Jurnal Jaringan Komputer dan Keamanan
JJKK, Vol. 04, No. 03, October 2023: 11-18
Received: 27 Agustus 2023; Revised: 27 September 2023; Accepted: 3 October 2023

Literature Review : Network Security Menggunakan Virtual Private Network L2TP/IPSEC, Port Knocking, Port Forwarding, Honeypot Dan Pfsense

Rianda Pratama
Program Magister Teknik Informatika
Universitas Bina Darma
email :riandapratama@student.binadarma.ac.id
Jl. A. Yani No. 12, Palembang 30624, Indonesia

Abstract

The current technological developments are so fast, many companies are competing to create an application or service via the internet as a form of business competition in order to attract customers or even make customers feel comfortable so that they will remain loyal to the companies. This has a huge impact on everyday life. Nowdays, little by little people's lives are starting to depend on the internet. Seeing this phenomenon in order to continue to form a conducive condition in carrying out daily life, a security system is needed that can keep services or services connected to the internet operating properly, so it is not imaginary that securing a network system is an important thing to support business activities. internet everyday. Of the many network security methods, there are several things that the author would like to highlight, namely how to detect attacks on networks, how to form encrypted networks, integrated security schemes. From this, the authors found several journals and research that discussed network security using the L2TP/IPsec virtual private network method, Port Knocking, Honeypot, Port Forwarding and Open Source Firewall Pfsense.

Kata kunci: *Network Security, vpn, L2TP/IPsec, Port Knocking, Honeypot, Port Forwarding dan PfSense*

Abstrak

Perkembangan teknologi saat ini sangatlah pesat, banyak perusahaan berlomba-lomba menciptakan suatu aplikasi atau layanan melalui internet sebagai bentuk persaingan bisnis agar dapat menarik hati pelanggan atau bahkan membuat pelanggan merasa nyaman sehingga tetap setia menggunakan jasa atau pelayanan dari perusaahaan tersebut. Hal tersebut sangat berdampak dalam kehindupan sehari-hari sedikit demi sedikit kehidupan masyarakat saat ini mulai bergantung dengan internet. Melihat fenomena tersebut agar tetap terbentuknya suatu kondisi yang kondusif dalam menajalankan kehidupan sehari-hari maka diperlukanlah suatu sistem pengamanan yang dapat menjaga pelayanan atau layanan yang terhubung di internet dapat beroperasi dengan baik maka tak khayal pengamanan suatu sistem jaringan merupakan suatu hal yang penting guna mendukung kegiatan ber-internet sehari-hari. Dari banyaknya metode pengaman jaringan ada beberapa hal yang penulis ingin soroti, yaitu cara mendeteksi serangan terhadap jaringan,cara membentuk jaringan yang terenkripsi, skema pengaman yang terpadu. Dari hal tersebut maka penulis menemukan beberapa jurnal

dan penelitian yang membahas tentang pengamanan jaringan dengan menggunakan metode virtual private netwok L2TP/IPsec, Port Knocking, Honeypot, Port Forwarding dan Open Source Firewall PFsense.

Kata kunci: *keamanan jaringan, vpn, L2TP/IPsec, Port Knocking, Honeypot, Port Forwarding dan PfSense*

1. PENDAHULUAN

Pengamanan akses jaringan merupakan suatu upaya untuk melindungi akses ke jaringan dari serangan dan ancaman keamanan. Seiring perkembangan jaman, jaringan menjadi sangat penting untuk bisnis dan organisasi, sehingga keamanan jaringan menjadi sangat krusial. Artikel ini membahas tentang teknik-teknik pengamanan akses jaringan, termasuk penggunaan firewall, VPN, port knocking, dan honeypot [1][2]. Penggunaan teknik-teknik ini dapat membantu melindungi jaringan dari serangan luar dan mencegah akses yang tidak sah. penerapan keamanan jaringan secara menyeluruh sangatlah penting, termasuk melindungi data sensitif, memperbarui perangkat lunak secara berkala, dan melakukan pelatihan keamanan untuk pengguna jaringan [3].

Dalam era digital yang semakin maju, pertumbuhan teknologi informasi telah mengubah cara organisasi dan individu berkomunikasi dan berbagi data. Namun, dengan kemajuan ini juga muncul ancaman keamanan yang semakin canggih. Keamanan jaringan menjadi aspek kunci dalam menjaga kerahasiaan, integritas, dan ketersediaan data. Salah satu alat yang efektif dalam memitigasi risiko ini adalah Virtual Private Network (VPN) [4][5].

