Volume 5 No. 1 Februari 2019
P-ISSN 2442-2436, E-ISSN: 2550-0120
Akreditasi Ristekdikti, No: 21/E/KPT/2018
http://ejournal.bsi.ac.id/ejurnal/index.php/jtk

JURNAL TEKNIK KOMPUTER AMIK BSI

DOI: 10.31294/jtk.v4i2

Perancangan Wide Area Network (WAN) Dengan Teknologi Virtual Private Network (VPN)

Syarif Hidayatulloh[1], Wahyudin[2]

STMIK Nusa Mandiri
e-mail: arrh56@gmail.com

[2]Universitas Bina Sarana Informatika Jakarta
e-mail: Wahyudin.whd@bsi.ac.id

Cara Sitasi: Hidayatulloh, S., & Wahyudin, W. (2019). Perancangan Wide Area Network (WAN) Dengan Teknologi Virtual Private Network (VPN). Jurnal Teknik Komputer AMIK BSI, 7-14.

Abstract *- The use of information technology and its use in collecting and processing data into information that is useful in decision making will play a role in determining the success of an organization or company in the future. This happened to PT. Jasa Cendekia Indonesia, the computer network that is owned has not met the needs of its employees. A good computer network is one that can serve sharing resources, data security, resources more efficiently and up-to-date information. Basically if a company can hold a computer network that serves the above for employees, of course it will make it easier for employees to do the work and improve the standards of the company itself. The proposed network built by the author for PT. Indonesian Scholar Services is a computer network built with Virtual Private Network technology. Because companies that have communication between the head office and branches that are good and safe, will be the capital for their companies in facing challenges in the era of globalization. Communication that is connected to a fast and secure computer network will make it easier for a company to supervise the activities of its company.*

Keywords: Virtual Private Network, Wide Area Network

PENDAHULUAN

Secara sederhana jaringan komputer dapat diartikan sebagai kumpulan beberapa komputer dan peralatan lain yang saling terhubung menggunakan aturan-aturan tertentu (Wahidin, 2007). Perkembangan teknologi jaringan komputer menunjukkan peningkatan yang sangat pesat seiring dengan semakin meningkatnya kebutuhan akan terhubungnya lokasi–lokasi yang terpisah secara jarak namun ingin tetap berbagi informasi dan menikmati layanan yang sama. Kebutuhan akan terhubungnya antar lokasi ini dirasakan benar pada level perusahaan. Sebuah perusahaan yang memiliki sejumlah unit usaha tentunya ingin agar setiap unit usahanya tersebut terhubung satu sama lain agar dapat bertukar informasi dan memiliki akses yang sama ke internet.

Oleh karena itu, dibutuhkan suatu sistem jaringan komputer untuk menghubungkan kantor pusat dengan kantor cabang yang letaknya berjauhan agar dapat saling bertukar informasi secara internal. Dalam melakukan komunikasi dan pengolahan informasi antara kantor pusat dengan kantor cabang yang tersebar di lokasi yang terpisah, dibutuhkan suatu jaringan yang terkoneksi secara sistematis dengan internet, sehingga jaringan yang berbeda tadi terhubung dalam satu sistem jaringan komputer secara luas dan aman. Sistem jaringan yang terpasang nantinya akan menjadi kerangka awal untuk pembangunan ataupun pengembangan jaringan kedepannya sehingga akan lebih mudah untuk perancangan pada pengembangan selanjutnya. Hal ini juga dapat memberi petunjuk bagi para pengguna jaringan agar tidak salah dalam menggunakan layanan yang tersedia pada sebuah jaringan. Pembangunan jaringan ini juga terpacu berdasarkan pada mekanisme pembangunan jaringan secara *virtual* dan dalam hal ini khusus tentang *Virtual Private Network* (VPN). VPN banyak digunakan untuk meningkatkan keamanan data-data komunikasi yang bersifat rahasia (Supriyono, Widjaya, & Supardi, 2013).

Dengan dikembangkannya jaringan *Virtual Private Network* (VPN) yang teraplikasi pada jaringan *Wide Area Network* (WAN) proses pengaksesan data dapat dilakukan dimana saja selama terkoneksi dengan internet, sehingga memungkinkan komunikasi data jarak jauh yang relevan. Karena memiliki manfaat sangat yang baik, kemudian dikembangkan berbagai jenis VPN seperti PPP, *winsock*, *IPsec* dan *Open* VPN (Khasanah, 2014).

