Strategi Pengamanan Akses Jaringan Dengan L2TP *Over IP Security Pre-shared Key* Dan *Port Knocking*

Rianda Pratama*[1], Alex Wijaya[2], Fatoni[3], Suryayusra[4]
[1,2,3,4]Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Binadarma
E-mail: *[1]riandapratama08@palembang.go.id, [2]alex_wj@binadarma.ac.id,
[3]fatoni@binadarma.ac.id, [4]suryayusra@binadarma.ac.id

Abstrak

Pesatnya perkembangan teknologi mempengaruhi pola hidup masyarakat di berbagai lini, Berbagai macam pertukaran data terjadi melalui internet sehingga menyebabkan internet menjelma menjadi sebuah kebutuhan dasar bagi sebagian besar masyarakat. Maka dari itu Pemerintah melihat perlu adanya suatu sistem yang mengakomodir kebutuhan tersebut melalui Peraturan Presiden nomor 95 tahun 2018 tentang sistem pemerintahan berbasis elektronik. Dalam pelaksanaannya salah satu hal yang dibutuhkan adalah pengelolaan akses terhadap data yang tersimpan pada server pemerintah. Agar dapat menunjang kebutuhan pengelola server pemerintah dibutuhkanlah suatu terknologi yang dapat mengakomodir kebutuhan keamanan dalam pengaksesan server tersebut, maka penulis merancang akses tersebut melalui Virtual private server Layer 2 Tunneling Protocol Over IP Security dan port knocking yang memungkinan para pengelola yang memiliki hak akses dapat mengakses jaringan lokal melalui jaringan internet publik secara aman.

Kata kunci: *Teknologi , VPN l2TP over IPsec, Port Knocking, MikroTik*

Abstract

The rapid development of technology affects people's lifestyles in various lines. Various kinds of data exchange occur through the internet causing the internet to become a basic need for most people. Therefore, the Government sees the need for a system that accommodates these needs through Presidential Regulation number 95 of 2018 concerning an electronic-based government system. In its implementation, one of the things needed is the management of access to data stored on government servers. In order to support the needs of government server managers, a technology that can accommodate security needs in accessing the server is needed, the authors design this access through a Virtual private server Layer 2 Tunneling Protocol Over IP Security and port knocking which allows managers who have access rights to access the network. locally via the public internet network securely.

Key Word: Technology , VPN l2TP over IPsec, Port Knocking, MikroTik

1. PENDAHULUAN

Perkembangan teknologi mempengaruhi pola hidup masyarakat salah satu nya adalah cara masyarakat berkomunikasi dan melakukan pertukaran informasi. Sebagian besar masyarakat saat ini telah beralih menggunakan internet sebagai sarana pertukaran informasi dikarenakan dinilai lebih cepat dari sarana konvensional seperti berkirim surat. Maka tanpa disadari internet menjelma menjadi sebuah kebutuhan dasar bagi sebagian besar masyarakat. Dalam hal ini pemerintah melihat perlunya suatu sistem pemerintahan yang mengakomodir kebutuhan tersebut, salah satunya dengan keluaranya Peraturan Presiden nomor 95 tahun 2018 tentang pemerintahan berbasis elektronik. Dalam hal penerapannya, pemerintah

membutuhkan server data yang terpusat dan pengelolaan akses terhadap data pada server-server tersebut. Keamanan akses terhadap data tersebut dinilai penting agar dapat melindungi dari potensi serangan siber dan pencurian data. Agar pengelola dapat melakukan konfigurasi system dan jaringan secara aman melalui jaringan publik atau internet maka dibutuhkanlah suatu skema akses yang dapat yang dapat mengakomodir kebutuhan tersebut, salah satunya yaitu dengan cara membuat jalur khusus diatas jaringan publik dengan enkripsi tertentu seperti *layer 2 tunneling protocol over IP Security pre-shared key* dan menambahkan skema otentikasi seperti *port knocking* setelah mengakses melalui jalur tersebut serta memaksimalkan peran *firewall* dengan melakukan *filtering port* agar dapat mengatur akses port tertentu berasal dari jaringan yang telah ditentukan.

