P-ISSN: 2548-9704
E-ISSN: 2686-0880

OPTIMALISASI MANAJEMEN TRAFIK DAN KEAMANAN DATA PADA JARINGAN *INTRANET* IBI-K 1957 DENGAN METODE *USER BEHAVIOUR ANALYSIS*

SYAMSU HIDAYAT[1], ASTRIED SILVANIE[2], AYUNI ASISTYASARI[3,] , YOSEP NURYAMAN[4]

Institut Bisnis dan Informatika Kosgoro 1957 [1,2] ,Universitas Bina Sarana Informatika [3,4]
Jl . Moch Kahfi II No. 33 Srengseng Sawah Jakarta Selatan[1,2] , Jl. Cileduk Raya No. 168 Pesanggrahan Jakarta Selatan[3,4]
Email : [1]syamsuhi3009@gmail.com, [2]astried.silvanie@gmail.com, [3]ayuni.yas@bsi.ac.id,[4]yosep.ynu@bsi.ac.id

ABSTRACT

The incident of a data breach at one of the national banks as a result of the merger of several Islamic banks in Indonesia for economic reasons has significantly increased concerns about the security of the data of all organizations, including educational organizations such as universities, where there are such as a personal data system and also educational data for the academic community, the open internet sharing systems enabled by universities are highly vulnerable to cyber attacks. For this reason, an optimization measure for the security of the campus network was implemented in this study and, in addition, the Internet connection was made more stable, as it is perceived as very slow at certain hours or during working hours. The use of Mikrotik as a network security tool designed to establish a network security fortress against intruders. In addition to the fact that Mikrotik devices are easy to obtain and inexpensive, and have good security features, the use of the method of analyzing user behavior consists in using a firewall to detect users who download activities with certain criteria are recorded and marked by the firewall , to then restrict access for the user. The. In addition to utilizing Mikrotik's firewall capabilities, the Queue feature is also used with the Simple Queue and Queue Tree methods. In the Simple Queue method, it designates one of the hosts whose bandwidth is limited, while in Queue Tree, it limits the network segments that provide users with maximum bandwidth limits and guarantees bandwidth. Both can be used side by side and work optimally.

Keywords: Firewall, Network Management Traffic, Simple Queue, Queue Tree, Mikrotik

ABSTRAK

Peristiwa pembobolan data yang dialami salah satu Bank Nasional hasil dari merger beberapa Bank Syariah di Indonesia dengan motif ekonomi sangat meningkatkan kepedulian atas keamanan data yang dimiliki oleh setiap organisa tidak terkecuali organisasi pendidikan seperti Universitas dimana terdapat sistem data kepegawaian dan juga data pendidikan civitas akademi, terbukanya sistem berbagi internet yang difasilitasi oleh kampus sangat rentan akan terjadinya serangan cyber. Untuk itu dalam peneliitian ini diterapkan sebuah kegiatan optimalisasi atas keamanan jaringan kampus, disamping itu untuk membuat koneksi internet lebih stabil dikarenakan disaat jam-jam tertentu atau jam kerja penggunaan dirasa sangatlah lambat. Penggunaan Mikrotik sebagai alat keamanan jaringan yang dimanfaatkan untuk dapat membuat suatu benteng keamanan jaringan dari para penyusup. Selain perangkat Mikrotik mudah didapat dan murah serta memiliki fitur keamanan yang baik.penggunaan metode user behavious

P-ISSN: 2548-9704
E-ISSN: 2686-0880

analysys dengan cara memanfaatkan firewal untuk dapat mendeteksi pengguna yang melakukan aktifitas download dengan kriteria tertentu maka akan dicatat dan di tandai oleh firewall untuk kemudian dilakukan suatu pembatasan akses atas pengguna tersebut. Selain dengan pemanfaatan fitur firewall pada Mikrotik juga digunakan fitur Queue dengan metode Simple Queue dan Queue Tree, untuk metode Simple Queue menentukan salah satu host yang akan dibatasi banwidthnya sedangkan untuk Queue Tree melakukan pembatasan secara segment network dimana memberikan batasan maksimal bandwith yang diterima penguguna dan jaminan bandwith. Keduanya dapat diterapkan beriringan dan sangat bekerja optimal.

