Journal of Information System and Technology, Vol.03 No. 02, July 2022, pp.257-269 257
ISSN: 2775-0272

Analisa dan Penerapan Pencadangan Pusat Data Antar Site dengan Teknologi VPN

Zulkarnain[1], Jackie[2]
Program Sarjana Sistem Informasi, Fakultas Ilmu Komputer, Universitas Internasional Batam
Indonesia
E-mail: Zulkarnain.lec@uib.ac.id, 1831170.jackie@uib.edu

Abstrak

Teknologi informasi telah menjadi bagian penting bagi banyak industri dalam menjalani kegiatan operasional di era digital ini. Penggunaan teknologi informasi sudah hampir tidak terhindarkan lagi karena dapat membuat pekerjaan manusia menjadi lebih efektif dan efisien. Namun meningkatnya kebutuhan infrastruktur pada data *center* membuat perusahaan kesusahan karena biayanya yang tidak murah. Sehingga mengoptimalkan penggunaan perangkat keras untuk mencapai efektivitas dan efisiensi tanpa mengurangi layanan menjadi hal yang perlu dipertimbangkan. Salah satu aspek terpenting dari infrastruktur TI agar layanan bisa selalu tersedia adalah sistem *backup* dan replikasi. Tujuan dari penelitian ini adalah melakukan pencadangan pusat data antar dua *site* yang berbeda lokasi disertai dengan jaringan yang aman dalam pertukaran data. Metode yang digunakan pada penelitian ini adalah *Network Development Life Cycle* (*NDLC*), dengan menggunakan beberapa tahapan yaitu *analysis, design, implementation, dan monitoring.* Pada tahap analisis, proses *backup* dan replikasi data akan menggunakan sebuah aplikasi yang dapat melakukan *backup* data produksi secara otomatis dan terjadwal yaitu *Veeam Backup & Replication.* Untuk menghubungkan *site server* utama ke *site server* cadangan menggunakan jaringan VPN dengan protokol L2TP/IPsec. L2TP menggunakan *Password Authentication Protocol* (*PAP*) untuk mengenkapsulasi paket L2TP ke dalam IPsec untuk keamanan tambahan.

***Kata Kunci**: Backup, Replikasi, Server, VMware,Veeam, VPN, L2TP, NDLC*

Abstract

Information technology has become an important part for many industries in undergoing operational activities in this digital era. The use of information technology is almost inevitable because it can make human work more effective and efficient. But the increasing need for infrastructure in data centers makes the company difficult because the cost is not cheap. Thus optimizing the use of hardware to achieve effectiveness and efficiency without reducing service is something to consider. One of the most important aspects of IT infrastructure for services to always be available is backup and replication systems. The purpose of this study was to backup data centers between two different location sites accompanied by a secure network in the exchange of data. The method used in this study is the Network Development Life Cycle (NDLC), using several stages, namely analysis, design, implementation, and monitoring. In the analysis stage, the data backup and replication process will use an application that can perform automatic and scheduled production data backups, namely Veeam Backup & Replication. To connect the main server site to the backup server site using a VPN network with the L2TP/IPsec protocol. L2TP uses Password Authentication Protocol (PAP) to encapsulate L2TP packets into IPsec for added security.

***Keywords :** Backup, Replication, Server, VMware,Veeam, VPN, L2TP, NDLC*

I. PENDAHULUAN

Seiring perkembangan zaman, teknologi informasi dan komunikasi sudah menjadi bagian kebutuhan utama dalam kehidupan sehari-hari. Pada dunia bisnis sekarang memicu peningkatan kebutuhan infrastruktur data *center* dalam pengelolaan dan pertukaran informasi. Semakin tinggi intensitas bisnis perusahaan maka semakin besar juga kebutuhan infrastruktur yang diperlukan. Pengelolaan sistem dan teknologi perlu dilakukan secara efektif dan efisien. Agar infrastruktur yang tersedia dapat dioptimalkan untuk menyediakan layanan yang *high availability* dan memberikan kemudahan dalam *maintenance, backup* dan r*ecovery*. Maka dari itu banyak perusahaan menerapkan teknologi virtualisasi pada pusat data mereka [1][2][3].

Server merupakan sistem utama komputer yang bertugas memberikan layanan tertentu dan menyediakan sumber daya secara *real-time* dalam jaringan komputer [4][5]. Layanan yang tidak tersampaikan bisa terjadi karena kegagalan dari sisi *server*. Penyebab kegagalan tersebut yaitu *server down* yang disebabkan bencana alam, kesalahan manusia, ataupun tindak kejahatan cyber, dan tidak didukung ada server cadangan yang dapat langsung menggantikan peran *server* utama [5].

Teknologi virtualisasi server VMware ESXI *server* yang bersifat *bare metal* atau *hypervisor* tipe 1 banyak digunakan untuk membangun pusat data. Sistem operasi ini dapat di install dan berjalan langsung diatas perangkat *hardware* untuk mengelola mesin virtual didalam *server* ESXi nya [2]. Virtualisasi adalah teknologi yang diterapkan pada mesin *server* untuk membangun beberapa mesin virtual di dalamnya yang memberikan layanan berbeda[6]. Sistem virtualisasi dapat mengoptimalkan sumber daya yang berlebihan pada *server* seperti *CPU, RAM*, dan *storage* agar dapat menghasilkan beberapa mesin virtual baru [1]. Keuntungan dari virtualisasi ini yang awalnya dikerjakan oleh beberapa *server* khusus, sekarang dapat dikerjakan oleh 1 *server* dengan spesifikasi yang lebih besar sehingga mengurangi jumlah mesin *server* fisik dan menghemat tempat ruang yang diperlukan. Serta pemeliharaan sistem menjadi lebih efisien dengan menerapkan sistem *backup* dan *recovery* [7][8].

Backup adalah teknik menyalin sebuah *file* atau data komputer dan disimpan pada tempat penyimpanan yang berbeda dengan data aslinya. Apabila terjadi kerusakan dan kehilangan *file* akibat sebuah bencana, maka data *backup* akan digunakan untuk memulihkan (*restore*) data yang terhilang dan kondisi sistem komputer setelah bencana (*disaster recovery*) dari titik terakhir *backup* dilakukan [9][10]. *Backup* berperan penting dalam menjaga *high availability* dalam sistem *server*. Apabila terjadi gangguan pada *server* utama maka masih ada *server* cadangan yang dapat menggantikan karena didalam terdapat data *backup* dari *server* utama [6][11].

Agar proses perpindahan data *backup* dari *site* utama dapat menuju *site* cadangan dengan aman, maka perlu diterapkan teknologi *Virtual Private Network* (VPN). VPN dapat menghubungkan sejumlah jaringan lokal melalui jaringan publik internet, seolah-olah kedua jaringan itu berada di satu jaringan intranet yang sama [12]. Dalam pertukaran data antar jaringan lokal, vpn akan mengenkripsi data-data melalui *tunneling* internet sebelum dikirimkan menuju tujuan sehingga komunikasi bersifat *secure* [13].

