan *tools* yang digunakan untuk melihat *bandwidth* secara *realtime* berapa pemakaian *bandwidth* pada setiap komputer. Dengan begitu dapat mengawasi penggunaan *bandwidth* pada setiap komputer pad Tabel 7 dan Tabel 8.

Tabel 7.*Torch* klas IP 192.168.110.0/24

No	*IP Address*	Tx	Rx
1.	192.168.110.249	4,3 Mbps	39,9 kbps
2.	192.168.110.88	2,0 Mbps	28,8 kbps
3.	192.168.110.183	1263,3 kbps	13,8 kbps
4.	192.168.110.228	392,0 kbps	32,1 kbps
5.	192.168.110.188	70,6 kbps	32,1 kbps
6.	192.168.110.173	7,3 kbps	1440 bps
7.	192.168.110.142	2,9 kbps	1440 bps
8.	192.168.110.167	2,8 kbps	0 kbps
9.	192.168.110.176	2,5 kbps	1264 bps
10.	192.168.110.178	2,5 kbps	960 bps

Tabel 8.*Torch* klas IP 192.168.10.0/24

No	*IP Address*	Tx	Rx
1.	192.168.10.65	8,1 Mbps	112,7 kbps
2.	192.168.10.105	5,3 Mbps	44,8 kbps
3.	192.168.10.233	4,3 Mbps	120,0 kbps
4.	192.168.10.241	2,4 Mbps	26,8 kbps
5.	192.168.10.54	1641,0 kbps	30,6 kbps
6.	192.168.10.102	1234,7 kbps	35,4 kbps
7.	192.168.10.90	238,2 kbps	6,0 kbps
8.	192.168.10.77	191,1 kbps	2,4 kbps
9.	192.168.10.54	121,9 kbps	31,4 kbps

10.	192.168.10.212	103,6 kbps	68,0 kbps

Berdasarkan Tabel 7 dan Tabel 8 dapat disimpulkan bahwa rata – rata penggunaan *user* setelah di terapkannya metode *Hierarchical Token Bucket* dapat terkontrol dan tidak ada *user* atau *client* yang melebihi alokasi *bandwidth* yang sudah diterapkan di q*ueue list* dan q*ueue tree* di Mikrotik.

3.2. Hasil Penerapan *Port Knocking*

Pengujian terhadap penerapan metode *Port Knocking* dan *Port Blocking* juga dapat dilakukan menggunakan *torch* dengan melakukan pengecheckan apakah ada *bandwidth* yang masuk setelah dilakukan nya *blocking* pada port 443 Tabel 9 dan Tabel 10.

Tabel 9.Hasil *Port Blocking*

No	***IP Address***	**Tx**	**Rx**
1.	192.168.110.212:51237	0bps	0bps
2.	192.168.110.129:43050	0bps	0bps
3.	192.168.110.129.58568	0bps	0bps
4.	192.168.110.129.49888	0bps	0bps
5.	192.168.110.151:44272	0bps	0bps
6.	192.168.110.129:41202	0bps	0bps
7.	192.168.110.129:39528	0bps	0bps
8.	192.168.110.129:47978	0bps	0bps
9.	192.168.110.232:43821	0bps	0bps
10.	192.168.110.129:37266	0bps	0bps

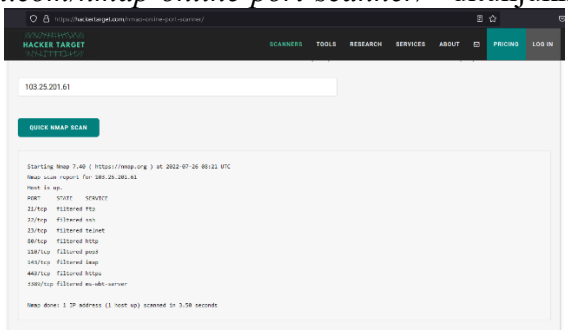
Tabel 10.Hasil *Port Knocking*

No	***IP Address***	***Tx***	***Rx***
1.	192.168.10.87:59592	4,4Mbps	108,7kbps
2.	192.168.10.181:48742	967,1 kbps	3,0 kbps
3.	192.168.10.90:38343	237,7 kbps	26,1 kbps
4.	192.168.10.210:64378	89,5 kbps	26,1 kbps
5.	192.168.10.210:50830	62,9 kbps	9,9 kbps
6.	192.168.10.194:55146	52,2 kbps	12,5 kbps
7.	192.168.1.87:60695	47,3 kbps	24,1 kbps
8.	192.168.10.120:58269	31,2 kbps	3,0 kbps
9.	192.168.10.87:55379	25,6 kbps	27,3 kbps
10.	192.168.10.87:64110	19,7 kbps	14,6 kbps

Berdasarkan Tabel 9 dan Tabel 10 dapat dijelaskan bahwa penerapan metode keamanan *port blocking* dan *port knocking* dalam manajemen jaringan sudah berhasil dengan pembuktian sebagai berikut :

a. *Range ip address* 192.168.110.0/24 tidak ada koneksi yang masuk melalui *port* 443 dibuktikan dengan Tabel 9.
b. *Range ip address* 192.168.10.0/24 dapat melakukan akses ke *port* 443, hal ini dibuktikan dengan ada nya koneksi yang masuk dari beberapa *ip address* yang aktif dari *client* seperti Tabel 10.