Kata Kunci : Firewall, Manajemen Trafik Jaringan, Simple Queue, Queue Tree, Mikrotik

1. PENDAHULUAN

Keamanan data menjadi sangat penting baik bagi individu maupun organisasi. Berdasarkan kejadian kebocoran data yang dialami beberapa perusahaan nasional beberapa waktu lalu seperti yang dialami oleh salah satu bank milik BUMN hasil merger beberapa bank Syariah. Dengan motif ekonomi pelaku penyerangan meminta sejumlah uang untuk dapat memberikan password untuk membuka beberapa file yang sudah dikunci. Hal ini harus benar disadari dan menjadi perhatian bagi seorang yang menggeluti bidang *IT Security* bahwasanya data yang sudah terkoneksi dengan jaringan terlebih jaringan internet maka resiko untuk mengalami kebocoran sangat besar. Jadi harus dilakukan tindakan pencegahan untuk dapat meminimalisir kerugian yang besar. Jadi keamanan *computer* adalah sebuah tindakan atas usaha pencegahan dari upaya serangan pengguna yang mengakses computer jaringan yang tidak bertanggung jawab [1] Beberapa tindakan pencegahan dan deteksi dini harus dilakukan untuk menghindari pelaku yang tidak memiliki autoritas dalam sistem *computer* [2].

Penggunaan *Firewal* adalah satu cara dalam pengamanan *data* dalam suatu jaringan, *Firewall* tersedia dalam berbagai bentuk seperti *Software Firewall, Hardware Firewall,* dan *Cloud Firewall* . Dalam penelitian ini peneliti menggunakan salah satu produk *Firewall* dalam bentuk *hardware,* yakni *firewall* yang ada pada perangkat *RouterOS MIkrotik.* Penggunaan perangkat *Mikrotik* ini dikarenakan mudah ditemui dipasaran dan juga harganya terjangkau serta memiliki fitur-fitur keamanan yang baik tanpa harus ada biaya atas penambahan lisensi fitur-fitur tersebut.

Institut Bisnis dan Informatika Kosgoro 1957 (IBI-K57) sebagai lembaga pendidikan yang memiliki karyawan baik tenaga pengajar maupun *staff* umum juga mahasiswa. Menggunakan fasilitas internet dalam kegiatan sehari-harinya baik sebagai operasional kampus untuk *staff* umum maupun untuk proses belajar mengajar para dosen dan mahasiswa. Seiring banyaknya pengguna dalam satu area yang sama mengakibatkan jumlah *traffic* meningkat sehingga mempengaruhi performa koneksi *internet* yang dapat berakibat koneksi menjadi lambat , selain itu untuk mencegah penyebaran virus atau malware yang bisa terjadi karena aktifitas *sharing internet* dalam satu jaringan tidak menutup kemungkinan salah satu perangkat *computer* dari pengguna membawa *virus* atau *malware*. Pada penelitian sebelumnya yang dilakukan oleh [3] , mendapatkan hasil bahwa optimalisasi penggunaan *Mikrotik* pada perusahaan dapat membuat koneksi *internet* lebih stabil.

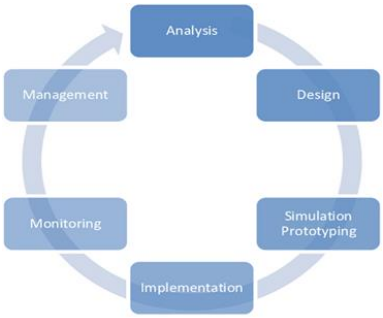
2. METODOLOGI PENELITIAN

2.1 Jenis Penelitian

Peneliti menggunakan beberapa metode dalam penelitian ini yakni

P-ISSN: 2548-9704
E-ISSN: 2686-0880

metode *Network Development Life Cycyle (NDLC)* dan juga metode *User Behavior Analytics*.penggunaan metode NDLC dalam penelitian ini untuk merancang atas perancangan yang telah dibuat atau sudah ada sebelumnya[4] dengan pendekatan kualitatif dimana semua kegiatan bermuara kepada hasil. Sedangkan metode *User Behavior Analytics* adalah sebuah alat analisa perilaku pengguna. Di era globalisasi ini penggunaan *User Behaviour Analytics* sangat penting , ini bisa dijadikan sebagai alat yang dapat membantu memperkuat kerangka kerja keamanan perusahaan [5]. Adapun metode ini peneliti gunakan untuk melihat tren penggunaan *bandwith* pengguna dalam kurun waktu tertentu dengan memanfaatkan fitur *firewall* pada *Mikrotik.*



Gambar 2.1. *Network Development Life Cycle*

Adapun objek dari penelitian ini adalah Manajemen trafik dan keamanan data pada jaringan Intranet kampus Institut Bisnis dan Informatika Kosgoro 1957 (IBI-K57) dengan memanfaatkan fitur *firewall* pada *Mikrotik.* Peneliti menggunakan pemodelan interaktif Miles dan Huberman untuk analisa, adapun diantaranya adalah dengan mengumpulkan data mentah untuk kemudian data tersebut ditampilkan dan dilanjutkan dengan mereduksi data hingga proses verifikasi dan perolehan kesimpulan atas data tersebut.

