Simpatik: Jurnal Sistem Informasi dan Informatika
Volume 2 No. 1 Juni 2022

Implementasi Teknologi Cloud Computing Pada PT Zurich Topas Life Jakarta

Ahmad Yusroni[1], **Anton**[2]

[1,2] Universitas Nusa Mandiri
Jalan Damai No. 8, Warung Jati Barat, Ragunan, Pasar Minggu, Jakarta Selatan, Indonesia
e-mail: [1]12207088@nusamandiri.ac.id, [2]anton@nusamandiri.ac.id

Artikel Info : Diterima : 12-03-2022 | Direvisi : 16-06-2022 | Disetujui : 30-06-2022

Abstrak - Pandemi Covid 19 menuntut pelaku bisnis bergerak cepat untuk menyesuaikan lini bisnis dengan keadaan yang terjadi. Pembatasan regulasi kehadiran karyawan dalam Gedung perkantoran mengharuskan Perusahaan menerapkan flexible working, bekerja dari kantor dan bekerja dari rumah untuk karyawannya. Cloud Computing merupakan Jawaban tepat atas kebutuhan itu. Cloud Computing adalah model Infrastruktur jaringan yang efektif, efisien dan mengutamakan keamanan Jaringan menjadi hal wajib di era sekarang ini (Rumetna, 2018). Karyawan tidak harus datang ke kantor untuk bekerja, namun bisa mengerjakan pekerjaan dari rumah. Dengan menerapkan cloud computing, maka perbedaan bekerja di kantor dan di rumah tidak lagi menjadi suatu hambatan. Analisis Infrastruktur Jaringan yg digunakan oleh ZTL untuk mendukung karyawan yg dalam menerapkan flexible working, mengetahui apakah Infrastruktur yang digunakan sudah tepat dengan kebutuhan pengguna, serta apa saja yang bisa ditingkatkan, mengetahui solusi dari Permasalahan Infrastruktur Jaringan yang digunakan. Pembahasan Internet breakout di kantor ZTL untuk keperluan optimalisasi bandwith data yang digunakan. Bagaimana teknologi VPN yang digunakan oleh karyawan ZTLdapat membantu agar data karyawan tetap aman selama bekerja, serta model cloud yang cocok untuk karyawan yang diterapkan perusahaan

Kata Kunci: *Cloud Computing, Internet Breakout, VPN*

Abstracts **-** *The Covid 19 pandemic requires business people to move quickly to adapt their business lines to the current situation. Restrictions on employee attendance regulations in office buildings require the Company to implement flexible working, working from the office and working from home for its employees. Cloud Computing is the right answer to that need. Cloud Computing is a network infrastructure model that is effective, efficient and prioritizes network security, which is mandatory in today's era(Rumetna, 2018). Employees do not have to come to the office to work, but can do work from home. By implementing cloud computing, the difference between working in the office and at home is no longer an obstacle. Analysis of the Network Infrastructure used by ZTL to support employees who implement flexible working, find out whether the infrastructure used is appropriate to the user's needs, and what can be improved, find out solutions to the problems of the network infrastructure used. Discussion on Internet breakout at ZTL office for optimizing the data bandwidth used. How the VPN technology used by ZTL employees can help keep employee data safe while working, as well as the cloud model that is suitable for employees that the company implements.*

Keyword: Cloud Computing, Internet Breakout, VPN

PENDAHULUAN

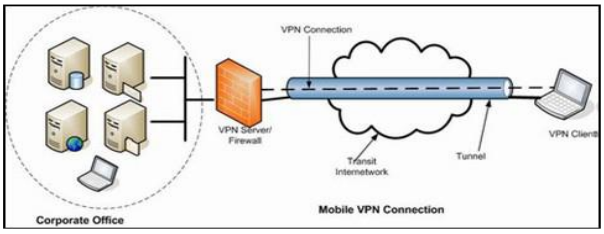
Kehadiran *cloud computing* sebagai layanan baru dalam tataran teknologi informasi yang memanfaatkan kemajuan teknologi komputer dan internet dapat dimanfaatkan untuk menyediakan akses informasi dalam secara lebih mudah, efektif, dan efisien. Dalam menyikapi perubahan teknologi ini, PT Zurich Topas Life Jakarta (ZTL) yang berkantor di Mayapada Tower 2, Jakarta menerapkan standar infrastruktur global yang telah di implementasikan di Indonesia. ZTL yang merupakan bagian dari Zurich Group Global merupakan perusahaan asuransi yang terkemuka di dunia. Penggunaan *cloud desktop* berbasis *cloud computing* dan VPN untuk keamaan jaringan yang dapat diakses dimanapun dan kapan pun (Ahmed & Ashraf Hossain, 2014). Serta kemudahan karyawan dalam bekerja secara fleksibel agar bisa bekerja dari rumah *(WFH)* dan bisa bekerja dari kantor *(WFO)*.

Selama pandemi Covid-19 Teknologi *cloud* memiliki peran utama dalam memerangi epidemi dan membantu program pemerintah dan organisasi di berbagai bidang kehidupan. Secara tidak langsung teknologi cloud berkontribusi untuk meningkatkan kehidupan di semua wilayah di dunia selama Covid-19 Utamanya dalam masa pembatasan sosial dan pembatasan interaksi langsung, teknologi *cloud* adalah jalan keluar agar perusahaan tetap berjalan dan tetap mengikuti peraturan pemerintah dalam upaya mencegah penularan virus. Keberadaan *cloud computing* sendiri telah mengubah cara kerja sistem teknologi informasi perusahaan. Penulis mencoba memaparkan hasil riset bagaimana implementasi dan pemanfaatannya bagi karyawan dan perusahaan

TINJAUAN PUSTAKA

1. Virtual Private Network (VPN)

Virtual Private Network (VPN) adalah suatu teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan lokal menggunakan jaringan publik yang tersedia.