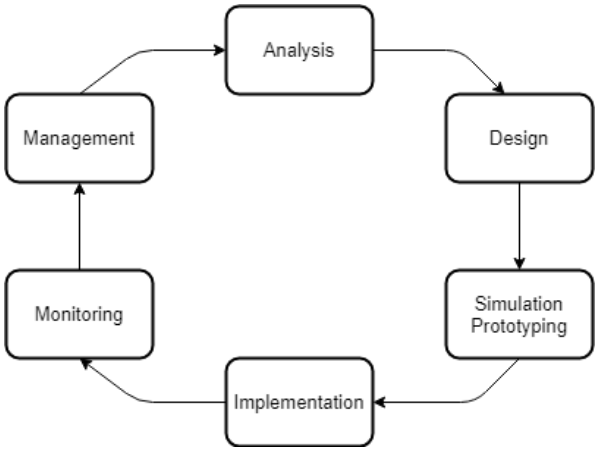
Saat ini terdapat organisasi yang masih mengelola pusat data secara mandiri, selain itu belum memiliki mekanisme *backup* yang baik. Terdapat juga organisasi yang memiliki *backup* tapi berada dalam satu tempat yang sama, sehingga jika terjadi hal yang tidak diinginkan pada tempat tersebut maka data utama dan cadangan dapat hilang [14]. Oleh karena ini pada penelitian ini akan membahas bagaimana merancang pusat data cadangan yang aman menggunakan tempat yang berbeda menggunakan VPN dengan metode NDLC.

II. METODE PENELITIAN

1. NDLC

Untuk melakukan rancangan backup infrastruktur dimana framework yang digunakan penulis adalah Network Development Life Cycle (NDLC). NDLC merupakan siklus proses berupa tahapan mekanisme yang diperlukan dalam rancangan proses pengembangan atau pembangunan sebuah

sistem jaringan komputer. NDLC terbagi menjadi 6 tahapan (Lihat Gambar 1), yaitu:



Gambar 1. Metode NDLC (Network Development Life Cycle)

1. *Analysis*: penelitian ini dimulai dengan tahap analisa yaitu menganalisa terhadap kebutuhan yang diperlukan serta permasalah yang muncul. Analisa keinginan pengguna dan analisa topologi jaringan yang telah ada. Tahapan ini dapat dilakukan dengan beberapa cara seperti wawancara, studi pustaka atau membaca *blueprint* dokumentasi.
2. Design: dari data analisis yang didapatkan, penulis akan melakukan pengambaran topologi yang akan digunakan untuk penerapan *backup* & replikasi pada *server* utama dan cadangan
3. Implementation: pada tahap ini penulis akan melakukan implementasi virtualisasi menggunakan Vmware vSphere, *backup* & replikasi menggunakan aplikasi Veeam Backup & Replication serta konfigurasi VPN L2TP pada Mikrotik router.
4. Monitoring: setelah penerapan rancangan *backup server* selesai dijalankan, penulis akan melakukan pemantauan dan pengujian terhadap *backup job* yang telah ditentukan. Agar proses *backup* dan replikasi dapat berjalan dengan baik dan benar.

III. HASIL DAN PEMBAHASAN

IMPLEMENTASI

Pada bab ini penulis akan melakukan penjabaran secara keseluruhan dari metode yang dijelaskan pada bab sebelumnya sebagai berikut:

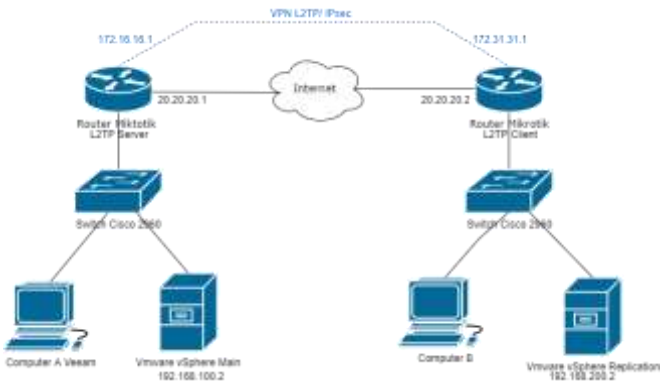
a. **Analisa**

Data sekarang menjadi bagian penting dari strategi perusahaan. Memanfaatkan data memungkinkan organisasi untuk mengembangkan strategi yang sensitif dan akurat untuk mengatasi tantangan bisnis. Itulah mengapa istilah perusahaan yang digerakkan oleh data muncul. Ini adalah perusahaan yang menggunakan data sebagai dasar utama untuk pengambilan keputusan. Salah satu aspek terpenting dari infrastruktur TI adalah sistem *backup* dan replikasi. Di area ini menggunakan *Veeam Backup & Replication*, sebuah solusi yang dapat melakukan *backup data* produksi secara otomatis dan terjadwal. *Veeam Backup & Replication* mendukung pusat data yang menggunakan infrastruktur VMware vSphere.

Agar proses *backup* dan replikasi dapat berjalan dengan baik, maka jaringan merupakan hal yang sangat penting. Pada kasus ini untuk menghubungkan *site server* utama ke *site server* cadangan menggunakan jaringan VPN. Protokol VPN yang akan digunakan adalah L2TP/IPsec. L2TP menggunakan *Password Authentication Protocol (PAP)* untuk mengenkapsulasi paket L2TP ke dalam IPsec untuk keamanan tambahan. L2TP/IPsec menggunakan *port* UDP 1701 untuk komunikasi.

b. Desain

Penulis telah membuat sebuah rancangan topologi berdasarkan hasil analisa yang telah dikumpulkan. Topologi yang dirancang dapat menghubungkan *site server* utama dan *site server* cadangan dengan jaringan VPN L2TP/IPsec dalam mendukung proses *backup* dan replikasi.

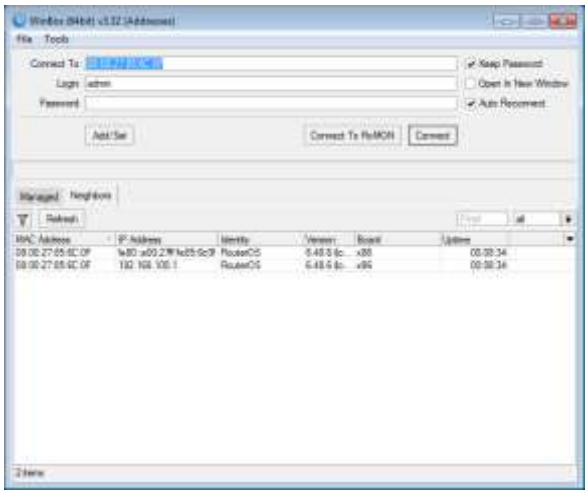


Gambar 2. Topologi Jaringan L2TP/IPsec Site-to-Site

c. Implementasi

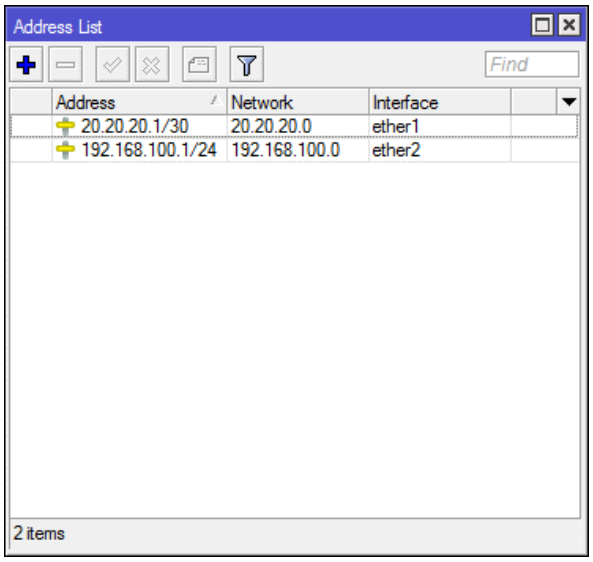
1. L2TP/IPsec Site-to-Site

Tahap pertama buka aplikasi WinBox pada *Computer* A untuk melakukan konfigurasi L2TP/IPsec *server*, kemudian tekan tab *Neighbors* dan refresh. Pilih router mikrotik yang telah muncul dan klik *connect.*



