Jurnal Pendidikan Teknologi dan Kejuruan
Vol. 21, No. 2, Juli 2024
P-ISSN: 0216-3241 E-ISSN: 2541-0652

DESAIN DATA CENTER PERBANKAN DENGAN METODE NETWORK DEVELOPMENT LIFE CYCLE (NDLC) (STUDI KASUS PT. BPR XYZ)

I W. Yudik Pradnyana[1)], K. Y. E. Aryanto[2)], I G. Aris Gunadi[3)]
[1,2,3] Program Studi Ilmu Komputer Program Pascasarjana,Universitas Pendidikan Ganesha
Email: yudik.pradnyana@gmail.com, yota.ernanda@undiksha.ac.id, igedearisgunadi@undiksha.ac.id

ABSTRAK

Perkembangan teknologi informasi telah menghasilkan berbagai produk dan layanan yang sangat dinamis mengikuti kebutuhan masyarakat termasuk dalam bidang perbankan. Untuk dapat menjalankan sistem elektronik ini, infrastruktur pusat data (*data center*) menjadi unsur penting yang harus dimiliki oleh institusi perbankan. Hal yang sama dibutuhkan oleh PT. BPR XYZ yang saat ini masih belum mengelola dengan baik pusat datanya. Kondisi topologi jaringan antar kantor saat ini belum baik sehingga perlu adanya topologi usulan. Perancangan keamanan *data center* dalam penelitian ini menggunakan *framework Open Enterprise Security Architecture* (O-ESA). *Framework* tersebut difokuskan pada penggunaan *Security Technology Architecture* pada bagian arsitektur layanan keamanan *(security services).* Metode yang digunakan dalam penelitian ini adalah *Network Development Life Cycle* (NDLC) sebagai acuan pada proses pengembangan keamanan *data center* di PT. BPR XYZ. Penelitian ini merekomendasikan desain jaringan antar kantor. Desain yang diberikan sudah melalui proses simulasi untuk membuktikan desain usulan lebih baik dari desain yang ada, sehingga desain usulan dapat diterapkan untuk keamanan *data center* pada PT. BPR XYZ. Pada topologi usulan menggunakan jaringan *dedicated* sebagai *virtual private network* (VPN) *server* dan pengamanan jaringan menggunakan traditional *firewall*. Topologi usulan mendukung *high avalability* dengan teknik *failover*.

Kata kunci: Desain, *Data Center*, Perbankan, *Security Technology Architecture, Network Development Life Cycle*

ABSTRACT

The development of information technology has produced a variety of products and services that are very dynamic following the needs of the community, including in the banking sector. To be able to run this electronic system, data center infrastructure is an important element that must be owned by banking institutions. The same thing is needed by PT BPR XYZ, which currently does not manage its data center properly. The current condition of the network topology between offices is not good so there is a need for a proposed topology. The data center security design in this research uses the Open Enterprise Security Architecture (O-ESA) framework. The framework is focused on the use of Security Technology Architecture in the security services architecture section. The method used in this research is Network Development Life Cycle (NDLC) as a reference to the data center security development process at PT BPR XYZ. This research recommends an inter-office network design. The design given has gone through a simulation process to prove that the proposed design is better than the existing design, so that the proposed design can be applied to data center security at PT BPR XYZ. The proposed topology uses a dedicated network as a virtual private network (VPN) server and network security using a traditional firewall. The proposed topology supports high avalability with failover techniques.

Keywords : *Design, Data Center, Banking, Security Technology Architecture, Network Development Life Cycle*

1. PENDAHULUAN

PT. BPR XYZ merupakan salah satu bank pekreditan rakyat (BPR) ada di Provinsi Bali. PT. BPR XYZ siap untuk memberikan pelayanan terbaik kepada masyarakat dan mendukung

perkembangan usaha mikro dan kecil yang berada Bali. Teknologi informasi dalam perbankan saat ini berkembang dengan sangat dinamis, mengikuti kebutuhan masyarakat terhadap produk serta layanan yang dimiliki institusi perbankan. Agar biaya operasional lebih efisiensi dan kualitas pelayanan lebih baik terhadap masyarakat, maka perbankan perlu untuk menyelenggarakan teknologi informasi. Penyelenggaraan yang dimaksud berupa sistem elektronik *core banking system* (aplikasi inti perbankan) yang digunakan untuk proses akhir seluruh transaksi perbankan serta pemutakhiran data dalam pembukuan.

Untuk menempatkan sistem elektronik tersebut, maka perbankan membutuhkan atau mengelola sebuah infrastruktur pusat data *(data center). Data center* merupakan gedung yang digunakan untuk menempatkan infrastruktur maupun perangkat lainya yang dipergunakan untuk menyimpan dan mengelolah infomasi oleh perusahaan [1]. Taylor [2] mendefinisikan *data center* sebagai sebuah infrastruktur yang terdiri dari sumber daya komputasi dan penyimpanan yang dapat memungkinkan distribusi aplikasi perangkat lunak dan data secara bersama serta menjadi krusial dalam mendukung operasional harian perusahaan dan kebutuhan konsumen. Menurut Ayoub, Omran [3] serta Shi, Bin [4] tujuan dari penggunaan *data center* yang utama adalah memberikan dukungan operasional kritis dan menyediakan layanan digital dengan menyimpan dan mengelola infrastruktur IT. *Data center* juga digunakan untuk memaksimalkan penggunaan sumber daya yang tersedia untuk meningkatkan ketangguhan suatu proses bisnis sebuah organisasi [5]. Desain *data center* harus fleksibel mendukung layanan baru dengan cepat [6]. Pada *data center* terdapat fasilitas peralatan elektronik yang dipergunakan untuk pemrosesan,dan penyimpanan data serta komunikasi *(network equipment)* dengan tujuan menunjang kelangsungan bisnis pada perusahaan [7]. Dengan adanya perkembangan jaringan dapat memperluas fungsionalitas jaringan pada *data center* dengan baik [8].