Perusahaan yang bergerak di bidang *Internet Service Provider* yang selalu memperhatikan kebutuhan

konsumen akan keamanan di internet (Galih & Prakoso, 2015). Namun ketika konsumen melakukan pertukaran informasi ada pihak yang melakukan pencurian data selama ditransmisikan di internet. Pihak yang tidak berwenang bisa dengan leluasa menggunakan dan menyalahgunakan data untuk kepentingan mereka sendiri. Salah satu cara untuk membangun keamanan komunikasi data dalam jaringan internet adalah dengan menggunakan jaringan VPN (Meyatmaja & Syafrizal, 2012).

PT Jasa Cendekia Indonesia merupakan perusahaan yang bergerak di bidang konsultan dan layanan penyedia tenaga kerja bagi perusahaan di bidang IT, *energy*, komunikasi, elektronik dan perbankan. Berdasarkan masalah yang terjadi disini adalah belum adanya komunikasi yang baik karena belum adanya komunikasi data antar pegawai yang aman dan belum terstruktur dengan baik antara jaringan komputer kantor pusat yang berada di Jakarta dengan kantor cabang yang ada di Bali.

METODOLOGI PENELITIAN

Metode penelitian adalah suatu cara bagaimana seorang peneliti dapat memahami suatu pembahasan, permasalahan, dan pemecahan masalah dalam sebuah sistem. Berikut adalah metode penelitian yang penulis gunakan:

1. Analisa Kebutuhan
   Tahap penelitian ini adalah menganalisa kebutuhan atas masalah yang sering timbul pada jaringan yang ada dengan tujuan untuk merancang jaringan yang lebih baik dan sistematis. Sebagai tahap awal untuk pengembangan sistem, Analisa kebutuhan juga untuk mendefinisikan perkiraan kebutuhan-kebutuhan sumber daya apa saja yang akan digunakan nanti kedepannya.
2. Perancangan
   Tahap dimana setelah analisis sistem yang menentukan hasil sebuah proses yang diperlukan oleh sistem baru. Langkah-langkah yang dilakukan adalah menyiapkan rancangan jaringan terperinci yang sesuai kebutuhan dan menyiapkan usulan untuk implementasi dalam hal ini peneliti mendesain jaringan dengan topologi *star* pada PT. Jasa Cendekia Indonesia.
3. Pengujian
   Pada tahap ini dibuat beberapa poin-poin hasil uji pada rancangan yang akan disesuaikan dan disepakati pada jaringan usulan sebelum dimplementasikan dalam hal ini berupa simulasi jaringan pada *Cisco Packet Tracer*
4. Implementasi
   Tahap dimana rancangan jaringan komputer dibentuk, diimplementasikan dan disimulasikan. Dalam hal ini rancangan jaringan komputer di implementasikan pada *Cisco Packet Tracer*.

HASIL DAN PEMBAHASAN

1. Manajemen Jaringan Usulan
   Tujuan jaringan usulan ini adalah menghubungkan kantor pusat yang berada di Jakarta dengan cabang yang berada dibali dengan menggunakan teknologi VPN. Sesuai pembahasan perancangan dan pembangunan jaringan yang menggunakan VPN mempunyai fungsinya yaitu membuat jaringan *private* atau khusus dengan melewati jaringan publik seperti internet, sehingga teknologi ini aman karena menggunakan metode enkripsi dan *access list*.
   Sedangkan protokol *routing static* merupakan penghubung jaringan kantor pusat dengan cabang untuk memudahkan klien dalam berbagi informasi yang akan memudahkan melakukan pekerjaan. Dalam jaringan usulan ini akan menggunakan beberapa perangkat keras, antara lain :

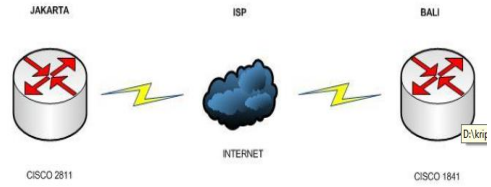
Tabel 1. Perangkat Jaringan Usulan

Perangkat	Jumlah	Tipe
Router	1	Cisco 2811
Router	1	Cisco 1841
Switch Managable	2	Cisco WS-C2950-24 (24 port)
Access point	2	Cisco-Linksys WAP54G
Server	3	HP / PC Rakitan