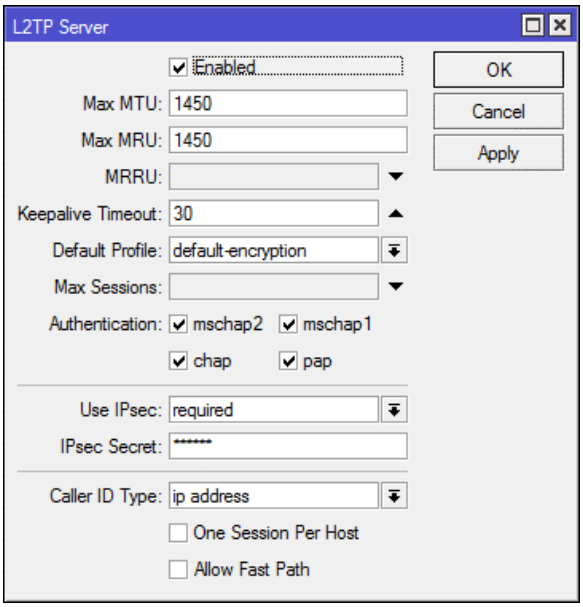
Gambar 3. Tampilan Awal Winbox L2TP/IPsec Server

Kemudian tekan tab IP dan pilih opsi *addresses*. Masukkan *IP Address* 20.20.20.1/30 dengan *network* 20.20.20.0 pada ether1 dan 192.168.100.1/24 dengan *network* 192.168.100.0 pada ether2.



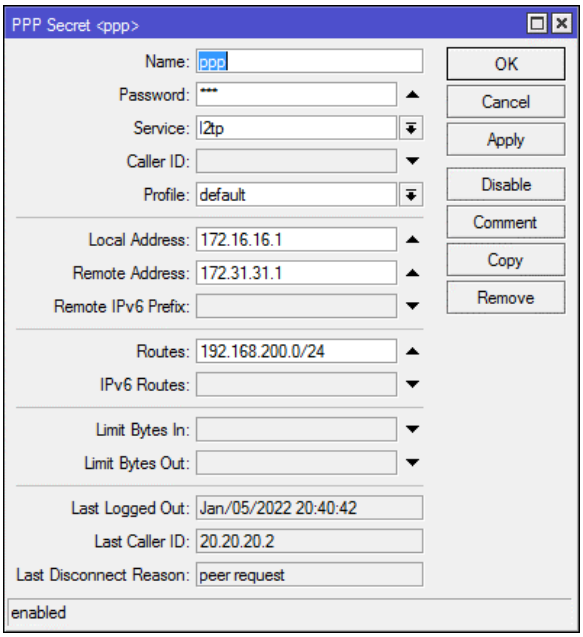
Gambar 4. Tampilan Address List L2TP/IPsec Server

Selanjutnya tekan tab PPP, dan pilih tab *interface*. Tekan tombol *add* dan pilih L2TP/IPsec Server. Centang opsi *Enabled*. Pada Use IPsec ubah menjadi *Required* dan isi *IPsec secret* dengan 12345678.



Gambar 5. Tampilan Konfigurasi L2TP/IPsec Server

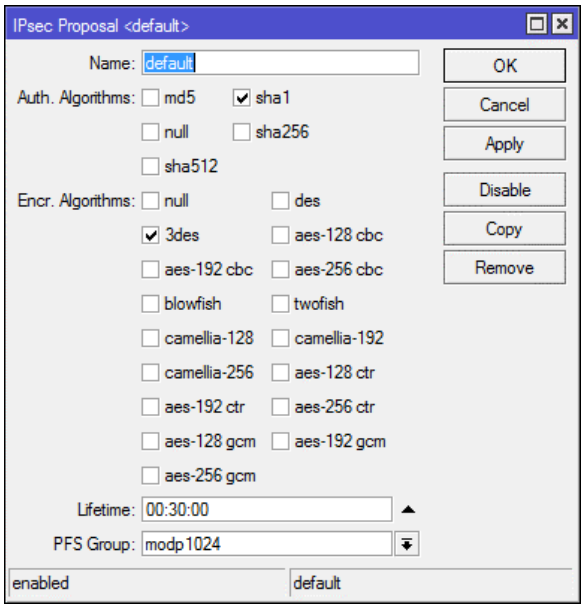
Tahap selanjutnya adalah membuat *secret*, tekan tab *secrets* dan tekan tombol *add* untuk menambahkan secret baru. Kemudian mengisi *name* dengan ppp, *password* dengan ppp, *service* sebagai l2tp, *local address* dengan *IP Address* 172.16.16.1, *remote address* dengan *IP Address* 172.31.31.1, dan *routes* dengan *IP Address* 192.168.200.0/24.



Gambar 6. Tampilan Konfigurasi PPP Secret L2TP/IPsec Server

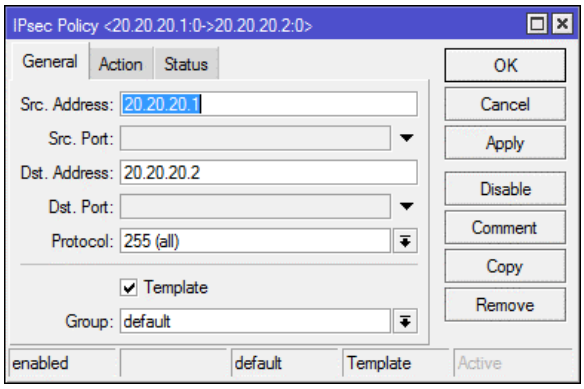
Diteruskan dengan konfigurasi IPsec. Tekan tab IP kemudian pilih IPsec. Tekan tab

proposal dan pilihlah proposal yang tersedia. Centang algoritma 3des dan hilangkan centang pada aes-128 cbc, aes-192 cbc, dan aes-256 cbc.



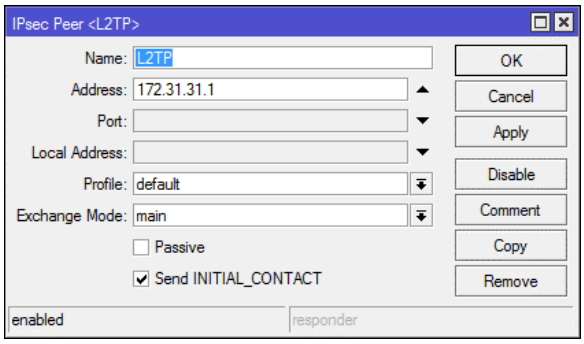
Gambar 7. Tampilan Konfigurasi IPsec Proposal L2TP/IPsec Server

Kemudian tekan tab Policies dan pilihlah proposal yang tersedia. Masukan src address dengan IP Address 20.20.20.1 dan dst address dengan IP Address 20.20.20.2.



