MANAJEMEN PADA JARINGAN MIKROTIK MENGGUNAKAN METODE HIERARCHICAL TOKEN BUCKET (HTB) DAN KEAMANAN FIREWALL INTRUSION DETECTION SYSTEM (IDS)

Arif setiadi[1], Prita Haryani[2], Suwanto Raharjo[3]

[1,2,3]Jurusan Teknik Informatika, Institut Sains & Teknologi AKPRIND Yogyakarta
Jl Kalisahak No. 28 Komplek Balapan Tromol Pos 45, Yogyakarta 55222 Telp : (0274) 563029
Email: arifsetiadi126@gmail.com[1], pritaharyani@akprind.ac.id[2],wa2n@akprind.ac.id[3]

ABSTRACT

The need for the use of the internet today is needed to support all activities, to facilitate the use of the internet at the Semali Village Hall, an internet network that is commonly used by employees at the Semali Village Hall has been provided. The absence of a bandwidth management system and a security system provided can affect the quality of the available internet network, therefore the aim of this study is to implement a bandwidth management system and the application of a security system so that every user can use the internet network optimally. The method used for bandwidth management uses the Hierarchical Token Bucket (HTB) method and the security system uses a ping flood and port knocking security system. In this study using a method with a quantitative approach. Quantitative methods are used to measure network parameters in the form of throughput, packet loss, delay and jitter values. Based on the results of the research, the final value of throughput with the application of the HTB method got a value of 25.34% with a moderate index, 2.10% packet loss with a very good index, a delay of 294 ms with a good index and a jitter of 30.50 ms with a good index, while for the final value the results testing without using the HTB throughput method got a final value of 11.75% with a bad index, a packet loss of 1.76% with a very good index, a delay of 296ms with a good index and a jitter of 47.30% with a good index and for the IDS security system using ping The flood results from several tests took 4 seconds to block the ping that was congesting the network to the Mikrotik router, while the application of the port knocking system which limits login access for IPs that logged in without doing a knock took about eight seconds before finally failing to log in and entered into list address list as intruders.

Keywords: *Bandwidth, Hierarchical Token Bucket* (HTB)**,***security system*

INTISARI

Kebutuhan penggunaan internet pada zaman sekarang ini dibutuhkan untuk menunjang segala aktivitas, untuk memfasilitasi penggunaan internet pada Balai Desa Semali telah disediakan sebuah jaringan internet yang biasa digunakan oleh karyawan yang berada di Balai Desa Semali. Belum adanya sistem pemanajemenan *bandwidth* dan sistem keamanan yang disediakan dapat mempengaruhi kualitas jaringan internet yang tersedia, maka dari itu tujuan penelitian ini adalah menerapkan sistem pemanajemenan *bandwidth* dan penerapan sistem keamanan agar setiap *user* dapat menggunakan jaringan internet secara maksimal. Metode yang digunakan untuk pemanajemenan *bandwidth* menggunakan metode *Hierarchical Token Bucket* (HTB) dan pada sistem keamanan menggunakan sistem keamanan *ping flood* dan *port knocking*. Pada penelitian ini menggunakan metode dengan pendekatan kuantitatif. Metode kuantitatif digunakan untuk pengukuran parameter jaringan berupa nilai *throughput, packet loss, delay* dan *jitter*. Berdasarkan hasil dari penelitian nilai akhir *throughput* dengan penerapan metode HTB mendapat nilai 25,34% dengan indeks sedang, *packet loss* 2,10% dengan indeks sangat baik, *delay* 294ms dengan indeks baik dan *jitter* 30,50ms dengan indeks baik sedangkan untuk nila akhir hasil pengujian tanpa menggunakan metode HTB *throughput* mendapat nilai akhir 11,75% dengan indeks tidak baik, *packet loss* 1,76% dengan indeks sangat baik, *delay* 296ms dengan indeks baik dan *jitter* 47,30% dengan indeks baik dan untuk sistem keamanan IDS menggunakan *ping flood* hasil dari beberapa kali pengujian dibutuhkan waktu 4 detik untuk mengeblok *ping* yang sedang memadati jaringan yang menuju

router mikrotik sedangkan penerapan sistem *port knocking* yang membatasi akses *login* untuk IP yang melakukan *login* tanpa melakukan *knock* membutuhkan waktu sekitar delapan detik sebelum akhirnya gagal *login* dan dimasukan kedalam daftar *address list* sebagai penyusup.