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan public dan menggunakannya untuk dapat bergabung dengan jaringan lokal. [1]

Port-knocking adalah sebuah konsep menyembunyikan layanan jarak jauh di dalam sebuah firewall yang memungkinkan akses ke port tersebut hanya untuk mengetahui service setelah klien berhasil diautentikasi ke firewall. Hal ini dapat membantu untuk mencegah pemindai untuk mengetahui service apa saja yang saat ini tersedia di host.[2]

Port scanning adalah teknik mendeteksi port-port yang terbuka pada sebuah komputer. Kita dapat melakukan port scanning pada komputer lain melalui jaringan. Tujuannya hanyalah untuk melihat port-port berapa saja yang terbuka pada komputer tersebut.[2]

L2TP adalah protokol layer 2 yang mengkombinasikan keunggulan keunggulan fitur protokol L2F (*Layer 2 Forwarding*) yang di kembangkan oleh Cisco dan PPTP (*Point-to-Point Tunneling Protocol*) yang dikembangkan oleh Microsoft, L2TP menyediakan akses *remote dial-up* ke suatu jaringan korperasi dengan beragam *protocol* dan terenkripsi melalui Internet [3]

IPSec menyediakan layanan keamanan pada lapisan IP dengan mengizinkan sistem untuk memilih protokol keamanan yang diperlukan, menentukan algoritma yang akan digunakan pada layanan, dan menempatkan kunci kriptografi yang diperlukan . IPSec dapat digunakan untuk melindungi satu atau lebih jalur antara sepasang *host,* antara sepasang *security gateway*, atau antara *security gateway* dengan *host.* [3]

2. METODE PENELITIAN

Penelitian akan menerapkan pengembangan sistem dengan menggunakan metode *Network Development Life Cycle (NDLC)*. Adapun tahapan dalam menggunakan metode NDLC terdiri dari: *Analysis, Design, Simulation/Prototyping, Implementation, Monitoring, Management.*[4] Adapun tahapan dalam penerapan metode NDLC dapat dilihat pada gambar 1 dibawah ini.

Gambar 1.Diagram NDLC

2.1 Analysis

Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan pengguna, dan analisa topologi jaringan yang sudah ada saat ini. Metode yang digunakan adalah sebagai berikut:

2.1.1. Pengamatan (*Observasi)*

Yaitu dengan cara mengambil data secara langsung di lokasi penelitian yang dalam hal ini berarti Dinas komunikasi dan informatika kota Palembang.

2.1.2. Wawancara *(Interview)*

2.1.3.

Yaitu dengan cara bertanya langsung dengan pihak pihak yang terkait dalam memberikan informasi mengenai pengelolaan jaringan yang dilakukan pada Dinas komunikasi dan informatika kota Palembang.

2.1.4. Literatur

Yaitu dengan mengumpulkan *data* dengan cara mencari dan mempelajari *data-data* yang diperoleh dan juga mencari referensi lain yang berhubungan dengan penulisan laporan penelitian tugas akhir.

2.2 Design

Pada tahap ini, dilakukan pembuatan topologi rancangan berdasarkan dari data yang diperoleh pada saat proses *analysis* dan menentukan skema yang diinginkan dalam penerapan port knocking.

2.3 Simulation/Prototyping

Setelah merancang *design* topologi jaringan dan skema *port knocking*, dilakukan ujicoba dengan melakukan konfigurasi Mikrotik RB951G-2HnD.

2.4 Implementtation

Pada tahap ini penulis melakukan konfigurasi terhadapat router mikrotik CCR 1036-12G-4S untuk server L2TP/IPSec, CCR 1009-8G-1S-1S+ untuk Skema PortKnocking dan konfigurasi vpn client pada Laptop HP Envy 13.

2.5 Monitoring

Pada tahap ini, dilakukan pengamatan hasil implementasi untuk melihat dan memastikan konfigurasi berjalan sesuai dengan harapan dan memonitor pengguna layanan dengan Bot Telegram.

2.6 Management

Pada tahap management, dilakukan dengan membuat aturan yang disepakati guna mengatur pengguna sistem yang sudah dikembangkan agar dapat berlangsung lama dan dapat memenuhi harapan.

2.7 Waktu Penelitian

Waktu penelitian yang dilaksanakan pada Dinas Komunikasi dan Informatika mulai bulan1 Juni 2022 dan diperkirakan akan berakhir sampai bulan 13 Juli 2022.

