Volume 2 No. 1 2025, 74 - 81
DOI : https://doi.org/10.62335

Indonesian Journal of Community Empowerment
https://manggalajournal.org/index.php/maju
E-ISSN 3032-369X

KOLABORASI MAHASISWA DAN PT PROXI DALAM PENGEMBANGAN KEAHLIAN KEAMANAN JARINGAN UNTUK MENDUKUNG TRANSFORMASI DIGITAL YANG AMAN

Tirawati[1], Gina Purnama Insany[2]

[1,2]Program Studi Teknik Informatika, Universitas Nusa Putra Sukabumi, Jawa Barat

E-mail: tirawati_ti21@nusaputra.ac.id

ARTICLE INFO

Article history:
Received :23-12-2024
Revised :-04-01-2025
Accepted: 11-01-2025

Key words: *Network Security , Digital Transformation , Mikrotik , Firewall , Industry Collaboration*

DOI: *https://doi.org/10.62335*

ABSTRACT

This community service activity aims to improve students competence in network security strategies through collaboration with PT Proxi, an internet service provider company. This training focuses on the use of MikroTik devices and Winbox applications for firewall configuration as an effort to improve network security. Simulations are carried out using a simple topology between MikroTik and laptop devices to implement network filtering with certain rules. The results of this activity show that the firewall configuration is able to block access to unwanted sites or IP addresses, increasing protection against cyber threats. Thus, this activity is expected to not only increase student capacity but also provide benefits to the community in supporting a safer and more sustainable digital transformation.

ABSTRAK

Kegiatan pengabdian ini bertujuan untuk meningkatkan kompetensi mahasiswa dalam strategi keamanan jaringan melalui kolaborasi dengan PT Proxi, sebuah perusahaan penyedia layanan internet. Pelatihan ini berfokus pada penggunaan perangkat MikroTik dan aplikasi Winbox untuk konfigurasi firewall sebagai upaya meningkatkan keamanan jaringan. Simulasi dilakukan menggunakan topologi sederhana antara MikroTik dan perangkat laptop untuk menerapkan filtering jaringan dengan aturan tertentu. Hasil kegiatan ini menunjukkan bahwa konfigurasi firewall mampu memblokir akses ke situs atau alamat IP yang tidak diinginkan, tentunya meningkatkan perlindungan terhadap ancaman siber. Dengan demikian, kegiatan ini diharapkan tidak hanya meningkatkan kapasitas mahasiswa tetapi juga memberikan manfaat bagi

masyarakat dalam mendukung transformasi digital yang lebih aman dan berkelanjutan.

PENDAHULUAN

PT Proxi merupakan perusahaan berbasis teknologi informasi, sebagai penyedia layanan internet ternama di Indonesia. Berkantor pusat di Batam, Proxinet hadir untuk memenuhi kebutuhan internet di era digital masa kini, dengan tim yang profesional dan berpengalaman, serta orientasi pada kualitas layanan. PT Proxi sebagai lokasi dalam pelaksanaan pengabdian kepada masyarakat untuk upaya meningkatkan keamanan jaringan. Selain sebagai penyedia layanan, juga membantu dalam mendukung kualitas layanan yang aman dan nyaman.

Internet menjadi bagian terpenting dalam kehidupan dan memberikan manfaat untuk kehidupan sehari-hari. Namun, akses yang dilakukan untuk mendapatkan informasi dari internet tidak lain diperoleh dari suatu jaringan. Jaringan merupakan serangkaian perangkat yang saling terhubung dan dapat berkomunikasi antar perangkat baik secara lokal maupun global melalui kabel atau nirkabel. Banyak sekali pertimbangan dalam mengakses jaringan terutama dalam skala global, karena hal ini berkaitan dengan data dan juga sumber daya jaringan. Yang mana ketika suatu jaringan tidak aman, maka hal ini tentu akan berdampak pada penggunaan dan akan terjadi hal-hal yang dapat merugikan baik masyarakat maupun pihak penyedia layanan. Dalam hal ini, penulis melakukan pelatihan yang akan diimplementasikan untuk membuat filtering keamanan jaringan menggunakan mikrotik untuk membuat suatu kebijakan ataupun aturan bagaimana trafik jaringan yang diakses oleh pengguna.