Kata kunci: *Bandwidth, Hierarchical Token Bucket* (HTB), sistem keamanan.

PENDAHULUAN

Balai Desa Semali merupakan salah satu instansi pemerintahan yang berada di Desa Semali Kecamatan Sempor Kabupaten Kebumen. Di Balai Desa Semali telah memanfaatkan jaringan internet sebagai penunjang aktivitas kegiatan sehari hari pegawai yang ada. Pemanfaatan jaringan komputer di Balai Desa Semali telah cukup lama tersedia namun tidak adanya staf khusus yang menangani jaringan komputer menyebabkan jaringan yang ada di sana belum bisa dimanfaatkan secara optimal dari segi kualitas *bandwidth* dan keamanan jaringan, maka dengan itu perlu adanya *maintenance* mengenai pemanajemenan *bandwidth* dan sistem keamanan.

Belum adanya pemanajemenan *bandwidth* menyebabkan *bandwidth* yang tersedia tidak terbagi secara merata sesuai kebutuhan *user*. Selain belum adanya pemanajemenan *bandwidth*, sistem keamanan jaringan yang ada pun masih standar, maka perlu adanya sistem keamanan tambahan untuk meningkatkan kualitas sistem keamanan jaringan agar terhindar ancaman pihak luar yang menyebabkan gangguan jaringan. *Ping flood* dan *port knocking* merupakan salah satu ancaman yang bisa menyebabkan jaringan bermasalah sehingga mengganggu aktivitas *user* yang sedang berjalan.

Berdasarkan latar belakang permasalahan, maka dapat diperoleh rumusan masalah, yaitu manajemenan *bandwidth* menggunakan metode *Hierarchical Token Bucket* (HTB) dan penerapan sistem keamanan *Firewall* menggunakan metode *Intrusion Detection System* (IDS) Di Balai Desa Semali dengan tujuan untuk meningkatkan kualitas jaringan sehingga client dapat menggunakan jaringan disediakan secara maksimal.

Berdasarkan latar belakang masalah yang telah dikemukakan diatas, maka batasan masalah dalam penelitian ini adalah manajemen bandwidth hanya menggunakan metode HTB dan penerapakan sistem keamanan IDS hanya dilakukan pengujian menggunakan *ping flood* dan *port knocking*. Tujuan penelitian ini bertujuan untuk:

1. Mengelolah dan memantau hasil manajemen menggunakan metode HTB dan menerapkan sistem keamanan *firewall* IDS pada router IDS.
2. Untuk mengetahui perbandingan kecepatan pada *client* setelah diterapkan metode HTB.
3. Menguji kinerja *bandwidth* dengan parameter *throughput*, *packet loss*, *delay* dan *jitter.*
4. Untuk mengukur berapa lama waktu yang dibutuhkan router mikrotik setelah diterapkannya metode keamanan IDS dalam mendeteksi adanya *ping flood* dan *Port Knocking*.

METODE PENELITIAN

Penelitian tentang “Penerapan Manajemen *Bandwidth* Menggunakan Metode *Hierarchical Token Bucket* Pada Layanan *Hotspot* Mikrotik Undiksha” bertujuan untuk mengetahui penerapan manajemen *bandwidth* menggunakan *Hierarchical Token Bucket* (HTB) pada layanan *hotspot* mikrotik Undiksha. Hasil pengujian kualitas layanan internet dari parameter *Quality of Service* (QoS) yang sudah diterapkan menggunakan (HTB). Metode penelitian yang digunakan adalah menggunakan pendekatan *Network Development Life Cycle* (NDLC), dengan melalui beberapa tahapan yaitu analisis, desain, simulasi, implementasi, monitoring, dan manajemen. Hasil pengukuran dengan menggunakan dua metode manajemen, *diperoleh* hasil rata-rata *download* dan *upload* dari HTB lebih besar dibandingkan dengan *simple queue* (Putra, Gede, & Kesiman, 2020).

Penelitian monitoring jaringan yang berjudul “Monitoring Jaringan *Wireless* Terhadap Serangan *Packet Sniffing* Dengan Menggunakan IDS” bertujuan untuk mengamankan *access point* dari berbagai ancaman serangan, salah satu contoh serangan adalah dengan menggunakan *packet sniffing*. Penelitian ini membahas pendeteksi serangan *packet sniffing* pada fasilitas *access point* dengan menggunakan sistem IDS. IDS adalah sebuah sistem yang melakukan pengawasan

terhadap *traffic* jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan di dalam sebuah sistem jaringan. Pada saat IDS *snort* dijalankan, maka IDS akan memonitoring jaringan internet yang sedang terhubung. Ketika menemukan kegiatan-kegiatan yang mencurigakan terutama sebuah serangan *packet sniffing* dengan indikasi *arp spoofing*, maka IDS akan memberikan *alert* berupa text "*Overwrite Attack*" pada PC yang sudah terinstal (Fauzi, 2018).

