Blantika : Multidisciplinary Jornal
Volume 2 Number 1, Februari, 2023
p- ISSN xxxx-xxxx e-ISSN 2985-4199

ANALISIS PENINGKATAN KEAMANAN PADA *SIMPLE NETWORK TIME PROTOCOL* (SNTP) UNTUK MENDETEKSI *CYBERCRIME* DALAM AKTIFITAS JARINGAN MENGGUNAKAN METODE *FIREWALL*

Deddy Rezano Akhiruddin[1], Tata Sutabri[2]
Fakultas Ilmu Komputer Pasca Sarjana, Universitas Bina Darma, Indonesia[12]
rezanodeddy@gmail.com[1], tata.sutabri@binadarma.ac.id[2]

INFO ARTIKEL

Diterima: 15 Februari 2023
Direvisi: 20 Februari 2023
Disetujui: 25 Februari 2023

ABSTRAK

Sebuah Sistem Jaringan Komputer yang handal dan tangguh sangatlah diperlukan dalam membantu pelaksanaan tugas dan fungsi pokok organisasi pemerintahan, apalagi di era Teknologi Informasi yang terus berkembang dengan pesat seperti ini. Serangan terhadap keamanan sistem informasi (*security attack*) dan Kejahatan computer (*cybercrime)* seringkali terjadi dan dilakukan oleh sekelompok orang yang berusaha menembus suatu keamanan sebuah sistem untuk untuk mencari, mendapatkan, mengubah, dan bahkan menghapus informasi yang ada pada sistem tersebut. Tujuan dari penelitian ini adalah untuk menganalisa dan meningkatkan keamanan dalam mengenali jenis serangan yang sering terdapat di sistem jaringan dan memberikan proteksi seluruh komputer client dari segala serangan seperti *malware, virus, worm, Trojan* pada jaringan komputer Badan Pengelola Keuangan dan Aset Daerah Kabupaten Ogan Komering Ilir. Peneliti menggunakan Metode *Firewall* untuk mengontrol akses ke jaringan dan memblokir akses yang tidak diizinkan. Dalam konteks ini, *firewall* dapat digunakan untuk memblokir paket SNTP yang tidak valid atau yang berasal dari sumber yang tidak dikenal. Hasil akhir dari penelitian ini adalah sebuah sistem jaringan yang dikombinasikan dengan perangkat *MikroTik* dan *Firewall* untuk mengawasi serangan yang masuk ke dalam jaringan lokal.

Kata kunci: ***Cyber Crime; Firewall*; Keamanan Jaringan Komputer**

ABSTRACT

A reliable and robust computer network system is needed in assisting the implementation of the main tasks and functions of government organizations, especially in the era of information technology that continues to grow rapidly like this. Attacks on information system security (security attacks) and computer crimes (cyber crimes) often

occur and are carried out by a group of people trying to penetrate the security of a system to search, obtain, change, and even delete information on the system. The purpose of this study is to analyze and improve security in recognizing the types of attacks that are often found in network systems and to provide protection for all client computers from all attacks such as malware, viruses, worms, Trojans on the computer network of the Financial Management Agency and Regional Assets of Ogan Komering Ilir Regency. Researchers use the Firewall Method to control access to the network and block unauthorized access. In this context, a firewall can be used to block invalid SNTP packets or those from unknown sources. The end result of this research is a network system that is combined with MikroTik devices and firewalls to monitor incoming attacks on the local network.

Keywords: Cyber Crime; Firewal; Network Security; Computer Network System

PENDAHULUAN

Analisis peningkatan keamanan pada Simple Network Time Protocol (SNTP) merupakan hal yang penting dalam mendeteksi *cyber crime* di dalam aktivitas jaringan (Sutabri, 2023). Metode *firewall* digunakan untuk meningkatkan keamanan SNTP dengan cara mengontrol akses jaringan dan memblokir akses yang tidak sesuai dengan aturan yang ditentukan. Dengan menggunakan *firewall*, aktivitas jaringan dapat diawasi dan dianalisis untuk mendeteksi kegiatan yang tidak diinginkan seperti serangan (Prayudi & Kom, 2018). Analisis ini akan mengevaluasi efektivitas metode *firewall* dalam meningkatkan keamanan SNTP dan mengurangi risiko *crime* di dalam aktivitas jaringan.