2.8 Tempat Penelitian

Lokasi yang menjadi tempat penulis melaksanakan penelitian adalah Dinas komunikasi dan informatika kota Palembang, Jl. Nyoman Ratu No. 1271 Kel. Sungai pangeran Kecamatan Bukit kecil Kota Palembang

3. HASIL DAN PEMBAHASAN

Dalam penelitian ini, penulis melaksanakan penelitian berdasarkan metode yang di pilih yaitu *Network Development Life Cycle (NDLC)* secara berurutan, mulai dari *analysis,design,simulation/prototyping,monitoring* hingga ke *management.*

3.1 Analysis

Pada Tahapan ini penulis melakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan pengguna, dan analisa topologi jaringan yang sudah ada saat ini. Metode yang digunakan adalah sebagai berikut:

a. Pengamatan (*Observasi)*

Dalam tahap ini, penulis melakukan observasi langsung di kantor Dinas Komunikasi dan Informatika Kota Palembang dengan mengambil data secara langsung dengan cara melihat perangkat yang digunakan dan melakukan *Port Scanning* dengan menggunakan Nmap-Zenmap 7.92 terhadap server sehingga mendapatkan data port yang terbuka yaitu FTP = 21, SSH = 22, MySql = 3306, Apache httpd = 80, 443 dan 8080 dimana port-port tersebut dapat langsung diakses melalui jaringan publik/internet.

Tabel. 1 Hasil Uji Coba Akses Open Port Dari Jaringan Publik/Internet

L2TP/IPSec PSK	Port Knocking	Akses Port					
		21	22	80	443	8080	3306
x	x	☑	☑	☑	☑	☑	☑

x	Tidak Ada
☑	Sukses

b. Wawancara *(Interview)*

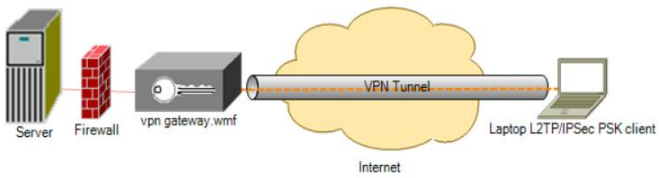
Wawancara dilakukan dengan bertanya kepada pihak-pihak yang terkait yaitu kepala seksi tata kelola dan kepala seksi infrastruktur bidang E-Government dan kepala seksi persandian bidang teknologi informasi persandian dalam memberikan informasi mengenai pengelolaan jaringan dan keamanan yang diinginkan Dinas Komunikasi dan Informatika kota Palembang.

c. Literatur

Yaitu dengan mengumpulkan data dengan cara mencari dan mempelajari data-data yang diperoleh dan juga mencari referensi lain yang berhubungan dengan penulisan penelitian seperti, VPN L2TP/IPSec Pre-Shared Key, Port Knocking, Port Scanning, Firewall.

