Jurnal Jaringan Komputer dan Keamanan
JJKK, Vol. 04, No. 03, October 2023: 1-10
Received: 9 July 2023; Revised: 27 September 2023; Accepted: 2 October 2023

Perancangan dan Implementasi VPN Metode IPSEC Site to Site Menggunakan Fortigate Pada PT Linksindo Makmur

Muhammad Gages Alvisyahri, Sidik

Program Studi Teknik Informatika, Fakultas Teknologi Informasi
Universitas Nusa Mandiri
email : muhammadgages24@gmail.com
Jl. Damai Raya No 8, Jakarta 12150, Indonesia

Abstract

PT. Linksindo Makmur is a company engaged in providing contact center services, starting from contact center applications, recruiting employees for contact centers, and places for contact centers. PT. Linksindo Makmur daily exchanges data and information as well as communication between the head office and branch offices. The problems that occur in PT. Linksindo Makmur is the frequent disconnection of network connections between the head office and branches when you don't want it, because the equipment at the branch office is not the same as the equipment at the head office so that these problems interfere with the performance of PT.Linksindo Makmur employees. Due to the company's problems, the design of a VPN (Virtual Private Network) with the IPsec Site to Site method using Fortigate is one of the authors' proposals for a secure means of communication and data transfer and maintaining data validity. The results of the design and implementation that the author made is very good because there are no longer obstacles to the disconnection of the network connection between the head office and branch offices. The advantage of this research is that using a VPN IPsec Site to Site will be safer and easier to implement. The Fortigate device not only functions as a Firewall but also acts as a router, gateway, antivirus, VPN hub, anti spyware, antispam, proxy, and traffic shaping. Fortigate is very important for companies that care about data security. The drawback of this research is that it is almost non-existent, maybe for people who are not used to it, it will take time to get used to it.

Kata kunci: *Fortigate, IPSec, VPN*

Abstrak

PT. Linksindo Makmur merupakan perusahaan yang bergerak di bidang penyedia layanan contact center, mulai dari aplikasi contact center, perekrutan karyawan untuk contact center, dan tempat untuk contact center. PT. Linksindo Makmur setiap hari melakukan pertukaran data dan informasi serta komunikasi antar kantor pusat dan kantor cabang. Permasalahan yang terjadi pada PT. Linksindo Makmur yaitu sering terputusnya koneksi jaringan antar kantor pusat dan cabang disaat yang tidak inginkan, dikarenakan perangkat pada kantor cabang tidak sama dengan perangkat yang ada di kantor pusat sehingga permasalahan tersebut mengganggu kinerja karyawan PT.Linksindo Makmur. Dikarenakan permasalahan pada perusahaan tersebut, maka perancangan VPN (Virtual Private Network) dengan metode IPsec Site to Site menggunakan Fortigate merupakan salah satu usulan penulis agar sarana komunikasi dan transfer data yang aman dan menjaga validitas data. Hasil dari perancangan dan implementasi

yang penulis buat ini sangat baik karena tidak ada lagi kendala terputusnya koneksi jaringan antar kantor pusat dan kantor cabang. Kelebihan dari penelitian ini yaitu dengan menggunakan VPN IPsec Site to Site akan lebih aman dan mudah untuk di implementasikan. Pada perangkat Fortigate tidak hanya berfungsi sebagai Firewall saja namun juga berperan sebagai router, gateaway, antivirus, hub VPN, anti spyware,antispam, proxy, dan traffic shapping. Fortigate sangat penting untuk perusahaan yang mementingkan keamanan data. Kekurangan dari penelitian ini yaitu hampir tidak ada, mungkin bagi orang yang belum terbiasa akan membutuhkan waktu agar terbiasa.

Kata kunci: *format, paper, template (min. 3, maks. 5 kata, sesuai urutan abjad)*

1. PENDAHULUAN

VPN (Virtual Private Network) adalah teknologi komunikasi yang memanfaatkan koneksi internet untuk membangun tunnel melalui jaringan publik dan menggunakannya untuk terkoneksi langsung ke jaringan lokal, dengan cara itu maka diperoleh hak akses dan policy yang sama, seperti halnya berada di dalam sebuah jaringan local walaupun sebenarnya adalah menggunakan jaringan public. Jaringan VPN (Virtual Private Network) yaitu jaringan yang dibangun di atas sebuah tunnel [1][2][3]. Pada VPN terdapat banyak protokol untuk mendukung keamanan data. Protokol yang dapat digunakan untuk pengembangan VPN adalah Internet Protocol Security (IPSec). IPSec adalah suatu protocol yang menyediakan transmisi data terenkripsi yang aman pada network layer dalam jaringan [4][5].