HTB adalah metode yang berfungsi untuk mengatur pembagian, pembagian dilakukan secara *hirarki* yang dibagi-bagi ke dalam kelas sehingga mempermudah pengaturan *bandwidth* dengan tepat sehingga penggunaannya menjadi maksimal. HTB diklaim menawarkan kemudahan pemakaian dengan teknik peminjaman dan implementasi pembagian *traffic* yang lebih akurat. Teknik antrian HTB memberikan fasilitas pembatasan *traffic* pada setiap level maupun klasifikasi, yang tidak terpakai dapat digunakan oleh klasifikasi yang lebih rendah. HTB berperan dalam mengontrol penggunaan terhadap *link* yang diberikan kepada *client*. HTB memungkinkan penggunaan fisik *link single* untuk menampilkan *multiple link* dan untuk mengirimkan jenis *traffic* yang berbeda pada tampilan *link* yang berbeda. Dengan kata lain, HTB sangat berguna untuk membatasi atau mengatur *bandwidth* pada saat *download* dan *upload*, dengan demikian *client* tidak dapat langsung menggunakan semua kapasitas (Ichwan, Lipur , & Yunanto, 2019).

IDS adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas *inbound* dan *outbound* dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan penyusupan. Deteksi penyusupan (*Intrusion Detection*) adalah aktivitas untuk mendeteksi penyusupan secara cepat dengan menggunakan program khusus. Program yang digunakan untuk pendeteksian disebut sebagai IDS (Yudhi, 2017).

Manajemen *Bandwidth* merupakan teknik pengelolaan jaringan sebagai usaha untuk memberikan performa jaringan yang adil dan memuaskan. Manajemen juga digunakan untuk memastikan yang memadai untuk memenuhi kebutuhan *traffic* data dan informasi serta mencegah persaingan antara aplikasi. Manajemen menjadi hal mutlak bagi setiap jaringan, semakin banyak aplikasi yang dapat dilayani oleh suatu jaringan akan berpengaruh pada penggunaan *link* dalam jaringan tersebut. *Link-link* yang ada harus mampu menangani kebutuhan *user* akan aplikasi tersebut bahkan dalam keadaan kepadatan *traffic* sekalipun (Ilham & Ahmad , 2018).

Keamanan jaringan komputer merupakan salah satu hal penting dan mendasar dalam pemanfaatan sebuah sistem. *Vulnerability* dalam sebuah sistem jaringan komputer seringkali dikesam*ping*kan, hingga apabila terjadi suatu ancaman atau serangan *logic* maupun *physic* yang merusak pada sistem tersebut. Salah satu bentuk yang ditempuh diantaranya adalah melakukan sebuah analisis secara periodik, baik itu *logic* dan *physic*, sehingga nantinya diharapkan dari analisis tersebut menghasilkan suatu laporan audit yang berisi deteksi dari berbagai macam *vulnerability* yang ada, untuk kemudian diambil langkah-langkah proteksi yang tepat, yang Diperlukan sebagai jaminan keamanan untuk keberlangsungan sistem tersebut (Didi , 2017).

HASIL DAN PEMBAHASAN

Parameter kualitas jaringan dalam pengujian ini meliputi *packet loss*, *delay, jitter* dan *throughput*. Sistem yang akan dianalisis mengenai tingkat pencapaian kualitas jaringan, adapun metode yang digunakan dalam pengelolahan *bandwidth* ini yaitu metode HTB. Pengujian kualitas *bandwidth* dilakukan dengan *software network analyzer wireshark*. Dalam pengujian ini dilakukan kepada empat *client* dan dilakukan perulangan sebanyak tiga kali, untuk membebani *traffic* jaringan yang ada setiap *client* akan melakukan *download* dengan ukuran *file* 150 Mbps dan *streaming video* dengan kualitas gambar 1080pixel secara bersamaan. Selain *download* dan *streaming video* beban jaringan juga ditambah dengan dilakukannya *ping flood* yang menyebabkan *traffic* pada jaringan mencapai sekitar 40 Mbps.