Sumber: Hasil penelitian

Router Cisco 2811 digunakan di kantor pusat, 1841 untuk kantor cabang dan ke duanya penghubung *internet services provider* (ISP), sementara *switch* Cisco WS-C2950-24 digunakan sebagai penghubung jaringan lokal komputer pada kantor pusat dan kantor cabang serta untuk *web server*. Untuk ke LAN antar lantai dapat digunakan *switch* yang ada yaitu *switch* TP-LINK TL-SG1016 dan untuk jaringan *wireless* menggunankan Cisco-Linksys WAP54G untuk yang mambawa laptop. *Server* sendiri digunakan penulis untuk membuat *server email* dan AAA *server* jenis RADIUS (*Remote Authentication Dial In User Service)*. Untuk aplikasi yang digunakan di *server* AAA banyak jenisnya seperti TekRADIUS.

2. Topologi Jaringan
   a. Desain topologi protokol *routing static*
      Static routing merupakan protokol *routing* yang akan digunakan. Karena pada saat ini memang baru ada satu kantor cabang. Tapi untuk kedepannya tidak menutup kemungkinan akan terkoneksi lebih banyak *router* dan tentunya lebih banyak kantor cabang.

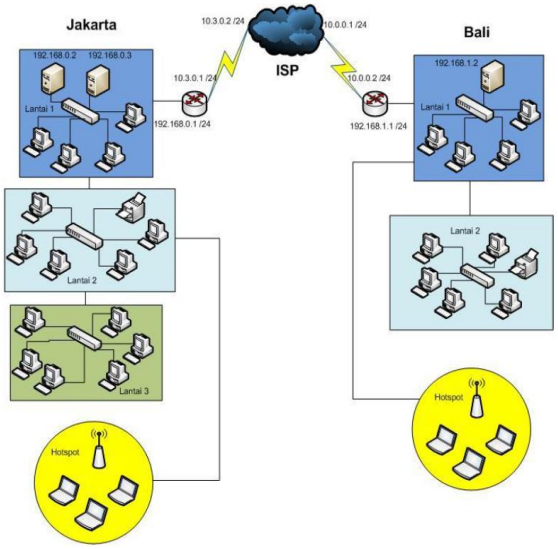


Sumber: Hasil penelitian

Gambar 1. Topologi *routing static*

b. Desain topologi VPN kantor pusat dengan cabang

Dalam hal ini dasain topologinya menggunakan *router* ISP yang seakan-akan merupakan internet, karena dalam *Cisco Packet Tracer* tidak dapat melakukan simulasi internet. VPN server terdapat pada kantor pusat di Jakarta, sedangkan VPN *clients* merupakan perangkat-perangkat yang terdapat di kantor cabang Bali. Untuk topologi di bawah hanya menggambarkan beberapa PC untuk mewakili jaringan yang ada. Sedangkan untuk keseluruhan jaringan ada di skema jaringan usulan.

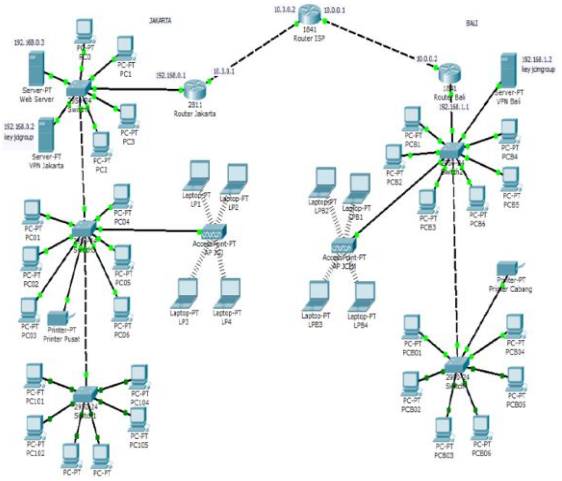


Sumber: Hasil penelitian

Gambar 2. Topologi VPN kantor pusat dan cabang

3. Skema Jaringan

Jaringan usulan yang telah dibuat diimplementasikan dalam bentuk simulasi menggunakan *software* simulator jaringan. *Software* yang digunakan adalah *Cisco Packet Tracer*. Untuk jaringan usulan dapat dilihat berikut ini.