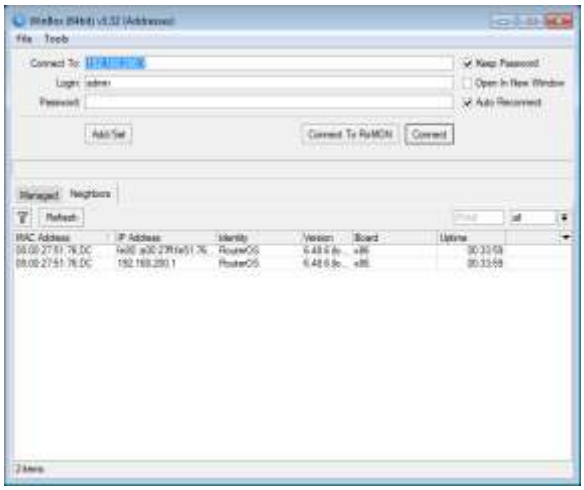
Gambar 8. Tampilan Konfigurasi IPsec Policy L2TP/IPsec Server

Tahap Selanjutnya tekan tab Peers dan tekan tombol *add* untuk membuat peer baru. Isi *name* dengan L2TP dan address dengan IP Address 172.31.31.1.



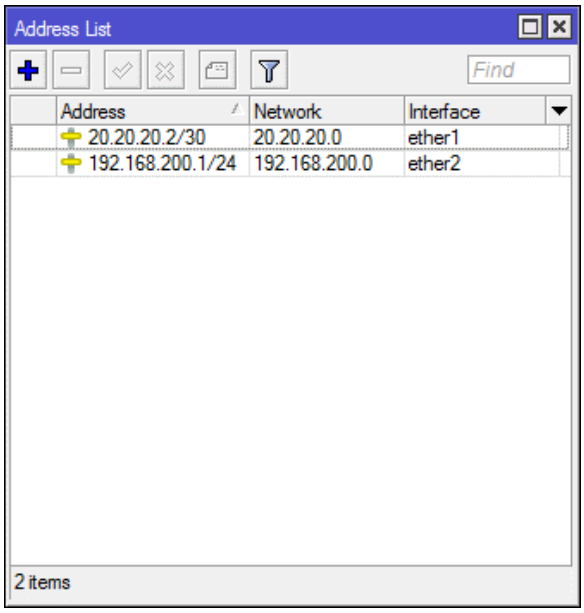
Gambar 9. Tampilan Konfigurasi IPsec Peer L2TP/IPsec Server

Buka aplikasi WinBox pada Computer B untuk melakukan konfigurasi L2TP/IPsec Client, kemudian tekan tab *Neighbors* dan refresh. Pilih router mikrotik yang sudah muncul dan tekan connect.



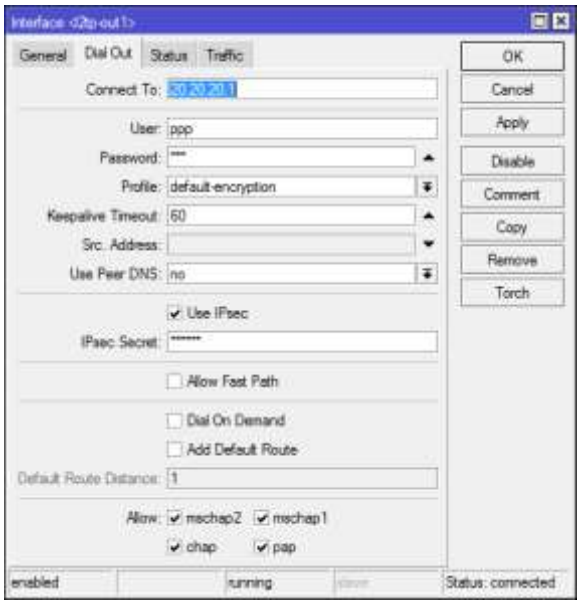
Gambar 10. Tampilan Halaman Awal Winbox L2TP/IPsec Client

Kemudian tekan tab IP dan pilih *addresses*. Masukan IP Address 20.20.20.2/30 dengan *network* 20.20.20.0 pada ether1 dan 192.168.200.1/24 dengan *network* 192.168.200.0 pada ether2.



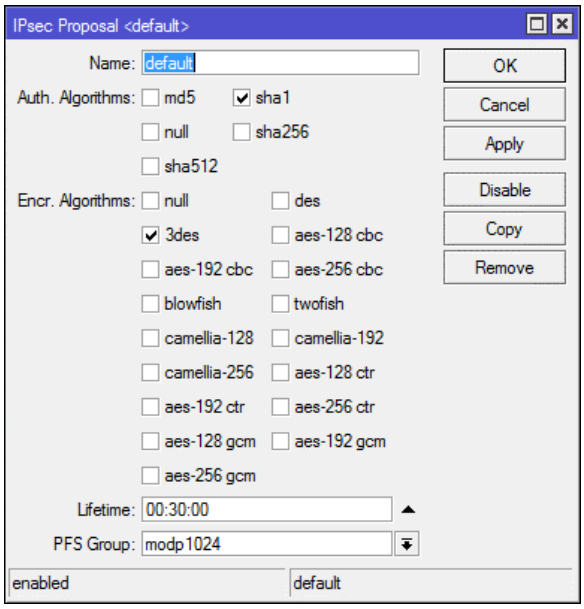
Gambar 11. Tampilan Address List L2TP/IPsec Client

Selanjutnya tekan tab PPP, dan pilih tab *interface.* Tekan tombol *add* dan pilih L2TP/IPsec *Client*. Isi *Connect* to dengan IP Address 20.20.20.1, user dengan ppp, *password* dengan ppp, centang use IPsec, dan isi *IPsec secret* dengan 12345678.



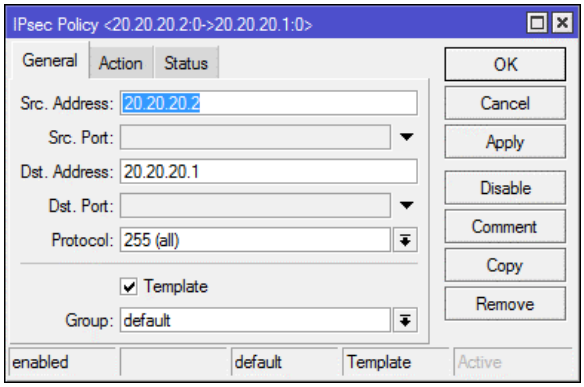
Gambar 12. Tampilan Konfigurasi Interface L2TP/IPsec Client

Diteruskan dengan konfigurasi IPsec. Tekan tab IP kemudian pilih IPsec. Tekan tab proposal dan pilihlah proposal yang tersedia. Centang algoritma 3des dan hilangkan centang pada aes-128 cbc, aes-192 cbc, dan aes-256 cbc.



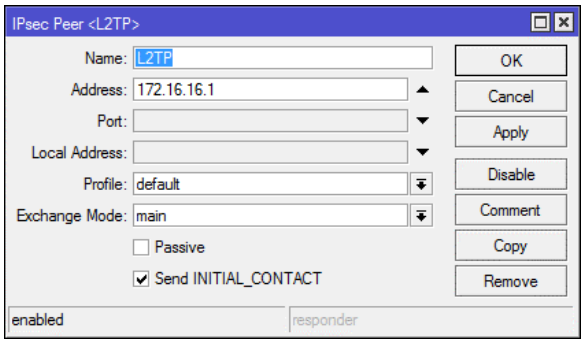
Gambar 13. Tampilan Konfigurasi IPsec Proposal L2TP/IPsec Client

kemudian tekan tab Policies dan pilihlah proposal yang. Isi src address dengan IP Address 20.20.20.1 dan dst address dengan IP Address 20.20.20.2.