Sumber :Ferguson & Huston (1998)

Gambar 1. Koneksi VPN

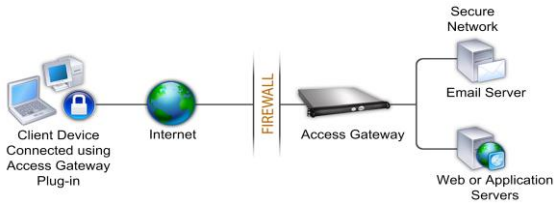
2. Teknologi Tunneling

Teknologi *tunnel*ing merupakan teknologi yang bertugas untuk manangani dan menyediakan koneksi *point*-to-*point* dari sumber ke tujuannya. Teknologi ini dapat dibuat diatas jaringan dengan pengaturan *IP Addressing* dan *IP Routing* yang sudah matang. Yakni antara sumber *tunnel* dengan tujuan *tunnel* telah dapat saling berkomunikasi melalui jaringan dengan pengalamatan IP. Apabila komunikasi antara sumber dan tujuan dari *tunnel* tidak dapat berjalan dengan baik, maka *tunnel* tersebut tidak akan terbentuk dan VPN gagal. Apabila *tunnel* tersebut telah terbentuk, maka koneksi *point*-to-*point* tersebut dapat langsung digunakan untuk mengirim dan menerima data. *Tunnel* dilengkapi dengan sebuah sistem enkripsi untuk menjaga data-data yang melewati *tunnel* tersebut. Proses enkripsi inilah yang menjadikan teknologi VPN menjadi aman dan bersifat *private* (Dewi, Riyadi, Suwastitaratu, & Hikmah, 2020).

3. *Citrix Gateway Plug-In SSL VPN*

Konsep dan Teknologi SSL *(Secure Socket Layer)* VPN dapat menjawab kebutuhan untuk mengakses sumberdaya perusahaan melalui penggunaan jaringan internet yang sudah tersedia dan jangkauannya luas. SSL VPN menggunakan infrastruktur publik yang sudah ada di internet untuk melakukan pertukaran data antara kantor pusat sebuah perusahaan dan kantor cabangnya. Karena dilewatkan pada sebuah jaringan internet publik, yang kemudian menjadi salah satu masalah jaringan internet *(IP public*) adalah tidak mempunyai dukungan yang baik terhadap keamanan. SSL VPN digunakan untuk mengatasi masalah keamanan tersebut, yakni penggunaan infrastruktur IP untuk koneksi jaringan suatu perusahaan dengan kantor cabangnya dengan cara pengalamatan secara *private* dengan melakukan pengamanan terhadap transmisi paket data.

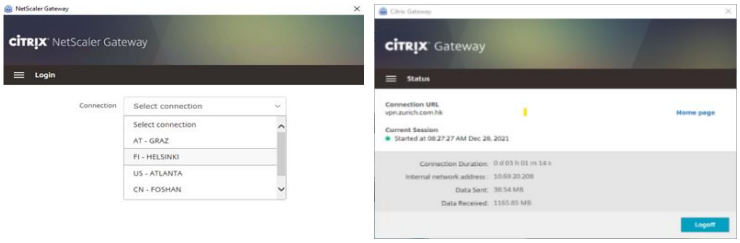
Citrix Gateway Plugin adalah software yang digunakan sebagai gateway koneksi VPN. Ketika pengguna mencoba mengakses sumber daya jaringan di *tunnel* VPN, plug-in *Citrix Gateway* mengenkripsi semua lalu lintas jaringan yang ditujukan untuk jaringan internal organisasi dan meneruskan paket ke *Citrix Gateway*. Citrix Gateway mengakhiri *tunnel* SSL, menerima lalu lintas masuk yang ditujukan untuk jaringan pribadi, dan meneruskan lalu lintas ke jaringan pribadi. Citrix Gateway mengirimkan lalu lintas kembali ke komputer jarak jauh melalui *tunnel* yang aman. Setelah masuk Analisis Titik Akhir (*End Point Analist*), yang juga disebut pemeriksa *host*, memeriksa apakah perangkat pengguna memenuhi keamanan tertentu sebagai persyaratan untuk membangun koneksi akses jarak jauh. Setelah pemeriksaan berhasil, pengguna akan diminta otentikasi dengan menggunakan otentikasi faktor ke-2 berdasarkan sertifikat mesin dan *tunnel* VPN dibuat antara laptop dan *gateway Netscaler*. Dalam hal ini ZTL menggunakan *OKTA Verify* sebagai otentikasinya.



Sumber : Systems & Statement (2013)

Gambar 4. Citrix gateway

Saat karyawan mengetik alamat web koneksi VPNnya, mereka diminta memasukkan user ID Akun dan passwordnya untuk login. Jika kredensial benar, *Citrix Gateway* menyelesaikan *Handshake*/Konfirmasi dengan perangkat pengguna. Jika pengguna berada di belakang server proxy, pengguna dapat menentukan server proxy dan kredensial otentikasi.