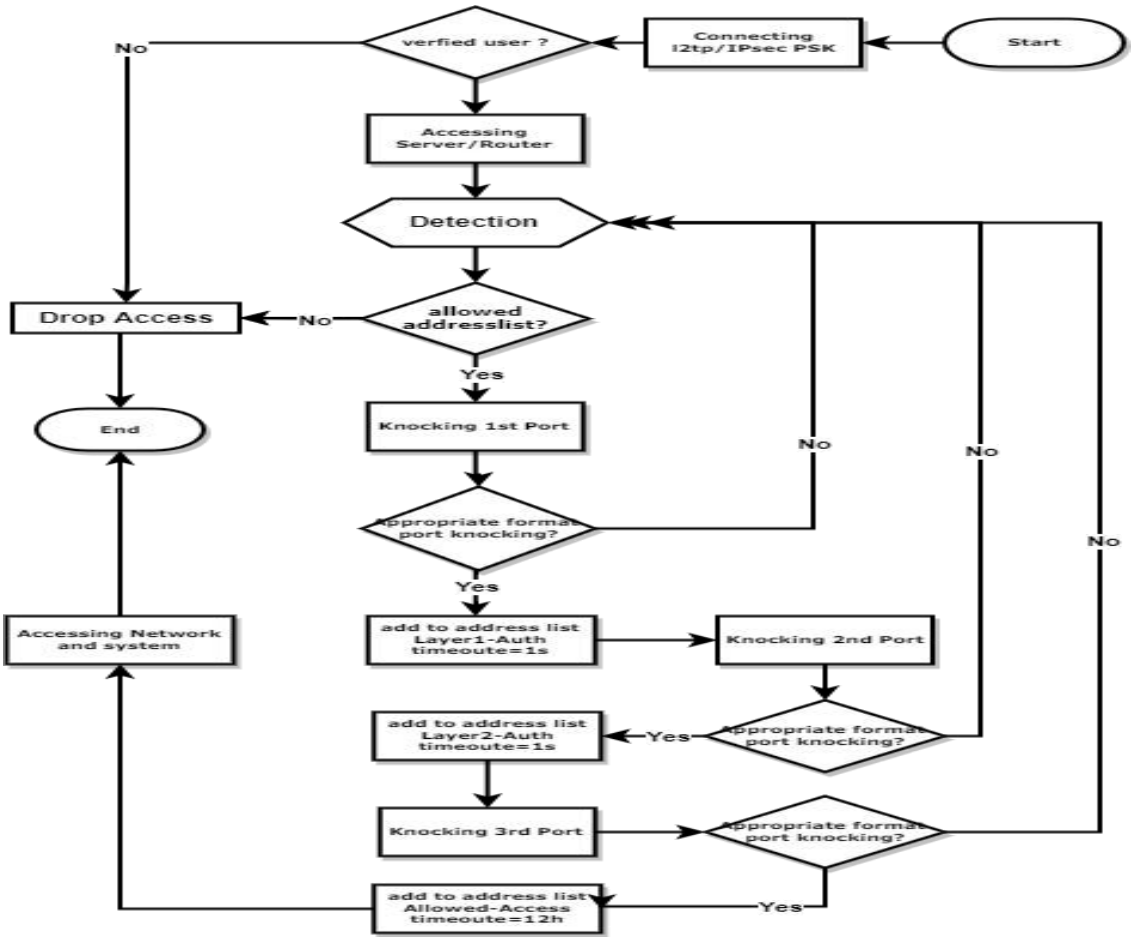
3.2 *Design*

Pada tahap ini, dilakukan perencanaan dan pembuatan topologi rancangan berdasarkan dari data yang diperoleh pada saat proses *analysis* dan menentukan skema yang diinginkan dalam penerapan port knocking. *Design* topologi yang dirancang yaitu remote akses pengguna terhadap jaringan dan server di dinas Komunikasi dan Informatika Kota Palembang seperti yang dijelaskan pada Gambar 2. Topologi Jaringan VPN.



Gambar 2. Topologi Jaringan VPN

Setelah menetapkan topologi jaringan, penulis melanjutkan perancangan dengan membuat skema akses terhadap jaringan dan server dimana pengguna harus mendapatkan akses melalui VPN L2TP/IPsec PSK kemudian melakukan skema *port knocking* yang telah disepakati seperti yang dijelaskan pada Gambar 3. Skema alur akses Server di bawah ini.



Gambar 3. Skema alur akses server

3.3 *Simulation/Prototyping*

Setelah merancang *design* topologi jaringan dan skema alur akses server, selanjutnya dilakukan uji coba dengan melakukan konfigurasi Mikrotik RB951G-2HnD yang nanti nya konfigurasi di dalam router ujicoba ini akan di terapkan ke dalam router *Mikrotik CCR 1009+* dan *Mikrotik CCR 1036.*

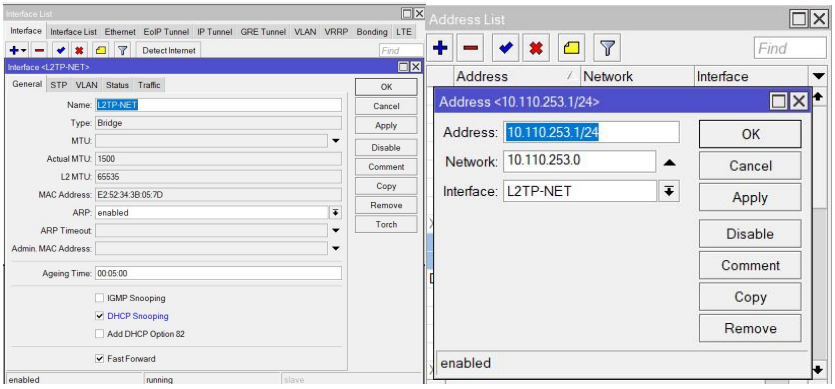
3.4 *Implementation*

Pada tahap ini penulis melakukan konfigurasi terhadapat router mikrotik CCR 1036-12G-4S untuk server L2TP/IPSec, CCR 1009-8G-1S-1S+ untuk Skema PortKnocking dan konfigurasi vpn client pada Laptop HP Envy 13.