Sumber: Hasil penelitian

Gambar 3. Skema jaringan usulan

Untuk pengalamatan IP sebaiknya dibuat tabel yang berisi pengalamatan masing-masing user baik yang terdapat pada kantor pusat dan cabang untuk memudahkan dalam melakukan konfigurasi pada *user*. Berikut tabel IP *user* yang digunakan dalam rancangan jaringan usulan.

Tabel 2. Usulan pengalamatan IP router

Router	Port Fa 0/0	Port Fa 0/1
Kantor Pusat	10.3.0.1/24	192.168.0.1/24
Router Kantor Cabang	10.0.0.2/24	191.169.1.1/24
Router ISP	10.3.0.2/24	10.0.0.1/24

Sumber: Hasil penelitian

Untuk pengalamatan IP di jaringan kantor pusat dan cabang juga dapat dilihat tabel di bawah ini.

Tabel 3. Usulan IP kantor pusat

Lantai	Perangkat	IP
1	Server AAA	192.168.0.2/24
1	Server Web/Mail	192.168.0.3/24
1	PC1	192.168.0.5/24
1	PC2	192.168.0.6/24
1	PC3	192.168.0.7/24
1	PC4	192.168.0.8/24
1	LP1	192.168.0.50/24
1	LP2	192.168.0.51/24
1	LP3	192.168.0.52/24
1	LP4	192.168.0.53/24
2	PC01	192.168.0.10/24
2	PC02	192.168.0.11/24
2	PC03	192.168.0.12/24
2	PC04	192.168.0.13/24
2	PC05	192.168.0.14/24
2	PC06	192.168.0.15/24
2	PC07	192.168.0.16/24
2	PC08	192.168.0.17/24
2	PC09	192.168.0.18/24
2	LP5	192.168.0.54/24
2	LP6	192.168.0.55/24

Lantai	Perangkat	IP
2	LP7	192.168.0.56/24
2	LP8	192.168.0.57/24
2	Printer pusat	192.168.0.20/24
3	PC101	192.168.0.30/24
3	PC102	192.168.0.31/24
3	PC103	192.168.0.32/24
3	PC104	192.168.0.33/24
3	PC105	192.168.0.34/24
3	PC106	192.168.0.35/24
3	LP9	192.168.0.58/24
3	LP10	192.168.0.59/24

Sumber: Hasil penelitian

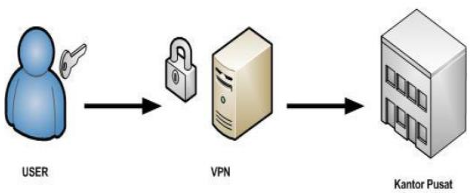
Tabel 4. Usulan IP kantor cabang

Lantai	Perangkat	IP
1	Server AAA	192.168.1.2/24
1	PCB1	192.168.1.5/24
1	PCB2	192.168.1.6/24
1	PCB3	192.168.1.7/24
1	PCB4	192.168.1.8/24
1	PCB5	192.168.1.9/24
1	PCB6	192.168.1.10/24
1	LPB1	192.168.1.20/24
1	LPB2	192.168.1.21/24
1	LPB3	192.168.1.22/24
2	PCB01	192.168.1.11/24
2	PCB02	192.168.1.12/24
2	PCB03	192.168.1.13/24
2	PCB04	192.168.1.14/24
2	PCB05	192.168.1.15/24
2	PCB06	192.168.1.16/24
2	PCB07	192.168.1.17/24
2	LPB4	192.168.1.23/24
2	LPB5	192.168.1.24/24
2	Printer cabang	192.168.1.40/24

Sumber: Hasil penelitian

4. Keamanan Jaringan
   Untuk keamanan jaringan usulan, penulis dapat menggunakan *Standard Access List* atau *Extended Access List.* Namun di jaringan usulan ini hanya digunakan *Standard Access List.*
   Standard Access List (ACL *Standard*) adalah fitur yang terdapat pada *router* yang berfungsi untuk menyaring paket untuk menentukan apakah sebuah paket bisa dilewatkan atau tidak. ACL hanya dapat melakukan *filtering* berdasarkan IP *host* atau IP *network sourcenya* saja. Untuk konfigurasinya sedekat mungkin dengan tujuan.