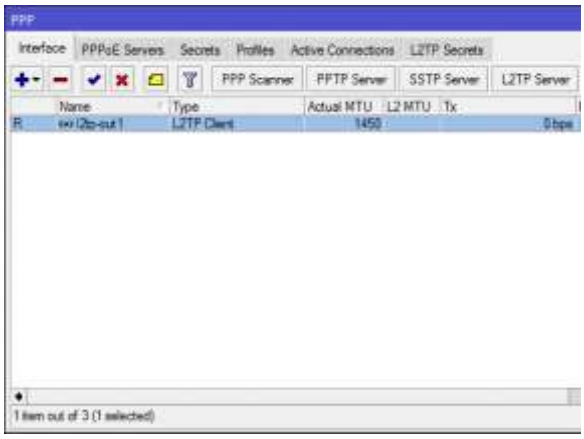
Gambar 14. Tampilan Konfigurasi IPsec Policy L2TP/IPsec Client

Selanjutnya tekan tab Peers dan tekan tombol *add* untuk membuat peer baru. Isi *name* dengan L2TP/IPsec dan address dengan IP Address 172.31.31.1.



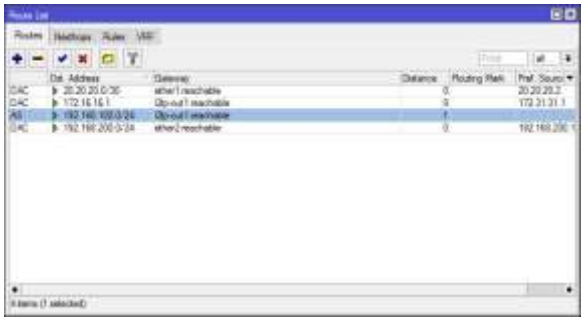
Gambar 15. Tampilan Konfigurasi IPsec Peer L2TP/IPsec Client

Mengecek apakah sudah muncul huruf R disebelah kiri nama l2tp-out1 untuk mengkonfirmasi bahwa VPN sudah terhubung.



Gambar 16. Tampilan Interface L2TP/IPsec Client

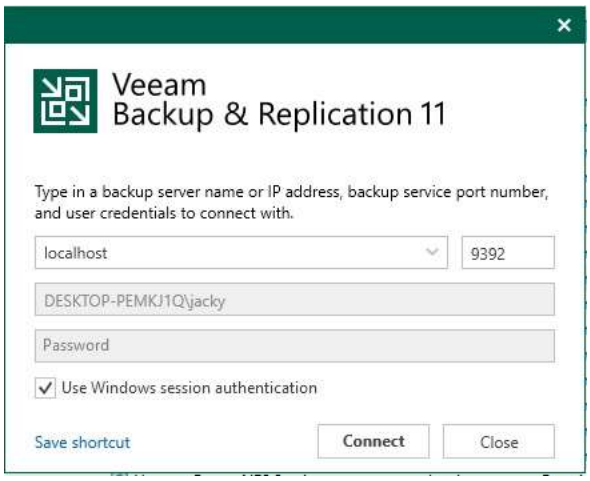
Tekan tab IP, dan pilih *routes.* Tekan tombol *add* untuk menambahkan IP *routes* dst address 192.168.100.0/24 dengan *gateway* l2tp-out1.



Gambar 17. Tampilan Route List L2TP/IPsec Client

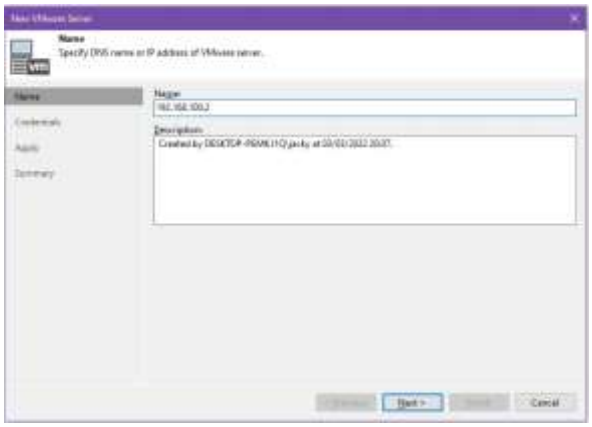
2. Konfigurasi Veeam BackUp dan Replikasi

Tahap pertama buka aplikasi Veeam, klik connect untuk login ke tampilan dashboard Veeam.



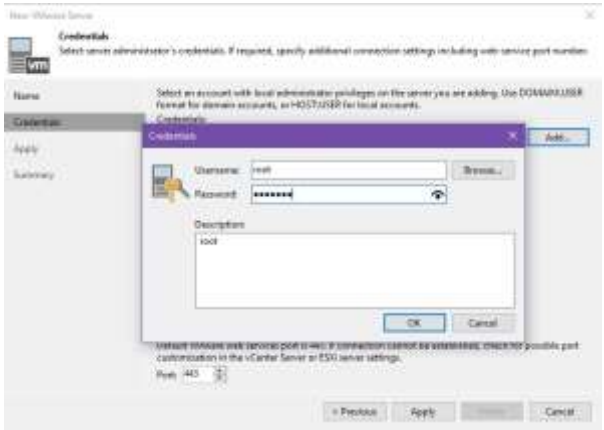
Gambar 18. Tampilan Login Veeam Backup & Replication

Selanjutnya klik pada *tab Backup Infrastructure* kemudian klik *Managed Servers* dan pilih opsi *Add Server* untuk menambahkan *server main*. Isilah *Name* dengan IP *Address* 192.168.100.2.



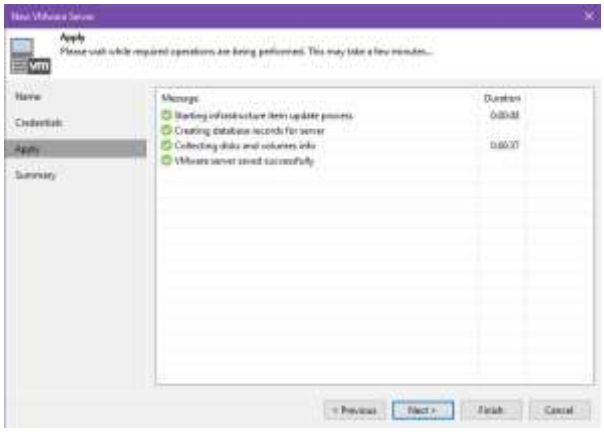
Gambar 19. Tampilan Konfigurasi Name Server Main

Tahap selanjutnya pada *Credentials* klik *add* dan isi *User* dengan *root* dan *password server main*. Klik *apply*



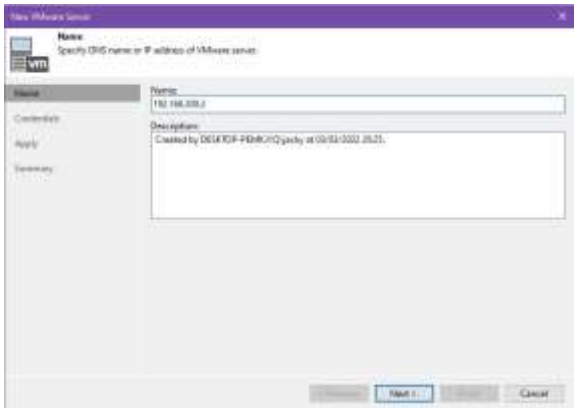
Gambar 20. Tampilan Konfigurasi Credentials Server Main

Setelah itu tunggu beberapa saat sampai *server main* berhasil ditambahkan.