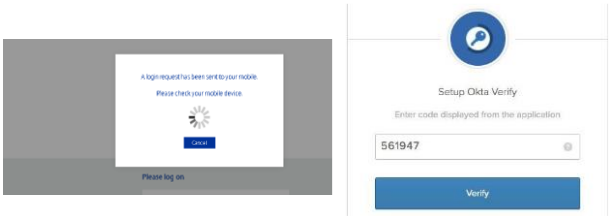
Sumber: Area & Services (2018)

Gambar 5. Citrix gateway

4. OKTA *Verify*

Okta Verify adalah aplikasi MFA *(Multi Factor Authentication)* dan autentikator yang dikembangkan oleh Okta. Aplikasi ini digunakan untuk mengonfirmasi identitas pengguna saat mereka masuk ke akun Okta mereka, dalam hal ini akun ZTL sudah terhubung dengan otentikasi OKTA(Datasheet, Using, & Verify, 2018).

Pendaftaran pengguna dan token untuk pertama kali untuk Karyawan perlu menginstal aplikasi seluler yang disebut "*OKTA Verify*" di ponsel mereka (iOS atau Android) untuk mendapatkan *Soft Token* atau pemberitahuan push. *Soft Token* adalah nomor unik 6 digit per pengguna yang dihasilkan dari Verifikasi OKTA dan berubah setiap 60 detik. Aplikasi ini digunakan untuk mengkonfirmasi identitas pengguna saat mereka masuk ke akun mereka.



Sumber : Okta Datasheet (2018)

Gambar 9. Permintaan *push* notifikasi dan *token code* OKTA

5. Citrix SD WAN

Untuk mendukung kinerja Jaringan yang optimal, ZTL membutuhkan perangkat Network optimizer yang berfungsi sebagai berikut :

a. Optimalisasi Bandwith Internet dan Intranet

ZTL Menggunakan Citrix Cloud Desktop yang berada di Regional yang digunakan karyawan untuk bekerja dari dalam Desktop *virtual* dimana terdapat aplikasi dan transfer file data didalamnya. Citrix SDWAN ini juga mendukung teknologi HDX yang memungkinkan melakukan Video-Audio call lebih jernih. Sehingga *Virtual* meeting video dan audio menjadi lancar dan optimal.

b. Internet Breakout

Breakout adalah fitur SD-WAN yang memungkinkan tautan Internet untuk memecah lalu lintas langsung dari sebuah situs. Misalnya, jika Anda ingin memberikan akses Internet kepada tamu yang mengunjungi perusahaan, dapat menggunakan *route* lokal untuk membagi lalu lintas *guess* secara lokal dari situs

langsung ke Internet . Dalam hal ini alamat website microsoft office 365 enterprise yang digunakan karyawan ZTL telah didaftarkan dalam *system* breakout sehingga jika karyawan mengakses aplikasi Office 365 Microsoft akan terbaca oleh sistem dan diarahkan aksesnya agar melalui link Internet agar penggunaan bandwith lebih optimal (Habib & Yliopisto, 2015).

Sumber : Paolo, Candidato & Passaro(2020)

Gambar 10. Perangkat Citrix SDWAN

6. Cloud Computing

NIST (*National Institute of Standards and Technology*) mendefinisikan *Cloud Computing* sebagai "sebuah model untuk kenyamanan, akses jaringan on-demand untuk menyatukan berbagai pengaturan konfigurasi sumber daya komputasi (seperti, server, media penyimpanan, jaringan, aplikasi, dan layanan) yang dapat dengan cepat ditetapkan dan dirilis dengan usaha manajemen yang minimal atau interaksi dengan penyedia layanan (Sistem Informasi Fakultas Ilmu Komputer Universitas Sriwijaya ,2011)

7. Model Layanan *Cloud Computing*

Ada tiga model layanan dari *cloud computing*, yaitu :

1. *Software as a Service* (SaaS).

Jenis layanan cloud melibatkan suatu lisensi aplikasi perangkat lunak kepada penggunanya. Lisensi ini biasanya diberikan menggunakan metode *pay-as-you-go* atau *on-demand*. Contohnya di Microsoft Office 365, Customer Relationship Management (CRM), Salesforce.com

2. *Platform as a Service (PaaS).*

Jenis *cloud computing* platform as a service umumnya disebut sebagai komputasi awan yang paling Kompleks. Sebenarnya, PaaS mempunyai cara kerja yang hampir dengan SaaS. Perbedaannya, PaaS adalah platform yang digunakan untuk membuat software SaaS yang bisa diakses melalui internet. Beberapa contohnya adalah Windows Azure dan Heroku.

3. Infrastructure as a Service (IaaS)

Infrastructure as a Service atau biasa disebut IaaS merupakan sebuah perangkat hardware komputer yang berupa "virtualisasi". IaaS sendiri dikelola dengan jaringan internet yang didalamnya terdapat elemen - elemen seperti bandwidth, IP address, serta keamanan dalam ruang lingkup satu layanan IaaS. IaaS sendiri adalah sebuah infrastruktur dari *cloud computing*. Contoh IaaS adalah Citrix Cloud Desktop , Arupa Cloud Desktop.