Penggunaan infrastruktur yang handal pada jaringan komputer sangatlah berpengaruh untuk mendukung kinerja/ performanya. Firewall Adalah suatu sistem yang dirancang untuk mencegah akses yang tidak diinginkan dari atau ke dalam suatu jaringan internal. firewall bekerja dengan cara melacak dan mengendalikan [6][7]. Firewall merupakan suatu mekanisme/system/cara yang digunakan baik terhadap perangkat keras (hardware), perangkat lunak (software) ataupun system itu sendiri bertujuan untuk melindungi suatu jaringan komputer, baik dengan membatasi, menyaring bahkan menolak kegiatan/hubungan segment jaringan pribadi dengan segment jaringan luar yang bukan merupakan ruang lingkup jaringan tersebut. Segment itu bisa merupakan sebuah Server, Workstation, Router, atau LAN. FortiGate merupakan sebuah sistem keamanan jaringan komputer berupa firewall yang dikeluarkan oleh perusahaan yang bernama Fortinet sebagai pemimpin pasar untuk Unified Threat Management (UTM) [8][9][10].

Fortinet adalah perusahaan yang berasal dari California yang berfokus pada pengembangan layanan produk computer security dan cyber security. FortiGate hadir sebagai salah satu produk perangkat yang menawarkan sistem keamanan menyeluruh dalam paket yang dilengkapi dengan beragam fleksibilitas dan kemudahan serta fungsi pendukung firewall lainnya. PT Linksindo Makmur merupakan sebuah perusahaan yang bergerak di bidang penyedia jasa contact center, penyedia tempat contact center dan penyedia aplikasi system jaringan untuk contact center. Perusahaan ini berdiri sejak tahun 2000, yang pusatnya berlokasi di Proklamasi Jakarta pusat dan cabangnya yang berada di Borobodur Jakarta Pusat.

2. METODOLOGI PENELITAN

Metode penelitian adalah suatu cara bagaimana seorang penulis mendapatkan data yang dilakukan secara sistematis untuk memahami suatu bahasan, permasalahan, dan pemecahan masalah tersebut dalam sebuah system [11[12]. Berikut adalah metode penelitian yang digunakan:

2.1 Metode Pengumpulan Data

Untuk memperoleh data yang penulis butuhkan, penulis menggunakan metode penelitian sebagai berikut :

A. Observasi

Penulis melakukan peninjauan langsung dan mengamati proses kerja khususnya pada bagian jaringan Local Area Network (LAN) dan Wide Area Network (WAN) di PT Linksindo Makmur.

B. Wawancara

Melakukan pengumpulan data dan informasi dengan cara melakukan tanya jawab secara langsung dan sistematis, dan penulis melakukan wawancara secara langsung kepada kepala IT
yaitu Pak Rio dan kepada karyawan yang memakai jaringan komputer di PT Linksindo Makmur.

C. Studi Pustaka

Untuk memeriksa masalah secara mendalam yang berhubungan dengan penulisan skripsi ini, maka penulis melakukan studi pustaka dengan mengumpulkan data teoritis dan mempelajari buku atau literature dengan maksud untuk mendapatkan teori dan bahan yang berkaitan dengan masalah tersebut.

2.2 Analisis Penelitian

Dalam skripsi yang dibuat ini, penulis melakukan analisa penelitiannya dengan menggunakan [13][14][15]:

A. Analisa Kebutuhan

Tahap ini dilakukan analisis pada topologi jaringan yang ada, dan menganalisis kebutuhan user, serta menganalisis sistem jaringan yang akan diterapkan.

B. Desain

Di tahap desain ini yaitu membuat desain topologi jaringan yang akan dibangun dengan menggunakan metode Virtual Private Network (VPN) dari data-data yang diperoleh sebelumnya.