Keamanan jaringan sangat penting karena jaringan merupakan sarana utama untuk berkomunikasi dan berbagi informasi dalam era digital saat ini (Sutabri, 2016). Menurut Tata Sutabri Sistem informasi adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian yang mendukung fungsi operasi organisasi yang bersifat manajerial dengan kegiatan strategi dari suatu organisasi untuk dapat menyediakan kepada pihak luar tertentu dengan laporan-laporan yang diperlukan (Sutabri, 2012, p. 46). Oleh karena itu, analisis ini akan memberikan pandangan secara mendasar tentang bagaimana cara meningkatkan keamanan jaringan SNTP dan mengurangi risik *crime* dengan menggunakan metode *firewall*. Dengan meningkatkan keamanan jaringan, diharapkan dapat meningkatkan efisiensi dan produktivitas dari aktivitas jaringan, serta meningkatkan rasa aman dan kepercayaan dari pengguna jaringan (Maulani, 2020). Modus kejahatan di dunia saat ini sangat beragam. Cara yang digunakan oleh

penyerang semakin beragam dan kompleks. Berbagai serangan tersebut melibatkan *malicious software* atau yang biasa disebut *malware* yang merupakan suatu program jahat (Hidayatulloh, 2014). Ancaman *malware* dan penyebarannya bisa melalui berbagai cara. Salah satu cara yang sering dilakukan untuk menyebarkan *malware* dengan cara menyisip-kannya di sebuah aplikasi ataupun *file* tertentu (Subandi, Sugara, & Aryani, 2022). Jadi keamanan sebuah sistem mutlak diperlukan dalam melindungi data dan informasi yang tersimpan didalamnya. Menurut Tata Sutabri (2003 : 18), data merupakan kenyataan yang menggambarkan suatu kejadian serta merupakan suatu kesatuan yang nyata, merupakan bentuk yang masih mentah sehingga perlu diolah lebih lanjut melalui suatu model untuk menghasilkan informasi (Sutabri, 2012).

Firewall didefinisikan sebagai satu atau lebih komponen yang berfungsi untuk membatasi akses antara jaringan yang dilindungi dan internet, atau antara beberapa jaringan lainnya. Dengan kata lain, *firewall* bertindak sebagai penghalang yang dapat membatasi atau mengendalikan akses ke jaringan yang dilindungi dari luar atau antara beberapa jaringan yang berbeda. Fungsi *firewall* adalah untuk melindungi jaringan dari ancaman dan serangan yang dapat membahayakan keamanan jaringan dan sistem yang terhubung ke dalamnya (Mardiyati, 2015). *Firewall* merupakan solusi untuk mengatasi tantangan keamanan di dunia internet, baik itu keamanan komputer maupun keamanan jaringan. Saat ini, internet dihadapkan pada berbagai ancaman dari dalam maupun luar, sehingga firewall menjadi salah satu cara untuk melindungi data dan sistem yang terhubung pada jaringan. Dengan melakukan konfigurasi yang tepat pada firewall, keamanan data atau komputer dalam jaringan dapat terjamin dengan lebih baik. Dengan demikian, firewall sangat penting dalam menjaga keamanan jaringan dan melindungi sistem dari berbagai jenis ancaman yang muncul pada internet (Purwaningrum, Darmadi, & Purwanto, 2018). Konfigurasi firewall adalah proses mengatur aturan akses yang akan diterapkan pada perangkat firewall. Firewall dapat dikonfigurasi untuk mengizinkan atau menolak akses jaringan berdasarkan kriteria yang ditentukan, seperti alamat IP, protokol jaringan, atau port (Sutabri, Wijaya, Seprina, & Amalia, 2023). Semua konfigurasi firewall yang digunakan harus sesuai dengan kebutuhan dan kondisi jaringan yang digunakan dan diperbarui secara berkala untuk menjamin kontinuitas dan keamanan jaringan yang lebih baik. Dengan meningkatkan keamanan pada jaringan komputer kantor yang kita miliki kita dapat melakukan pencegahan dengan terkelola sehingga dapat membantu tim keamanan dan IT Infrastruktur Jaringan. Dengan memperbaharui *Simple Network Time Protocol* dapat memberikan dukungan dan pemantauan multiregional se-panjang waktu, serta merespon ancaman secara langsung bila diperlukan (Sitompul, 2012). Keamanan jaringan yang ada Badan Pengelola Keuangan dan Aset Daerah Kabupaten Ogan Komering Ilir masih membutuhkan pengembangan agar dapat menyesuaikan dengan kemajuan teknologi dan mampu mengurangi resiko segala bentuk serangan yang mungkin bisa masuk ke dalam sistem jaringan. MikroTik router adalah salah satu sistem operasi yang dapat digunakan sebagai router jaringan yang handal, mencakup berbagai fitur lengkap untuk jaringan dan wireless

serta dapat juga berfungsi sebagai firewall (Langobelen, Rachmawayi, & Iswayudi, 2019).