METODE PENELITIAN

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

1. Interview
   Penulis melakukan wawancara dengan karyawan dan Departemen Terkait Analisis Jaringan
2. Observasi
   Penulis melakukan pengamatan jaringan langsung terhadap terhadap *system* yang berjalan di ZTL
3. Studi Pustaka
   Penulis melakukan studi pustaka terkait materi yang dibahas dengan melalui riset berdasarkan jurnal dalam dan luar negeri terkait pembahasan masalah dalam penulisan

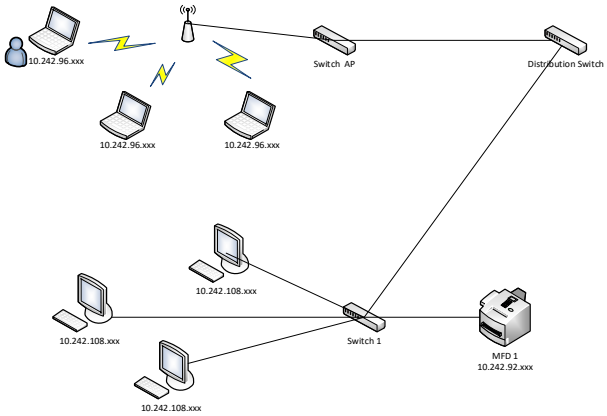
HASIL DAN PEMBAHASAN

1. Skema Jaringan

Di Head Office ZTL, setiap meja *dedicated* di ZTL terpasang port LAN dengan POE *(Power On Ethernet*) sehingga bisa dipasang Avaya deskphone untuk kebutuhan telephony dan data untuk dikoneksikan ke laptop. Topologi yang dipakai dalam LAN adalah topologi star, sedangkan koneksi nirkabel menggunakan *access point* wifi dengan 2 SSID, untuk intranet dan internet .Dalam pengalamatan IP, ZTL menggunakan IPv4 dengan menggunakan DHCP server sebagai pusat layanan yang otomatis memberikan IP address ke perangkat

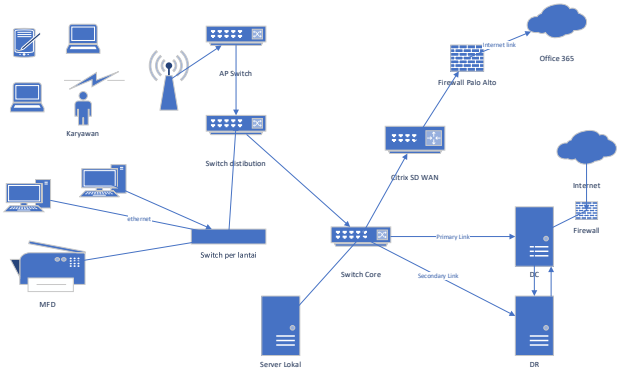
pengguna. Adapun kelas subnet dan IP ditangani oleh tim network regional. IP yang ada di ZTL menggunakan Class A. DHCP Server berada di Regional APAC, oleh karenanya pengaturan subnet IP dan sebagainya terkait network di diskusikan dengan tim IT Regional APAC terkait perubahan (penambahan, pengurangan dan *dismantle*) melalui *Change Management system* (CR), dimana didalamnya sudah di definisikan tim dan person yang menangani perubahan tersebut. Perubahan harus di setujui masing-masing entitas dalam struktur CR dengan menyertakan tujuan dan mengisi *risk assessment*.

Server – Server ZTL kebanyakan berada di regional data center APAC yang saling selaras *(sync)* dengan pusat data di Indonesia (*Mirroring*) hal ini terkait regulasi OJK yang berlaku. Namun untuk server-server tekait kebutuhan local , misal : PABX, server printer, *access* card dan lainnya berada di kantor ZTL.



Sumber: Hasil Penelitian (2021)

Gambar 14. Topologi star digunakan dalam LAN ZTL



Sumber : Hasil Penelitian (2021)

Gambar 15. Skema jaringan ZTL

Seperti pada skema diatas yang merupakan contoh skema jaringan setiap lantai, dimana setiap laptop yang terkoneksi dengan jaringan LAN akan diteruskan menuju switch per lantai dan diteruskan ke switch core utama dan meneruskan permintaan menuju server yang diminta. Setiap segment dibedakan berdasarkan lokasi lantai, jenis device dan sumber koneksi. Misalnya jika user terkoneksi menggunakan laptop di lantai 3 dengan koneksi *ethernet* maka akan mendapatkan IP 10.242.108.xxx namun jika menggunakan *wifi* akan mendapatkan IP 10.242.96.xxx. Segment server dan *device appliance* juga dibedakan IPnya untuk memudahkan tracing.

2. Keamanan Jaringan

Keamanan jaringan merupakan sebuah proses mencegah serta mengidentifikasi pihak pengguna computer yang tidak semestinya ada dalam jaringan computer (penyusup) yang memiliki tujuan merugikan jaringan computer yang disusupi.

Dalam pengamanan jaringan di ZTL, beberapa yang menjadi catatan :

a. Jaringan dalam kantor pusat ZTL terdapat firewall, konfigurasi meneruskan konfigurasi dari Regional.
b. Perubahan konfigurasi jaringan harus melalui persetujuan regional dan tim yang terlibat di dalamnya.
c. Waktu perubahan diatur berdasarkan jadwal *Change Management* setiap negara.