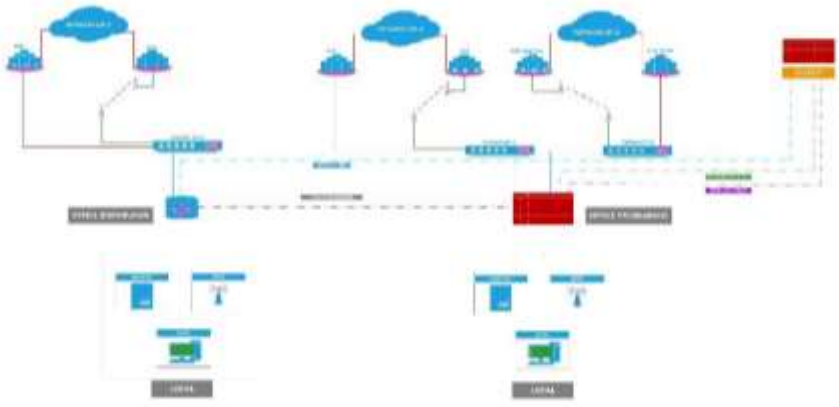
C. Testing

Tahap ini penulis akan melakukan testing menggunakan software GNS3 dan VMWare.

3. HASIL DAN PEMBAHASAN

3.1 Topologi Jaringan

Setelah melakukan riset di PT. Linksindo Makmur, penulis dapat menyimpulkan bahwa topologi yang dipakai adalah topologi star. Karena adanya penggunaan beberapa router utama yang terhubung ke router utama lain nya.



Gambar 1: Topologi Jaringan PT. Linksindo Makmur

3.2 Arsitektur Jaringan

Kantor pusat PT. Linksindo Makmur menggunakan protocol TCP/IP. Protokol ini mencakup protokol DHCP, DNS, SMTP dan masih banyak lainnya. Dalam pengalamatan IP di kantor ini menggunakan IP Versi 4 (IPv4) dengan menggunakan metode DHCP server sebagai pusat layanan jaringan yang otomatis memberikan IP address ke perangkat user dengan menggunakan IP kelas C, dikarenakan jumlah computer user ataupun alat network lainnya masih dalam skala kecil.

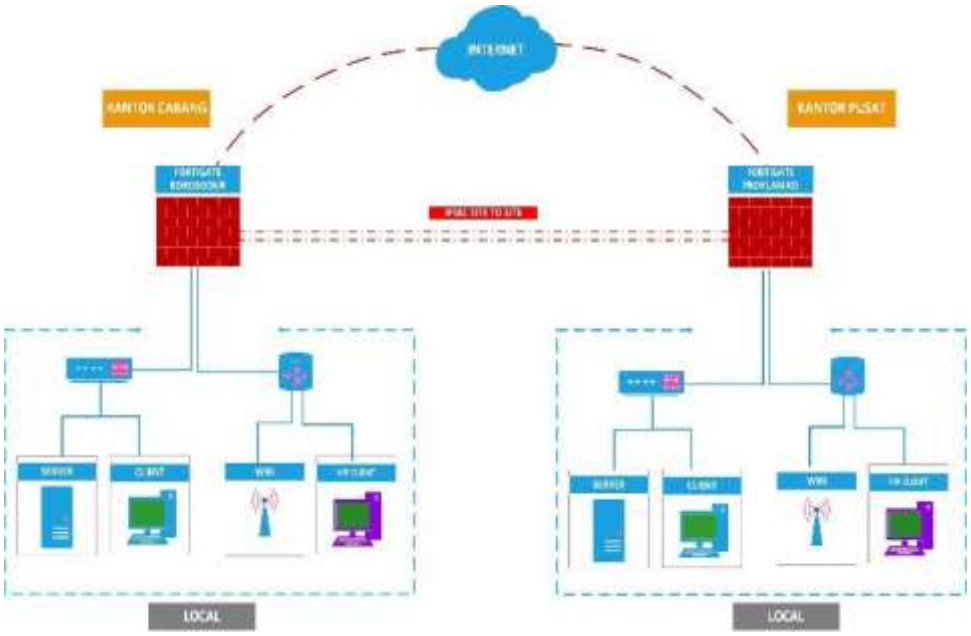
Model sistem yang digunakan adalah sistem Client-Server, sebuah aplikasi dibagi menjadi dua bagian yang terpisah, tetapi masih merupakan sebuah kesatuan yaitu komponen client dan komponen server.

Komponen client biasa disebut sebagai front end, sedangkan komponen server biasa disebut sebagai back end. Komponen client menyiapkan data-data yang akan dimasukkan oleh user dengan memakai teknologi pemrosesan tertentu lalu mengirimkannya kepada komponen server, pada umumnya dalam bentuk permintaan terhadap layanan yang dimiliki oleh server.