1. Hasil *Speedtest* data Oleh *wireshark* dengan HTB

Berdasarkan hasil pengujian dengan menerapkan metode HTB terhadap empat client dan dilakukan *ping flood* untuk menambah beban *traffic* mendapatkan hasil seperti pada tabel IV.1, dengan nilai rata-rata *throughput* mencapai 25,34%, *packet* loss mencapai 2,10%, *delay* mencapai 294 ms dan *jitter* mencapai 30,50 ms.

Tabel 1 Hasil pengujian dengan HTB

Parameter	Hasil pengujian			Rata-rata
	1	2	3	
Throughput	23,14%	23,80%	29,10%	25,34%
Packet loss	6,32%	0,00%	0,00%	2,10%
Delay	382ms	316ms	184ms	294ms
Jitter	26,96ms	32,67ms	31,88ms	30,50ms

Hasil dari pengujian kualitas jaringan menggunakan parameter QOS pada metode HTB mendapat hasil berupa indeks dari masing-masing parameter. *Throughput* mendapat indeks dengan kategori sedang, *packet loss* mendapat indeks dengan kategori sangat baik, *delay* mendapat indeks dengan kategori baik dan *jitter* mendapat nilai indeks dengan kategori baik. Hasil keseluruhan dapat dilihat pada tabel IV.2.

Tabel 2 Hasil Nilai rata-rata pengujian dengan HTB

Parameter	Nilai rata-rata	Nilai	Indeks
Throughput	25,34%	2	Sedang
Packet loss	2,10%	4	Sangat Baik
Delay	294ms	3	Baik
Jitter	30,50ms	3	Baik

2. Hasil *speedtest* data oleh *wireshark* tanpa HTB

Berdasarkan hasil pengujian tanpa menerapkan metode HTB dan dilakukan pengujian selama tiga kali mendapat hasil seperti pada tabel IV.3, dengan nilai rata-rata *throughput* mencapai 11,75%, *packet* loss mencapai 1,76%, *delay* mencapai 396 ms dan *jitter* mencapai 47,30 ms.

Tabel 3 Hasil pengujian tanpa HTB

Parameter	Hasil pengujian			Rata-rata
	1	2	3	
Throughput	8,49%	15,30%	11,48%	11,75%
Packet loss	0,00%	0,00%	5,29%	1,76%
Delay	436ms	487ms	266ms	396ms
Jitter	59,37ms	50,56ms	31,98ms	47,30ms

Hasil dari pengujian kualitas jaringan menggunakan parameter QOS tanpa metode HTB mendapat hasil berupa indeks dari masing-masing parameter. *Throughput* mendapat indeks dengan kategori tidak baik, *packet loss* mendapat indeks dengan kategori sangat baik, *delay* mendapat indeks dengan kategori baik dan *jitter* mendapat nilai indeks dengan kategori baik. Hasil keseluruhan dapat dilihat pada tabel IV.4.

Tabel 4 Hasil nilai rata-rata tanpa HTB

Parameter	Nilai rata-rata	Nilai	Indeks
Throughput	11,75%	1	Tidak baik
Packet loss	1,76%	4	Sangat Baik
Delay	396ms	3	Baik
Jitter	47,30ms	3	Baik

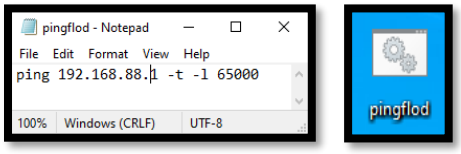
Secara umum perbandingan nilai akhir pada hasil *speedtest* yang dilakukan pada *queue tree* menggunakan metode HTB dan *queue tree* tanpa menggunakan metode HTB memiliki hasil yang tidak jauh berbeda, namun apabila dibandingkan kembali dengan menggunakan nilai tiap-tiap

parameter QOS berdasarkan besan *bandwidth* yang ditentukan maka akan terlihat perbedaan yang ada setelah diterapkannya metode HTB.