3. Penerapan keamanan jaringan ZTL

Dalam penerapannya, ZTL sudah melakukan penerapan dalam bidang keamanan yang baik,diataranya sebagai berikut :

a. Laptop dan *Personal Computer* (PC) karyawan

1) Komputer /laptop harus terdaftar,jika device tidak terdaftar maka tidak mendapatkan IP.
2) Port USB dan *memory card* untuk media penyimpanan diblokir.
3) Laptop non-ZTL dilarang terkoneksi dengan Intranet ZTL, hanya bisa terkoneksi dengan SSID wifi publik
4) Aktivitas Laptop di monitoring Crowstrike Antivirus
5) BitLocker Encryption Drive

BitLocker adalah sebuah fitur enkripsi *full-disk* yang telah tersedia dalam sistem operasi Microsoft Windows, baik versi *Ultimate* maupun *Enterprise* yang didesain untuk melindungi data dengan melakukanenkripsi terhadap keseluruhan partisi. Secara default, BitLocker Drive Encryption menggunakan algoritma Advanced Encrypted Standard (AES) dalam mode Code Block Chaining (CBC) dengan panjang kunci 128-bit, yang digabungkan dengan Elephant diffuser untuk meningkatkan keamanannya(Wahid, 2019).

b. Server

Untuk akses remote, harus menggunakan laptop ZTL yang terhubung kedalam intranet. Adapun untuk loginnya harus menggunakan *Password Access Request* (PAR). Hanya user yang sudah mendapatkan akses yang bisa mendapatkan password PAR-nya. Seperti halnya dengan OS di laptop karyawan, Setiap server juga menggunakan standar Regional untuk software yang di *install*, mengacu pada CSLO ZTL 2020 (*Customer Service Level Operations*).

4. Keamanan *Cloud Computing*

Management DHCP, Active Directory, dan Firewall di maintain oleh regional, karena ZTL mengikuti standar infrastruktur Zurich Asia Pasific (APAC) yang terpusat di Hongkong. Tim IT masing-masing negara mempunyai kewenangan dalam hal akses untuk menambahkan group Active Directory (AD) dan dan akses administrasi menggunakan PAR (*Password Access Request*) yang terkoneksi dengan *OKTA Verification* sehingga password hanya bertahan paling lama 23 Jam

5. Spesifikasi Hardware dan Software Jaringan

A. Server dan Jaringan

ZTL yang berkantor di Gedung Mayapada Tower 2, mempunyai spesifikasi Jaringan yang berjalan Sebagai berikut:

Tabel 1. Perangkat Jaringan

No	Perangkat	Tipe	Fungsi
1	Switch	Cisco Catalys 2960 48 Port	Main Switch
2	Switch	Cisco Core Switch 3650	Switch core
3	Switch	Tp-Link Switch POE TL-SF1008P	Distribution Switch
4	Switch	Arista Switch	Switch AP Arista
5	Access Point	Arista Access Point	Access Point SSID
6	Router	Citrix SD WAN	Bandwith optimizer
7	Modem	Indosat Link Enterprise	Link Indosat
8	Modem	Telkom SIP link	Link Telkom
9	Modem	Biznet Link	Link Biznet
10	Firewall	Palo Alto PA850	Firewall

Sumber : Hasil Penelitian (2021)

Tabel 2. Server

NO	Server	Fungsi
1	Dell PowerEdge R320	Server local VM
2	HP Proliant DL380 Gen 9	Server untuk developer
3	Lenovo IBM LP1440	Backup Server
4	Rainer SV311C4	SMS Gateway

Sumber : Hasil Penelitian (2021)

Tabel 3. Appliance

NO	Appliance	Fungsi
1	Media Gateway G450	PABX
2	Veeam TAPE Backup	TAPE media backup

Sumber: Hasil Penelitian (2021)

Untuk Operating System yang ada Server di ZTL sbb :
1. Windows Server 2012 dan 2016
2. Linux Redhat untuk Server PABX

6. Perangkat yang digunakan karyawan ZTL

Cloud Client adalah perangkat keras atau perangkat lunak yang digunakan untuk mengakses layanan *cloud*. Sistem komputer, tablet, perangkat navigasi, perangkat otomatisasi rumah, ponsel dan perangkat pintar lainnya, sistem operasi, dan browser semuanya dapat menjadi *cloud client*. Dalam hal ini *cloud client* karyawan ZTL adalah perangkat yang digunakan untuk bisa mengakses pekerjaan.

A. Laptop yang sudah terstandarisasi.

Setiap laptop yang diberikan Tim IT kepada karyawan sudah standar dari regional. Tim IT melakukan instalasi *OS* melalui *network*. *Boot system* melalui *Ethernet* untuk mengunduh image dari server. *Image OS* ini adalah Windows 10 Professional yang sudah terinstal aplikasi standar di dalamnya. Adapun aktivasi lisensinya mengikuti ID sistem karyawan yang berlaku.

1. Spesifikasi Laptop :

Tabel 4. Spesifikasi laptop karyawan ZTL

No	Brand	Model	Spesifikasi
1	Dell	Lattitude 5290	12,5 " Display , Intel i5 8th Gen, 256 GB SSD NVME 8GB RAM
2	Dell	latitude 5300	12,5" Display, Intel i5 8th Gen, 256 GB SSD NVME 8GB RAM
3	Dell	latitude 7200	14" Display, Intel i7 8th Gen, 512 GB SSD NVME 8GB RAM

Sumber : Hasil Penelitian (2021)

2. Spesifikasi Thin Client di ZTL

Tabel 5. Spesifikasi Thin Client karyawan ZTL

No	Model	Tipe
1	DELL	WYSE 5070
2	DELL	WYSE Tx0
3	DELL	WYSE Cx0

Sumber: Hasil Penelitian (2021)

3. Software Pre-Install (SCCM Image)
   a) Windows 10 20H2 Enterprise 64 Bit
   b) Microsoft Office 365 Enterprise
   c) Crowdsrike Antivirus
   d) Microsoft OneDrive
   e) Citrix Gateway

Jika karyawan memerlukan software tambahan selain standar ini maka perlu membuat permintaan melalui platform yang sudah disediakan bernama *"MyAccess"*. Akses yang telah disetujui akan menambahkan granting software tersebut kedalam profile karyawan dalam *Active Directory* (AD).Profil ini secara otomatis menambahkan software yang di request kedalam "*Sofware Center"* laptop. Misalkan user merequest menambahkan akses Microsoft Power BI, Setelah approval sistem di berikan maka otomatis akan terdownload di *software center*, dan user tinggal meng-klik "Install" di *software center*. Proses Instalasi berjalan silence di background sistem. Baik jika user memakai *Cloud Desktop* maupun laptop melalui koneksi VPN.