SNTP (*Simple Network Time Protocol*)

Adalah protokol jaringan yang digunakan untuk menyinkronisasikan waktu dalam jaringan komputer. SNTP digunakan untuk menyinkronisasikan waktu pada sistem yang menggunakan protokol NTP (*Network Time Protocol*) yang lebih kompleks. SNTP hanya mengirim dan menerima paket waktu yang sederhana dan tidak memiliki fitur seperti algoritma koreksi waktu yang canggih seperti NTP. Namun, SNTP cukup efektif dalam menyinkronisasikan waktu pada jaringan yang tidak terlalu kompleks dan tidak memerlukan ketelitian yang tinggi. Komputer yang menggunakan *Simple Network Time Protocol* (SNTP) dapat terhubung ke server waktu yang menyediakan waktu yang sesuai dengan standar waktu yang ditentukan. Server waktu ini dapat diakses melalui jaringan internet atau jaringan lokal. Komputer yang menggunakan SNTP dapat menyinkronisasikan waktu dengan server waktu tersebut dengan mengirim permintaan waktu dan menerima paket waktu yang diterima dari server. Kemudian komputer akan menyesuaikan waktu sistem lokalnya sesuai dengan perbedaan waktu yang diterima dari server. SNTP dapat digunakan pada berbagai sistem operasi seperti *Windows*, *Linux*, dan *Mac* OS. Banyak perangkat keras juga dilengkapi dengan dukungan SNTP, seperti *router*, *firewall*, *switch*, dll. Beberapa perangkat *embedded system* juga menggunakan SNTP untuk menyinkronisasikan waktu. SNTP dapat digunakan pada berbagai jenis jaringan, mulai dari jaringan lokal hingga jaringan global. SNTP juga dapat digunakan pada jaringan yang tidak terlalu kompleks dan tidak memerlukan ketelitian yang tinggi, seperti jaringan kantor atau jaringan rumah .

Firewall

Firewall atau yang bila diartikan kedalam Bahasa Indonesia berarti Dinding Api adalah sebuah sistem atau perangkat yang memberikan izin dalam suatu lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Pada umumnya, sebuah *Firewall* diterapkan dalam sebuah mesin yang berjalan pada suatu *gateway* antara jaringan lokal dan jaringan lainnya. *Firewall* juga digunakan untuk mengontrol akses terhadap apapun yang memiliki akses terhadap jaringan pribadi dari pihak luar. Saat ini banyak perusahaan yang memiliki akses ke internet, maka perlindungan terhadap modal digital perusahaan tersebut dari serangan orang-orang yang tidak bertanggung jawab, mata-mata, ataupun pencuri data lainnya menjadi hal yang penting. Menurut Rendra Towidjojo (2013), *firewall* adalah perangkat yang berfungsi untuk memeriksa dan menentukan paket data yang diizinkan untuk masuk atau keluar dari suatu jaringan. Dengan kemampuan untuk memilih paket data mana yang dapat melewati jaringan, *firewall* bertindak sebagai pelindung jaringan dari serangan yang berasal dari luar jaringan. Selain itu, firewall juga dapat digunakan untuk melindungi satu host atau yang biasa disebut sebagai single host. Dengan demikian, fungsi utama firewall adalah untuk mengamankan jaringan dari ancaman luar dan melindungi host dari serangan yang dapat merusaknya.(Naufal, Vahlevi, Widayana, Zulfa, & Juardi, n.d.).

Mikrotik

Menurut Rendra Towidjojo pada tahun 2013, *Mikrotik* berasal dari kata "mikrotikls" dalam bahasa Latvia yang berarti "jaringan kecil". Ada dua jenis *Mikrotik* yang tersedia, yaitu perangkat keras (Routerboard) dan perangkat lunak (RouterOS). Mikrotik terkenal sebagai router, yaitu perangkat jaringan yang digunakan untuk menghubungkan beberapa jaringan dan memilih rute untuk paket data dalam jaringan yang lebih kompleks. Menurut Tim Citraweb pada tahun 2014, *Mikrotik RouterOS* adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer sebagai router jaringan yang handal. Ini dilengkapi dengan berbagai fitur untuk jaringan IP dan jaringan nirkabel, yang cocok untuk digunakan oleh ISP dan provider hotspot. *Winbox* adalah perangkat lunak khusus yang dirancang untuk mengkonfigurasi router *Mikrotik* dengan antarmuka pengguna grafis (*Graphic User Interface*). Perangkat lunak *Winbox* bekerja pada port 8291 dan dapat diunduh secara gratis melalui situs web http://www.mikrotik.com/download (Irawan, Djaohar, & Duskarnaen, 2018).

Virus dan *Malware*

Virus komputer merupakan program komputer yang memiliki kemampuan untuk memperbanyak diri dengan menambahkan sebagian atau seluruh kode programnya ke dalam program lainnya. Akibatnya, program yang terinfeksi akan mengalami gangguan dan berjalan dengan lambat. *Malware* atau perangkat lunak jahat adalah jenis perangkat lunak yang diciptakan dengan tujuan untuk merusak atau mengganggu kinerja sistem operasi komputer. Dalam hal ini, Malware dapat melakukan berbagai hal seperti mencuri informasi data penting atau bahkan mengambil alih kontrol komputer target tanpa seizin pemiliknya. *Malware* bisa berbentuk *script*, kode, konten aktif, ataupun perangkat lunak. (Ryansyah & Maulana, 2018).