5. Rancangan Aplikasi

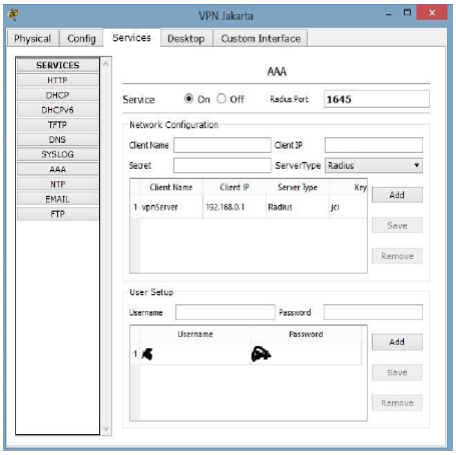


Sumber: Hasil penelitian

Gambar 4. Diagram alur *user* dalam mengakses jaringan

Hasil dari rancangan jaringan yang telah dibuat akan diterapkan dalam *software* simulasi jaringan komputer yaitu menggunakan *Cisco Packet Tracer*.

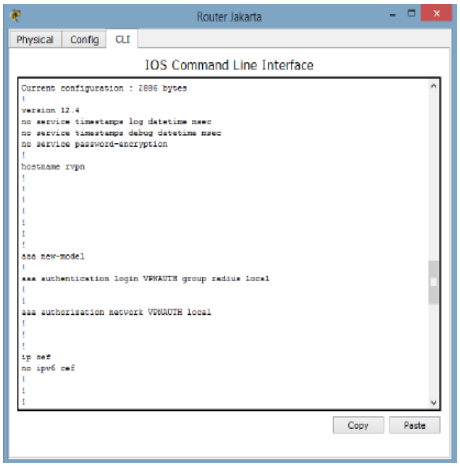
a. Konfigurasi *Server* VPN
   Pada *server* VPN penulis melakukan konfigurasi pada *services* AAA (*Authentication*, *Authorization*, dan *Accounting*) dengan mengisi *radiusport*, *secret*, *client* IP, *user name* dan *password* yang nanti akan di gunakan untuk koneksi ke *router* VPN dan komputer *client*.



Sumber: Hasil penelitian

Gambar 5. Konfigurasi *server* VPN

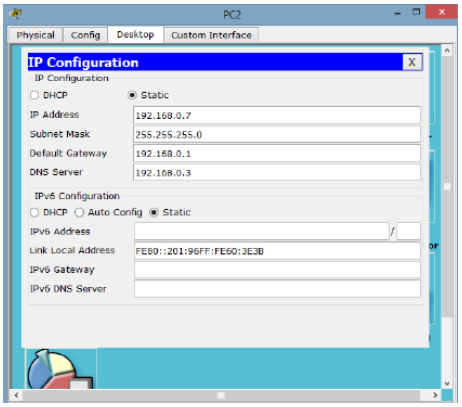
b. Konfigurasi *router* VPN



Sumber: Hasil penelitian

Gambar 6. Konfigurasi *router* VPN

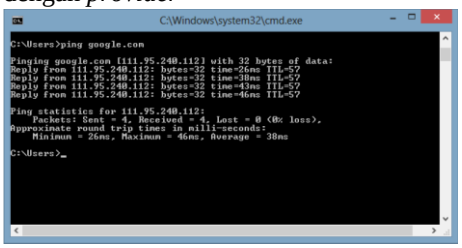
c. Konfigurasi komputer *client*
   Untuk konfigurasi komputer *client* dilakukan *setting* IP *address* dengan *static* IP *address*.