B. Thin *Client*

Thin *Client* adalah komputer yang berjalan dari sumber daya yang disimpan di server pusat. Walaupun Thin *Client* memiliki spesifikasi teknis sendiri namun alih-alih hard drive lokal. Thin *client* bekerja dengan menghubungkan dari jarak jauh ke lingkungan komputasi berbasis server tempat sebagian besar aplikasi, data sensitif, dan memori, disimpan. Thin *Client* dimanfaatkan ZTL untuk mengakses *Cloud Desktop* yang beroperasi di Regional. *Cloud Desktop* ini merupakan salah satu contoh dari jenis IaaS yang dimiliki ZTL.

C. Perangkat Mobile

Setiap Karyawan bisa mengakses Microsoft Office 365 di perangkat mobile (Android/iOS) yang sudah mendapatkan *granting system*. *Granting* ini berdasarkan konfirmasi persetujuan dari atasan dan tujuan aksesnya telah sesuai disetujui. Karyawan hanya perlu mendownload software tambahan yang dibutuhkan untuk bisa

mengaksesnya. Dalam hal ini Ada beberapa kebutuhan untuk Akses Microsoft 365 Mobile :

1. *Mobile Device Management (MDM)*

ZTL memilih menggunakan platform MDM untuk dipakai karena dinilai lebih cocok. Dengan Intune MDM, perusahaan dapat memastikan bahwa semua perangkat pribadi karyawan mematuhi kebijakan keamanan informasi. Penggunaan MDM ini juga memudahkan dari sisi management data. misalnya ketika handphone user hilang, maka IT Service desk tinggal membuka portal admin untuk mereset / enroll data user jika akan menggunakan handphone baru yang akan di install *Intune Company Portal* kembali.

2. Microsoft Authenticator

Microsoft Authenticator adalah aplikasi otentikasi dua faktor dari Microsoft. Cara menggunakan aplikasi ini sama seperti kebanyakan aplikasi otentikasi dua faktor lainnya, pengguna dapat masuk ke akun dan akun meminta kode. Aplikasi ini menghasilkan serangkaian angka secara berputar sekitar 30 detik. Dengan kata lain, aplikasi menghasilkan kode enam digit setiap 30 detik.

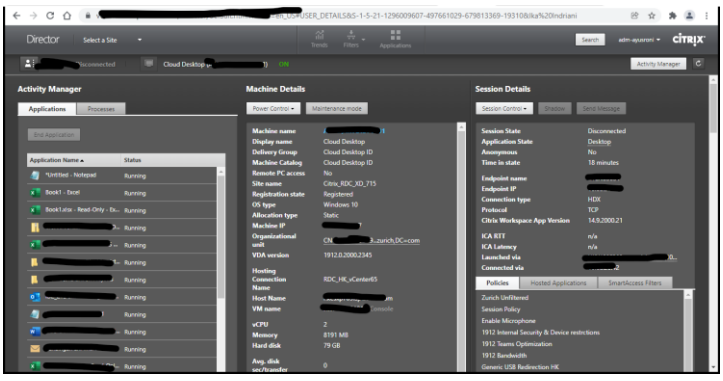
D. *Cloud Desktop*

Cloud Desktop yang digunakan ZTL adalah *Citrix VDI Cloud Desktop*, sebuah platform cloud yang menampung semua layanan yang diperlukan untuk mengatur workstation digital. Citrix memiliki cloud ini secara langsung, ia terlibat dalam pemeliharaannya dan menyediakan SLA yang ditentukan(IT Central Station, 2021).

Cloud desktop ZTL dapat diakses melalui 2 cara, melalui internet dan intranet. Adapun kedua cara ini hanya dibedakan link alamatnya saja. Jalur antara internet dan intranet dibedakan agar memaksimalkan koneksi yang digunakan. Aplikasi di dalam cloud desktop telah terintegrasi dengan *Active Directory* (AD) dan SCCM (*Microsoft System Center Configuration Manager*) sehingga profile user yang login dan aplikasi yang terinstal di dalamnya akan selaras dengan akses yang di didapatkan seperti dalam laptop.

Spesifikasi dari cloud desktop standar ZTL (Citrix cloud desktop VDI) :
Prosesor : Intel Xeon 8280 (2 CPU)
RAM : 8 GB
Storage : 80 GB

Adapun spesifikasi diatas bisa disesuaikan dengan permintaan pengguna, bisa di naikan versi prosesor, RAM, maupun Storagenya. Namun perlu dicatat bahwa ada *additional cost* yang berlaku bila ingin mendapatkannya. tim IT Service desk mempunyai tools bernama VDI director (web based) sehingga bisa diketahui kondisi mesin cloud desktop dan detail lainnya seperti penggunaan resource hardware, latensi jaringan dll. Password monitoring tools ini juga mengunakan PAR.