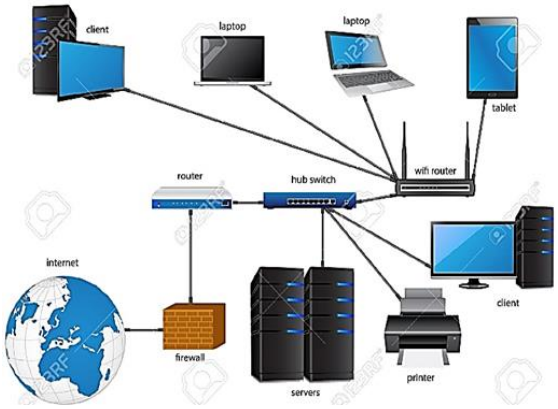
Port

Port adalah sebuah terminologi dalam komputer yang mengacu pada sebuah jalur komunikasi yang digunakan untuk menghubungkan komputer dengan perangkat lain seperti printer, scanner, atau jaringan. Setiap perangkat yang terhubung ke komputer memiliki nomor port yang unik yang digunakan untuk mengidentifikasi perangkat tersebut dan mengatur aliran informasi ke dan dari perangkat tersebut. Port bisa diartikan sebagai titik masuk dan keluar informasi pada sebuah computer. Port scanning adalah suatu teknik untuk mengidentifikasi port yang terbuka pada sebuah komputer. Meskipun *port* memiliki penggunaan yang sah dalam mengelola jaringan, melakukan port scanning juga dapat menjadi potensi bahaya bagi komputer Anda. Sebab, seseorang yang melakukan port scanning bisa saja mencari celah untuk masuk ke dalam sistem komputer Anda dan menemukan titik akses yang lemah untuk masuk ke komputer Anda. (Pratiwi, 2018).

Internetworking

Internetworking adalah proses menghubungkan dua atau lebih jaringan komputer agar dapat saling berkomunikasi. Hal ini dilakukan dengan menggunakan perangkat seperti router, switch, atau gateway untuk menghubungkan jaringan yang

berbeda. Internetworking memungkinkan pembagian sumber daya jaringan, peningkatan keamanan, dan peningkatan fleksibilitas dalam mengelola jaringan. Internetworking juga memungkinkan komunikasi antar jaringan yang berbeda jenis seperti LAN, WAN, dan jaringan internet. TCP/IP (*Transmission Control Protocol/Internet Protocol*) bertujuan untuk membangun suatu koneksi antar jaringan (*network*), dimana biasa disebut internetwork, atau intenet, yang menyediakan pelayanan komunikasi antar jaringan yang memiliki bentuk fisik yang beragam. Tujuan yang jelas adalah menghubungkan empunya (*hosts*) pada jaringan yang berbeda, atau mungkin terpisahkan secara geografis pada area yang luas. TCP/IP adalah sebuah standar jaringan terbuka yang bersifat independen terhadap prosedur transport jaringan fisik yang digunakan, sehingga dapat digunakan di mana saja. Protokol ini memakai skema pengalamatan yang sederhana yang disebut sebagai alamat IP (*IP Address*) yang mengizinkan hingga beberapa ratus juta komputer untuk dapat saling berhubungan satu sama lainnya di Internet. Protokol ini juga bersifat routable yang berarti protokol ini cocok untuk menghubungkan sistem-sistem berbeda (seperti *Microsoft Windows* dan keluarga *UNIX*) untuk membentuk jaringan yang heterogeny.



Gambar 1. Jaringan Internet

METODE PENELITIAN

Metode yang digunakan pada penelitian ini adalah studi pustaka atau studi kepustakaan adalah teknik pengumpulan data dengan melakukan penelaahan terhadap buku, literatur, catatan, serta berbagai laporan yang berkaitan dengan masalah yang ingin dipecahkan. Berikut beberapa tahapan dari penelitian ini, yaitu:

1. Studi Literatur dan Pengumpulan Data. Merupakan proses membaca sejumlah referensi yang rata-rata berupa tulisan (baik buku, artikel, jurnal, dan lain-lain) yang nantinya dijadikan sebagai sumber rujukan untuk tulisan yang disusun serta melakukan pengumpulan informasi yang berhubungan dengan penelitian yang dilakukan.
2. Perancangan Sistem Jaringan, adalah melakukan persiapan untuk merancang jaringan atau sering disebut rancang bangun jaringan yang menggambarkan bagaimana jaringan dibentuk, dapat berupa penggambaran, perencanaan, dan pembuatan sketsa atau pengaturan beberapa elemen terpisah ke dalam satu