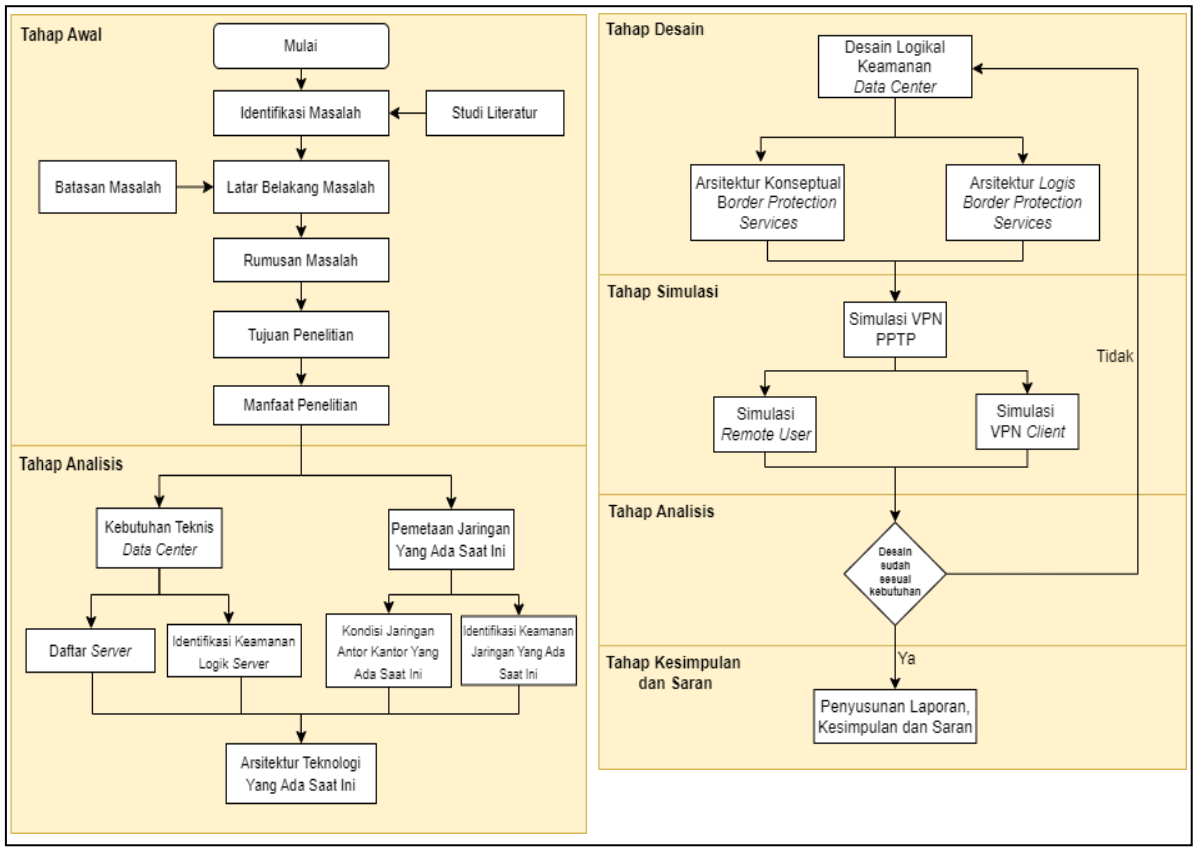
Berdasarkan hasil pengamatan pada pusat data PT. BPR XYZ didapatkan kenyataan bahwa *server* belum terkelola maupun terlindungi dengan baik. Selain itu infrastruktur jaringan belum terlindungi dengan baik sehingga tentunya memiliki kerentanan yang berpotensi untuk dapat dieksploitasi. Salah satu permasalahan yang menyebabkan hal tersebut adalah dikarenakan *data center* yang berada di PT. BPR XYZ belum memiliki standarisasi yang baku. *Data center* tidak memiliki standarisasi tersebut berimbas pada permasalahan keamanan sudah tentu berpotensi untuk membahayakan proses transaksi dalam institusi perbankan. Kerahasian informasi *data center* ini perlu diperhatikan [9].

Darmawan [10] melakukan penelitian sejenis dalam lingkungan fakultas dalam perguruan tinggi dan menemukan bahwa terdapat kerentanan baik secara fisikal maupun logikal dalam lembaga tersebut. Kendala pada penelitian tersebut ialah belum diketahui lebih detail mengenai kerentanan yang ada sehingga perlu dilakukan prosedur *vulnerability assessment* yang lebih dalam. Selain itu juga belum dijelaskan secara detail desain yang diusulkan. Dengan permasalahan yang serupa, sudah tentu perlu dilakukan pencermatan lebih mendalam terhadap permasalahan keamanan pada PT. BPR XYZ. Pada penelitian ini penulis akan menganalisis lebih dalam keamanan *data center* PT. BPR XYZ dan merancang suatu konsep keamanan *data center* usulan dengan menggunakan *framework Open Enterprise Security Architecture* (O-ESA). *Enterprise architecture* menerapkan prinsip-prinsip desain teknik dan menyediakan struktur lengkap untuk merancang dan membangun organisasi menggunakan skema klasifikasi dan representasi deskriptif [11]. *Virtual private network* (VPN) termasuk layanan yang dapat diterapkan pada *border protection service*. VPN digunakan untuk membuat saluran komunikasi yang aman dan terenkripsi melalui jaringan internet [12]. VPN diinstalasi pada *router mikrotik* dengan sistem operasi *linux base* [13]. Menggunakan jaringan pribadi virtual, atau VPN untuk memecahkan masalah keamanan jaringan [14]. VPN bekerja dengan berbagai cara. PPTP atau *point to point tunneling protocol* adalah salah satunya. Perlindungan informasi melalui *client* ke *server* pribadi disediakan oleh PPTP, komponen dari protokol jaringan [15]. Paket diubah menjadi datagram IP melalui PPTP dalam aplikasi [16].