Dan pengujian terhadap penerapan *port blocking* yang di terapkan pada *IP Public* Perumdam Tirta Satria yang dilakukan menggunakan *web* aplikasi *"www.hackertarget.com/nmap-online-port-scanner/"* ditunjukkan pada Gambar 5.

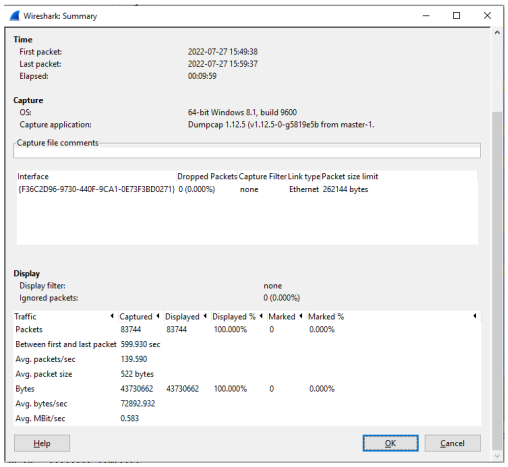


Gambar 5.Hasil *Port Blocking IP Public*

Berdasarkan Gambar 5. terlihat hasil *scan* menggunakan *web* aplikasi *online scan port* menujukkan *status port* tersebut adalah *filtered.* Hal tersebut dapat dipastikan bahwa penerapan metode *port knocking* dan *port blocking* sudah berjalan dengan baik. Dikarenakan dengan *status filtered* tersebut menujukkan bahwa akses yang akan masuk ke dalam jaringan melalui *IP public* 103.25.201.61 Perumdam Tirta Satria sudah di *filter* atau di tentukan oleh settingan yang terpasang di Mikrotik Perumdam Tirta Satria tersebut sesuai dengan konsep awal metode *Port Knocking.*

3.3 PENGUJIAN *QUALITY OF SERVICE* (QoS)

Untuk mendapatkan hasil pengujian *Quality Of Service* dari penerapan metode *Hierarchical Token Bucket* dan metode *Port Knocking* yang telah di implementasikan, Penelitian ini mencoba mengambil *data data sampling* dari *server*.



Gambar 6.*Capture File Wireshark*

Berdasarkan Gambar 6. dapat diambil beberapa data yaitu berupa:

Tabel 11.Hasil data *delay*

No	Nama Hasil	Nilai Hasil
1.	Waktu pengamatan	10 menit
2.	Total *delay*	599,930 *sec*
3.	Total paket diterima	83,744
4.	Total paket yang dikirim	43,830,662
5.	Total paket data yang diterima	43,830,662

1) Pengujian *Delay*

Berdasarkan data pada Tabel 11 dapat di hitung berapa *delay* yang di peroleh dengan rumus yaitu :

$$\textit{Delay}\ \text{Rata – rata} = \frac{\text{Total } \textit{delay}}{\text{Total paket yang diterima}}$$

$$\textit{Delay}\ \text{Rata – rata} = \frac{599{,}930}{83744}$$

$$\textit{Delay}\ \text{rata – rata} = 0{,}007163\ \text{ms}$$

Hasil yang didapat adalah 0,007163 ms atau < 1ms dan berdasarkan indeks pada Tabel 3 termasuk dalam kategori **"sangat bagus".**

2) Perhitungan *Jitter*

Untuk perhitungan *jitter* dapat dimasukkan ke rumus sebagai berikut :

$$\textit{Jitter} = \frac{\text{Total variasi } \textit{delay}}{\text{Total paket yang diterima - 1}}$$

$$\textit{Jitter} = \frac{69{,}79}{83744 - 1}$$

$$\textit{Jitter} = 0{,}000833\ \text{ms}$$

Hasil yang didapat adalah 0,000833 ms atau < 1ms dan masuk dalam indeks Tabel 4 **"sangat bagus".**

3) Perhitungan *Throughput*

Berdasarkan data *wireshark* dapat dihitung *throughput* yang dikirim *server* ke klas IP 192.168.110.0/24 yaitu sebagai berikut :

$$\textit{Throughput} = \frac{\text{Paket data yang diterima}}{\text{Lama Pengamatan}}$$

$$\textit{Throughput} = \frac{43830662}{599{,}930}$$

$$\textit{Throughput} = 73{,}059\text{kbps}$$

Hasil yang didapat adalah 73,059 dan berdasarkan indeks pada Tabel 5 termasuk dalam kategori **"Bagus"**.