Berikut beberapa tahapan-tahapan dari penelitian yang sudah dikerjakan oleh peneliti :

1. Melalukan sesi wawancara dengan beberapa pimpinan, staff karyawan, dosen dan mahasiswa hal ini sebagai proses identifikasi mengenai pendapat mereka atas performa koneksi internet yang disediakan oleh kampus.
2. Memanfaatkan beberapa sumber seperti jurnal, buku, online artikel sebagai literatur dari penelitian yang sedang dilakukan.
3. Membuat gambaran sebuah kerangka pemikiran untuk dapat melakukan optimalisasi penggunaan fitur keamanan yang ada pada *Mikrotik.*
4. Melakukan sebuah simulasi atas kerangka rancangan yang sudah dibuat, hal ini untuk dapat dilakukan evaluasi sebelum implementasi dilakukan.
5. Melakukan evaluasi untuk segera dilakukan perbaikan atas kekurangan yang ditemukan pada saat proses simulasi.

2.2 Alur Kerja

Dibawah ini adalah gambar mengenai alur kerja dari penelitian yang dilakukan.

Gambar 2.2. Alur kerja penelitian

P-ISSN: 2548-9704
E-ISSN: 2686-0880

2.3. Literatur Penelitian

Peneliti mengambil beberapa penelitian sebelumnya sebagai sumber pustaka atas penelitian ini berikut adalah beberapa sumber yang berasal dari jurnal penelitian yang telah melakukan publikasi, buku pengetahuan, serta artikel online dari sumber yang dapat dipertanggungjawabakan, adapun beberapa penelitian sebelumnya yang peneliti jadikan sebagai literature adalah diantaranya sebagai berikut .

Penelitian yang dilakukan oleh [4] dengan penelitian yang berjudul Optimalisasi Jaringan Tunnel Menggunakan *RouterOS* Untuk Mendukung Kelangsungan Operasional PT. KLK Agriservindo di Masa Pandemik Covid-19. Adapun hasil dari penelitian ini adalah karyawan terbantukan untuk bekerja dari rumah selama masa pandemic dengan menggunakan fasilitas jaringan tunnel VPN optimalisasi perangkat *RouterOS.*

Penelitian yang dilakukan oleh [6] dengan penelitian berjudul Implementasi *Virtual Private Network* (VPN) Sebagai Solusi Security Selama *Work From Home*. Hasil dari penelitian ini adalah dengan penerapan Work From Home bagi karyawan menjadikan biaya *relative* murah.

Penelitian yang dilakukan oleh [7] dengan Judul Penelitian Manajemen *Bandwith* Pada *Mikrotik* Dengan Limitasi Bertingkat Menggunakan Metode *Simple Queue.* Mendapatkan Hasil bahwa penerapan limitasi dengan metode *Simple Queue* berfungsi dengan baik sebagai manajemen bandwith menggunakan *Router Mikrotik*. Penelitian yang dilakukan oleh [8] dengan judul penelitian yang berjudul Manjemen *Bandwith Internet* Menggunakan *Mikrotik Router* Di Politeknik Tri Mitra Karya Mandiri. Dalam penelitiannya menyimpulkan bahwa penerepan bandwith management dengan metode *Queue Tree* bisa mengatur besar kecilnya *bandwith* yang dibutuhkan oleh para pengguna secara dinamis.

Penelitian yang dilakukan oleh (Syahputra & Iqbal, 2022) dalam penelitiannya yang berjudul *Implementing Bandwith Management on Computer Networks Using Mikrotik Router*. Dalam penelitiannya memberikan kesimpulan bahwa penerapan metode Simple Quee untuk manajemen bandwith dapat melimitasi dengan baik untuk tiap-tiap pengguna.