Keamanan jaringan merupakan kumpulan aturan, teknologi, dan praktik yang digunakan untuk melindungi keamanan komputer dari ancaman, serangan, atau akses yang tidak sah (Yel et al., n.d.). Tujuan keamanan jaringan yaitu untuk memastikan integritas, kerahasiaan, dan ketersediaan data serta sumber daya jaringan. Keamanan jaringan sangat penting untuk dilakukan agar tidak terjadi kerugiaan dalam mengakses segala informasi atau berbagi data melalui internet (Pratomo, 2023).

Strategi yang dilakukan untuk meningkatkan keamanan jaringan dimulai dengan melakukan simulasi pada perangkat jaringan yaitu mikrotik dan laptop. Mikrotik merupakan sistem operasi router atau router OS yang dapat diinstall di hardware. Dengan perangkat lunak winbox, maka dilakukan konfigurasi untuk proses filtering jaringan dengan topologi sederhana yaitu antara mikrotik dan laptop. Dimana proses simulasi ini dilakukan untuk meningkatkan dan menguji aturan atau kebijakan jaringan yang akan digunakan dengan skala yang besar dan diimpelementasikan kepada masyarakat sesuai dengan kebutuhan dan tidak merugikan baik pihak penyedia layanan maupun masyarakat.

Keamanan jaringan ini dilakukan dengan menggunakan firewall pada mikrotik untuk membuat aturan trafik jaringan. Dengan membuat kebijakan dari firewall mikrotik, penulis berharap beberapa akses yang mencurigakan dapat difilter dan tidak dapat akses dengan tujuan menjaga keamanan jaringan (Eka Putra et al., 2024). Selain itu, tentunya juga dapat menjaga data masyarakat. Adanya pengabdian yang dilakukan dengan berfokus pada keamanan jaringan menjadi salah satu langkah dalam memberikan pemahaman serta praktik nyata bahwa apa yang didapatkan dari internet bukan hanya manfaatnya saja, melainkan juga terdapat dampak negatif yang bisa didapatkan apabila jaringan yang diakses tidak aman. Oleh karena itu, filtering dengan firewall sebagai pencegahan dari kerugian yang bisa terjadi terhadap keamanan dan kenyamanan masyarakat dalam memperoleh segala informasi yang diakses melalui internet.

Tanpa pengetahuan yang mendalam mengenai bahaya dan ancaman yang didapatkan dari siber, tentunya membuat penulis lebih berhati-hati dan berupaya dalam menjaga keamanan jaringan dengan sebaik mungkin. Apalagi internet dan melakukan browsing baik untuk mencari informasi, hiburan, atau yang lainnya menjadi kebiasaan dan tidak terpisahkan dari kehidupan sehari-hari. Selain pengetahuan, adanya tindakan preventif yang bisa dilakukan oleh ISP dan melibatkan mahasiswa ini dalam bentuk pengabdian menjadikan dorongan dan motivasi untuk mengembangkan keterampilan yang dapat bermanfaat bagi masyarakat dan semua pengguna internet. Saat ini, banyak kejahatan melalui berbagai cara di internet seperti penipuan online, pencurian identitas, malware dan ransomware, cyberbullying, penyebaran konten ilegal, phising, dan lain-lain.

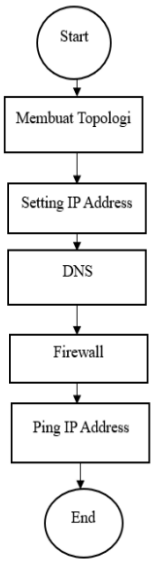
Kegiatan ini dirancang untuk membantu mahasiswa dan ahli dalam bidang keamanan jaringan melalui kerja sama dengan mitra industri yaitu PT Proxi. Melalui pelatihan yang berfokus pada strategi keamanan jaringan menggunakan mikrotik, mahasiswa diharapkan mampu merancang dan menerapkan solusi keamanan yang sesuai kebutuhan. Hasil dari pelatihan ini nantinya diharapkan dapat diapliksikan pada jaringan dikomunitas atau organisasi mayarakat, guna meningkatkan perlindungan terhadap ancaman siber dan mendukung transformasi digital yang lebih aman dan berkelanjutan.

METODE PELAKSANAAN

Dalam pelaksaan pengabdian ini, ada beberapa metode yang dilakukan untuk keberhasilan dalam menjaga keamanan data dari siber dan menerapkan filtering jaringan yaitu sebelum memulai untuk mengimplementasikan filtering jaringan, tentu harus mengetahui terlebih dahulu topologi yang digunakan dan bagaimana konfigurasi yang akan dilakukan. Analisis topologi bertujuan untuk memahami struktur jaringan secara menyeluruh, sehingga langkah-langkah selanjutnya dapat dilakukan dengan lebih efektif dan efisien (Sukma et al., n.d.).