Sumber: Hasil penelitian

Gambar 7. Konfigurasi komputer *client*

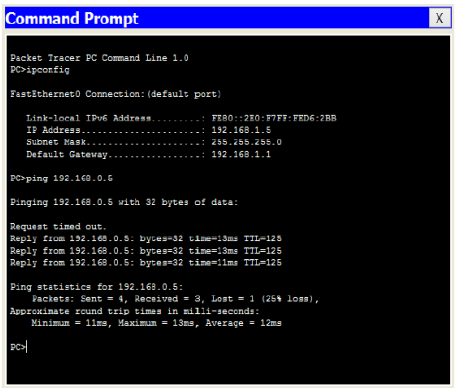
6. Pengujian Jaringan
   a. Pengujian awal
      Pada pengujian jaringan di PT. Jasa Cendekia Indonesia, jaringan awal diuji dengan menggunakan tes koneksi lewat command promt dengan perintah "*ping*" dengan network yang sama dan *gateway* yang sama yang di dapat dari *Internet Service Provider*. Berikut gambar koneksi jaringan awal kantor pusat dengan *provider*



Sumber: Hasil penelitian

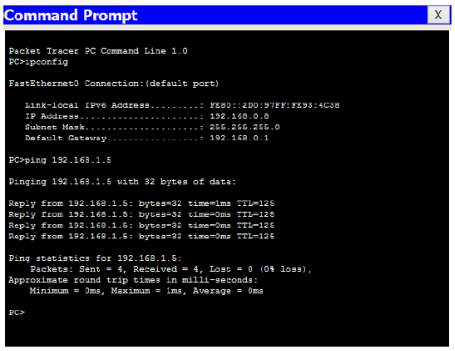
Gambar 8. Koneksi jaringan awal kantor pusat dengan *provider*

   b. Pengujian akhir
      Pada pengujian akhir peneliti melakukannya dengan melakukan *ping* dan koneksi VPN pada masing-masing PC dan *router* kantor pusat dengan kantor cabang juga sebaliknya. Hasilnya dapat dilihat untuk semua perangkat yang terhubung dapat di *ping* oleh perangkat lainnya. Pengujian juga dilakukan dengan perintah-perintah yang terdapat pada IOS *Cisco*.
      1) Tes koneksi menggunakan ping
         Pada pengujian dilakukan tes koneksi pada PC kantor cabang ke kantor pusat dan juga sebaliknya dengan perintah *ipconfig* dan *ping* IP *address* pada *command prompt*.



Sumber: Hasil penelitian

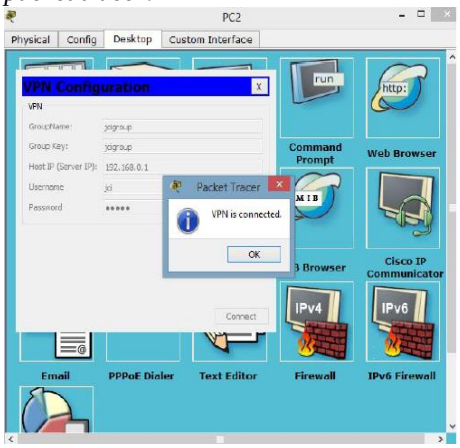
Gambar 9. Tes koneksi dari kantor cabang ke kantor pusat



Sumber: Hasil penelitian

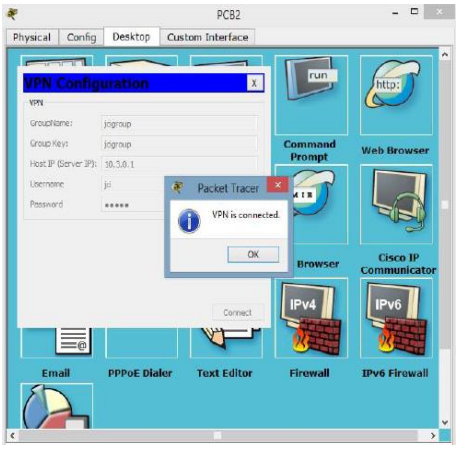
Gambar 10. Tes koneksi dari kantor pusat ke kantor cabang

2) Koneksi *server* VPN Jakarta
   Dalam hal ini peneliti menghubungkan PC kantor pusat dan kantor cabang ke *server* VPN Jakarta dengan menggunakan fasilitas VPN yang ada pada aplikasi *cisco packet tracer*.