a) Proses Pembuatan VPN L2TP/IPsec Pre-Shared Key

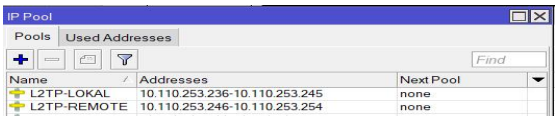
Langkah pertama yaitu proses Input IP address dengan menggunakan IP Public pada interface bridge public pada menu IP>addresses>add yang mana IP tersebut akan digunakan sebagai IP server L2TP/IPsec Pre-Shared Key. Kemudian Membuat interface bridge L2TP-NET

pada menu Bridge>add Name L2TP-NET dan input IP pada interface tersebut pada menu IP>address>add. IP 10.110.253.1/24, Interface L2TP-NET.



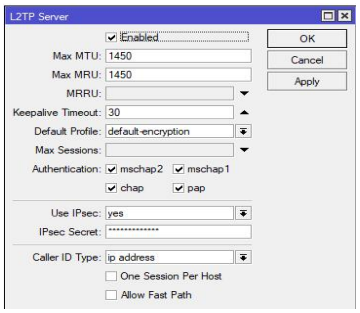
Gambar 4. Proses Pembuatan *interface bridge* L2TP-NET dan input IP pada *interface bridge*

Membuat IP Pool untuk L2TP-LOKAL dan L2TP-REMOTE pada menu IP>Pool>add



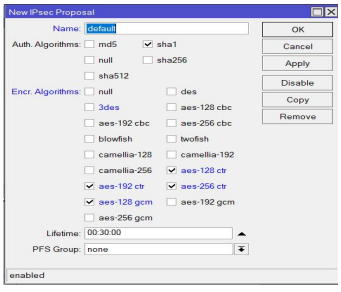
Gambar 5. Membuat *IP POOL* untuk *L2TP*

Mengaktifkan L2TP server di menu PPP>interface>L2TP Server>enable pada router Mikrotik dan mengaktifkan IPsec dan memasukan IPsec Secret



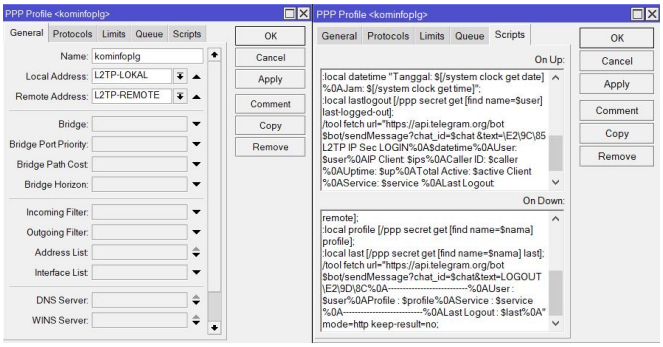
Gambar 6. *Enabling L2TP Server* dan aktifasi *IPsec*

Setelah melakukan setting terhadap L2TP server konfigurasi dilanjutkan dengan melakukan setting terhadap IPsec dengan memilih algoritma enkripsi yang diinginkan pada menu IP>IPSec Tab Proposals.



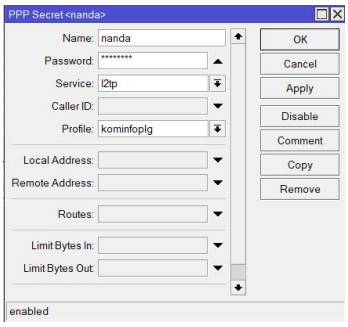
Gambar7 . IPsec Proposal

Untuk mengatur akun user yang akan dibuat guna pengaksesan L2TP server agar akun tersebut mendapatkan IP yang telah ditentukan sebelumnya yaitu pada IP Pool L2TP-LOKAL dan L2TP-REMOTE maka pembuatan profile *pada* menu PPP>profiles>general pada *form Local Address* dipilih L2TP-LOKAL dan *Remote Address* dipilih L2TP-REMOTE dan agar pengelola dapat memantau pengguna VPN L2TP/IPsec, maka diperlukan konfigurasi script dengan memasukan BOT_ID dan CHAT_ID API Bot telegram yang telah dibuat pada aplikasi telegram. Setelah *Script* selesai dibuat maka script tersebut dapat dimasukan pada menu PPP>Profiles>kominfoplg>Scripst>On Up dan On Down.