Penelitian yang dilakukan oleh [10] dalam penelitannya yang berjudul Analisis Keamanan Jaringan Menggunakan Metode *Sniffing* dan Implementasi Keamanan Jaringan Pada Mikrotik RouterOS V6.48.3 Menggunakan Metode *Port Knocking*. Dalam hasil percobaan melakukan penyerangan dengan metode *Sniffing* attacker dalam hal ini menyimpulkan bahwa peneliti mendapatkan informasi penting yang dikirimkan oleh target tujuan ke penerima.

Penelitian yang dilakukan oleh (Devita & Hartika Zain, 2022) dalam penelitiannya yang berjudul *Development Of Mikrotik Router Bandwith Managemen Application.* Dalam penelitiannyanya memberikan kesimpulan Penerapan penjualan dan informasi atas produk secara daring memudahkan dalam proses penjualan produk.

2.4. Mikrotik

Mikrotik merupakan sebuah perangkat lunak dengan sistem operasi RouterOS. Perangkat lunak ini dapat di install dalam beberapa perangkat keras (*hardware*) baik dalam bentuk *Router Board* maupun kedalam sebuah komputer *server*. *Mikrotik* merupakan nama sebuah brand perangkat jaringan yang berasal dari Latvia digunakan untuk dapat mengatur jaringan baik jaringan local maupun jaringan internet. Adapun pada awal kemunculannya perangkat Mikrotik hanya digunakan oleh provider internet untuk memberikan distribusi layanan akses internet kepada para

P-ISSN: 2548-9704
E-ISSN: 2686-0880

pelanggan baik korporate maupun rumahan. Tetapi kini banyak digunakan oleh rumah tangga-rumah tangga dalam membagi konektivitas diantara anggota keluarga, karena perangkat *Mikrotik* dapat dengan mudah ditemukan dipasaran dengan harga terjangkau dan fitur keamanan yang dmiliki (Ghani, 2021).

2.5. Firewall

Firewall (Maiwald, 2003) adalah sebuah piranti lunak yang terdapat dalam jaringan yang berfungsi untuk melakukan monitoring lalu lintas data jaringan dan membuat sekat pemisah antara jaringan yang dipercaya dan jaringan yang tidak terpercaya. Fungsi *Firewall* adalah membloking semua lalu lintas tidak terpercaya untuk mengakses kedalam jaringan yang merupakan garis terdepan dalam pertahanan untuk melindungi jaringan, sistem dan data yang terdapat didalamnya.

2.6. Jaringan Komputer

Sofana (Iwan Sofana, 2013) dalam bukunya menyebutkan bahwa jaringan adalah suatu kumpulan yang terdiri atas beberapa interkoneksi dari sejumlah computer, atau dapat diterjemahkan bahwa jaringan komputer merupakan himpunan atas beberapa *computer* dan beberapa perangkat jaringan seperti *router, switch* dan lainnya. Adapun menurut para ahli bahwa jaringan terklasifikasi sebagai berikut :

a. Berdasarkan wilayah atau skala

b. Berdasarkan media yang menghantarkan

c. Berdasarkan fungsionalitasnya.

2.7. Queue Tree

Salah satu metode pembagian bandwith yang terdapat pada perangkat Mikrotik adalah *Queue Tree,* Teknik pada metode ini masuk kedalam advance karena dibutuhkan kemampuan teknik dalam melakukan *setup* atas perangkat Mikkrotik, didahului dengan melakukan penandaan *traffic input dan output* dari pengguna untuk kemudian dapat diketahui berdasarkan traffik tersebut trafik yang berasal dari pengguna mana yang harus dibatasi(Pendidikan, 2021).

2.8. Metode *Simple Queue*

Penerapan metode *Simple Queue* adalah metode *Queue* yang paling mudah pada *Mikrotik* kita dapat melakukan pengaturan atau limitasi bandwith yang digunakan oleh pengguna secara sederhana dengan mengacu pada *IP Address Client* dengan penentuan kecepatan *upload* dan download maksimum yang dapat digunakan oleh pengguna.

2.9. Metode User Behaviour Analystics

Penggunaan metode ini diterapkan pada *firewall* untuk dapat mendeteksi karakter pengguna yang menggunakan *bandwith* diluar kewajaran dalam kurun waktu tertentu misalnya dalam satu jam , misalkan dalam kurun waktu satu jam pengguna tersebut melebihi batas besaran download dan kecepatan yang digunakan maka secara automatis *firewall Mikrotik* akan mendaftarkan alamat *host* pengguna tersebut untuk dipantau atau dilakukan suatu eksekusi pembatasan akses internet.