Tabel *5* Perbandingan hasil speedtest

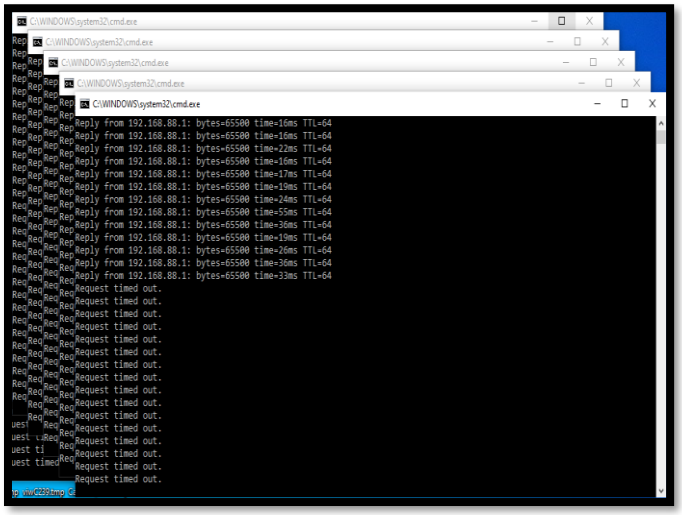
Parameter QOS	*Queue tree* dengan HTB		*Queue tree* tanpa HTB	
	Indeks	Kategori	Indeks	Kategori
Throughput	2	Sedang	1	Tidak baik
Paket Loss	4	Sangat baik	4	Sangat Baik
Delay	3	Baik	3	Baik
Jitter	3	Baik	3	Baik

Pada uji coba sistem keamanan *firewall* ini pengujian dilakukan dua kali uji coba. Pada dua kali *uji coba* tersebut akan dibagi menjadi uji coba sebelum diaktifkan *rule* pada *firewall* untuk sistem keamanan *ping flood* dan sesudah diaktifkan *rule* pada *firewall* untuk sistem keamanan *ping flood*. Untuk mempermudah pengujian sistem keamanan *ping flood* buatlah *script* pada notepad dan simpan dengan ekstensi .bat.



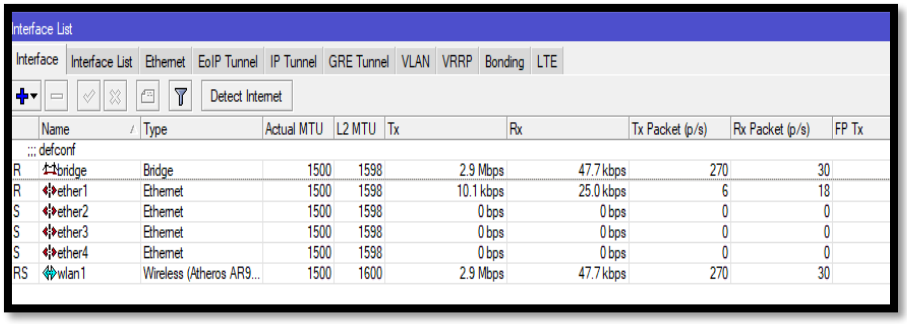
Gambar 1 Membuat script pada notepad dengan ekstensi .bat

Setelah sistem keamanan firewall diaktifkan butuh beberapa detik untuk menghentikan serangan *ping flood* yang sedang terjadi setelah *rule firewall* untuk mencegah *ping flood* diaktifkan. Setelah *rule firewall* diaktifkan *ping* yang menuju ke router mikrotik mengalami hambatan atau *time out*. Prinsip kerja dari *rule firewall* ini adalah memblok seluruh aktivitas *ping* yang sedang terjadi.



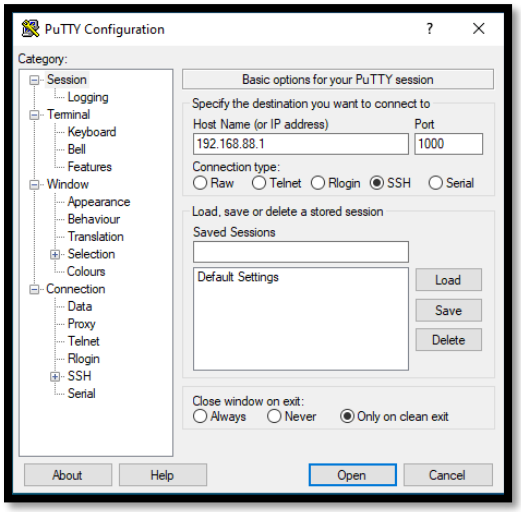
Gambar 2 *Ping flood* sesudah diaktifkan *rule firewall*

Setelah *rule firewall* untuk mencegah *ping flood* diaktifkan, kondisi *traffic bandwidth* dan CPU *load* mengalami penurun. Penurunan *traffic bandwidth* dan CPU *load* dapat dilihat pada gambar IV.3, dengan adanya *rule firewall* untuk mencegah *ping flood* bisa membuat *traffic bandwidth* lebih stabil sehingga router mikrotik menjadi lebih baik untuk menanggapi permintaan dari *client* atau *user*.