Sumber : Hasil Penelitian (2021)

Gambar 20. Monitoring menggunakan vdidirector

E. Cloud Access karyawan

Penggunaan *Cloud Computing* ZTL saat ini menggunakan beberapa cara :

1) Akses Cloud Desktop

Karyawan dapat mengakses Cloud Desktop melalui 2 cara, yakni via Laptop dan menggunan Thin Client. Akses Cloud Desktop melalui laptop yakni karyawan menginput alamat web Cloud desktop ZTL dan melalukan otentikasi OKTA Verify agar dapat menggunakan system. Software update dilakukan berkala oleh system SCCM.

2) Akses VPN

Akses VPN hanya bisa digunakan oleh laptop ZTL yang sudah terdaftar. komputasi akan seluruhnya

bergantung performa laptop . Adapun untuk mengakses VPN ZTL, plugin Citrix Gateway sudah terinstall dalam laptop saat laptop pertama kali diserahkan dari tim IT kepada karyawan.

3) *Mobile devices*

Karyawan dapat menggunakan perangkat mobile yang dimiliki untuk dapat mengakses Cloud ZTL melalui berbagai applikasi kantor, misalnya Microsoft Outlook, Microsoft Onedrive, dan Microsoft 365 lainnya dengan menginstal Intune Company Portal dan Microsoft Autenthicator.

Ketiga Metode diatas sangat membantu karyawan untuk bekerja secara fleksibel. Applikasi dari setiap perangkat akan bisa di perbaharui melalui system yang disediakan ZTL.Monitoring akses karyawan juga disediakan agar IT Service Desk bisa membantu jika karyawan yang mengalami masalah dengan akses cloudnya melalui *dashboard system OKTA, Active Directory*, VDI Director web dan Monitoring akses internet.

7. Permasalahan

Selama penulis melakukan riset di ZTL ini hampir tidak pernah penulis menemukan masalah dalam sistem jaringannya, hanya saja ada beberapa kendala yang sering ditemui oleh para *Technical Support (TS)* di lapangan saat ada user yang diharuskan mengupdate Windows ke versi terbaru misalnya, hanya bisa efektif dilakukan update dari kantor pusat. Dalam hal ini TS meminta user harus membawa laptopnya. Jika mencoba update dari tempat user melalui panduan video call microsoft teams, koneksi vpn sangat tidak ideal untuk mendownload file berukuran besar melalui *SCCM* (Microsoft System Center Configuration Manager) software yg tertanam di dalam laptop tersebut Kendala ini bisa diatasi dengan meminta pihak IT regional untuk melakukan penyesuaian bandwith untuk update software, waktu dan besaran bandwith data hendaknya diatur agar tidak mengganggu performa koneksi akibat penyesuaian bandwith yang baru.

Cloud Desktop yang diakses oleh karyawan dari rumah (WFH) sangat bergantung pada kestabilan jaringan internet yang digunakan. Tidak semua operator internet di Indonesia dapat berjalan smooth. hal ini bisa di trace route dari dashboard cloud yang diakses oleh tim *IT Service Desk* ZTL. Nilai latensi jaringan berpengaruh dengan kestabilan dan kenyamanan pada saat karyawan bekerja menggunakan cloud desktop. ZTL memberikan akses cloud sesuai keperluan karyawan, bisa akses Cloud Desktop, VPN maupun hanya akun Office O365 saja

Adapun Kecenderungan karyawan yang mengeluhkan tentang tidak mudahnya data keluar dari sistem ZTL adalah salah satu indikator bahwa ZTL telah menggunakan pengamanan yang baik, yaitu hanya bisa keluar melaui jalur yang sudah mendapatkan otorisasi pihak terkait

KESIMPULAN

1. Jaringan Usulan

Dari hasil riset yang dilakukan, yaitu:

a. Topologi jaringan ZTL sudah baik. penulis menilai tidak perlu merubah topologi utama yang sudah berjalan. Perubahan yang mungkin dilakukan yaitu penyesuaian bandwith Internet dan link Intranet ZTL bisa disesuaikan. Bisa dilihat dari status monitoring di web untuk penggunaan bandwith karyawan, jika dirasa sudah memenuhi 70% link, opsi upgrade harus dipertimbangkan.
b. Perubahan minor mungkin dilakukan untuk upgrade perangkat berkala dan optimalisasi sinyal penangkapan jaringan Wifi yang ada di kantor agar tata letaknya bisa menutupi area *blankspot* di area kerja dengan penambahan Access Point, dibeberapa titik area workspace ZTL, penulis menemukan sinyal penerimaan wifi hanya 2 bar dimana harusnya setiap laptop di area kerja dapat sinyal 4 bar. Hal ini kadang berpengaruh ketika karyawan melakukan panggilan video yang kurang optimal. Tim IT perlu memetakan kembali cakupan area SSID sehingga penerimaan sinyal selalu full 4 bar.
c. Penyesuaian Link Internet
   ZTL memiliki 100 MB Dedicated Internet. Untuk jumlah karyawan 200 orang jika dengan pembagian WFH - WFO 50:50 akan lebih dari cukup, namun jika semua karyawan WFH perlu dilakukan penyesuaian.
d. Alternatif secondary Link.
   Link primary ZTL menggunakan provider Indosat dengan alokasi bandwith 100MB Dedicated FO. Adapun Link Secondary menggunakan provider Indosat pula namun dengan metode Radio Link. Penggunaan provider yang berbeda untuk secondary link bisa dipertimbangkan. Mengingat kecenderungan provider yang masih dalam satu area akan terdampak jika menggunakan provider yang sama jika terjadi gangguan massal.