3. HASIL DAN PEMBAHASAN

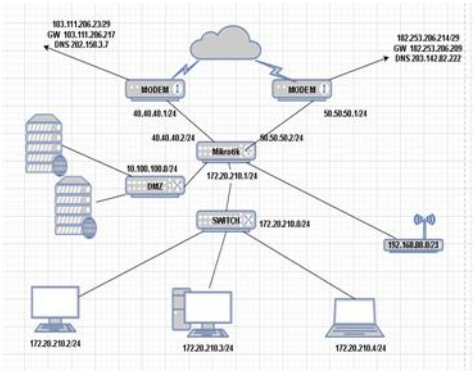
3.1. Penerapan Topologi Jaringan

Topologi jaringan yang diterapkan di Institut Bisnis dan Informatika Kosgoro 1957 (IBI-K57) adalah topologi *Tree.* Penggunaan topologi jenis ini dikarenakan merupakan perpaduan dari beberapa topologi jaringan diantaranya topologi Star dan topologi Bus,

P-ISSN: 2548-9704
E-ISSN: 2686-0880

bentuknya yang mirip pohon maka topologi ini disebut dengan topologi *Tree.* Dalam jaringan dengan topologi *Tree* ini sekumpulan computer host dan server terkoneksi oleh beberapa switch dengan hirarki yang berbeda. Dengan penempatan hirarki sebagaimana mestinya .Selain itu pemilihan topologi *Tree* dikarenakan memiliki beberapa kelebihan. Berikut adalah beberapa kelebihan dan juga beberapa kekurangan dari penggunaan topologi tree diantaranya adalah sebagai berikut (Towidjojo, 2012).

1. Kelebihan penerapan topologi *Tree*
    - Mudah untuk diimplementasikan dan dikembangkan dari cakupan jaringan yang kecil menjadi cakupan jaringan yang lebih luas.
    - Mudah dalam melakukan maintenance jika terdapat kendala kerusakan dan juga lebih baik dalam manajemen data
2. Kekurangan penerapan topologi *Tree*
    - Kinerjanya kurang optimal atau lambat
    - Fungsinya sangat tergantung dengan keberadaan dan fungsi switch.
    - Memerlukan investasi biaya yang lebih mahal karena membutuhkan lebih banyak perangkat jaringan *switch.*
    - Kendala pada *computer* yang terdapat pada hirarki yang tinggi dapat mempengaruhi computer yang berada ditingkat hirarki yang rendah.



Gambar 3.1 ***Network Topologi Tree***

3.2 Manajemen Trafik Jaringan

Didalam lingkungan kampus penggunaan koneksi internet oleh aktivis kampus baik, pejabat , staff , dosen dan mahasiswa sangatlah tinggi guna memenuhi kebutuhan atas data dalam kegiatan belaja mengajar dan operasional kampus. Terdapat 3 Jalur koneksi *internet* yang dibagi kepada aktivis kampus tersebut, untuk kantor kampus menggunakan jaringan kabel dengan perangkat computer desktop terhubung, sedangkan untuk mahasiswa diberikan akses internet melalui jaringan tanpa kabel (Wireless) dan untuk *server* aplikasi sistem menggunakan kabel terpisah (DMZ)

Penggunaan koneksi *internet* oleh Civitas akademi sebelum diterapkannya Manajemen *traffic* jaringan tidak terbatas, semua bisa mengakes semua situs dan aplikasi , melakukan unduhan file dengan kapasitas data yang tidak terbatas,dan dalam waktu kapan saja yang dapat menyebabkan lalulintas data menjadi naik tinggi dan mengakibatkan internet menjadi lambat, dan ini sangat tidak efisien. Lalu dengan diterapkannya Manajemen *Network Trafik* dengan menggunakan perangkat *RouterOS Mikrotik.* Kemudian selanjutnya dilakukan beberapa kegiatan diantaranya melakukan konfigurasi sistem keamanan dengan *Routerboard Mikrotik* menggunakan *tool* bawaannya yakni *winbox.*

P-ISSN: 2548-9704
E-ISSN: 2686-0880

a. Melakukan *setup* konfigurasi *IP Address* diantaranya untuk port WAN interface yang mengarah ke *Internet* dan *LAN interface* yang mengarah kepada jaringan *local*. Adapun Ip address antar interface yang mengarah ke tiap tiap jaringan menggunakan IP Address yang berbeda.