Penulis membuat topologi sederhana yang terdiri dari mikrotik dan laptop untuk perangkat filtring keamanan jaringan. Langkah awal dalam konfigurasi ini, yaitu dilakukan pemberian alamat IP pada mikrotik yang akan dihubungkan dengan ISP (Internet Service Provider) untuk mengelola jaringan yang akan masuk maupun keluar. Hal ini bertujuan untuk meningkatkan keamanan dan mengetahui traffic jaringan yang masuk ataupun keluar. Dalam hal ini tim pengabdian bersama dengan

mitra yaitu PT Proxi melakukan proses filtering dengan firewall filter rules pada perangkat lunak winbox untuk mikrotik (Hairun et al., 2023). Adapun langkah yang akan dilakukan yaitu sesuai flowchart berikut.



Gambar 1 Flowchart Simulasi Filtering

HASIL DAN PEMBAHASAN

Kegiatan pengabdian ini dilaksanakan dalam bentuk pengembangan kompetensi mahasiswa di bidang jaringan dan kolaborasi dengan PT Proxi guna meningkatkan keamanan jaringan. Yang mana dilaksanakan pada tanggal 23 bulan September yang berlokasi di PT Proxi. Kegiatan yang melibatkan mahasiswa ini bertujuan untuk memberikan pemahaman dan pengalaman praktis mengenai pentingnya menjaga keamanan jaringan baik secara lokal maupun global. Dengan menggunakan perangkat milik PT Proxi, penulis diperkenalkan dengan server dan perangkat pendukung untuk membuat filtering jaringan.

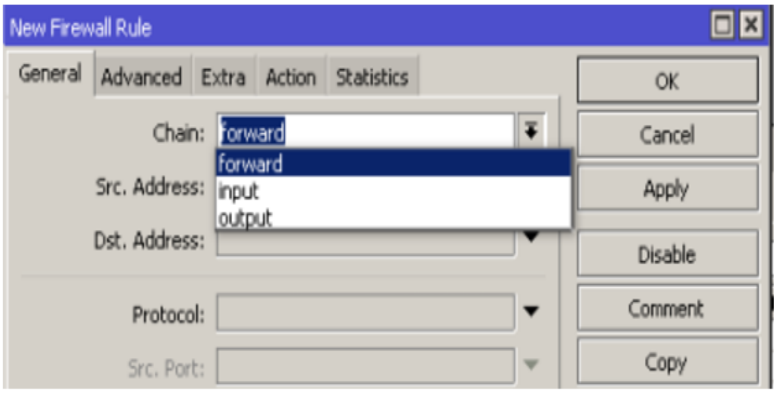
Hasil dari pengabdian ini yaitu memberikan pelayanan dan keamanan kepada masyarakat mengenai keamanan data dan juga informasi pribadi. Filtering yang dilakukan mampu menangani proses data yang hanya melewati router dengan memberikan respon yang sesuai. Adapun yang dilakukan oleh tim pengabdian bersama PT Proxi membuat filtering dengan firewall filter rules chain forward. Dalam firewall filter rules memiliki 3 chain yaitu input untuk memproses paket data yang masuk ke router, output untuk menangani paket data yang dikirim oleh router, dan forward yaitu untuk menangani paket data yang hanya melewati router.

Dengan topologi yang dibuat, maka penulis dengan PT Proxi memulai untuk melakukan filtering jaringan dengan menggunakan chain forward karena filtering ini berfokus pada keamanan jaringan yang diakses hanya melewati router. Yang mana apabila pengguna mengakses situs ataupun domain tertentu secara langsung akan meneruskan proses tersebut ke router dan memberikan balasan mengenai respon yang telah dilakukan oleh pengguna.

Dengan topologi sederhana yaitu perangkat mikrotik dan laptop, maka penulis memberikan IP address secara statis atau manual. Hal ini dilakukan agar penulis juga dapat memahami secara mendalam mengenai konsep dasar jaringan dalam pemberian alamat IP dengan cara static. Namun, pada implementasinya secara global atau luas alamat IP diberikan dengan dynamic yang mana tentunya tergantung pada ketentuan ataupun kebutuhan dari topologi dan perangkat yang digunakan. Setelah masing-masing perangkat mendapatkan alamat IP, tidak lupa untuk menerapkan firewall NAT dengan action masquiride bertujuan untuk menghubungkan jaringan lokal ke public. Dimana pada dasarnya saat kita mengakses suatu situs alamat IP perangkat bukan lagi IP pribadi melainkan IP publik karena sudah diterjemahkan dengan action masquiride. NAT (Network Address Translation) yaitu sebuah proses pemetaan alamat IP dimana perangkat jaringan komputer akan memberikan alamat IP publik ke perangkat jaringan lokal sehingga banyak IP private yang akan mengakses IP public.