Gambar 8. Konfigurasi *VPN user Profile*

Setelah pembuatan profile dilanjutkan Kembali untuk pembuatan user pengguna VPN L2TP/IPsec pada menu PPP>Secrests>add dan gunakan profile kominfoplg yang telah dibuat sebelumnya.



Gambar 9. Secret PPP, Username dan Password untuk VPN

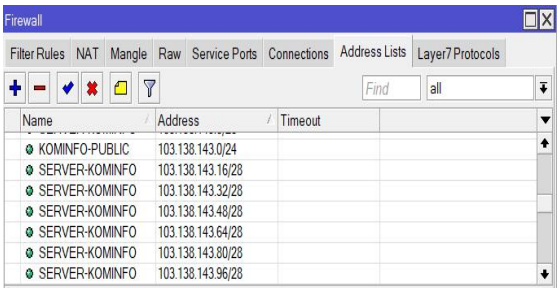
a) Konfigurasi VPN L2TP/IPsec Pres-Shared Key pada *client.*

Pada tahap ini penulis menggunakan sistem operasi *Windows 10 64bit.* Konfigurasi dilakukan pada menu *Windows>Settings>Network & Internet>VPN>Add a VPN connection* dengan memasukan IP Public yang telah di input pada interface bridge PUBLIC, VPN type L2TP/IPsec with pres-shared key, masukan pre-shared key yang telah dibuat pada saat pembuatan L2TP server IPsec secret pada Langkah diatas, gunakan *user name and password* pada type of sign-in info dan masukan *username dan password* yang telah dibuat.

b) Proses Pembuatan Skema Port Kncoking

Pada tahap ini penulis membuat rule pada firewall agar memblokir akses terhadap port tujuan server kominfo yang telah ditentukan dari Internet maupun intranet yang diawali dengan

membuat *Address List* KOMINFO-PUBLIC dan SERVER-KOMINFO pada menu *IP>Firewall>Address Lists>add*



Gambar 10. *Firewall Address Lists*

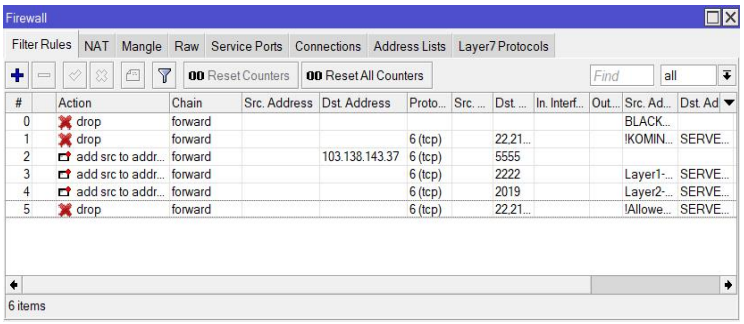
Membuat *Firewalls Rules* pada menu *IP>Firewall>Filter Rules>Add>Chain = Forward, Protocol TCP, Dst Port =21,22>Advanced Src addresslist = KOMINFO-PUBLIC* dengan ! *Dst Address List* = SERVER-KOMINFO> Action Drop.

Setelah membuat *rule block port* dari internet, langkah selanjutnya proses pembuatan skema port knocking dengan cara menangkap IP yang melakukan knocking terhadap port 5555 timeoute 1 detik ,2222 timeout 1 detik dan 2019 ke IP 103.138.143.37 secara berurutan dengan memasukan IP tersebut ke dalam Address List Layer1-Auth, Layer2-Auth dan Allowed-Access. Jika proses knocking dilakukan secara benar sesuai format maka IP tersebut akan dimasukan ke dalam *Allowed-address* yang memiliki time out 12 Jam.

Konfigurasi *Layer1-Auth* pada menu firewall > Filter Rules > Add. *Chain forward, Protocol TCP, Dst Port 5555 > Src Address List* KOMINFO-PUBLIC , *Dst Address List* SERVER-KOMINFO> Action add *src to address list ,address list Layer1-Auth, Time Out 00:00:01.*

Konfigurasi *Layer2-Auth* pada menu firewall>Filter Rules>Add. *Chain forward, Protocol TCP, Dst Port 2222 > Src Address List Layer1-Auth, Dst Address List* SERVER-KOMINFO > Action add *src to address list, address list Layer2-Auth, Time Out 00:00:01.*

Konfigurasi *Allowed-Access* pada menu firewal l> Filter Rules > Add. *Chain forward, Protocol TCP, Dst Port 2019 > Src Address List Layer2-Auth, Dst Address List* SERVER-KOMINFO > Action add *src to address list, address list Allowed-Access, Time Out 12:00:00.*



Gambar 11. *Firewall Filter Rules List*

3.5. *Monitoring*

Pada tahap ini, dilakukan pengamatan hasil implementasi untuk melihat dan memastikan konfigurasi berjalan sesuai dengan harapan dengan cara mencoba skema yang telah ditentukan dan memonitor pengguna layanan dengan Bot Telegram.