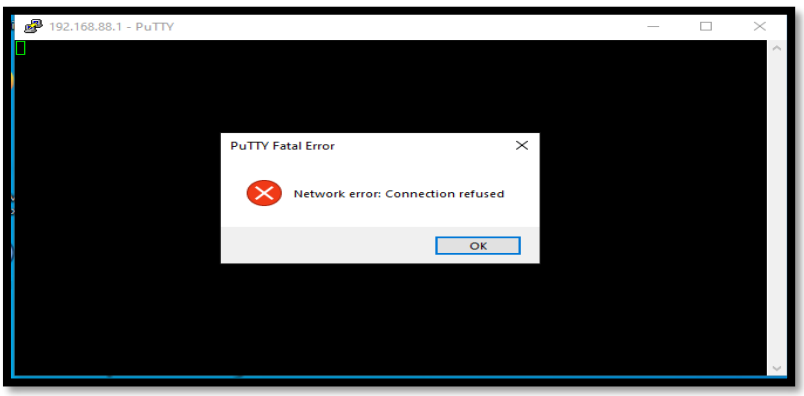
Gambar 3 Kondisi *traffic bandwidth* setelah di *aktifkan rule firewall*

Penerapan sistem keamanan *Port Knocking* digunakan untuk membatasi *user* yang ingin masuk ke router mikrotik. Pengujian *Port Knocking* dilakukan dengan *login* menuju router mikrotik melalui *port* winbox, SSH dan webfig. Setiap *user* yang akan *login* ke router mikrotik harus melakukan *knock* terlebih dahulu menuju *port* 1000. Untuk melakukan *knock* kepada *port* 1000 menggunakan *software putty*, pada *host name* isikan IP router mikrotik yang akan di*knock* seperti pada gambar IV.4.



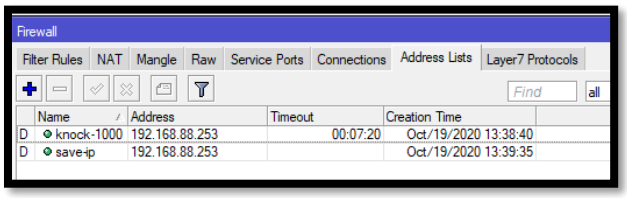
Gambar 4 *Knock port* 1000 menggunakan *putty*

Setelah *knock* ke *port* 1000 dilakukan maka akan muncul pesan *network error* pada *putty* seperti pada gambar IV.5 karena *knock* ke *port* 1000 hanya digunakan untuk mengirimkan pesan ke router mikrotik agar bisa diizinkan *login*.



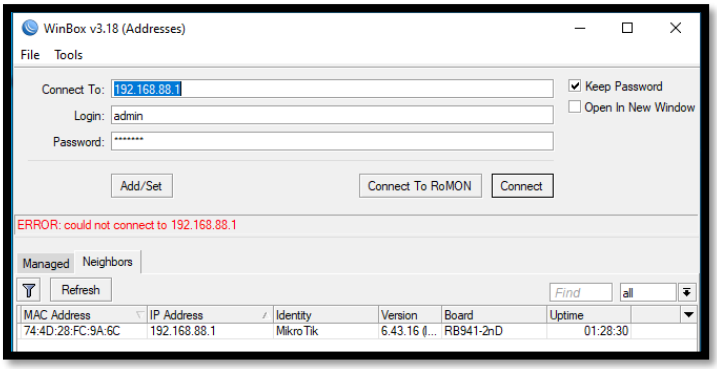
Gambar 5 Notifikasi *error* setelah dilakukan *knock* 1000

Pada gambar IV.6 dapat dilihat *address list* yang telah melakukan *knock* ke *port* 1000 dan *login* ke router mikortik. IP yang melakukan *knock* ke *port* 1000 akan dimasukan ke kategori *address list knock*-1000 dan IP yang sudah melakukan *knock* lalu kemudian *login* ke mikrotik akan dimasukan ke kategori *save*-IP. Selain berhasil *login* ke router mikrotik menggunakan winbox, *login* ke router mikrotik menggunakan SHH dan wibfig juga berhasil dilakukan.