Komponen server akan menerima permintaan dari client, dan memprosesnya lalu mengembalikan hasil pemrosesan tersebut kepada client. Client pun akan menerima informasi hasil pemrosesan data yang dilakukan oleh server dan menampilkannya kepada user, dengan menggunakan aplikasi yang berinteraksi dengan user.

3.3 Skema Jaringan

Setelah penulis melakukan riset di PT. Linksindo Makmur, penulis dapat menggambarkan topologi bentuk jaringan komputer yang berada di PT. Linksindo Makmur. Adapun skema jaringan komputer pada PT. Linksindo Makmur yaitu terdapat pada gambar sebagai berikut:



Gambar 2: Skema Jaringan PT. Linksindo Makmur

3.4 Keamanan Jaringan

Keamanan jaringan yang ada pada PT. Linksindo Makmur sudah sangat bagus dengan adanya firewall pada konfigurasi hardware seperti router serta keamanan lainnya menggunakan

software antivirus. Akan tetapi, penulis mengusulkan jika dalam jaringan PT. Linksindo Makmur menggunakan Virtual Private Network (VPN) dengan metode IPsec site to site pada Fortigate.

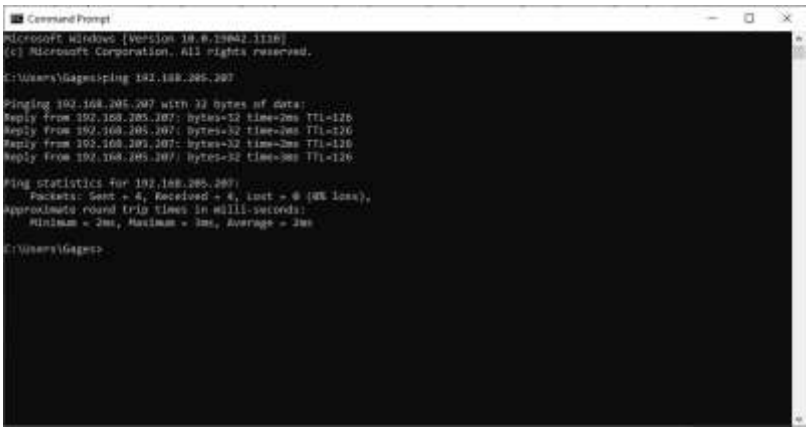
3.5 Pengujian Jaringan

Dalam hal membangun suatu jaringan komputer perlu dilakukan pengujian terhadap jaringan yang telah dirancang dan dibangun sebelumnya, hal ini untuk memastikan bahwa semua sistem yang sudah dibuat berjalan dengan baik dan normal serta sesuai dengan yang direncanakan.

3.6 Pengujian Jaringan Awal

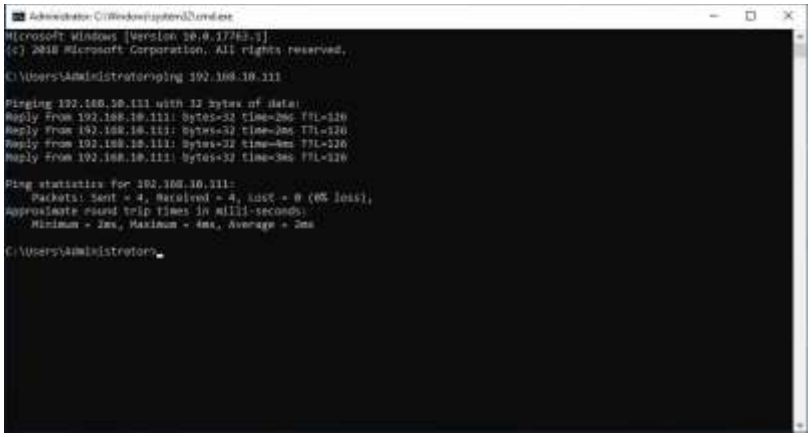
Dalam pengujian jaringan awal dimana pada simulasi belum diterapkan rancangan usulan yang penulis berikan untuk jaringan pada PT. Linksindo Makmur. Dimana belum diterapkannya fortigate pada kantor cabang, jaringan aman dan lancar namun karena perbedaan perangkat router antar kantor seringkali IPsec terputus dan harus mengkoneksikan ulang secara manual.