Metode yang dipergunakan pada penelitian ini yaitu metode pengembangan sistem *Network Development Life Cycle* (NDLC). Metode tersebut dijadikan sebagai acuan pada proses pengembangan keamanan *data center* di PT. BPR XYZ. Metode *Network Development Life Cycle* (NDLC) melibatkan pengukuran kinerja jaringan dan desain topologi [17]. Pada penelitian ini dihasilkan desain jaringan antar kantor dan berhasil dilakukan simulasi untuk membuktikan desain usulan lebih baik dari desain yang telah ada saat ini. Pada topologi usulan terdapat *internet service provider* (ISP) ganda yang digunakan sebagai VPN *server* dan pengamanan jaringan menggunakan traditional *firewall* serta mendukung *high avalability*. Konfigurasi topologi *firewall* yang tidak lengkap dan banyak fitur *firewall* yang berbeda akan menyebabkan lalu lintas menjadi sangat besar dan diproses secara tidak benar [18].

2. METODE

Berdasarkan referensi dari penelitian pengembangan sistem, metode digunakan yaitu *Network Development Life Cycle* (NDLC). Berikut adalah tahap-tahap pada penelitian ini yang dapat dilihat pada Gambar 1.



Gambar 1. Tahapan penelitian

Tahap awal pada penelitian ini yaitu mengidentifikasi masalah dan latar belakang masalah yang digunakan untuk merancang perumusan masalah. Selanjutnya menentukan batasan masalah, tujuan dan manfaat penelitian. Kemudian dilakukan analisis terhadap kondisi yang ada saat ini. Data yang didapatkan seperti kebutuhan teknis *data center* dan pementaan jaringan yang ada saat ini. Kemudian dilanjutkan dengan tahap desain usulan keamanan *data center* logikal menggunakan *Open Enterprise Security Architecture* (O-ESA). Pada penelitian ini difokuskan pada penggunaan *security technology architecture* saja karena tujuan dari penelitian ini adalah menghasilkan desain usulan yang dapat diterapkan untuk keamanan *data center* di masa yang akan datang. Setelah dilakukan tahap desain dilanjutkan dengan tahap simulasi, dimana pada tahap ini berhasil disimulasikan bagaimana *user* melakukan akses ke *server* menggunakan *virtual private network* (VPN).

3. HASIL DAN PEMBAHASAN

Dari hasil analisis keamanan kondisi yang ada saat ini, baik pada kebutuhan teknis *data center* dan pemetaan jaringan didapat data kelemahan keamanan *data center* yang berupa daftar *server*, identifikasi keamanan logik *server*, kondisi jaringan antar kantor saat ini, identifikasi keamanan jaringan saat ini dan arsitektur teknologi saat ini.

Dari data tersebut perlu diusulkan desain keamanan *data center* yang baru. Keamanan yang dimaksud yaitu keamanan logikal *data center*. Pada perancangan usulan keamanan akan dibahas bagaimana rancangan pengamanan terhadap *server* pada lalu lintas data yang dilalui dan juga deteksi ancaman terhadap *server*.

A. Daftar *Server*

Berikut adalah daftar *server* di PT. BPR XYZ yang berhasil terobservasi dapat dilihat pada tabel di bawah ini.

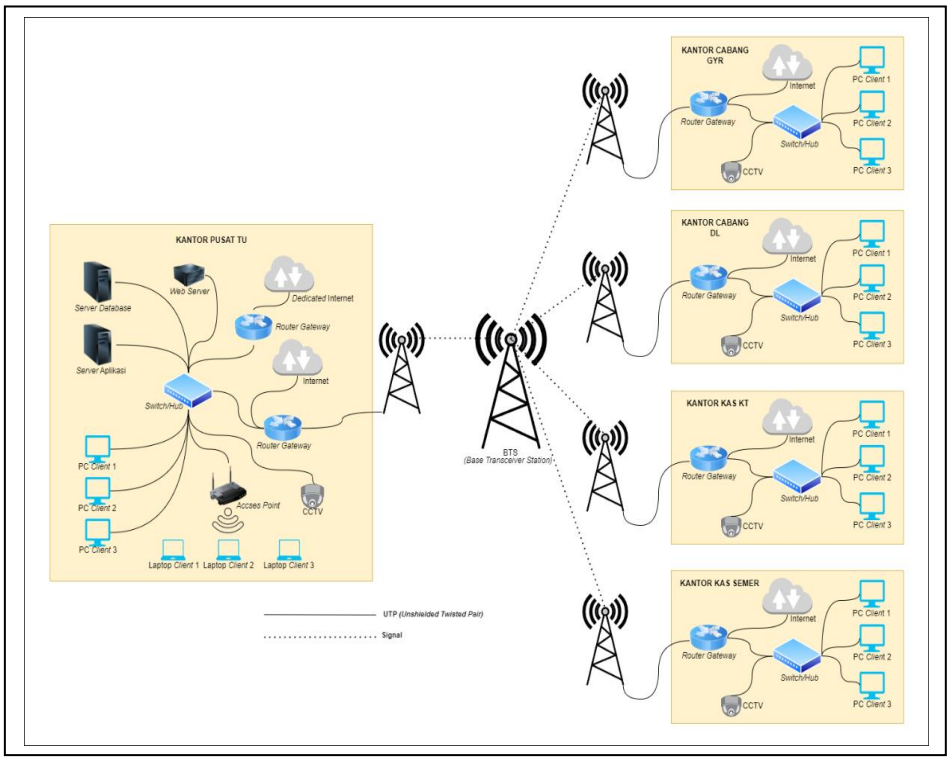
Tabel 1.Daftar server

No	IP *Local*	Fungsi	Layanan	*Operating System* (OS)
1.	172.20.20.2	*Server Database*	*Open* SSH, *Open mysql*	*Linux 2.6*
2.	172.20.20.3	*Server* Aplikasi	*Open http, Open mysql*	*Microsoft Windows 7*
3.	172.20.20.149	*Web Server*	*Open http, Open mysql*	*Windows 10 Pro*

Hasil observasi daftar *server* dapat dilihat pada Tabel 1. Untuk mendapatkan data daftar *server* digunakan *tools network mapper* (NMAP). Dari hasil observasi didapatkan data yang menunjukan bahwa *server* menggunakan sistem operasi yang belum diperbaharui.