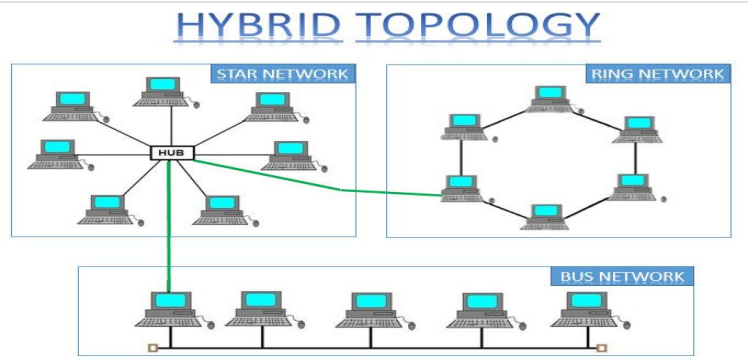
kesatuan yang utuh, termasuk mengkonfigurasikan komponen *software* dan hardware suatu jaringan.

3. Implementasi Jaringan adalah penerapan dan mengimplementasika rancang bangun jaringan yang sudah dibuat kemudian melakukan instalasi hardware dan software yang dibutuhkan untuk membentuk sistem jaringan lalu menginterkoneksikannya. Selanjutnya dilakukan konfigurasi mikrotik untuk membuat pengaturan baru firewall mikrotik.

HASIL DAN PEMBAHASAN

Gambaran Umum

Setiap lembaga atau organisasi mengadopsi komputasi heterogen yang melibatkan teknologi jaringan yang berbeda-beda. Salah satu teknologi jaringan yang paling umum digunakan adalah jaringan area lokal (LAN) (Amin et al., 2022). Terdapat berbagai teknologi yang digunakan dalam jaringan ini, dimana tiga topologi yang umum digunakan adalah bintang, ring, dan bus. Salah satu teknologi LAN yang paling umum digunakan adalah Ethernet dengan topologi busnya. Jaringan Komputer pada Badan Pengelola Keuangan dan Aset Daerah Kabupaten Ogan Komering Ilir menggunakan topologi jaringan Hybrid. Topologi *hybrid* adalah gabungan dari beberapa topologi berbeda yang membentuk jaringan baru (Hamzah & Rachmawati, 2018). Dengan kata lain, jika ada dua atau lebih topologi yang berbeda dan terhubung dalam satu jaringan, maka topologi jaringan tersebut akan membentuk topologi *hybrid*. Kelebihan topologi ini ialah ia bersifat fleksibel dan penambahan koneksi pada topologinya sangat mudah. Namun, proses instalasi memakan biaya yang banyak dan pengaturannya cukup rumit. Manajemen pada topologi ini pun sangat sulit untuk dilakukan.



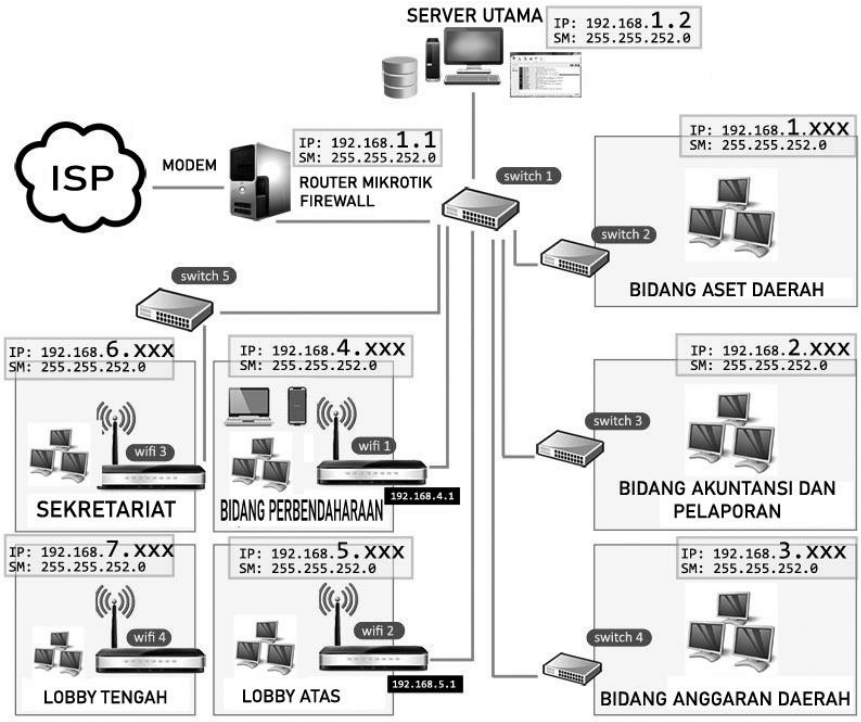
Gambar 2. Topologi Jaringan *Hybrid*

Setiap paket data melakukan perjalanan dari awal hingga akhir dengan melalui dua protokol yang berbeda dan menggunakan port TCP dan UDP Banyak terdapat 65.536 port yang berbeda yang dapat digunakan. Orang yang tidak bertanggung jawab sering melakukan pemindaian pada komputer korban untuk mengetahui port mana yang aktif dan mana yang tidak aktif. Setelah