Tabel 2. Tabel Uji Coba Skema Akses.

No	L2TP/IPSec PSK			Port Knocking			Akses VPN L2TP/ IPSec PSK	Masuk dalam Allowed Access	Akses Port					
	Username	Password	Pre-shared Key	port 5555	port 2222	Port 2019			21	22	80	443	8080	3306
1	X	x	x	x	x	X	☒	☒	☒	☒	☑	☑	☒	☒
2	X	x	x	✓	x	X	☒	☒	☒	☒	☑	☑	☒	☒
4	X	x	x	✓	✓	X	☒	☒	☒	☒	☑	☑	☒	☒
5	X	x	x	✓	✓	✓	☒	☒	☒	☒	☑	☑	☒	☒
6	✓	x	x	x	x	X	☒	☒	☒	☒	☑	☑	☒	☒
7	✓	x	✓	✓	x	X	☒	☒	☒	☒	☑	☑	☒	☒
8	✓	✓	x	✓	✓	X	☒	☒	☒	☒	☑	☑	☒	☒
9	✓	✓	x	✓	✓	✓	☒	☒	☒	☒	☑	☑	☒	☒
10	✓	✓	✓	x	x	X	☑	☒	☒	☒	☑	☑	☒	☒
11	✓	✓	✓	✓	x	X	☑	☒	☒	☒	☑	☑	☒	☒
12	✓	✓	✓	✓	x	✓	☑	☒	☒	☒	☑	☑	☒	☒
13	✓	✓	✓	✓	✓	X	☑	☒	☒	☒	☑	☑	☒	☒
14	✓	✓	✓	✓	✓	✓	☑	☑	☑	☑	☑	☑	☑	☑

X	Salah / Tidak Ada	☒	Gagal
✓	Benar	☑	Sukses

Dari tabel diatas, dapat diambil kesimpulan bahwa percobaan akses ke port 21,22,8080 dan 3306 tanpa menggunakan VPN dan port knocking tidak berhasil dan hanya dapat mengakases port 80 dan 443 dikarenakan yang memang tidak dilakukan filtering terhadapat kedua port tersebut dikarenakan sebagai sarana akses internet terhadap website di dalam server tesebut. Pengakses yang terhubung dengan VPN namun tidak mengetahui skema port knocking tidak dapat mengakses port 21,22,8080 dan 3306 tanpa membangun koneksi ke server L2TP. untuk mengakses server mengharuskan pengakses menggunakan L2TP/IPsec PSK dan melakukan *port knocking* sesuai skema dan dilakukan secara berurutan agar mendapatkan akses ke server. Apabila pengakses sukses membangun koneksi terhadap server VPN L2TP/IPsec Pre-Shared Key maka router akan mengirimkan notfikasi melalui chat bot telegram.

Gambar 12. Laporan *Chat Bot Telegram* pada group NetwatchEGOV

2.6 Management

Pada tahap *management*, dilakukan pembuatan aturan yang disepakati berdasarkan hasil implementasi dan monitoring guna mengatur pengguna sistem *VPN L2TP/IPsec Pre-Shared Key* yang sudah dikembangkan agar dapat berlangsung lama dan dapat memenuhi harapan.

Adapun aturan yang disepakati sebagai berikut:

a) Pihak yang dapat mengakses server adalah pihak yang memiliki akun VPN L2TP/IPsec Pre-Shared Key yang terdata pada Dinas Komunikasi dan Informatika Kota Palembang.
b) Pihak yang telah memiliki akun VPN L2TP/IPsec Pre-Shared Key yang terdata mendapatkan skema port knocking untuk akses lebih lanjut.
c) Dilakukan perubahan pre-shared key secara berkala.
d) Dilakukan perubahan skema port knocking secara berkala.
e) Pihak yang belum terdaftar sebagai pengguna akun VPN L2TP/IPsec Pre-Shared Key dapat mengajukan permohonan kepada Dinas Komunikasi dan Informatika Kota Palembang melalui seksi Persandian dan Infrastruktur dengan menyertakan data pendukung.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilaksanankan dengan judul Strategi Pengamanan Akses Jaringann Dengan *Layer 2 Tunneling Protocol IP Security pre-shared key* dan *Port Knocking* dapat diambil kesimpulan sistem pengamanan tersebut dapat mengurangi resiko serangan percobaan akses dan membuat pengakses yang tidak terdaftar/terdata tidak dapat mengakses ke port yang telah ditentukan agar tidak dapat melalui jaringan publik/internet. Chat Bot Telegram dapat membantu pengelola untuk memonitor kegiatan akses terhadap server L2TP/IPsec Pre-Shared Key.