b. Agar perangkat MIkrotik dapat terhubung ke Internet dilakukan routing ke semua tujuan 0.0.0.0/0 melalui jalur yang melewati pintu keluar atau *gateway.*

c. Melakukan setup DNS agar perangkat dapat melakukan proses terjemahan atas suatu host tujuan dari *name server* ke ip *address*

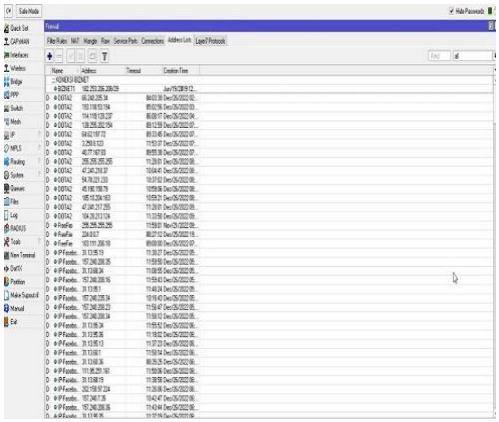
d. Melakukan segmentasi range ip dengan melakukan penentuan IP *Pool* yang dapat didistribusikan kepada *host-client* melalui *DHCP server* ke masing-masing jaringan pada masing-masing *interface.*

e. Membuat *DHCP Server* . Dengan menyesuaikan network IP Address yang akan didistribusikan kepada host-client.

f. Melakukan penandaan *traffic* dan *behavior* atas lalu linta data dari pengguna maupun paket yang diterima dari luar jaringan.

g. Melalukan *setup beberapa rule* untuk melakukan pendeteksian dan pencegahan atas aktivitas lalu lintas data yang berasal dari luar maupun dalam jaringan. Dengan penerapan *rule Policy Allow dan Block.*

h. Melalukan Setup pada fitur *Quee Tree* dalam melakukan suatu manajemen *bandwith* atas pengguna.



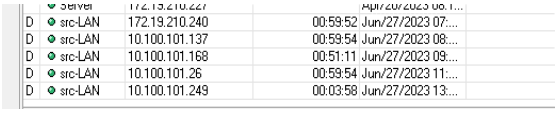
Gambar 3.2. *Address List* pada *RouterBoard*

Untuk dapat melihat traffik penggunaan *bandwith* oleh pengguna dengan menggunakan rule pada *firewall* dengan cara menetapkan sebuah *IP Addres* yang digunakan oleh pengguna melakukan aktivitas download *file* sebesar lebih dari 100 Mb dengan connection rate sebesar 1 Mbps sampai 100 Mbps. Dalam kurun waktu 1 jam, lalu bisa dilakukan automatisasi blocking atas koneksi yang berasal dari alamat-alamat tersebut atau dapat dimaukan kedalam pembatasan bandiwth dengan menggunakan metode simple queue yang mana ditujukan hanya untuk computer tersebut yang terindikasi menggunakan *bandwith internet* diluar kewajaran penggunaan.

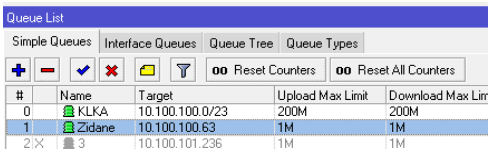
Gambar 3.3. Penandaan *Traffic* Pengguna

Setelah didapati *Ip Address* pengguna yang mengakses Internet dengan kapasitas diluar kewajaran maka selain dilakukan pemblokiran selama waktu terntentu maksimal 1 jam, bisa juga dengan melaikan pembatasan penggunaan *bandwith* menggunakan Metode *Simple Queue.*

P-ISSN: 2548-9704
E-ISSN: 2686-0880

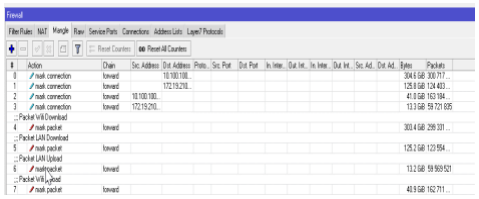


Gambar 3.4 Hasil Penandaan IP Pengguna



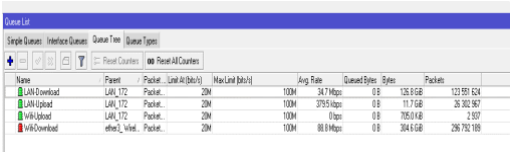
Gambar 3.5. *Limit Bandwith* dengan *Simple Queue*