identifikasi port terbuka oleh penyerang atau penyusup, mereka akan melanjutkan tindakan mereka. dapat mempersempit serangan ke jenis port tertentu di masa mendatang. Lain kali serangan port terjadi ketika penyerang mengirim paket ke mesin, mengubah port tujuan, penyerang dapat mengetahui layanan apa yang kami jalankan dan mendapatkan ide bagus tentang OS apa yang kami miliki. Banyak situs web saat ini melakukan pemindaian port sebanyak 12 kali atau lebih dalam satu hari atau satu jam. *Firewall* perlu mengawasi kegiatan ini karena sering kali komputer jarak jauh terhubung ke beberapa port secara simultan (Cahyanto, 2017).

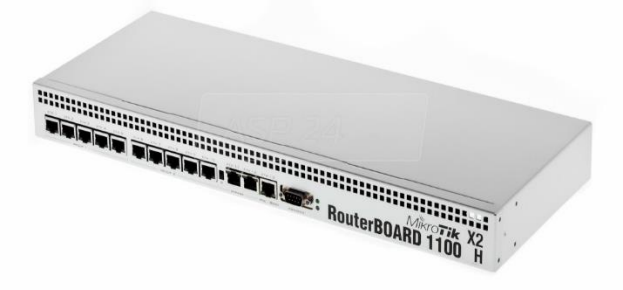
Rancangan Topologi Jaringan

Topologi jaringan yang dibuat pada penelitian ini adalah jaringan dengan router board Mikrotik, ISP (*Internet Service Provider*) dan beberapa client diantaranya server lokal, WLAN (*Wireless Local Area Network*) dan LAN (*Local Area Network*) (Kurniawan, 2016). Internet akan langsung masuk ke jaringan router, yang kemudian dibagi menjadi beberapa segmen yang dihubungkan oleh switch, tergantung letak ruangan dan lantai bangunan. Selain menggunakan switch jaringan, juga menempatkan beberapa titik akses di setiap lantai, dengan segmen alamat IP yang berbeda tergantung ruang. Secara keseluruhan, konstruksi topologi jaringan ditunjukkan pada Gambar 3.



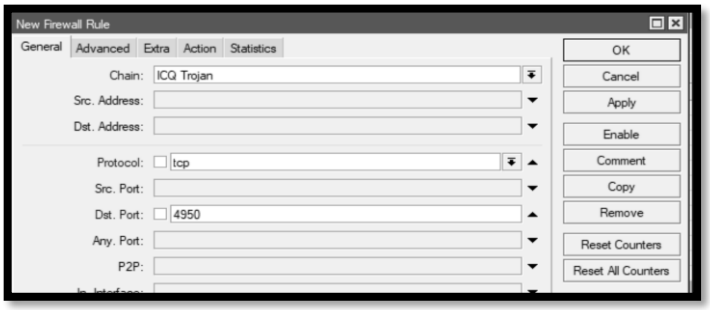
Gambar 3. Topolagi Jaringan BPKAD Kab. OKI

Dalam penelitian ini penulis menggunakan *router* mikrotik *tipe* RB1100 AHx2, yang memiliki 13 buah port gigabit ethernet, 1066 Mhz *network* processor, 2 buah switch chip dan 2 buah port "auto by pass on failure" dan casing 19 1U rackmount serta ada satu slot kartu microSD. Termasuk lisensi Mikrotik *Router* OS level 6 serta memiliki RAM 1GB. *Router* ini memiliki spesifikasi yang cukup baik dikarenakan dapat untuk pengembangan jaringan.



Gambar 4. *Router Mikrotik Tipe RB1100 AHX2*

A. Implementasi Jaringan Dengan *Firewall* Mikrotik



Gambar 5. Pengaturan *Firewall* baru Mikrotik

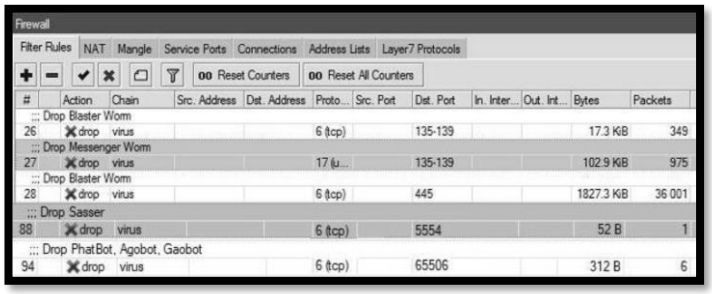
Untuk masuk kedalam penambahan rule pada pengaturan *firewall* maka dibutuhkan akses sebagai admin utama pada router board kemudian menambahkan rule seperti gambar diatas.