2. Keamanan Jaringan dan data

Dari sektor keamanan jaringan penulis berpendapat ZTL mengaplikasikan *end-to-end security* dengan baik, dari sisi perangkat laptop dan *thin client* untuk karyawan sampai ke tingkat server dan jaringan. ZTL secara rutin melakukan audit IT setiap tahun agar system yang berjalan sudah sesuai dengan CSLO dan SLA yang telah di tetapkan oleh manajemen. ZTL melindungi data dengan sejumlah teknologi dan metode pengamanan yang

berlapis. Untuk perangkat laptop dilengkapi enkripsi BitLocker dan Crowdstrike antivirus yang berjalan *seamless* tanpa menggangu karyawan yang sedang bekerja. ZTL melalui tim IT telah bekerja keras membangun sistem keamanan yang bisa melindungi karyawan dari serangan *cyber crime* melalui beberapa cara diantaranya:

1) Penggunaan PAR (Password Access Request)
2) Melindungi data dengan aturan di dalam jaringan ZTL
3) Melindungi karyawan dengan *system awareness* Regional

Terkait pengamanan data yang dirasa "menyusahkan" oleh sebagian user yang konservatif, perlu dilakukan edukasi oleh IT Security secara rutin agar setiap karyawan mempunyai pemahaman yang sama tentang aturan yang berlaku tentang perlindungan data perusahaan.

4. Penggunaan *Cloud Computing* di ZTL fleksibel

Karyawan bisa menggunakan model cloud yang cocok untuk kebutuhannya. misalnya :

1) Karyawan Head Office dan cabang dapat menggunakan Cloud Deskop atau VPN.

Cloud Desktop akan memudahkan karyawan dalam bekerja, karena cloud desktop running di server regional, maka tak masalah jika tiba-tiba karyawan kehabisan baterai laptop, karena mesin cloud akan tetap bekerja. Karyawan hanya perlu login ulang akun dan melanjutkan session di cloud desktop. Menggunakan VPN tanpa cloud desktop akan menghemat biaya lisensi yang digunakan ZTL di regional. Karyawan memaksimalkan penggunaan laptopnya, karena pemprosesan dan komputasi berjalan di laptop tersebut, namun untuk data penggunaan akan tetap berada di onedrive sebagai cloud storage utama.

2) Tenaga pemasaran atau vendor pihak ketiga.

Penggunaan akun dengan akses mobile o365 bagi tenaga pemasar (Agent) atau vendor yang bekerjasama dengan ZTL yang membutuhkan akun untuk testing aplikasi tertentu bisa menggunakan akses microsoft o365, dalam hal ini email dan akun yang diperlukan untuk menggunakan miscrosoft O365 basic.

5. Mendukung fleksibel working

Selama pandemi covid-19 infrastruktur ZTL sudah memadai untuk menerapkan fleksible working karena penggunaan *cloud computing*. Bahkan customer service ZTL sudah menggunakan *Softphone Avaya One-X* untuk menerima dan menghubungi nasabah. Tidak hanya menggunakan telepon meja biasa.

Penggunaan dan pelaksanaan *cloud computing* di ZTL sudah baik, semua kebutuhan karyawan bisa di akomodasi dengan baik oleh ZTL. Sebagian karyawan mungkin terlalu awam dalam menggunakan *cloud computing*, Tim IT mungkin perlu mendorong karyawan dalam suatu sesi seminar internal terkait penggunaan *cloud computing* agar menjadi lebih menyenangkan. Infrastruktur ZTL sudah baik akan sayang jika karyawan tidak memaksimalkannya.

REFERENSI

Ahmed, M., & Ashraf Hossain, M. (2014). Cloud Computing and Security Issues in the Cloud. *International Journal of Network Security & Its Applications*, *6*(1), 25–36. https://doi.org/10.5121/ijnsa.2014.6103

Area, S., & Services, I. (2018). Netscaler SSL VPN.

Datasheet, O., Using, O., & Verify, O. (n.d.). Authenticating to Okta Using Okta Verify Authenticating to Okta Using Okta Verify Install the Okta Verify App, 6–7.

Dewi, S., Riyadi, F., Suwastitaratu, T., & Hikmah, N. (2020). Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis. *Jurnal Sains Dan Manajemen*, *8*(1).

Ferguson, P., & Huston, G. (1998). *What is a VPN?*

Habib, M. A., & Yliopisto, J. (2015). *REDESIGN ENTERPRISE NETWORK BY LOCAL IN-TERNET BREAKOUT: CASE STUDY*.

IT Central Station. (2021). Citrix Virtual Apps and Desktops vs . Application Server (RAS), 1–10.

Paolo, S. P., Candidato, G., & Passaro, S. (2020). *POLITECNICO DI TORINO Study of applications and testing scenarios of Citrix SD-WAN solution*.

Rumetna, M. S. (2018). Title Case. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *5*(3), 305. https://doi.org/10.25126/jtiik.201853595

Sistem Informasi Fakultas Ilmu Komputer Universitas Sriwijaya Jl Raya Palembang-Prabumulih Km, J., Ogan Ilir, I., Ashari, A., Setiawan, H., Ilmu Komputer dan Elektronika, J., Mipa, F., & Gadjah Mada, U. (2011). Cloud Computing : Solusi ICT ? *Jurnal Sistem Informasi (JSI)*, *3*(2), 336–345.

Systems, C., & Statement, P. (2013). Access Gateway 10.

Wahid, A. A. (2019). *ANALISIS BITLOCKER DRIVE ENCRYPTION PADA MICROSOFT WINDOWS 10*.