Sumber: Hasil penelitian

Gambar 11. Koneksi VPN PC Kantor Pusat ke *Server* VPN Jakarta

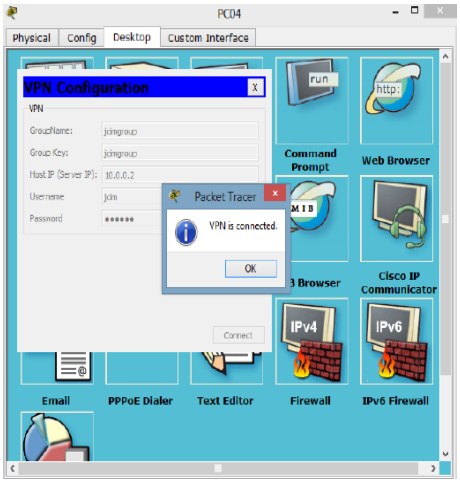


Sumber: Hasil penelitian

Gambar 12. Koneksi VPN PC Kantor Cabang ke *Server* VPN Jakarta

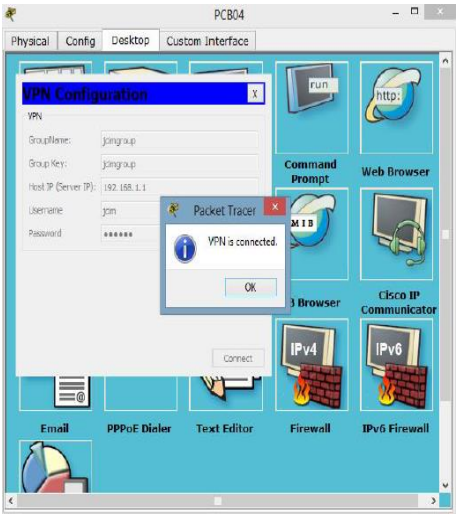
3) Koneksi *server* VPN Bali

Dalam hal ini peneliti mengkoneksikan PC kantor pusat dan kantor cabang ke *server* VPN Bali dengan meggunakan fasilitas VPN pada aplikasi *cisco packet tracert*, fungsi *router* VPN Bali ini sebagai *mirroring* dari VPN Jakarta.



Sumber: Hasil penelitian

Gambar 13. Koneksi VPN PC Kantor Pusat ke *Server* VPN Bali



Sumber: Hasil penelitian

Gambar 14. Koneksi VPN PC Kantor Cabang ke *Server* VPN Bali

4) Koneksi menggunakan IP *Route* dan IP *Crypto IPsec* pada *Router* Jakarta

Selain melakukan pengujian menggunakan *ping* dan koneksi VPN, pengujian juga dilakukan dengan menggunakan perintah yang terdapat pada IOS *Cisco* pada *router* Jakarta yang berupa *command show ip route* dan *show crypto ipsec transform-set*

```
rvpn#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 5 subnets
S       10.0.0.0 [1/0] via 10.3.0.2
S       10.1.0.0 [1/0] via 10.3.0.2
S       10.1.3.0 [1/0] via 10.3.0.2
S       10.1.4.0 [1/0] via 10.3.0.2
C       10.3.0.0 is directly connected, FastEthernet0/0
C    192.168.0.0/24 is directly connected, FastEthernet0/1
S    192.168.1.0/24 [1/0] via 10.3.0.2
rvpn#
```

Sumber: Hasil penelitian

Gambar 15. Show IP *route* pada *router* Jakarta

```
rvpn#sh crypto ipsec transform-set
Transform set mytrans: {    { esp-3des esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

Sumber: Hasil penelitian

Gambar 16. Show IP *crypto* IPsec pada *router* Jakarta

5) Koneksi menggunakan IP *route* dan IP *crypto* IPsec pada router Bali

```
rbali#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C       10.0.0.0/24 is directly connected, FastEthernet0/0
S       10.1.0.0/24 [1/0] via 10.0.0.1
S       10.1.0.0/32 [1/0] via 10.0.0.1
S       10.1.1.0/24 [1/0] via 10.0.0.1
S       10.1.1.0/32 [1/0] via 10.0.0.1
S       10.1.2.0/24 [1/0] via 10.0.0.1
S       10.3.0.0/24 [1/0] via 10.0.0.1
S       10.4.0.0/24 [1/0] via 10.0.0.1
S    192.168.0.0/24 [1/0] via 10.0.0.1
C    192.168.1.0/24 is directly connected, FastEthernet0/1
rbali#
```

Sumber: Hasil penelitian

Gambar 17. Show IP *route* pada *router* Bali

```
rbali#sh crypto ipsec transform-set
Transform set mytrans: {     { esp-3des esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