4) *Packet Loss*

Dan untuk perhitungan yang terakhir akan mencoba menghitung *packet loss* dari koneksi atau jaringan tersebut sebagai berikut :

$$\textit{Packet Loss} = \frac{\text{Paket data yang di kirim - Paket data yang diterima x 100\%}}{\text{Paket data yang dikirim}}$$

$$\textit{Packet Loss} = \frac{43830662 - 43830662}{43830662} \text{ X } 100\%$$

$$\textit{Packet Loss} = 0\%$$

Berdasarkan perhitungan yang telah dilakukan dapat dipastikan bahwa *packet loss* dari jaringan tersebut adalah 0% dengan berdasarkan indeks pada Tabel 6 termasuk dalam kategori **"Sangat Bagus"**.

4. KESIMPULAN

Kesimpulan yang dapat diambil dari penelitian ini adalah sebagai berikut:

1. Penerapan manajemen *bandwidth* menggunakan metode *Hierarchical Token Bucket (HTB)* yang diterapkan di perusahaan tersebut mendapatkan hasil *download* rata – rata di *9.00Mbps* dan *upload* rata – rata sebesar *9.06Mbps* sesuai dari hasil speedtest yang dilakukan.
2. Penerapan *port blocking* dalam jaringan lokal sangat efektif dikarenakan penggunaan *bandwidth* yang tidak sesuai dapat di minimalisirkan.
3. Penerapan *port knocking* dalam jaringan lokal perusahaan tersebut dapat mengatur hak akses *user / client* dalam mengakses suatu *server* atau *website*.
4. Hasil penerapan metode *port blocking* pada *IP Public* Perumdam Tirta Satria dapat menjaga keamanan dan kerahasiaan perusahaan. Karena dalam metode tersebut di atur darimana saja koneksi luar bisa masuk kedalam jaringan *public* perusahaan tersebut.

REFERENSI

[1] R. Albar, R. O. Putra, "Analisis Keamanan Jaringan Menggunakan Metode Sniffing dan Implementasi Keamanan Jaringan Pada Mikrotik Router OS V6.48.3 Menggunakan Metode Port Knocking", Journal of Informatics and Computer Science, Vol. 8, No. 1, pp. 1–11, 2022. e-ISSN : 2615-5346.

[2] M. W. Ketut Gede Widia Pratama Putra, Gede Saindra, "Penerapan Manajemen Bandwidth Menggunakan Metode Hierarchical Token Bucket pada Layanan Hotspot Mikrotik Undiksha", Journal of Computer Engineering, System and Science, vol. 5, no. 1, pp. 146–154, 2020.

[3] Y. Christian, "Analisis Sistem Pengamanan Akses Autentikasi Jaringan dengan Metode Port Knocking dan Action Tarpit pada Router Mikrotik", Jurnal Telcomatics, vol. 4, no. 1, pp. 1–6, 2019.

[4] S. Raharjo and C. Iswahyudi, "Analisis Keamanan Jaringan Mikrotik ISP Indonesia Menggunakan Search Engine Scada Shodan dengan Metode Exploit Winbox Critical Vulnerability", Jurnal JARKOM, vol. 09, no. 01, pp. 56–62, 2021.

[5] P. Ferdiansyah, R. Indrayani, and S. Subektiningsih, "Analisis Manajemen Bandwidth Menggunakan Hierarchical Token Bucket Pada Router dengan Standar Deviasi", Ju- rnal Nasional Teknologi dan Sistem Informasi, vol. 6, no. 1, pp. 38–45, 2020, doi: 10.25077/teknosi.v6i1.2020.38-45.

[6] A. Maulana, "Penerapan Manajemen Bandwidth Menggunakan Metode Hierarchical Token Bucket (HTB)", Jurnal *Snistek*, vol. 4, no. 14, pp. 102–107, 2022.

[7] P. F. Subektiningsih, Renaldi, "Analisis Perbandingan Parameter QoS Standar TIPHON Pada Jaringan Nirkabel Dalam Penerapan Metode PCQ", Jurnal *Explore*, vol. 12, no. 1, pp. 57–63, 2022.

[8] E.A. Darmadi, "Manajemen Bandwidth Internet Menggunakan Mikrotik Router Di Politeknik Tri Mitra Karya Mandiri", Jurnal IKRA-ITH Teknologi, Vol 3, No 3, pp. 7-13, 2019.

[9] R. Rizal, R. Ruuhwan, and K. A. Nugraha, "Implementasi Keamanan Jaringan Menggunakan Metode Port Blocking dan Port Knocking Pada Mikrotik RB-941," *J. ICT Inf. Commun. Technol.*, vol. 19, no. 1, pp. 1–8, 2020, doi: 10.36054/jict-ikmi.v19i1.119.

[10] F. Ulum, Amarudin, "Desain Keamanan Jaringan pada Mikrotik Router OS Menggunakan Metode Port Knocking", Jurnal TEKNOINFO, Vol. 12, No. 2, pp. 72–75, 2018. ISSN 2615-224X.

[11] S. Sukaridhoto, "Buku Jaringan Komputer I", Politeknik Elektronika Negeri Surabaya (PENS), 2014, [Online]: http://dhoto.lecturer.pens.ac.id/publications/book/2014/Dhoto-JaringanKomputer1.pdf.