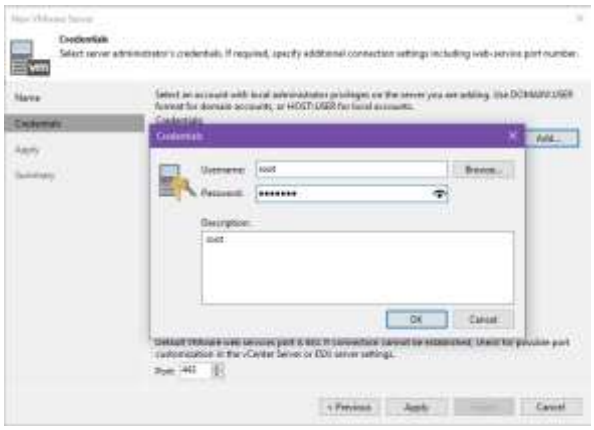
Gambar 21. Tampilan Proses Penyimpanan Konfigurasi Server Main

Untuk menambahkan *server replication* tidak jauh beda konfigurasinya dengan *server main*, hanya *Name* diisi dengan IP *Address* 192.168.200.2



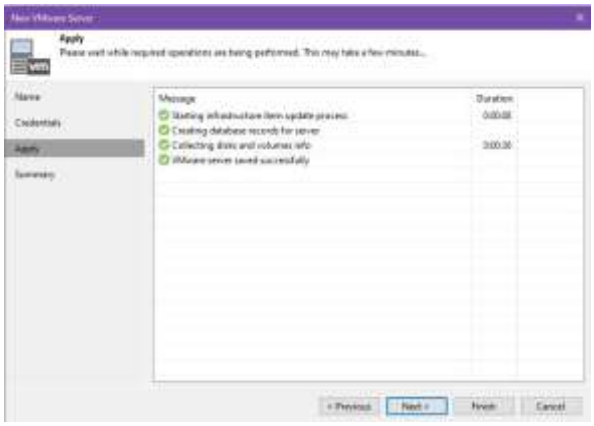
Gambar 22. Tampilan Konfigurasi Name Server Replikasi

Kemudian pada *Credentials* klik *add* dan isi *User* dengan *root* dan *password server replication*. Klik *apply*



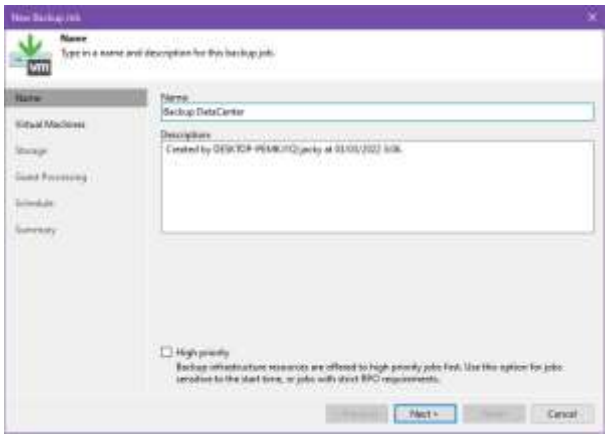
Gambar 23. Tampilan Konfigurasi Credentials Server Replikasi

Setelah itu tunggu beberapa saat sampai *server replication* berhasil ditambahkan.



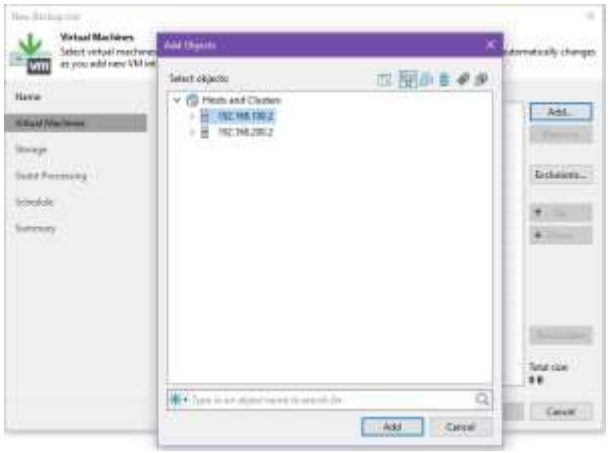
Gambar 24. Tampilan Proses Penyimpanan Konfigurasi Server Replikasi

Tahap selanjutnya yaitu membuat konfigurasi *backup* pada *server main*. Pertama tekan *tab home*, klik *tab Backup Job* dan pilih opsi *Virtual Machine*. Isilah *Name* dengan *Backup DataCenter*. Klik *next*



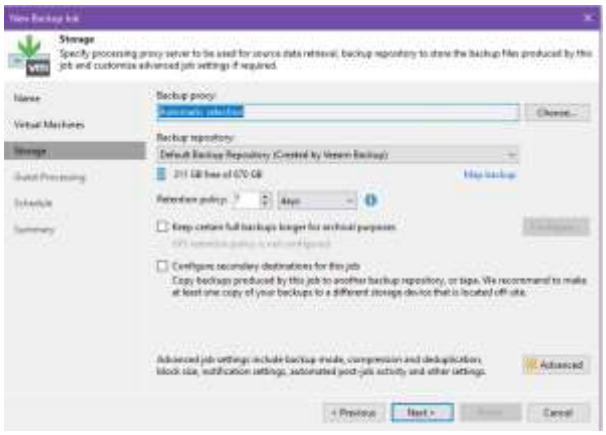
Gambar 25. Tampilan konfigurasi Name Backup Job

Kemudian pada bagian *Virtual Machines*, klik tombol *add* dan pilih IP *Address* 192.168.100.2 punya *server main*. Klik *next*



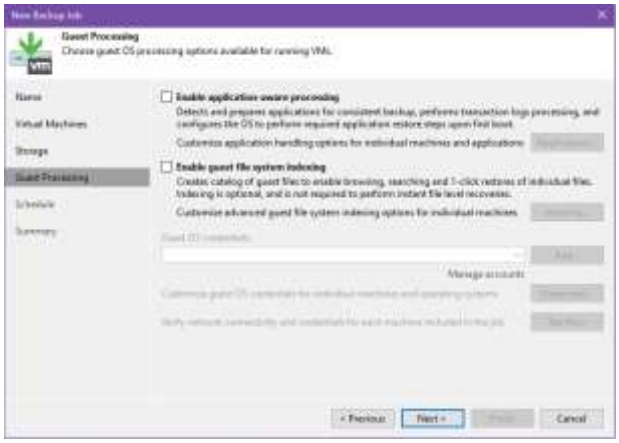
Gambar 26. Tampilan konfigurasi Virtual Machines Backup Job

Pada bagian *Storage*, konfigurasi sesuai *default* nya. Klik *next*



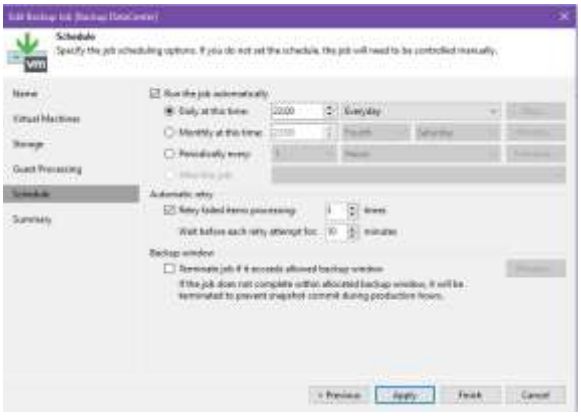
Gambar 27. Tampilan konfigurasi Storage Backup Job