Sumber: Hasil penelitian

Gambar 18. Show IP *crypto* IPsec pada *router* Bali

6) Standar *access list* pada *router* Bali

```
rbali#sh access-lists
Standard IP access list 16
    10 deny host 192.168.1.10
    20 permit any
rbali#
```

Sumber: Hasil penelitian

Gambar 19. *Show standart access list* pada *router* Bali

7) Koneksi menggunakan IP *router* pada *router* ISP

```
RISP>en
RISP#
RISP#
RISP#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
C       10.0.0.0/24 is directly connected, FastEthernet0/1
S       10.1.0.0/24 [1/0] via 10.0.0.2
                    [1/0] via 10.3.0.1
S       10.1.0.0/32 [1/0] via 10.3.0.1
S       10.1.1.0/24 [1/0] via 10.3.0.1
S       10.1.1.0/32 [1/0] via 10.3.0.1
S       10.1.1.100/32 [1/0] via 10.3.0.1
S       10.1.2.0/24 [1/0] via 10.3.0.1
S       10.1.3.0/24 [1/0] via 10.0.0.2
S       10.1.4.0/24 [1/0] via 10.0.0.2
C       10.3.0.0/24 is directly connected, FastEthernet0/0
S    192.168.0.0/24 [1/0] via 10.3.0.1
S    192.168.1.0/24 [1/0] via 10.0.0.2
RISP#
```

Sumber: Hasil penelitian

Gambar 20. *Show* IP *route* pada *router* ISP

KESIMPULAN

Berdasarkan hasil rancangan dan analisa jaringan yang telah dibuat, dalam hal ini dapat menarik kesimpulan yaitu Jaringan VPN yang dirancang merupakan jaringan yang aman dan baik karena data berjalan pada jaringan publik, dan untuk *user* yang ingin mengakses jaringan VPN akan terlebih dahulu dicek di *server* AAA untuk dipastikan dengan data yang ada di *server*.

Dari hasil pengujian didapat *user* yang menggunakan hak akses VPN dapat melakukan pengiriman data dan *sharing folder*, tetapi untuk yang tidak memilki hak akses VPN tidak dapat melakukan hal tersebut dan hanya mampu melakukan koneksi sampai *router* saja. Adapun alasan untuk memilih protocol *routing static* karena pada simulasi ini hanya mempunyai dua kantor yang saling terhubung. Tidak menutup kemungkinan jika terdapat kantor cabang baru akan menggunakan *routing* dengan teknik OSPF yang bisa bekerja berdasarkan *area*. Dan untuk keamanan akses jaringan hanya menggunakan s*tandart access list* kerena berdasarkan penelitian belum terlalu banyak *user* yang berbagi data.

REFERENSI

Galih, S. T., & Prakoso, S. A. (2015). ANALISIS DAN PERANCANGAN VIRTUAL PRIVATE NETWORK PADA PT. *KOMPUTAKI*, *1*(1), 50–71.

Khasanah, S. N. (2014). PERANCANGAN DAN IMPLEMENTASI WIDE AREANETWORK(WAN) DENGAN IP VPN Studi Kasus : PT. MDPU Finance. *Techno*, *XI*, 105–111.

Meyatmaja, E., & Syafrizal, M. (2012). PERANCANGAN VIRTUAL PRIVATE NETWORK PADA PT PIKA MEDIA KOMUNIKA. *JURNAL DASI*, *13*(ISSN: 1411-3201), 11–16. Retrieved from ojs.amikom.ac.id/index.php/dasi/article/download/123/109

Supriyono, H., Widjaya, J. A., & Supardi, A. (2013). Penerapan jaringan. *WARTA*, *16*(ISSN 1410-9344), 88–101.

Wahidin. (2007). *Jaringan Komputer Untuk Orang Awam*. Palembang: Mazikom.

PROFIL PENULIS

Syarif Hidayatulloh. Lulus Pasca Sarjana Magister Ilmu Komputer Konsentrasi E-business STMIK Nusa Mandiri Jakarta. Saat ini aktif sebagai dosen tetap STMIK Nusa Mandiri Jakarta.

Wahyudin. Lulus Program Pasca Sarjana Magister Ilmu Komputer Konsentrasi Managemen Information System STMIK Nusa Mandiri Jakarta. Saat ini aktif sebagai dosen tetap Universitas Bina Sarana Informatika Jakarta.