Keamanan jaringan adalah prioritas utama bagi organisasi dan individu. Ancaman seperti peretasan (hacking), penyusupan, dan pencurian data telah menyebabkan kerugian finansial dan kerusakan reputasi yang signifikan. Oleh karena itu, penting untuk mengamankan komunikasi dan data yang mengalir melalui jaringan [6].

VPN adalah teknologi yang memungkinkan pengguna untuk membentuk koneksi aman melalui jaringan yang tidak aman, seperti internet. Ini menciptakan "tunnel" enkripsi yang melindungi data yang dikirim melalui jaringan. Dengan demikian, VPN membantu mengamankan data dari potensi ancaman yang ada di jaringan publik [7]. VPN bekerja dengan mengenkripsi data sebelum mengirimkannya melalui jaringan. Ini memastikan bahwa bahkan jika data diretas oleh pihak yang tidak sah, mereka tidak dapat membacanya tanpa kunci enkripsi yang sesuai. Selain itu, VPN juga menyembunyikan alamat IP asli pengguna, yang dapat membantu melindungi privasi online [8].

Banyak organisasi menggunakan VPN untuk mengamankan komunikasi internal, terutama ketika anggota tim berada di lokasi yang berbeda. Ini juga digunakan untuk mengamankan koneksi karyawan saat mereka bekerja dari jarak jauh, mengakses data organisasi melalui internet. Organisasi modern sering kali mengandalkan komunikasi dan pertukaran data yang kritis melalui jaringan. Data sensitif seperti informasi pelanggan, rahasia perdagangan, dan informasi keuangan harus dilindungi dengan sangat baik dari ancaman siber. Ancaman siber terus berkembang dan semakin canggih. Serangan peretasan, malware, dan serangan siber lainnya dapat memiliki dampak serius terhadap operasi organisasi dan reputasinya.Terlebih lagi, banyak organisasi sekarang memungkinkan karyawan untuk bekerja dari jarak jauh, yang membutuhkan koneksi yang aman untuk mengakses sumber daya organisasi [9][10]. VPN adalah alat yang umum digunakan untuk menyediakan koneksi yang aman bagi karyawan yang bekerja dari luar kantor. Organisasi juga harus mematuhi peraturan privasi data yang ketat dan standar kepatuhan yang berlaku. Penggunaan VPN dapat membantu dalam menjaga privasi data

dan memenuhi persyaratan kepatuhan seperti GDPR (General Data Protection Regulation) di Eropa.

Penelitian mengenai penggunaan VPN dalam konteks organisasi dapat membahas berbagai aspek, termasuk keefektifan VPN dalam melindungi data, pengelolaan biaya dan sumber daya, serta dampaknya terhadap produktivitas dan kinerja. VPN juga berperan penting dalam memastikan ketersediaan sumber daya dan aksesibilitas yang diperlukan oleh anggota organisasi di berbagai lokasi geografis. Selain itu, penelitian tentang VPN dapat melibatkan inovasi teknologi, seperti pengembangan protokol keamanan baru, implementasi teknik kecerdasan buatan untuk mendeteksi ancaman, dan pengembangan VPN yang lebih efisien. Organisasi sering kali memiliki beragam pilihan solusi VPN, seperti VPN site-to-site, VPN remote access, atau VPN cloud. Penelitian dapat membantu organisasi memilih solusi yang paling sesuai dengan kebutuhan mereka.

2. METODOLOGI PENELITAN

2.1 Tahapan Penelusuran Artikel

1) Pertanyaan paduan: Bagaimana cara melakukan pengamanan jaringan? Kata kunci: Keamanan Jaringan, VPN, L2TP/IPsec, Port Knocking, Port Forwarding, honeypot dan PfSense
2) Kriteria : artikel yang memiliki judul dan isi relevan dengan tujuan, berbahasa Indonesia dan Inggris, fulltext, artikel penelitian yang dipublikasi
3) Data diperoleh dari database elektronik yakni ResearchGate, Google Scholar, academia.edu dan ieeexplore.ieee.org
4) Memilih 10 artikel untuk mengumpulkan informasi terntang pengamanan jaringan.