Pada bagian *Guest Processing*, konfigurasi sesuai *default* nya. Klik *next*



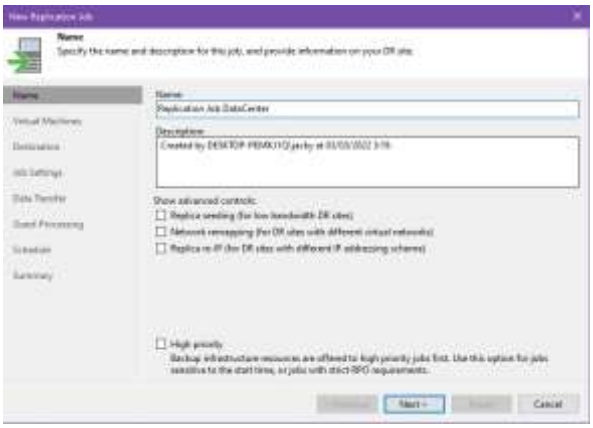
Gambar 28. Tampilan konfigurasi Guest Processing Backup Job

Selanjutnya *Schedule*, centang pada *Run the job automatically*. Pilihlah opsi *Daily at this time*, pada jam 22:00, dan *Everyday*. Centang juga *Retry failed item processing*, isi sebanyak 3 kali. Dan isi *Wait before each retry attempt for* 10 *minutes.* Klik *apply*



Gambar 29. Tampilan konfigurasi Schedule Backup Job

Tahap selanjutnya adalah membuat konfigurasi replikasi. Pertama tekan *tab home*, klik tab *Replication Job* dan pilih opsi *Virtual Machine*. Isilah *Name* dengan *Replication Job DataCenter*. Klik *next*

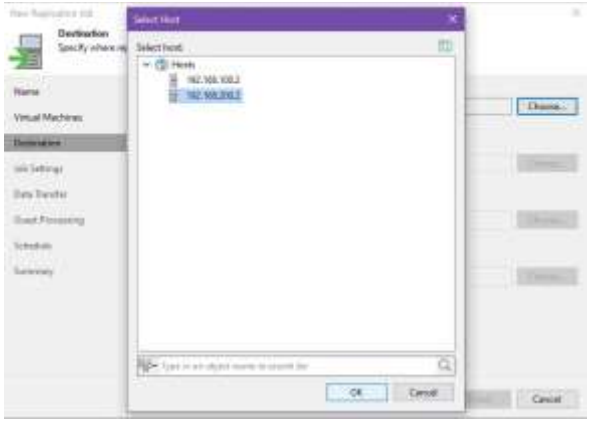


Gambar 30. Tampilan konfigurasi Name Replication Job

Kemudian pada bagian *Virtual Machines*, klik tombol *add* dan pilih IP *Address* 192.168.100.2 punya *server Main*. Klik *next*

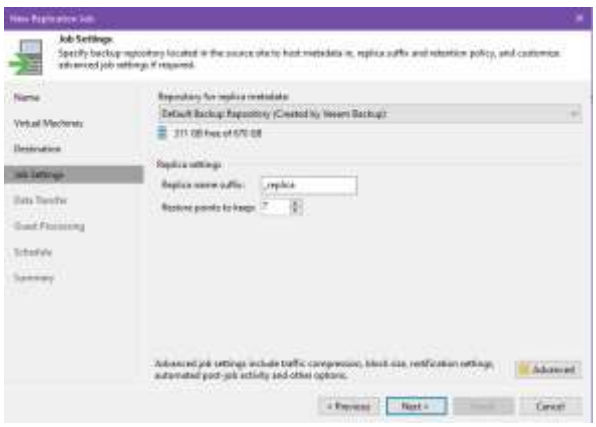
Gambar 31. Tampilan konfigurasi Virtual Machines Replication Job

Selanjutnya pada bagian *Destination*, pilihlah *Host or Cluster* dengan IP *Address* 192.168.200.2 punya *server* replikasi. *Klik next*



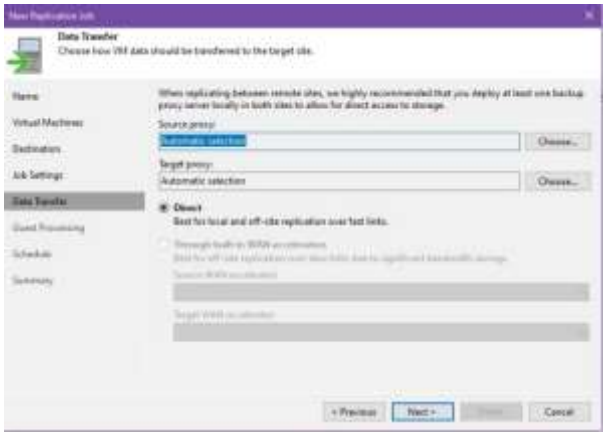
Gambar 32. Tampilan konfigurasi Destination Replication Job

Pada bagian *Job Setting*, konfigurasi sesuai *default* nya. Klik *next*



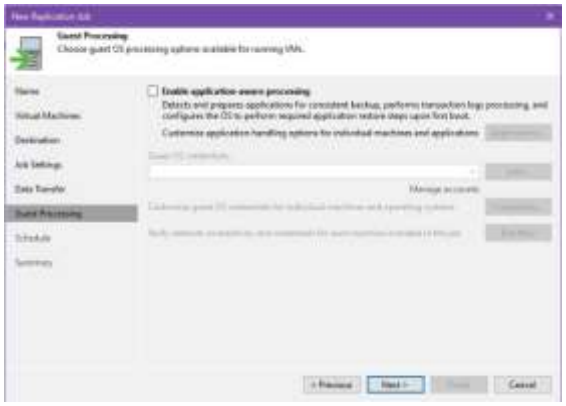
Gambar 33. Tampilan konfigurasi Job Setting Replication Job

Pada bagian *Data Transfer*, konfigurasi sesuai *default* nya. Klik *next*



Gambar 34. Tampilan konfigurasi Data Transfer Replication Job

Pada bagian *Guest Processing*, konfigurasi sesuai *default* nya. Klik *next*



Gambar 35. Tampilan konfigurasi Guest Processing Replication Job

Selanjutnya *Schedule*, centang pada *Run the job automatically*. Pilihlah opsi *Daily at this time*, pada jam 22:00, dan *Everyday*. Centang juga *Retry failed item processing*, isi sebanyak 3 kali. Dan isi *Wait before each retry attempt for* 10 *minutes*. Klik *apply*

Gambar 36. Tampilan konfigurasi Schedule Replication Job

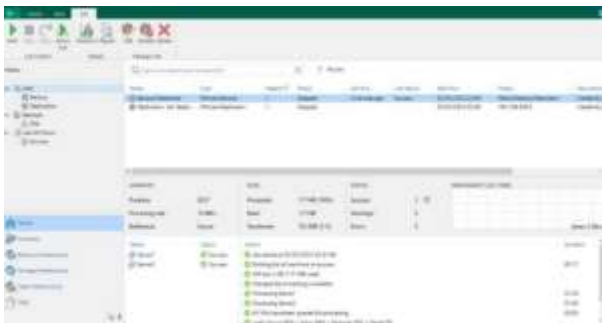
Terakhir pastikan bahwa *Backup job* dan *Replication Job* sudah berhasil dibuat pada *tab Home* Veeam Backup & Replication.