1. Ping dari local pusat ke local cabang.



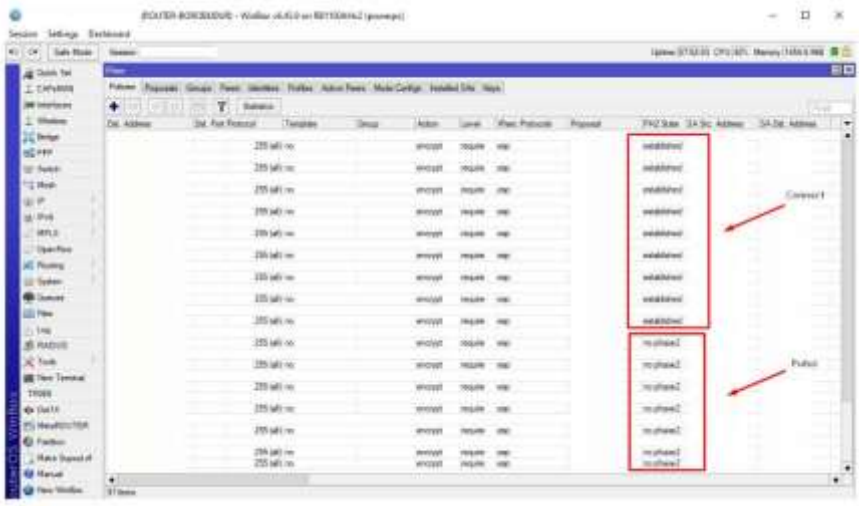
Gambar 3 Tampilan Ping Pusat ke Cabang Jaringan Awal