B. Kondisi Jaringan Antar Kantor yang Ada Saat Ini

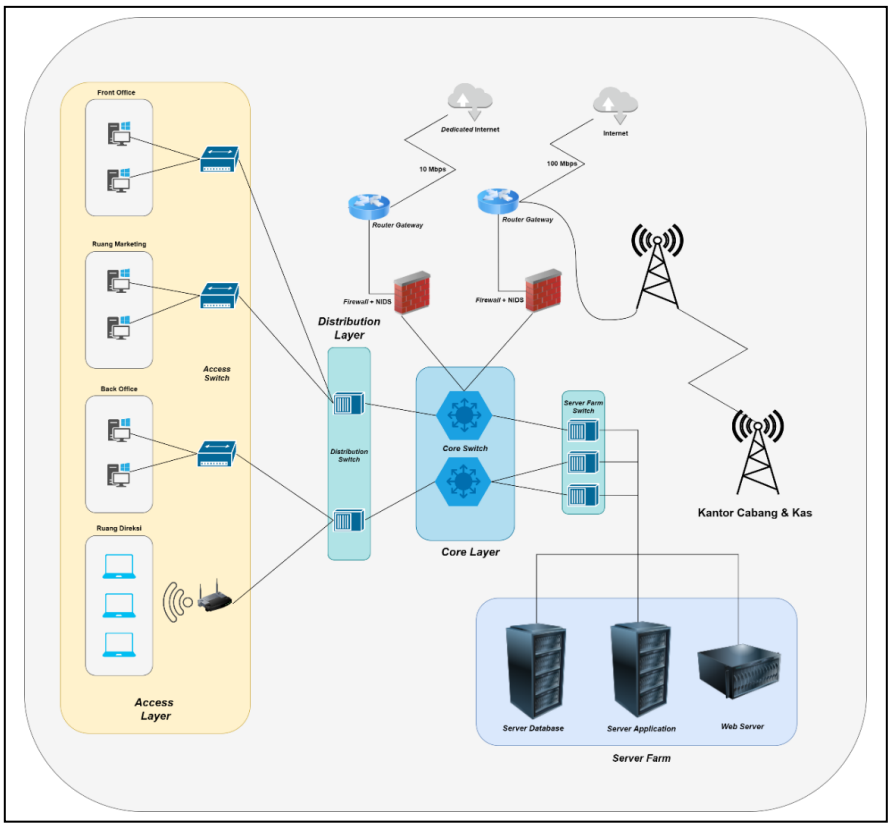
Berikut adalah topologi jaringan antar kantor saat ini di PT. BPR XYZ yang dapat dilihat pada Gambar *2*.



Gambar 2. Kondisi jaringan antar kantor yang ada saat ini

C. Arsitektur Teknologi yang Ada Saat Ini

Gambar 3. dibawah ini merupakan arsitektur teknologi yang sudah ada saat ini di PT. BPR XYZ.