Selanjutnya, diberikan DNS (Domain Name System) agar bisa mengakses situs bukan dari alamat IP saja melainkan juga nama domain. DNS merupakan suatu sistem yang menerjemahkan nama domain yang mudah diingat misalnya detik.com menjadi alamat IP yang digunakan oleh komputer untuk berkomunikasi satu sama lain di dalam jaringan. DNS ini diberikan dengan konfigurasi sebagai berikut:
IP/DNS/add server 8.8.8.8

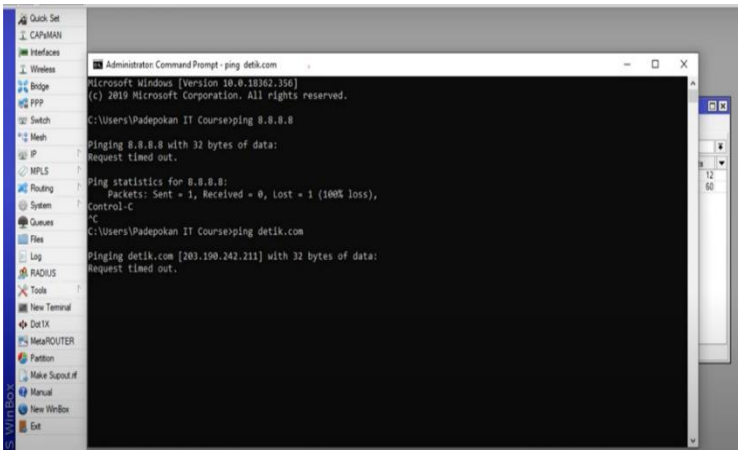
DNS yang diberikan yaitu DNS publik google, yang mana server DNS dapat mengubah nama domain menjadi alamat IP dan begitupun sebaliknya. Hal ini memudahkan pengguna ketika akan mengakses situs di internet, karena pengguna bisa melakukan pencarian dengan nama domain seperti detik.com dan tidak perlu mencari dengan alamat IP situs tersebut, terlebih jika kita tidak mengetahui alamat IP dari suatu situs.



Gambar 1 Filter rules

Gambar 2 merupakan antarmuka perangkat lunak winbox dimana konfigurasi filtering jaringan dilakukan dengan cara masuk ke IP firewall lalu pilih filter rules dan buat rule baru dengan chain forward yaitu untuk membuat kebijakan dari traffic mana saja yang boleh dilewati mikrotik. Setelah chain nya dipilih forward, maka pilih tab action drop (Jayanto et al., n.d.).

Dapat dilihat pada gambar 3 hasil pengetesan dengan melakukan ping ke DNS (Domain Name System) berhasil yaitu tidak dapat mengakses dan mendapatkan respon request time out karena setelah dilakukan filtering firewall filter rules maka saat akan mengakses situs atau IP Address domain tentu tidak dapat diakses. Hal ini menunjukan bahwa aturan firewall berhasil dalam memblok situs tersebut. Adapun aturan yang dipraktikan yaitu dengan memblok situs facebook. Namun, pada implementasinya, aturan dapat dibuat sesuai dengan kebutuhan dan kebijakan yang akan dibuat.



Gambar 3 Ping DNS

Gambar 4 Monitoring Trafik Jaringan

Gambar 5 Pengenalan Device Server

Melalui proses filtering keamanan jaringan ini selain pihak PT Proxi, mahasiswa juga terlibat dalam perencanaan dan pengembangan untuk melakukan tindakan preventif terhadap keamanan dan monitoring jaringan. Monitoring lalu lintas jaringan selalu dilakukan secara real time untuk megetahui bagaiamana lalu lintas yang diakses oleh pengguna dapat berjalan dengan baik atau memiliki kendala baik dari konfigurasi ataupun perangkat jaringan.

KESIMPULAN DAN SARAN

Kegiatan pengabdian kepada masyarakat yang melibatkan mahasiswa dan PT Proxi ini telah berhasil mencapai tujuan utama, yaitu peningkatan kompetensi dalam bidang keamanan jaringan, khususnya melalui konfigurasi firewall dengan memanfaatkan perangkat MikroTik. Melalui serangkaian simulasi dan implementasi yang dilakukan, mahasiswa tidak hanya belajar tentang teori, tetapi juga mendapatkan pengalaman praktis yang nyata.