Gambar 6. Pengaturan *Firewall Mikrotik*

Ini merupakan metode untuk membuat peraturan *firewall* sesuai dengan nama virus atau malware, protocol dan port. Bisa juga dengan menggunakan perintah / *ip firewall filter add chain= ICQ Trojan protocol=tcp dst-port=4950 action=drop comment="ICQ Trojan"*, maka akan didapatkan hasil seperti gambar dibawah ini.

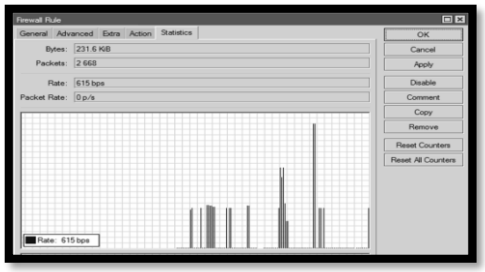
Gambar 7. Hasil Pengaturan *Firewall* pada *Mikrotik*

Metode ini sudah tersedia di router mikrotik, dan hasil pengaturan yang sudah dibuat ditampilkan pada gambar di atas. Sedangkan, untuk penambahan rule malware atau virus dengan *port-port*nya dan berbagai jenis *malware* dan virus lainnya bisa dikaji dan didapatkan dari berbagai sumber lainnya dikarenakan jumlah malware dan port yang terus bertambah (Ryansyah & Maulana, 2018). Dari hasil analisis ini, dengan melihat *byte* dan paket serta statistik dinyatakan bahwa terdapat lalu lintas malware pada jaringan. Dengan hasil analisa yang telah dikaji dan dipelajari, dapat dijelaskan bahwa malware ada pada setiap pengguna atau perangkat komputer yang digunakan dan router dapat mematikan akses malware sebelum menyebar ke seluruh jaringan, mencegah perangkat atau pengguna lain diserang oleh *malware* tersebut.



Gambar 8. Hasil pengaturan *firewall* baru di *mikrotik*

Untuk melihat statistik malware yang ada atau melintas didalam jaringan dapat dilihat pada tab menu statistics yang ada pada menu *firewall* di *mikrotik*.



Gambar 9. *Firewall Rule Mikrotik*

Hasil analisa dari analisa dan kajian penelitian ini sangat bermanfaat karena ternyata bukan hanya dari faktor bandwidth saja yang bisa membuat akses jaringan menjadi lambat melainkan ada faktor lain yang membuat lalu lintas jaringan menjadi padat dan besar seperti halnya serangan malware atau virus dari luar ataupun dalam jaringan. Dengan adanya metode *firewall* mikrotik seperti ini maka hasil analisa dari penelitian ini dapat segera diimplementasikan sehingga meminimalisir resiko gangguan akses pada lalu lintas jaringan Badan Pengelola Keuangan dan Aset Daerah Kabupaten Ogan Komering Ilir.

KESIMPULAN

Berdasarkan hasil analisa dari penelitian ini, dapat ditarik beberapa kesimpulan sebagai berikut: Dengan adanya fitur *firewall* filter *rules* mikrotik yang telah dikonfigurasi pada *Simple Network Time Protocol* (SNTP) akan dapat mendeteksi ancaman dari crime seperti serangan Malware atau Virus yang berpotensi mengganggu lalu lintas jaringan. Dengan dimplementasikannya metode ini maka jaringan komputer pada BPKAD Kab. OKI akan lebih aman dari gangguan *crime*, akses yang lebih cepat dan stabil bagi setiap pengguna yang terhubung pada jaringan. Dengan adanya *firewall* dalam suatu sistem jaringan *computer* diharapkan dapat melindungi informasi-informasi penting dandapat memanajemen lalu lintas pengaksesan dari dalam maupundari luar sistem. Guna meningkatkan kinerja seluruh bagian-bagian terkait mencapai kemaksimalan suatu koneksi atau jaringan dari dalam maupun luar yang memberi efek menguntungkan bagi si pengguna

DAFTAR PUSTAKA

Amin, Muhammad, Raja, Harmonvikler Dumoharis Lumban, Nur, Muh Nadzirin Anshari, Prasetio, Adhi, Sulaiman, Oris Krianto, Karim, Abdul, Muttaqin, Muttaqin, Sihotang, Jay Idoan, Simarmata, Janner, & Jamaludin, Jamaludin. (2022). *Teknologi Jaringan Nirkabel*. Yayasan Kita Menulis.