2. Ping dari local cabang ke local pusat.

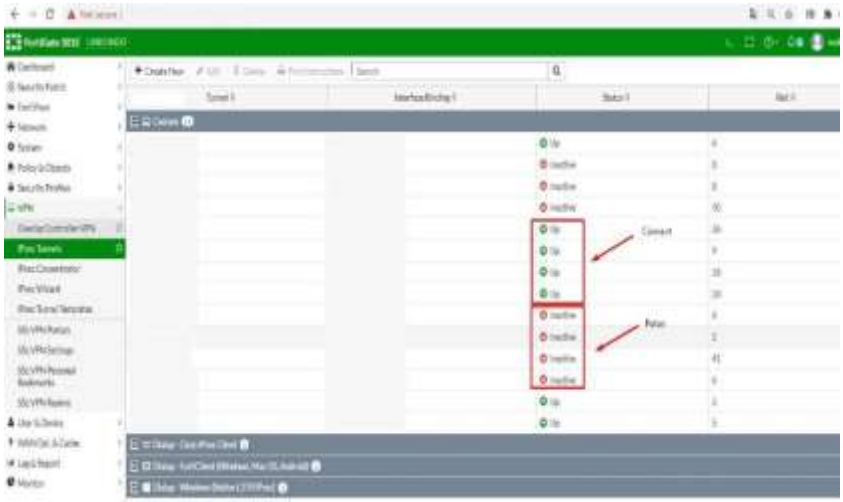


Gambar 4 Tampilan Ping Cabang ke Pusat Jaringan Awal

3. Koneksi IPsec pada kantor cabang saat terputus.



Gambar 5 Tampilan IPsec Router Cabang

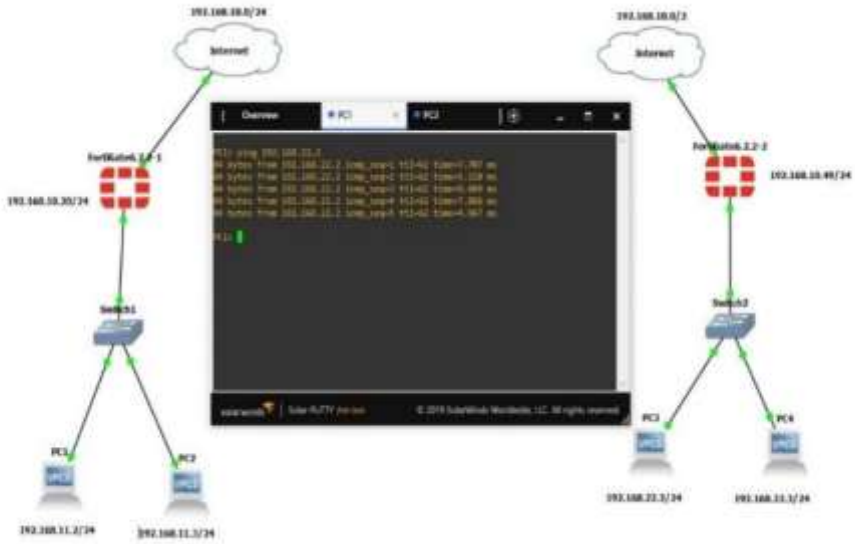


Gambar 6 Tampilan IPsec Router Pusat

3.7 Pengujian Jaringan Akhir

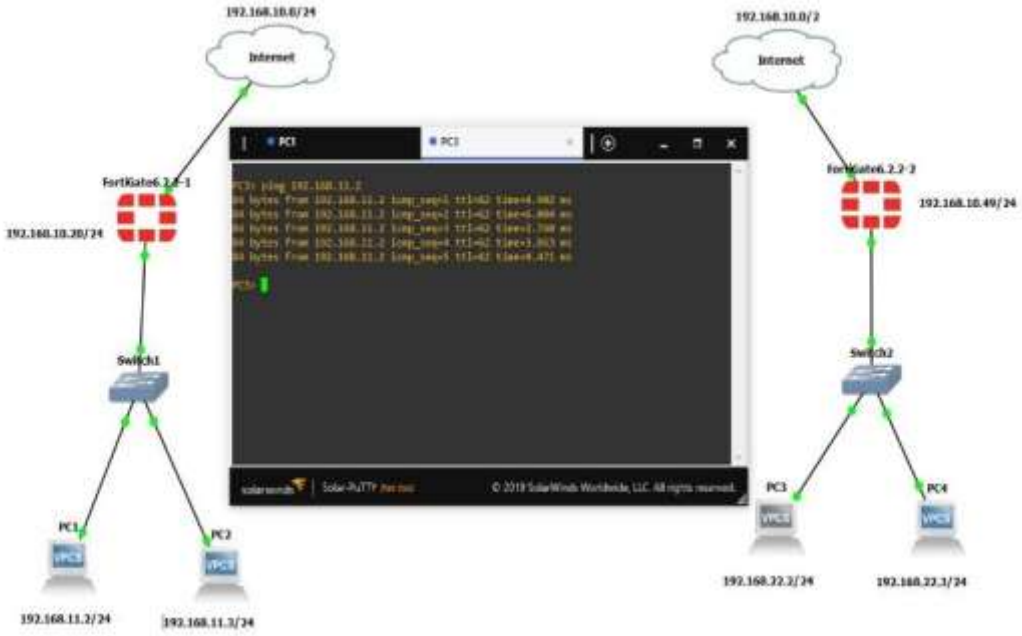
Hasil dari pengujian jaringan akhir yang telah menerapkan jaringan usulan yang penulis berikan untuk pemecahan masalah pada jaringan PT. Linksindo Makmur. Dengan memberikan tambahan fortigate pada kantor cabang, agar IPsec antar kantor tidak mengalami kendala terputus saat karyawan sedang berkomunikasi atau bertukar data antar kantor. Berikut hasil simulasi yang dibuat:

1. Ping dari local pusat ke local cabang.



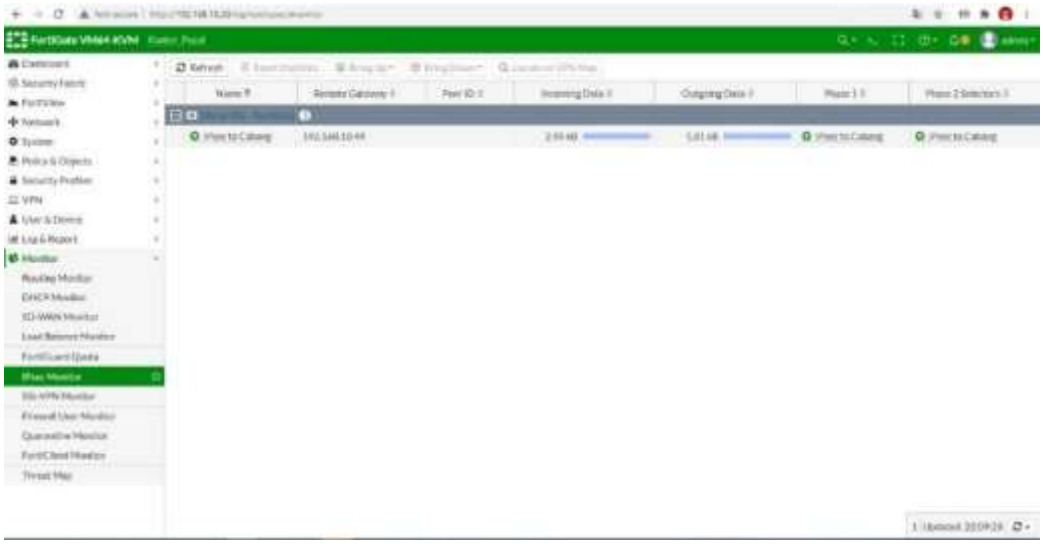
Gambar 7 Tampilan Ping Pusat ke Cabang Jaringan Akhir