Hasil yang diperoleh dari penerapan filter rules menunjukkan efektivitas yang signifikan dalam memblokir akses yang mencurigakan, sehingga secara langsung berkontribusi terhadap peningkatan keamanan data dan jaringan yang dikelola oleh komunitas.

Dari kegiatan ini, diharapkan dapat menjadi langkah awal yang kuat dalam menciptakan solusi keamanan jaringan yang lebih komprehensif dan dapat diterapkan secara luas pada berbagai komunitas atau organisasi masyarakat. Selain itu, kolaborasi antara mahasiswa dan PT Proxi ini juga menekankan pentingnya kerja sama yang erat antara kalangan akademisi dan industri. Kerja sama seperti ini tidak hanya memberikan manfaat langsung bagi peserta, tetapi juga menciptakan dampak yang lebih luas dan berkelanjutan bagi masyarakat digital secara keseluruhan.

Oleh karena itu, disarankan agar kegiatan serupa dilanjutkan dan diperluas ke topik-topik keamanan siber lainnya, serta melibatkan lebih banyak pihak dari berbagai latar belakang. Hal ini akan membantu menciptakan ekosistem keamanan yang lebih solid dan responsif terhadap tantangan yang terus berkembang di dunia digital. Dengan demikian, kita dapat memastikan bahwa masyarakat memiliki pengetahuan dan keterampilan yang diperlukan untuk menghadapi ancaman di era informasi ini.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada PT Proxi yang telah menjadi mitra dalam program pengabdian kepada masyarakat ini. Kerjasama yang terjalin telah memberikan banyak manfaat bagi masyarakat.

Terima kasih kepada seluruh tim PT Proxi yang telah aktif berpartisipasi, memberikan dukungan, serta berbagi pengetahuan dan pengalaman. Semoga kolaborasi ini dapat terus berlanjut dan memberikan dampak positif bagi masyarakat di masa mendatang.

Penulis juga mengucapkan terima kasih kepada semua pihak yang telah berkontribusi dalam pelaksanaan program ini. Semoga apa yang telah penulis lakukan dapat bermanfaat dan menginspirasi untuk kegiatan-kegiatan selanjutnya.

DAFTAR PUSTAKA

Eka Putra, F. P., Amir Hamzah, Agel, W., & Firmansyah Kusuma, R. O. (2024). Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking. *Jurnal Sistim Informasi Dan Teknologi*, 82–87. https://doi.org/10.60083/jsisfotek.v5i4.329

Hairun, A. N., Katili, M. R., Takdir, R., & Tuloli, M. S. (2023). Penerapan firewall di router OS mikrotik pada aplikasi e-rapor. *Jambura Journal of Informatics*, *5*(2), 108–119. https://doi.org/10.37905/jji

Jayanto, S., Tantoni, A., Asyari, H., Studi, P., Informatika, T., & Lombok, S. (n.d.). *Jurnal Ranah Publik Indonesia Kontemporer Implementasi Keamanan Jaringan dengan Packet Filtering Berbasis Mikrotik Untuk Internet Positif Di SMKN 1 Praya* (Vol. 1, Issue 2). https://rapik.pubmedia.id/index.php/rapik

Pratomo, A. B. (2023). *https://bufnets.tech https://doi.org/10.59688/bufnets BULLETIN OF NETWORK ENGINEER AND PENGEMBANGAN SISTEM FIREWALL PADA JARINGAN KOMPUTER BERBASIS MIKROTIK ROUTEROS DEVELOPING A FIREWALL SYSTEM ON A COMPUTER NETWORK BASED ON MIKROTIK ROUTEROS*. *1*(2). https://doi.org/10.59688/bufnets

Sukma, D., Mitro, S. S., kunci -Kemanan Jaringan, K., & Komputer, J. (n.d.). Penerapan Internet Positif Di SMK N 3 Pandeglang Berbasis Mikrotik Dengan Packet Filtering. *Jurnal POLEKTRO: Jurnal Power Elektronik*, *12*(3), 2023. www.facebook.com

Yel, M. B., Iskandar Mulyana, D., Renaldy, J., Dzaky Nurfaishal, M., & Toharudin, H. (n.d.). *OPTIMALISASI KEAMANAN FIREWALL PADA INFRASTRUKTUR JARINGAN SMK IDN BOGOR*.