Cahyanto, Triawan Adi. (2017). *Praktikum Mata Kuliah Keamanan Komputer*.

Hamzah, Amir, & Rachmawati, Rr Yuliana. (2018). Rancangan Infrastruktur Jaringan Backbone Hybrid Di Tiga Kampus IST AKPRIND Yogyakarta. *Jurnal Jarkom*, *6*(1), 34–41.

Hidayatulloh, Syarif. (2014). Analisis dan optimalisasi keamanan jaringan menggunakan protokol ipsec. *Jurnal Informatika*, *1*(2).

Irawan, Garry Tria, Djaohar, Mochammad, & Duskarnaen, M. Ficky. (2018). Perancangan Dan Implementasi Sistem Keamanan Jaringan Menggunakan Firewall dan Web Proxy Berbasis Mikrotik di SMA Negeri 1 Kota Sukabumi. *PINTER: Jurnal Pendidikan Teknik Informatika Dan Komputer*, *2*(1), 27–32.

Kurniawan, Rudi. (2016). Analisis Dan Implementasi Desain Jaringan Hotspot Berbasis Mikrotik Menggunakan Metode NDLC (Network Development Life Cycle) Pada BPU Bagas Raya Lubuk Linggau. *JURNAL ILMIAH BETRIK: Besemah Teknologi Informasi Dan Komputer*, *7*(01), 50–59.

Langobelen, Efrahim Sinyo Rio Ola Balen, Rachmawayi, Rr Yuliana, & Iswayudi, Catur. (2019). Analisis Dan Optimasi Dari Simulasi Keamanan Jaringan Menggunakan Firewall Mikrotik Studi Kasus Di Taman Pintar Yogyakarta. *Jurnal Jarkom*, *7*(2), 95–102.

Mardiyati, S. R. I. (2015). Mengoptimalkan Suatu Sistem Firewall Pada Jaringan Skala Global. *Faktor Exacta*, *7*(1), 72–83.

Maulani, Wihda. (2020). Penerapan Electronic Government Dalam Peningkatan Kualitas Pelayanan Publik (Studi Kasus Program E-Health Di Kota Surabaya). *AS-SIYASAH: Jurnal Ilmu Sosial Dan Ilmu Politik*, *5*(2), 44–54.

Naufal, Farhan Muhammad, Vahlevi, Muhammad Rizal, Widayana, Arif, Zulfa, Muhammad Luthfi, & Juardi, Didi. (n.d.). Implementasi Keamanan Hostpot Menggunakan Proxy dan Firewall Dalam Mengatasi Resiko Ancaman Serangan. *Jurnal Ilmiah Rekayasa Dan Manajemen Sistem Informasi*, *8*(2), 148–154.

Pratiwi, Dwi. (2018). Penerapan Metode Filtering Video Streaming dan Malware Pada Jaringan Local Area Network. *SISTEMASI*, *7*(3), 230–237.

Prayudi, Yudi, & Kom, M. (2018). *Simulasi Untuk Peningkatan Keamanan Data Pada Metarouter Yang Sudah Tereksploitasi*. Universitas Islam Indonesia.

Purwaningrum, Fajar Adhi, Darmadi, Eko Agus, & Purwanto, Agus. (2018). Optimalisasi jaringan menggunakan firewall. *Ikraith-Informatika*, *2*(3), 17–23.

Ryansyah, Muhamad, & Maulana, Muhammad Sony. (2018). Malware Security Menggunakan Filtering Firewall Dengan Metode Port Blocking Pada Mikrotik RB 1100AHx2. *JUSTIN (Jurnal Sistem Dan Teknologi Informasi)*, *6*(3), 116–120.

Sitompul, Josua. (2012). *Cyberspace, cybercrimes, cyberlaw: tinjauan aspek hukum pidana*. PT Tatanusa.

Subandi, Kotim, Sugara, Victor Ilyas, & Aryani, Adriana Sari. (2022). Peningkatan Keamanan Pada Simple Network Time Protocol (SNTP) Untuk Menditeksi Cyber Crime di dalam Aktifitas Jaringan. *Prosiding Semnastek*.

Sutabri, Tata. (2012). *Analisis sistem informasi*. Penerbit Andi.

Sutabri, Tata. (2016). *Sistem Informasi Manajemen (Edisi Revisi)* (2nd ed.). Yogyakarta: Andi.

Sutabri, Tata. (2023). Design of A Web-Based Social Network Information System. *International Journal of Artificial Intelligence Research*, *6*(1.1).

Sutabri, Tata, Wijaya, Alex, Seprina, Iin, & Amalia, Rahayu. (2023). Ticket Reservation System Design with Web-Based. *International Journal of Artificial Intelligence Research*, *6*(1.1).