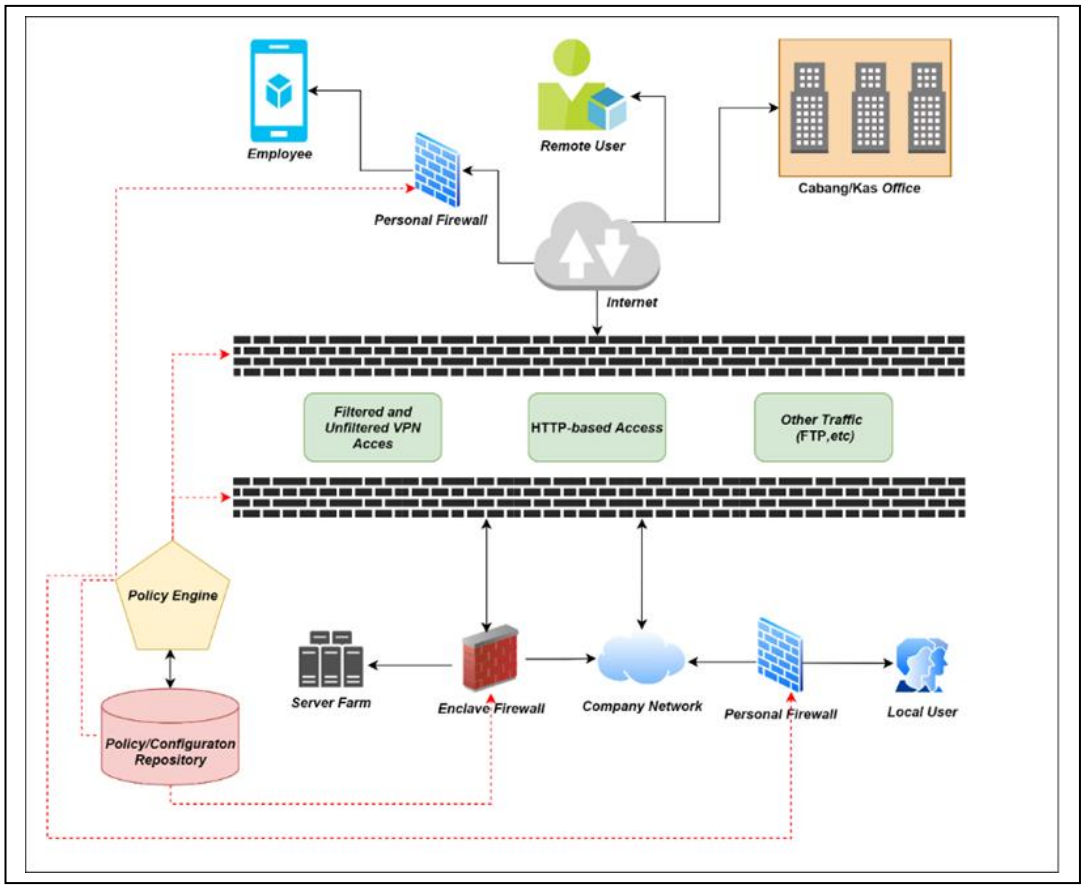


Gambar 3. Arsitektur teknologi yang ada saat ini

Gambar diatas adalah arsitektur teknologi yang di PT. BPR XYZ yang menggunakan arsitektur sistem informasi desentralisasi. Pada gambar diatas data disimpan secara terdistribusi. Semua *layer* yang berada dalam jaringan dibagi menjadi *core layer, distribution layer* dan *access layer*. Pada *access layer, client* menggunakan koneksi LAN (*local area network*) dengan perangkat keras berupa *switch* agar bisa terhubung dengan *server*. Sedangkan kantor cabang/kas menggunakan teknologi *wireless* agar bisa terhubung dengan *server*. Jaringan internet menggunakan dua koneksi dari penyedia layanan yaitu layanan *up to* dan *dedicated*. Pada arsitektur yang sudah ada, standar belum terpenuhi sehingga perlu diperbaiki.

D. Arsitektur Konseptual *Border Protection*

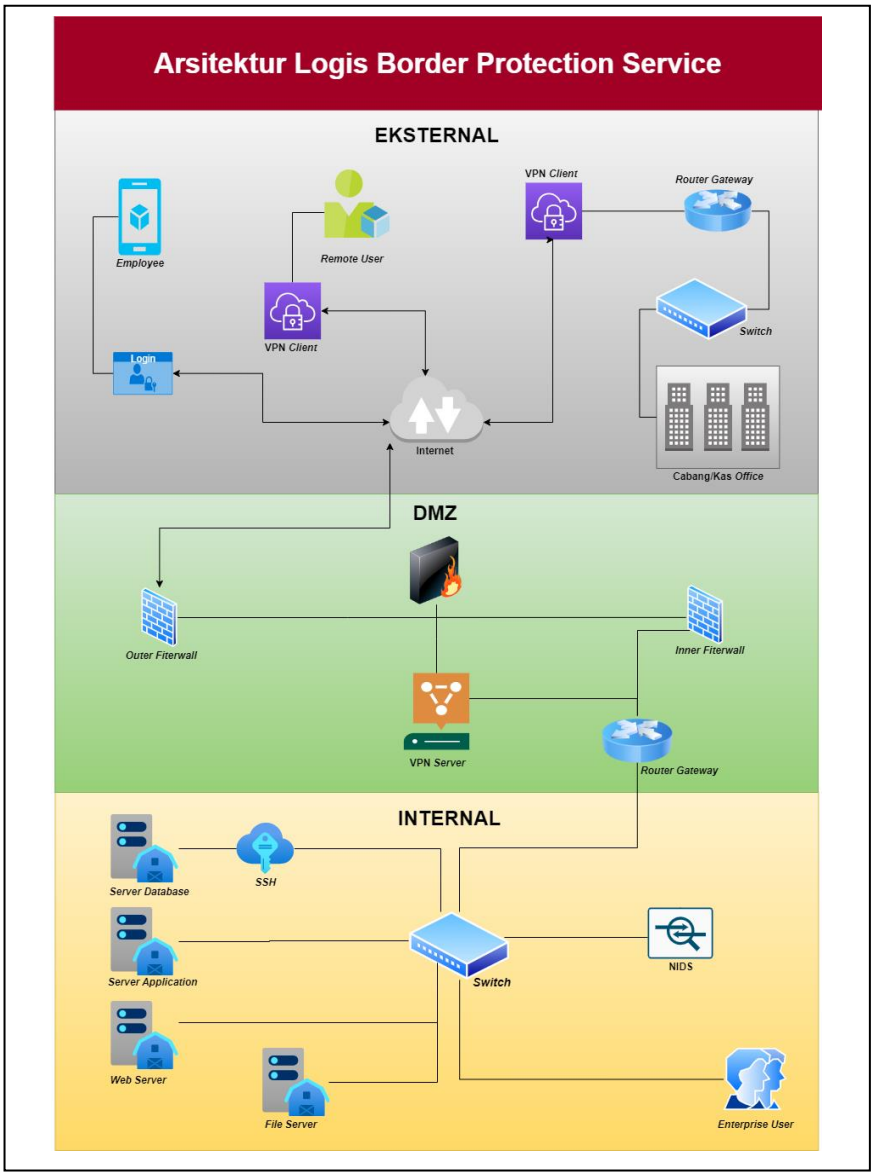
Border protection services mempunyai peran dalam pengendalian lalu lintas informasi yang melintas pada batas eksternal dengan internal diantara zona keamanan yang berdasarkan lokasi dari sumber lalu lintas dan tujuan lalu lintas secara fisik. Kebijakan pada *Open Enterprise Security Archictecture* (O-ESA) terdapat konfigurasi perangkat yang disediankan sebagai layanan perlindungi yang dikontrol dalam pusat kebijakan dan *resources* dengan penjelasan konfigurasi. Gambar dibawah ini merupakan arsitektur konseptual *border protection services*, *client* yang berada kantor cabang/kas, *remote user* dan employee dapat melakukan proses *remote login* dengan internet dengan memanfaatkan *virtual private network* (VPN) yang sudah ada pembatasannya *firewall* bagian dalam dan luar. Berikut adalah gambar arsitektur konseptual *border protection services* dapat dilihat pada Gambar 4.