Untuk pembagian secara rata menurut jaringan interface masing-masing maka digunakan pembagian *bandwith* dengan menggunakan metode *Queue Tree* . setiap pengguna mendapatkan secara rata pembagian bandwith dengan kecepatan maksimal sesuai dengan kapasitas bandwith yang dimiliki misal kampus menggunakan kapasitas bandwith sebesar 200 Mbps maka pengguna akan mendapatkan kapasitas *bandwith* sebesar itu selama hanya dia yang menggunakan koneksi *internet*, akan tetapi dia akan mendapat jaminan penggunaan *bandwith* jika jalur koneksi internet digunakan oleh banyak pengguna. Sebelumnya ditandai terlebih dahulu jalur masuk dan keluar menggunakan fitur mangle pada Firewall.



Gambar 3.6. Penandaan Trafik dengan *Mangle*

Lalu dilanjutkan dengan pembatasan bandwith berdasarkan interface jaringan local yang mengarah ke dan dari internet.



Gambar 3.7. *Limit Bandwith* dengan *Queue Tree*

3.3. Penerapan Keamanan Jaringan

3.3.1. Pengamanan Router

Sebelum penerapan keamanan atas jaringan maka dilakukan terlebih dahulu pengamanan atas *Router*. Adapun upaya pengamanan atas *router Mikrotik* adalah sebagai berikut :

a. *Disable service* yang tidak diperlukan.
b. Disable Macaddress network discovery.
c. Merubah *port-port service* dengan port yang tidak biasa.
d. Mendaftarkan *ip address* ataupun jaringan tertentu yang hanya dapat bisa mengakses *router.*
e. *Update Router* Periodik

3.3.2. Pengamanan Jaringan

Kemudian langkah selanjutnya adalah melakukan pengamanan atas jaringan yang berasal dan menuju dari internet. Diantaranya adalah.

a. Mengamankan jaringan dari *Virus* atau *Malware.*
b. Mengamankan jaringan dari penyusup.
c. Mengamankan jaringan dari penggunaan bandwith yang tidak efisien misalnya mengakses game atau aplikasi sosial media pada saat jam kantor berlangsung.
d. Mengamankan jaringan yang didalamnya terdapat *server* aplikasi dari akses pengguna dalam jaringan publik (*Wireless Public*) yang disedikan untuk digunakan mahasiswa dan civitas akademi lainnya.

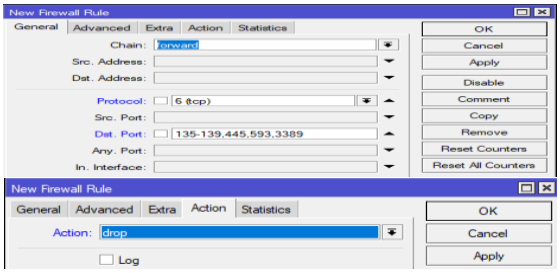
Atas informasi yang diberikan oleh *Microsoft*, bahwa serangan *malware* dengan memanfaatkan celah keamanan pda fitur SMB yang digunakan dalam file sharing di *Windows*, selain daripada itu *attacker* juga dapat menyerang melalui

P-ISSN: 2548-9704
E-ISSN: 2686-0880

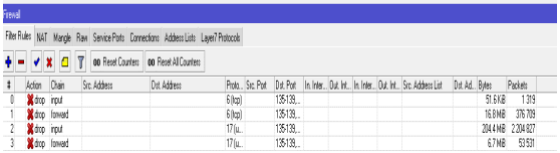
fitur RDP untuk RDP berjalan dijaringan pada protocol UDP port 137, 1378, dan TCP 137, 139, 445 sedangkan UDP mengunakan port 3389.

Gambar 3.8. *Ransomware Wannacry* (Sumber: citraweb.com)

Untuk mencegah penyebaran *malware* ini adalah dengan menerapkan *rule* pada *firewall* untuk mem*blocking* trafik yang melalui *port-port* tersebut.