Gambar 37. Tampilan Home Veeam Backup & Replication

d. Monitoring

1. Backup Job

Pengujian *Backup Job* menggunakan konfigurasi *Backup DataCenter* yang telah dibuat pada aplikasi *Veeam Backup & Replication*. Berikut hasil pengujian *backup* yang ditunjukkan pada gambar 38



Gambar 38. Tampilan Proses Backup Datacenter

2. Replication Job

Pengujian *Replication Job* menggunakan konfigurasi *Replication Job DataCenter* yang telah dibuat pada aplikasi *Veeam Backup & Replication*. Berikut hasil pengujian *Replication* yang ditunjukkan pada gambar 39

Gambar 39. Tampilan Proses Replication Job Datacenter

e. Pembahasan

Pada tahap desain penulis telah merancang sebuah topologi jaringan *site to site* berdasarkan hasil analisa. Dimana pada masing-masing *site* utama dan *site* cadangan terdapat 1 komputer, *server*, 1 switch cisco dan 1 router mikrotik yang terkoneksi ke jaringan publik (internet). Di router mikrotik tersebut akan di konfigurasikan VPN dengan protokol L2TP/IPsec yang dapat mengenkapsulasi setiap pertukaran informasi untuk menjaga kerahasiaan data dalam sebuah jaringan.

Pada tahap implementasi penulis melakukan konfigurasi VPN L2TP/IPsec pada router mikrotik menggunakan aplikasi Winbox. Pertama konfigurasi router mikrotik *site* utama sebagai L2TP *server* dan router mikrotik *site* cadangan sebagai L2TP *client*. Kemudian melakukan konfigurasi pada aplikasi *Veeam Backup & Replication*, terlebih dahulu memasukan sistem *server* main dan *server* cadangan kedalam aplikasi Veeam. Selanjutnya membuat rencana *Backup Job* dan *Replication Job* sehingga dapat melakukan *backup data* secara otomatis dan terjadwal.

Pada tahap *monitoring* penulis melakukan pengujian *backup* data pada *server* menggunakan rencana *Backup Job* dan *Replication Job* yang telah dibuat penulis di aplikasi *Veeam Backup & Replication*. Hasil pengujian menggunakan konfigurasi *Backup DataCenter* dan *Replication Job DataCenter* telah berjalan dengan lancar dan aman pada jaringan VPN yang sudah dibangun.

Gambar 40. Tampilan Dashboard Main Server ESXI

Gambar 41. Tampilan Dashboard Replikasi Server ESXI

IV. KESIMPULAN DAN SARAN

1. Kesimpulan

Berdasarkan hasil penelitian yang dilakukan penulis dalam penerapan *backup* pusat data antar *site* pada jaringan VPN L2TP/IPsec, dapat disimpulkan bahwa:

1. VPN dengan protokol L2TP/IPsec menggunakan perlindungan ganda yaitu *tunnelling* yang menyediakan koneksi *point-to-point* (PPP) dari sumber menuju tujuan dan IPsec untuk mengenkripsi data untuk menjaga keamanan dan kerahasiaan.
2. Dengan menggunakan aplikasi *Veeam Backup & Replication* dapat melakukan *backup data* secara berkala dan berkelanjutan sesuai konfigurasi yang telah di atur sehingga dapat meringankan beban kerja *admin server*.
3. Virtualisasi *server* menggunakan Vmware vSphere ESXI memudahkan *admin server* dalam mengelola sumber daya.

2. Saran

Saran yang diberikan oleh penulis untuk penelitian selanjutnya yaitu sebagai berikut:

1. Melakukan penelitian yang lebih mendetail mengenai keamanan sebuah sistem jaringan dalam proses pertukaran data di jaringan publik dan *private.*
2. Menganalisis protokol VPN lainnya seperti *Secure Socket Tunneling Protocol (SSTP)* dan *OpenVPN* dalam merancang jaringan komunikasi antar *site.*

DAFTAR PUSTAKA

[1] D. Irwan, H. Sukoco, and S. Wahjuni, "Service High Availability Pada Native Server dan Virtual Server Menggunakan Proxmox VE," *J. Kaji. Ilm.*, vol. 20, no. 2, pp. 137–144, 2020, doi: 10.31599/jki.v20i2.87.

[2] M. R. Julianti, S. Ramdhan, and A. Mulyana, "Perancangan Server Cloud Computing Model Infrastructure As A Service Berbasis Proxmox pada PT Fortuna Mediatama," *AJCSR(Academic J. Comput. Sci. Res.*, vol. 1, no. 1, pp. 1–6, 2019.

[3] S. N. Khasanah and S. J. Kuryanti, "Rancangan Virtualisasi Server Menggunakan VMWare Vsphare," *EVOLUSI - J. Sains dan Manaj.*, vol. 7, no. 1, pp. 42–46, 2019, doi: 10.31294/evolusi.v7i1.5091.

[4] H. P. Ginanjar and A. Setiyadi, "Penerapan Teknologi Cloud Computing Pada Katalog Produk di Balatkop Jawa Barat," *KOMPUTA(Jurnal Ilm. Komput. dan Inform.*, vol. 9, no. 1, 2020.

[5] Y. Pribadi, A. B. Pn, and M. A. Irwansyah, "Analysis of the Use of the Failover Clustering Method to Achieve High Availability on a Web Server (Case Study: Informatics Department Building)," *JUSTIN (Jurnal Sist. dan Teknol. Informasi)*, vol. 8, no. 2, 2020.

[6] D. Irwan, "Service Availability dan Performa Sumber Daya Prosessor Pada Infrastruktur Server Virtual," *J. Penelit. Ilmu Komput.*, vol. 5, no. 1, pp. 42–50, 2017.

[7] I. G. Ngurah, W. Arsa, and I. N. R. Hendrawan, "Analisis Konsolidasi Server dengan Virtualisasi Menggunakan Proxmox VE," *J. EKSPLORA Inform.*, pp. 13–19, 2020, doi: 10.30864/eksplora.v10i1.381.

[8] Sriyanta, W. W. Winarno, and Sudarmawan, "Optimalisasi Penggunaan Hardware Server Mempergunakan Virtualisasi Server Di Sman 1 Wonosari," *J. Inf. Politek. Indonusa Surakarta*, vol. 4, no. 2, pp. 35–42, 2018.

[9] E. Haryadi, Abdussomad, and Robi, "Implementasi Sistem Backup Data Perusahaan Sebagai Bagian dari Disaster

Recovery Plan," *Sains Dan Teknol.*, vol. 29, no. 2, pp. 6–11, 2019, [Online]. Available: https://ejournal.istn.ac.id/index.php/sainstech/article/view/331.

[10] A. Rosano and D. Sudaradjat, "Manajemen Backup Data untuk Penyelamatan Data Nasabah pada Sistem Informasi Perbankan (Studi Kasus : PT Bank XYZ)," *REMIK (Riset dan E-Jurnal Manaj. Inform. Komputer)*, vol. 4, no. 2, p. 1, 2020, doi: 10.33395/remik.v4i2.10507.

[11] N. Sadikin and M. Sari, "Replikasi Virtual Machine Antara Dua Lokasi Terpisah Untuk Backup Dan Disaster Recovery," *J. Maklumatika*, vol. 6, no. 2, pp. 81–88, 2020.

[12] E. Mufida, D. Irawan, and G. Chrisnawati, "Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus pada Yayasan Teratai Global Jakarta," *J. Matrik*, vol. 16, no. 2, p. 9, 2017, doi: 10.30812/matrik.v16i2.7.

[13] I. Ekawati and D. Irwan, "Implementasi Virtual Private Network Menggunakan PPTP Berbasis Mikrotik," *JREC (Journal Electr. Electron. ISSN*, vol. 9, no. 1, pp. 29–40, 2021.

[14] A. S. Tohir, "Pemodelan Sistem Data Terdistribusi Untuk Mengintegrasikan Data Akademik Dan Keuangan," *J. Intensif*, vol. 1, no. 1, p. 44, 2017, doi: 10.29407/intensif.v1i1.542.