Gambar 4. Arsitektur konseptual *border protection services*

E. Arsitektur Logis *Border Protection*

Dalam perancangan *Security Technology Architecture*, pada penelitian ini menetapkan *border protection* dan memprioritaskan arsitektur komunikasi berdasarkan diagram topologi jaringan serta *resource server farm* yang ada saat ini. Menurut standarisasi *Open Enterprise Security Architecture* (O-ESA) *Border Protection Service* merupakan layanan yang dipergunakan dalam mengontrol koneksi dari *server*. *Virtual private network* (VPN) termasuk layanan yang dapat diterapkan pada *border protection service*. Usulan yang akan dilakukan pada penelitian ini adalah penerapan VPN. Dengan adanya VPN komunikasi data antar kantor dan *remote client* keamanannya akan menjadi lebih baik. Berikut adalah gambar arsitektur logis *border protection* dapat dilihat pada Gambar 5.



Gambar 5. Arsitektur logis *border protection*

Pada gambar diatas digambarkan arsitektur logis *Border Protection Services* yang disesuaikan dengan kondisi saat ini. Ada tiga area dijelaskan pada gambar diatas. Area eksternal adalah area tempat *user* melakukan *login* akses*. area demilitarized zone* (DMZ) adalah area konektifitas antara external dengan internal. Area internal ini adalah area lingkungan *resource server farms* yang diletakan.

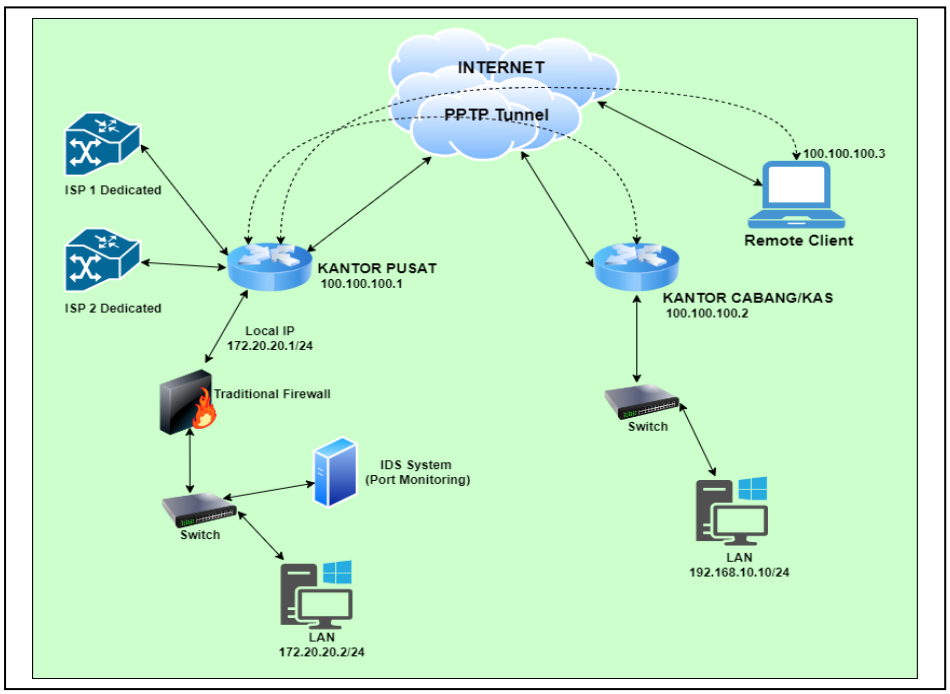
F. Simulasi Desain Usulan

G. Pada penelitian ini berhasil disimulasikan penerapan layanan *virtual private network* (VPN) dengan protokol PPTP *(point to point tunneling protocol)* pada jaringan antar kantor dan *remote user*. Untuk membuktikan desain usulan lebih baik daripada desain yang ada saat ini maka dilakukan simulasi terhadap desain yang diusulkan. Sebelum dilakukan simulasi berikut adalah topologi yang diusulkan untuk mengatasi permasalahan yang ada pada objek penelitian. Pada topologi usulan terdapat jaringan *dedicated* yang digunakan untuk VPN *server* dan pengamanan jaringan menggunakan traditional *firewall* serta mendukung *high avalability*. Berikut adalah gambar topologi usulan dapat dilihat pada

H.

I.

Gambar 6.



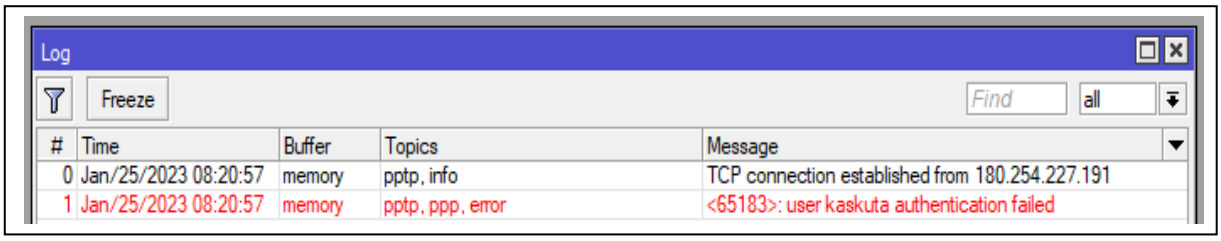
Gambar 6. Topologi usulan

Pada topologi ini sudah menerapkan konsep jaringan *client server*. Dalam topologi usulan menggunakan *internet service provider* (ISP) ganda. Jika ISP utama *down*, akan beralih otomatis ke ISP *backup*. Teknik yang digunakan pada topologi ini yaitu teknik *failover*. Dengan topologi usulan ini keamanan lebih baik dibandingkan topologi yang ada saat ini. Pada topologi usulan *server* yang digunakan sistem operasinya sudah diperbaharui. *Port* yang tidak digunakan ditutup dan juga proses memindai *port* tidak bisa dilakukan karena penyerang harus terhubung dengan *virtual private network* (VPN) untuk bisa mengetahui IP *address* lokal *server*.