Gambar 3.9. *Rule Blocking Traffic Malware*



Gambar 3.10. Tampilan hasil blocking *traffic Malware*

Dengan penerapan *rule* ini diharapkan setidaknya mencegah penyebaran *virus* dan *malware* terhadap perangkat komputer server ataupun *host client* dan juga koneksi *internet* lebih stabil dan bersih

4. KESIMPULAN

Dalam penelitian ini , peneliti mendapatkan hasil yang optimal atas pembagian bandwith dengan menggunakan dua metode yakni *Simple Queue* dan *Queue Tree*, yang mana diantara keduanya memiliki kelebihan masing-masing , simple queue untuk lebih mengkhususkan pembatasan atas salah satu host client sedangkan untuk *Queue Tree* diterapkan untuk satu *segmen* jaringan. Kemudian penerapan *rule* pada *firewall* guna untuk pengamanan jaringan atas berbagai serangan cukup efektik penggunaannya.

DAFTAR PUSTAKA

[1] John D. Howard and George Weaver, *An Analysis of security incidents on the internet*. 1997.

[2] Gollmann, *Computer Security"*. 1999.

[3] S. Hidayat *et al.*, "Optimalisasi jaringan tunnel menggunakan routeros untuk mendukung kelangsungan operasional PT. KLK Agriservindo di masa pandemik Covid-19," *Jurnal Sains dan Teknologi Widyaloka*, vol. 1, no. 1, pp. 1–14, doi: 10.54593/jstekwid.v1i1.44.

[4] S. Hidayat *et al.*, "Optimalisasi jaringan tunnel menggunakan routeros untuk mendukung kelangsungan operasional PT. KLK Agriservindo di masa pandemik Covid-19," *Jurnal Sains dan Teknologi Widyaloka*, vol. 1, no. 1, pp. 1–14, doi: 10.54593/jstekwid.v1i1.44.

[5] A. S. Patil and M. Oais Basit, "USER BEHAVIOUR ANALYSIS," *International Research Journal of Engineering and Technology*, 2020, [Online]. Available: www.irjet.net

[6] Subekti Rino, "IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN) SEBAGAI SOLUSI SECURITY SELAMA

P-ISSN: 2548-9704
E-ISSN: 2686-0880

WORK FROM HOME," *Jurnal Nasional Informatika*, vol. 1, pp. 57–65, Apr. 2020.

[7] M. Arya Darmawan, I. Fitri, and A. Iskandar, "MANAJEMEN BANDWIDTH PADA MIKROTIK DENGAN LIMITASI BERTINGKAT MENGGUNAKAN METODE SIMPLE QUEUE BANDWIDTH MANAGEMENT ON MIKROTIK WITH MULTILEVEL LIMITATIONS USING THE SIMPLE QUEUE METHOD," *Journal of Information Technology and Computer Science (INTECOMS)*, vol. 3, no. 2, 2020.

[8] Agus Darmadi EKo, "Manajemen Bandwidth Internet Menggunakan Mikrotik Router Di Politeknik Tri," 2019.

[9] K. W. Syahputra and M. Iqbal, "Implementing bandwidth management on computer networks using MIKROTIK router," 2022.

[10] R. Albar and R. O. Putra, "MENGGUNAKAN METODE PORT KNOCKING NETWORK SECURITY ANALYSIS USING THE METHOD SNIFFING AND IMPLEMENTATION OF NETWORK SECURITY ON MICROTIK ROUTER OS V6.48.3 USING PORT KNOCKING METHOD," *Journal of Informatics and Computer Science*, vol. 8, no. 1, 2022.

[11] R. Devita and R. Hartika Zain, "DEVELOPMENT OF MIKROTIK ROUTER BANDWIDTH MANAGEMENT APPLICATION," *INTERNATIONAL JOURNAL of DYNAMICS in ENGINEERING and SCIENCES (IJDES) LLDIKTI WILAYAH X*, vol. 7, no. 1, 2022, doi: 10.22216/jod.v7i1.1255.

[12] A. Ghani, "Jenis-Jenis Mikrotik," 2021. https://rumusbilangan.com/jenis-jenis-mikrotik/

[13] Eric. Maiwald, *Network security : a beginner's guide*. McGraw-Hill/Osborne, 2003.

[14] Iwan Sofana, *Membangun Jaringan Komputer : Mudah Membuat Jaringan Komputer (WIre & Wireless) Untuk Pengguna Windows dan Linux*. Bandung: Informatika, 2013.

[15] D. Pendidikan, "Mikrotik adalah," 2021. https://www.dosenpendidikan.co.id/mikrotik-adalah/

[16] R. Towidjojo, *Teori dan Implementasi Menggunakan Router Mikrotik*. Jasakom, 2012.