3. HASIL DAN PEMBAHASAN

VPN L2TP/IPSec adalah salah satu jenis VPN yang banyak digunakan untuk memperkuat keamanan jaringan. IPSec memberikan lapisan keamanan tambahan dengan enkripsi dan otentikasi yang kuat, sementara L2TP memfasilitasi tunel data. Kombinasi keduanya memberikan pertahanan yang handal terhadap ancaman keamanan seperti sniffing dan serangan man-in-the-middle (MITM). Port Knocking adalah teknik keamanan yang mengizinkan akses ke port tertentu pada server hanya setelah rangkaian permintaan koneksi yang tepat telah diterima dari alamat IP sumber yang benar. Ini membantu mencegah serangan port scanning dan mempersulit akses ilegal ke layanan jaringan. Port Forwarding memungkinkan lalu lintas dari port tertentu diarahkan ke alamat IP dan port lain. Ini sering digunakan untuk mengatur akses ke layanan di belakang firewall atau router. Meskipun memberikan fleksibilitas dalam mengatur jaringan, harus diterapkan secara hati-hati untuk menghindari risiko keamanan. Honeypot adalah sistem palsu yang didesain untuk menarik perhatian penyerang. Tujuan dari honeypot adalah untuk memantau dan mempelajari taktik dan teknik penyerangan yang digunakan oleh penyerang. Dengan memikat penyerang ke dalam lingkungan terkendali, tim keamanan dapat mengidentifikasi ancaman dan mengambil langkah-langkah pencegahan yang sesuai. pfSense mendukung VPN, Port Forwarding, dan banyak fitur keamanan lainnya yang dapat membantu meningkatkan pertahanan jaringan.

Judul Penelitian/jurnal	Penulis	Kesimpulan
Perancangan Implementasi VPN Server Menggunakan Protokol L2TPdan IPSec Sebagai Keamanan Jaringan [11].	P Wicaksana, F Hadi, AF Hadi - Jurnal KomtekInfo, 2021 - jkomtekinfo.org	Penelitian yang dilakukan Prayogi wicaksana memperlihatkan tahapan konfigurasi untuk membangun l2tp/ipsec server.
Implementasi Jaringan VPN (L2TP/Ipsec) Mikrotik Untuk Remote AccessSebagai Security Selama Work From Home [12].	BG Rahino, A Susila , 2022 journal.mediapublikasi.id	VPN L2TP/Ipsec terlihat pada aplikasi Wireshark, protokol ESP (Encapsulating Security Payload).File Data Customer(.xlsx) tidak dapat dapat terbaca isinya, file tersebut sudah terenkripsi. Membuktikan bahwa menggabungkan IPSec sebagai keamanan pada L2TP sangatlah baik.
Penerapan Protokol L2TP/IPSec dan Port Forwarding untuk Remote Mikrotik pada Jaringan Dynamic IP [13].	H Pratama, NF Puspitasari, 2021 - citec.amikom.ac.id	Pada peneltitian yang dilakukan saudara Hedy pratama menghasilakan informasi bahwa pot forwarding memungkinkan akses suatu tertentu melalui port yang telah di tentukan sebagai pintu masuknya
Analisa Aksesibilitas jaringan internet dengan menggunakan L2TP/IPSec menggunakan Virtual Private Network [15].	Muhammad Iqbal Riski Pazar, Tugas Akhir mahasiswa Fakultas Teknik Universitas\ Persada Indonesia Y.A.I	Pada penelitian yang dilakukan oleh saudara Muhammad Iqbal Pazar Riski bahwa terdapat penurunan kualitas jaringan dikarenakan peneliti menggunakan cloud hosted router (CHR) yang digunakan sebagai server vpn berbasis cloud yang menyebabkan terjadinya perbedaan kualitas jika dibandingkan direct VPN.