J. Kehandalan Keamanan Desain Usulan

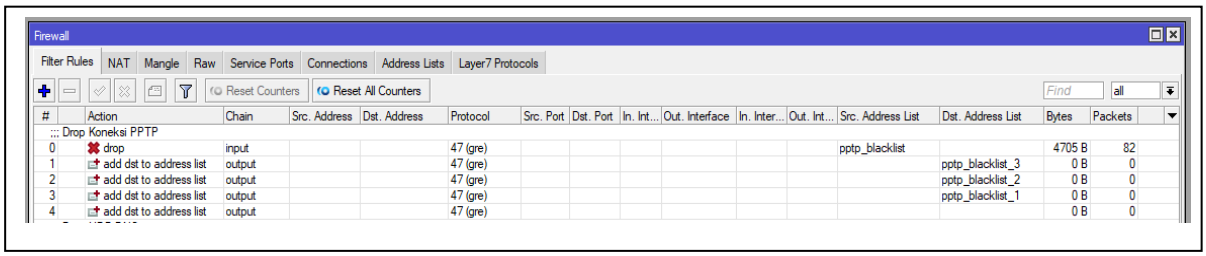
Pada simulasi keamanan komunikasi usulan menggunakan *protocol* TCP dengan port 1723 dan IP *protocol* 47/GRE. *Client* menggunakan *username* dan *password* agar bisa terhubung dengan komunikasi PPTP *server*. Kehandalan PPTP yaitu dapat menfilter serangan *bruto force* pada PPTP *server*.

Pada simulasi keamanan desain usulan terdapat *rule* baru yang berfungsi untuk mendeteksi koneksi *input* dari *port* GRE yang melakukan percobaan untuk terkoneksi ke PPTP *server*. *Rule* ini bekerja ketika ada koneksi ke PPTP *server* yang gagal terkoneksi karena *username* dan *password* salah dan apabila terdapat kesalahan selama tiga kali maka akan di *drop* selama satu hari. Jadi dalam satu hari IP publik *client* akan terblokir. Berikut adalah gambar PPTP *client* yang gagal terkoneksi karena salah *username* dan *password* dapat dilihat pada Gambar 7.



Gambar 7. PPPT *client* gagal terkoneksi

Pada gambar diatas disimulasikan *client* yang gagal melakukan proses autentikasi *client* yang dapat dilihat pada log *router*. Gambar 8. dibawah ini merupakan gambar untuk *drop* pada *rule* yang dibuat.



Gambar 8. *Drop* PPTP *client*

K. Perbandingan Desain yang Ada Saat Ini dengan Desain Usulan

Dari hasil akhir penelitian dilakukan perbandingan antara kondisi yang sudah ada saat ini dengan hasil desain kemanan usulan. Desain *data center* usulan standar yang digunakan adalah *Open Enterprise Security Architecture* (O-ESA). O-ESA memiliki layanan pada *border protection service* seperti adalah *virtual private network* (VPN), *secure shell* (SSH), packet *filtering service* dan *proxy*. Selain itu juga pada topologi usulan mendukung *high avalability*. Berikut adalah perbandingannya desain yang sudah ada saat ini dengan desain usulan dapat dilihat pada Tabel 2.

Tabel 2. Perbandingan desain yang ada saat ini dengan desain usulan

No.	Parameter	O-ESA	Kondisi yang Ada Saat Ini	Kondisi Usulan
	Penerapan layanan *border protection service*			
1.	Memiliki layanan v*irtual private network* (VPN) untuk akses *server* baik di kantor cabang/kas maupun *remote user*	Dibutuhkan	X	V
2.	Memiliki layanan *secure shell* (SSH) untuk media *transfer* data secara jarak jauh atau *remote*	Dibutuhkan	X	V
3.	Memiliki *fitur intrusion detection system* (IDS) dan manajemen akses	Dibutuhkan	X	V
4.	Mendukung *high avalability*	Dibutuhkan	X	V

Pada desain usulan menggunakan topologi *client server* sehingga fungsi dan aplikasi terpusat. Dengan penerapan teknologi *virtual private network* (VPN) pada desain usulan tingkat keamanan komunikasi data akan lebih baik karena data dikirim dan diterima melalui *tunnel* yang membutuhkan nama pengguna, kata sandi dan alamat *server* agar bisa terhubung ke *data center*. Dengan menggunakan VPN, *remote* layanan terhadap *secure shell* (SSH) bisa dilakukan secara jauh dengan memanfaatkan media internet dan dengan adanya desain usulan ini perbankan tidak lagi menggunakan jasa pihak ketiga untuk komunikasi datanya dan jika desain usulan ini diimpementasikan pada nantinya *network administrator* dapat akses penuh terhadap perangkat yang ada sehingga dapat dikonfigurasi dan diterapkannya *fitur intrusion detection system* (IDS) dan dapat dilakukan manajemen akses. Selain itu juga topologi usalan mendukung *high avalability* dengan teknik *failover.*

4. SIMPULAN DAN SARAN

Pada penelitian ini berhasil mengidentifikasi keadaan jaringan dan keamanan logik *server* yang ada saat ini dan dapat disimpulkan bagaimana desain arsitektur teknologi yang ada di perbankan. Selanjutnya dirancang desain usulan keamanan *data center* dengan standar yang ada. Berhasil disimulasikan layanan *virtual private network* (VPN) *point to point tunneling protocol* (PPTP) menggunakan *internet service provider* (ISP) *dedicated* ganda dengan traditional *firewall* serta topologi usulan mendukung *high avalability*. Dengan dilakukannya simulasi terhadap desain usulan dapat disimpulkan desain usulan lebih baik dari desain yang ada saat ini. Adapun saran yang dapat diuraikan dari hasil penelitian ini yaitu melakukan prosedur *vulnerability assessment* yang lebih dalam terhadap aspek keamanan *data center* dan sebaiknya PT. BPR XYZ segera menerapkan desain yang diusulkan untuk memitigasi risiko teknologi informasi.