2. Ping dari local cabang ke local pusat.



Gambar 8 Tampilan Ping Lokal Cabang ke Pusat Jaringan Akhir

3. Koneksi IPsec fortigate antar kantor pusat dan cabang yang sudah terhubung status nya akan berubah menjadi up dan terlihat traffic incoming dan outgoing data. Maka jaringan local kantor pusat dan cabang sudah bisa saling terkoneksi satu sama lain.



Gambar 9 Tampilan Koneksi IPsec Pada Fortigate Pusat

Gambar 10 Tampilan Koneksi IPsec Pada Fortigate Cabang

4. KESIMPULAN

Beberapa kesimpulan dari hasil yang didapat selama penulis melakukan perancangan dan implementasi jaringan pada PT Linksindo Makmur, adalah sebagai berikut:

1. Untuk mengatasi masalah pertukaran informasi data penting dengan ukuran yang besar dapat diterapkan sistem jaringan VPN IPsec pada jaringan komputer. Dengan diterapkannya jaringan VPN IPsec, maka antara kantor pusat dan cabang akan saling terhubung dengan mudah, sehingga memberikan akses data yang baik, cepat dan aman.

2. Jaringan VPN dengan metode IPSec merupakan protocol IP dengan teknik tunneling, dengan metode ini tingkat keamanan transfer data lebih baik dan dengan IP Security data juga akan terenkripsi.
3. IPsec menyediakan layanan keamanan Authentication, Data Integrity, dan Confidentiality, oleh karena itu, system security ini dapat di terapkan pada PT. Linksindo Makmur untuk kepentingan dan kerahasiaan data dan untuk kepentingan karyawan perusahaan tersebut.
4. Dari hasil implementasi jaringan pada PT.Linksindo Makmur, jaringan antar kantor pusat dan cabang berjalan dengan baik dengan Fortigate tanpa terputus dan tidak perlu mengkoneksikan kembali secara manual.

Referensi

[1]. T. E. Madhadi, "Analisis Perbandingan Performasi QoS VPN Encryption Protocol Pada Jaringan Berbasis Hybrid Cloud," *J. Ilm. Komputasi*, vol. 20, no. 1, pp. 69–82, Mar. 2021, doi: 10.32409/jikstik.20.1.2695.

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

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

[4]. I. Melyana and T. Indriyani, "Analisa Quality Of Service Dan Implementasi Voice Over Internet Protocol Dengan Menggunakan IPSEC VPN," *Integer J.*, vol. 1. No. 2, pp. 53–66, 2016.

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

[6]. A. Sutiman, Gunawan, "Firewall Port Security Switch Untuk Keamanan Jaringan Komputer Menggunakan Cisco Router 1600S Pada Pt. Tirta Kencana Tata Warna Sukabumi," *CONTEN (Computer Netw. Technol.*, vol. 1, no. 1, pp. 13–22, 2021.

[7]. 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.

[8]. H. Suryantoro, A. Sopian, and Dartono, "Penerapan Teknologi Fortigate Dalam Pembangunan Jatingan VPN-IP Berbasis IPSEC," *J. Elektro dan Inform. Swadharma(JEIS)*, vol. 01, no. 1, pp. 12–20, 2021.

[9]. 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*.

[10]. 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*.

[11]. 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.

[12]. 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.

[13]. 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).

[14]. Negara, E. S. (2017). Perbandingan Redistribusi Routing Protokol Dinamis pada Exterior Gateway Protokol. In *Seminar Nasional Teknologi Informasi dan Komunikasi (SEMNASTIK 2017)*.
[15]. Andryani, R. (2016). Pengukuran risiko pada penerapan cloud computing untuk sistem informasi (studi kasus universitas bina darma). *Jurnal Teknologi Technoscientia*, 173-179.