5. SARAN

Pengamanan Akses Jaringan Dengan *Layer 2 Tunneling Protocol IP Security pre-shared key* dan *Port Knocking* masih membutuhkan *assessment* lebih lanjut terhadap port-port yang digunakan dalam pengelolaan server dan memaksimalkan keamanan dengan mengguanakan IDS dan IPS pada firewall dan juga dapat menggunakan *honeypot* sebagai pengecoh penyerang terhadap server.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Allah subhanahu wa ta'ala yang memberikan kesempatan dan kemampuan penulis untuk menyelesaikan jurnal ini, kepada Nabi Muhammad Shallallahu alaihi wasallam yang membawa cahaya kebenaran hingga akhir zaman, kepada Kepala Dinas Komunikasi dan Informatika Kota Palembang Bp. H.Edison, S.Sos., M.Si. yang telah memberikan ijin untuk saya melakukan penelitian, kepada Universitas Binadarma khususnya kepada Bp. Alex Wijaya,S.Kom.,M.I.T. sebagai pembimbing pembuatan jurnal, Bp Fatoni,M.Kom, MM yang telah memberikan masukan dan saran, Bp. Suryayusra,M.Kom. yang telah memberikan masukan dan saran dan Kepada Orangtua, Istri, anak dan saudara yang telah memberikan support yang sebesar-besarnya.

DAFTAR PUSTAKA

[1] Rachmawan, A. (2018). Perbandingan Protokol L2TP dan PPTP Untuk Membangun Jaringan Intranet di Atas VPN. *Jurnal Manajemen Informatika*.

[2] Amarudin. (2018). Analisis Dan Implementasi Keamanan Jaringan Pada Mikrotik Router Menggunakan Metode Port Knocking. *Seminar Nasional Sains Dan Teknologi 2018*.

[3] Attabis, Aan Khusna.2011.Analisis Keamanan Protokol L2TPv3 Over IPsec pada site to site VPN (virtual private network). Tugas Akhir, Universitas Islam Indonesia,2011.

[4] Idhom, Muhammad. HE Wahanani & Akhmad Fauzi.2020. Network Security Application Using the Port Knocking Method. International Conference on Science and Technology 2019.

[5] Kusuma, A. P. 2016. Implementasi Simple Port Knocking Pada Dynamic Routing (OSPF) Menggunakan Simulasi GNS3. Jurnal Manajemen Informatika Volume 5 Nomor 2.

[6] Ayub, M., Maulana, A., & Fauzi, A. 2021. Penerapan Firewall Dan Protokol IpSec/L2TP Sebagai Solusi Keamanan Akses Jaringan Publik. *Computer Science (CO-SCIENCE).*, https://doi.org/10.31294/coscience.v1i2.435

[7] Amien, J. A. (2020). Implementasi Keamanan Jaringan Dengan Iptables Sebagai Firewall Menggunakan Metode Port Knocking. *Jurnal Fasilkom*

[8] Saputro, Andik., Nanang Saputro dan Hendro Wijayanto. 2020. Metode Demilitarized Zone dan Port Knocking Untuk Keamanan Jaringan Komputer. CybeSecurity dan Forensik Digital Col.3, No.2 Tahun 2020.

[9] Khan, S., Shiraz, M., Boroumand, L., Gani, A., & Khan, M. K. (2017, November 1). Towards port-knocking authentication methods for mobile cloud computing. *Journal of Network and Computer Applications*. Academic Press. https://doi.org/10.1016/j.jnca.2017.08.018.

[10] Major, W., Buchanan, W. J., & Ahmad, J. (2020). An authentication protocol based on chaos and zero knowledge proof. *Nonlinear Dynamics*, *99*(4), 3065–3087. https://doi.org/10.1007/s11071-020-05463-3.