DAFTAR PUSTAKA

[1] P. D. G. and H. J. L. de S. A.F. Santos, “New Data Center Performance Index: Perfect Designs Data Center-PDD,” *J. Clim.*, vol. October, 2020.
[2] P. Taylor, *Data Centers - Statistics & Facts. Statista*. 2022. [Online]. Available: https://www.statista.com/topics/6165/datacenters/#topicOverview
[3] O. Ayoub, O. Huamani, F. Musumeci, and M. Tornatore, “Efficient Online Virtual Machines Migration for Alert-Based Disaster Resilience,” *2019 15th Int. Conf. Des. Reliab. Commun. Networks, DRCN 2019*, pp. 146–153, 2019, doi: 10.1109/DRCN.2019.8713760.
[4] C.-Z. Hao, J., Ye, K., & Xu, “Live migration of virtual machines in OpenStack: A perspective from reliability evaluation,” *2th Int. Conf. Held as Part Serv. Conf. Fed. SCF 2019, San Diego, CA, USA, June 25–30, 2019*, 2019, [Online]. Available: https://doi.org/10.1007/978-3-030-23502-4_8
[5] B. Shi, H. Shen, B. Dong, and Q. Zheng, “Memory/Disk Operation Aware Lightweight VM Live Migration,” *IEEE/ACM Trans. Netw.*, vol. 30, no. 4, pp. 1895–1910, 2022, doi: 10.1109/TNET.2022.3155935.
[6] I. N. Somit Maloo, *Networking technology*, vol. 10, no. 5. 2022.
[7] M. T. K. and U. Y. K. S. H. A.A. Wahdini Fatimah, “Network Traffic Data Center Based on TIA-942 Standard:A Case Study in Bogor Government Office,” *J. Adv. Comput. Networks*, vol. 8, p. 1, 2020.
[8] M. Haranas, *Gartner’s Data Center And Cloud Networking Magic Quadrant Leaders*. 2020. [Online]. Available: https://www.crn.com/slide-shows/cloud/gartner-s-data-center-and-cloud-networking-magic-quadrant-leaders/3
[9] F. Nafisah, W. Putra, and A. Herlambang, “Evaluasi Keamanan Informasi Data Center Berdasarkan Standar ISO 27001:2013 (Studi Kasus PT. Pupuk Kalimantan Timur),” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 4, no. 6, pp. 1858–1865, 2020, [Online]. Available: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/7441
[10] M. T. K. I Gede Iswara Darmawan, “Desain Dan Analisis Best Practice Physical Security Dan Logical Security Pada Data Center Fakultas Rekayasa Industri Universitas Telkom Menggunakan Standar Tia-942 Dan Open Enterprise Security Architecture Design and Analysis of Best Practice Physical Sec,” vol. 2, no. 2, pp. 5576–5586, 2015.
[11] M. McClintock, K. Falkner, C. Szabo, and Y. Yarom, “Enterprise security architecture: Mythology or methodology?,” *ICEIS 2020 - Proc. 22nd Int. Conf. Enterp. Inf. Syst.*, vol. 2, no.

Iceis, pp. 679–689, 2020, doi: 10.5220/0009404406790689.
[12] R. M. Hicks, *Implementing Always On VPN*. 2022. doi: 10.1007/978-1-4842-7741-6.
[13] F. Ardianto, “Penggunaan mikrotik router sebagai jaringan server,” *Pengguna. Router Mikrotik*, vol. 1, no. 1, pp. 26–31, 2020.
[14] J. Wardana, M. A., Nusri, A. Z., & Juliandika, “Jaringan Virtual Private Network (VPN) Berbasis Mikrotik pada Kantor Kecamatan Marioriawa Kabupaten Soppeng,” *J. Ilm. Sist. Inf. dan Tek. Inform.*, vol. 5(2), pp. 107–116, 2022, [Online]. Available: https://doi.org/10.57093/jisti.v5i2.135
[15] A. S. Satryawati, E., Pangestu, D. A., & Budiman, “Implementasi virtual private network menggunakan point-to-point tunneling protocol,” *JEIS J. Elektro dan Inform. Swadharma*, vol. 2(1), pp. 36–42, 2022, [Online]. Available: https://doi.org/10.56486/jeis.vol2no1.160
[16] N. Anwar, R. S., & Agustina, “Implementasi dan Analisa Kinerja Jaringan Wide Area Network dengan Open VPN-Access Server,” *Informatics Educ. Prof. J. Informatics*, vol. 4(2), pp. 143–152, 2020, [Online]. Available: https://doi.org/10.51211/itbi.v4i2.1307
[17] A. Faizah, S., Pudjiarti, E., & Saryoko, “Perancangan Jaringan Dengan Menggunakan Static Routing Dan VPN PPTP Pada SMK Bina Putra,” *Bina Insa. ICT J.*, vol. 9(1), pp. 53–62, 2022.
[18] T. C. Hall, *Check Point Firewall Performance Optimization-Independently*. Max Power, 2020.