Optimasi Port Knocking dan Honeypot Menggunakan IPTABLES Sebagai Keamanan Jaringan pada Server [15].	Ma Yayank - 2020 - eprints.unram.ac.id	Port knocking merupakan skema pengamanan jaringan dengan melakukan knocking port tertentu dengan urutan tertentu sehingga membuat sang pengetuk mendapat akses terhadap port atau server tertentu yang dapat dikombinasikan dengan honeypot sebagai server pancingan atau jebakan yang disediakan pengelola jaringan atau server agar penyerang terfokus ke honeypot bukan ke jaringan atau server production.
Comparison of network security tools- Firewall, Intrusion Detection System and Honeypot [16].	T Kaur, V Malhotra, D Singh - Int. J. Enhanced Res. Sci. Technol. Eng, 2014 - academia.edu	Membahas tentang perbandingan tiga alat keamanan jaringan yang berbeda yaitu firewall, intrusion detection system dan honeypot. firewall merupakan alat keamanan jaringan yang paling umum digunakan dan berfungsi untuk memfilter lalu lintas jaringan dan memblokir akses yang tidak sah, IDS adalah alat yang memonitor aktivitas jaringan dan dapat mendeteksi serangan yang sedang terjadi dan honeypot merupakan alat untuk menarik perhatian penyerang dengan menyediakan perangkap didalamnya.
Implementasi Sistem Keamanan Web Server Menggunakan Pfsense [17].	M Arman, N Rachmat - Jusikom: 2020 - jurnal.univbinainsan.ac.id	Pfsense sebagai sistem keamanan web server dan menguji keamanannya terhadap serangan DDoS dan brute force attack. Metode yang digunakan dalam penelitian ini adalah metode eksperimen dengan menguji keamanan web server melalui simulasi serangan DdoS dan brute force attack.

Implementation of Honeypot, NIDs, and HIDs Technologies in SOC Environment [18].	R Dalbhanjan, S Chatterjee, R Gogoi, T Pathak… - 2021 - ieeexplore.ieee.org	kombinasi ketiga teknologi tersebut memberikan pendekatan komprehensif untuk deteksi dan pencegahan ancaman di lingkungan SOC. Honeypot efektif dalam mengidentifikasi dan menganalisis aktivitas penyerang, NID dapat mendeteksi serangan berbasis jaringan, dan HID dapat mendeteksi serangan pada host. Sehingga secara signifikan meningkatkan postur keamanan lingkungan SOC dengan meningkatkan deteksi dan pencegahan berbagai jenis ancaman.
A Review paper on pfsense an Open source firewall introducing with different capabilities & customization [19].	KC Patel, P Sharma - IJARIIE, 2017 - academia.edu	Pada review open source firewall peneliti membandungkan 3 jenis firewall yaitu untangle, pfsense dan IpFire. Peneliti memilih pfsense yang lebih memiliki fitur yang baik dan sebagai open source firewall. Pada penelitiannya peneliti menempatkan pfsense bukan hanya sebagai firewall namun juga menjadikannya sebagai router, proxy server dan dhcp server.
Strategi pengamanan akses jaringan dengan l2tp over ipsec preshared key dan port knocking [20].	R Pratama 2022 - jurnal.polsri.ac.id	Pada jurnal ini membuktikan bahwa metode port knocking dapat menambah layer pengamanan akses terhadap server dengan metode otentikasi berlapir mulai dari tunnelling di layer 2 dengan l2tp ditambah enkripsi dengan ipsec kemudian melakukan skema knocking port tertentu agar mendapatkan akses terhadap port tertentu pada server.

4. KESIMPULAN

Berdasarkan dari Jurnal/Artikel yang telah dibaca dapat disimpulkan bahwa VPN L2TP/Ipsec, Port Knocking, Port Forwarding, Honeypot dan Open Source Firewall PfSense dapat digabungkan untuk membangun suatu skema pengamanan jaringan yang komprehensif. Mulai dari terbentukan nya koneksi yang terenkripsi melaui VPN sebagai tunnel kemudian dilanjutkan dengan intrusion detection sistem dan intrusion prevention system oleh pfsense sebagai pertahanan lapis kedua setelah firewall utama lalu melakukan forwarding terhadap port port tertentu agar diarahkan menuju ke jebakan honeypot dan mengautentikasi akses dengan port knocking.

Referensi

[1]. Negara, E. S. (2019). Jaringan Komputer Routing dan Switching Essentials.

[2]. Manuhutu, M. A., Muttaqin, M., Irmayani, D., Tamara, T., Gustiana, Z., Hazriani, H., ... & Karim, A. (2021). *Pengantar Forensik Teknologi Informasi*. Yayasan Kita Menulis.

[3]. Negara, E. S. (2014). Implementasi Management Network Security Pada Laboratorium CISCO Universitas Bina Darma. *Jurnal Matrik*, *16*(1), 11-20.