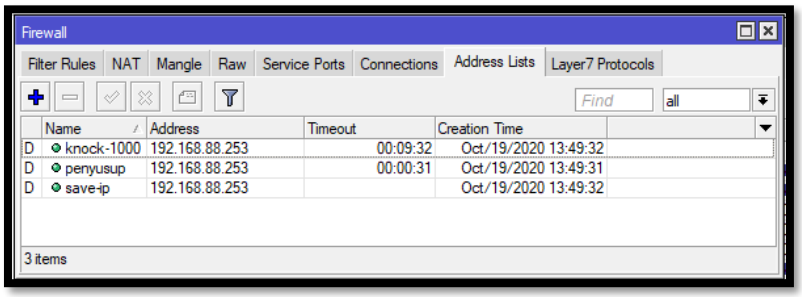
Gambar 6 Address list login pada winbox

Pengujian selanjutnya dilakukan tanpa melakukan *knock* ke *port* 1000 terlebih dahulu. Pada gambar IV.7 menunjukan kegagalan pada saat *login* ke router mikrotik menggunakan winbox, kegagalan ini karena *user* yang akan *login* ke router mikrotik tidak melakukan *knock* ke *port* 1000. IP yang melakukan *login* ke router mikrotik menggunakan winbox, SSH dan wibfig tanpa melakukan *knock* terlebih dahulu akan dikategorikan ke daftar penyusup.



Gambar 7 Pesan *error* saat *login* winbox

Pada saat *firewall rule* sistem kemanan *port knocking* diaktifkan tanpa membutuhkan waktu yang lama sistem akan langsung mendeteksi ip yang *login* pada winbox, SSH dan webfig. *User* yang *login* menuju router mikrotik melalui winbox, ssh dan webfig tanpa melakukan *knock* terlebih dahulu ke*port* yang sebeleumnya sudah ditentukan akan dimasukan ke *address list* dengan kategoroi penyusup. Dengan adanya pembatasan akes *login* melalu winbox, SSH dan webfig diharapkan dapat meminimalisir terjadinya akses masuk yang dilakukan oleh pikah yang tidak bertanggung jawab.



Gambar. 8 *Address list* dengan kategori IP penyusup

KESIMPULAN

Mengacu pada tujuan atau rumusan masalah dalam penelitian ini menghasilkan sebagai berikut:

1. Hasil dari pengelolahan manajemen *bandwidth* pada jaringan yang ada di Balai Desa Semali menggunakan metode *Hierarchical Token Bucket* (HTB) dinilai lebih efektif dalam membagi *bandwidth* secara adil dan merata kepada *client* yang diprioritaskan, terlihat dari pengujian yang dilakukan sebanyak tiga kali kepada empat *client* rata-rata *throughput* yang didapat pada pengujian pertama yaitu 23,14%, pengujian kedua 23,80%, dan pengujian ketiga 29,10%. Dari hasil pengujian kualitas *bandwidth* yang didapatkan *client* bisa dibilang stabil meskipun dalam keadaan *traffic* yang padat, sehinga *bandwidth* yang ada benar-benar dapat digunakan oleh *client* yang membutuhkan kualitas jaringan yang baik.
2. Setelah dilakukan pengujian kualitas *bandwidth* yang ada di Balai Desa Semali dengan parameter QOS, dan menerapkan metode HTB dan tanpa menggunakan metode HTB mendapat hasil akhir berupa perbedaan *throughput*. Nilai *throughput* dengan penerapan metode HTB mendapat nilai akhir 25,34% dengan indeks sedang, sedangkan *throughput* tanpa menerapkan metode HTB mendapat nilai akhir 11,75% dengan indeks tidak baik, perbedaan *throughput* tersebut menandakan penggunaan metode HTB untuk memanajemen *bandwidth* lebih baik dari pada tanpa menggunakan HTB karena jaringan yang menerapkan metode HTB telah menentukan batasan *bandwidth* pada saat *traffic* jaringan sedang padat sehingga *client* tetap dapat menggunakan jaringan internet dengan kualitas yang baik. Untuk nilai akhir hasil pengujian menggunakan metode HTB mendapat *packet loss* 2,10% dengan indeks sangat baik, *delay* 294ms dengan indeks baik dan *jitter* 30,50ms dengan indeks baik sedangkan untuk nila rata-rata hasil pengujian tanpa menggunakan metode HTB mendapat *packet loss* 1,76% dengan indeks sangat baik, *delay* 296ms dengan indeks baik dan *jitter* 47,30% dengan indeks baik. Pada parameter QOS *packet loss*, *delay* dan *jitter* tidak terdapat perbedaan yang signifikan karena ada faktor lain penyebab terjadinya *packet loss* disebabkan oleh *noise* atau kesalahan peralatan, terjadinya *delay* yang disebabkan oleh kepadatan aliran *traffic* pada jaringan sehingga mempengaruhi *jitter* dan membuat *buffer* penuh sebagai akibat antrian *packet*.
3. Pengujian kualitas *bandwidth* yang dilakukan dengan membebani *traffic* jaringan menggunakan *ping flood* yang menyebabkan *traffic* jaringan menjadi padat sehingga *bandwidth* yang seharusnya didapatkan client menjadi kurang maksimal namun dengan adanya manajemen *bandwidth* dengan metode HTB setiap IP client yang diprioritaskan akan tetap mendapatkan *bandwidth* karena pada metode HTB telah ditentukan batas maksimal pada saat *traffic* normal dan batas minimal pada saat *traffic* padat sehingga pada saat pengujian menggunakan metode HTB hasil akhir perhitungan dengan parameter QOS mendapatkan throughput sebesar 25,34 % dengan kategori sedang, sedangkan untuk pengujian tanpa menggunakan metode HTB mendapatkan nilai akhir throughput sebesar 11,75 %.
4. Berdasarkan hasil pengujian penerapan sistem keamanan *ping flood* pada jaringan mikrotik yang ada di Balai Desa Semali dapat merespons dengan baik ketika ada *ping* yang memadati jaringan yang menyebabkan meningkatnya *traffic* secara tiba-tiba sehingga kualitas *bandwidth* yang ada menurun. Respons dari sistem keamanan yaitu mengeblok ping yang memadati jaringan pada router mikrotik sehingga *traffic* yang tadinya padat menjadi normal kembali. Hasil dari beberapa kali pengujian dibutuhkan waktu empat detik untuk mengeblok *ping* yang sedang memadati jaringan yang menuju router mikrotik, sedangkan penerapan sistem *port knocking* yang membatasi akses *login* juga dapat dengan cepat merespon ketika ada seseorang yang akan melakukan *login* menuju router mikrotik, sehingga IP yang tidak dikenal akan dikategorikan sebagai penyusup, IP melakukan *login* tanpa melakukan *knock* membutuhkan waktu sekitar delapan detik sebelum akhirnya gagal *login* dan dimasukan kedalam daftar *address list* sebagai penyusup.

Saran

Adapun hal-hal yang menjadi saran sebagai pertimbangan untuk pengembangan jaringan yang ada agar menjadi lebih baik lagi adalah sebagai berikut:

1. Penggunaan manajemen *bandwidth* dengan metode HTB dapat dikombinasikan dengan metode *Per Connection Queue* untuk mencapai QOS yang lebih baik.
2. Membuat manajemen *hotspot* secara kompleks dan *interface* dengan menggunakan metode *Queue Tree*.
3. Sistem keamanan dapat ditingkatkan lagi dengan mengkombinasikan *firewall server* dan *proxy server.*

Daftar Pustaka

D. J. (2017). Kajian Vulnerability Keamanan Jaringan Internet Menggunakan Nessus. *Syntax Jurnal Informatika Vol. 6 No.*, 11-19.

Fauzi, A. R. (2018). Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan Ids. *Jurnal Manajemen Informatika. Volume 8 Nomor 2*, 11-17.

I. F., & A. F. (2018). Analisis Qos Pada Implementasi Manajemen Bandwith Menggunakan Metode Queue Tree Dan Pcq (Per Connection Queueing). *Jurnal Penelitian Teknik Informatika Universitas Prima Indonesia (Unpri) Medan Volume 1 Nomor 1*, 137-142.

Ichwan, M. I., L. S., & Yunanto, P. W. (2019). Analisis Manajemen Bandwidth Hierarchical Token Bucket (Htb) Dengan Mikrotik Pada Jaringan Smk Negeri 22 . *Jurnal Pinter Vol. 3 No. 2*, 122-126.

Putra, K. G., Gede, S. S., & Kesiman, M. W. (2020). Penerapan Manajemen Bandwidth Menggunakan Metode Hierarchical Token Bucket Pada Layanan Hotspot Mikrotik Undiksha. *Journal Of Computer Engineering System And Science Vol. 5 No. 1*, 146-154.

Y. A. (2017). Implementasi Intrusion Detection System Pada Rule Based System Menggunakan Sniffer Mode Pada Jaringan Lokal. *It Journal Research And Development Vol.2, No.1*, 43-50.