[4]. Kaunang, F. J., Karim, A., Simarmata, J., Iskandar, A., Ardiana, D. P. Y., Septarini, R. S., ... & Widyastuti, R. D. (2021). Konsep Teknologi Informasi. Yayasan Kita Menulis.

[5]. Kartolo, R., & Negara, E. S. (2022). Analisis Kinerja Private Cloud Computing Menggunakan Metode Reability, Maintanability, Availability dan Security. *INOVTEK Polbeng-Seri Informatika*, *7*(1), 136-146.

[6]. Edi, S. N. (2022). Analisis Dan Perancangan Arsitektur Teknologi Informasi Berbasis Cloud Computing Untuk Institusi Perguruan Tinggi Di Sumatera Selatan. Analisis Dan Perancangan Arsitektur Teknologi Informasi Berbasis Cloud Computing Untuk Institusi Perguruan Tinggi Di Sumatera Selatan.

[7]. Putra, E. M., Tujni, B., & Negara, E. S. (2018). Analisis Kemanan Jaringan Internet (Wifi) Dari Serangan Packet Data Sniffing Di Universitas Muhammadiyah Palembang. *Jurnal Ilmiah Teknologi Informasi*.

[8]. Andryani, R. (2016). Pengukuran risiko pada penerapan cloud computing untuk sistem informasi (studi kasus universitas bina darma). *Jurnal Teknologi Technoscientia*, 173-179.

[9]. Negara, E. S., Keni, K., & Andryani, R. (2020, July). BCube and DCell Topology Data Center Infrastructures Performance. In *IOP Conference Series: Materials Science and Engineering* (Vol. 852, No. 1, p. 012129). IOP Publishing.

[10]. Mukmin, C., & Negara, E. S. (2019). Analisis Kinerja Redistribusi Routing Protokol Dinamik (Studi Kasus: Rip, Eigrp, Is-Is). *Klik-Kumpul. J. Ilmu Komput*, *6*(3), 284.

[11]. Mukti, A. R., & Negara, E. S. (2016). Studi Performa Migrasi Ipv4 Ke Ipv6 pada Metode Dual Stack. In *Annual Research Seminar* (Vol. 2, No. 1, pp. 14-22).

[12]. Negara, E. S. (2017). Perbandingan Redistribusi Routing Protokol Dinamis pada Exterior Gateway Protokol. In *Seminar Nasional Teknologi Informasi dan Komunikasi (SEMNASTIK 2017)*.

[13]. Pratama, R. (2022). Strategi Pengamanan Akses Jaringan Dengan L2TP Over IP Security Preshared Key Dan Port Knocking. JUPITER (Jurnal Penelitian Ilmu Dan Teknik Komputer), 14(2-b), 306-316.

[14]. Patel, K. C., & Sharma, P. (2017). A Review paper on pfsense-an Open source firewall introducing with different capabilities & customization. IJARIIE, 3, 2395-4396.

[15]. Pratama, H., & Puspitasari, N. F. (2021). Penerapan Protokol L2TP/IPSec dan Port Forwarding untuk Remote Mikrotik pada Jaringan Dynamic IP. Creative Information Technology Journal, 7(1), 51.
[16]. Prayogi Wicaksana, Hadi, F., & Aulia Fitrul Hadi. (2021). Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan. Jurnal KomtekInfo, 169–175.
[17]. Arman, M., & Rachmat, N. (2020). Implementasi Sistem Keamanan Web Server Menggunakan Pfsense. Jusikom : Jurnal Sistem Komputer Musirawas, 5(1), 13–23. Yayank, M. A. (2020). Optimasi Port Knocking Dan Honeypot Menggunakan Iptables Sebagai Keamanan Jaringan Pada Server (Doctoral dissertation, Universitas Mataram).
[18]. Dalbhanjan, R., Chatterjee, S., Gogoi, R., Pathak, T., & Sahay, S. (2021). 3 Implementation of Honeypot, NIDs, and HIDs Technologies in SOC Environment.
[19]. Kaur, T., Malhotra, V., & Singh, D. (2014). Comparison of network security tools-firewall, intrusion detection system and Honeypot. Int. J. Enhanced Res. Sci. Technol. Eng, 200204.
[20]. Rahino, B. G., & Susila, A. (2022). Implementasi Jaringan VPN (L2TP/Ipsec) Mikrotik Untuk Remote Access Sebagai Security Selama Work From Home. OKTAL: Jurnal Ilmu Komputer dan Sains, 1(11), 1911-1918.