Jurnal Indonesia : Manajemen Informatika dan Komunikasi
www.journal.amikindonesia.ac.id/jimik/ Vol 4 No 3, September (2023)
E-ISSN: 2723-7079, P-ISSN: 2776-8074

OPTIMALISASI KINERJA JARINGAN VPN DENGAN METODE DMVPN

Jodi Juliansah [1*], Yuma Akbar [2]

[1*, 2] Program Studi Teknik Informatika, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta, Indonesia.

Email: jodi.jlnsh12@gmail.com [1*], yuma.pjj@gmail.com [2]

Histori Artikel:
Dikirim 28 Juli 2023; *Diterima dalam bentuk revisi* 20 Agustus 2023; *Diterima* 28 Agustus 2023; *Diterbitkan* 10 September 2023.

Abstrak

DMVPN (*Dynamic Multipoint Virtual Private Network*) merupakan sebuah teknologi VPN yang mampu mempermudah proses konfigurasi dan meningkatkan efisiensi jaringan. Tujuan dari penelitian ini dilakukan sebagai respon terhadap kendala yang dialami perusahaan dalam performa jaringan VPN yang tidak memenuhi harapan serta mengurangi biaya operasional dan infrastruktur yang tinggi terkait kinerja jaringan VPN saat ini. Selain itu untuk mengetahui sejauh mana penggunaan DMVPN dapat meningkatkan kinerja jaringan VPN pada perusahaan. Metode yang digunakan adalah pengumpulan data melalui observasi dan wawancara, serta analisis data yang telah terkumpul. Hasil penelitian menunjukkan bahwa penggunaan DMVPN dapat meningkatkan efisiensi jaringan VPN pada perusahaan dengan mengurangi beban trafik dan mempercepat proses transmisi data. Oleh karena itu, teknologi DMVPN sangat direkomendasikan untuk perusahaan yang memerlukan jaringan VPN yang kompleks dan membutuhkan kinerja jaringan yang optimal. Penelitian ini memberikan pemahaman yang lebih dalam tentang teknologi DMVPN dan manfaatnya bagi perusahaan yang menggunakan jaringan VPN.Hasil penelitian ini diharapkan dapat memberikan pemahaman yang lebih baik tentang potensi dan efektivitas penggunaan DMVPN dalam mengoptimalkan kinerja jaringan VPN pada perusahaan. Diharapkan bahwa implementasi DMVPN dapat meningkatkan kecepatan transfer data, mengurangi latensi, serta meningkatkan keamanan data dalam jaringan VPN. Selain itu, diharapkan juga bahwa penggunaan DMVPN dapat mengurangi biaya operasional dan infrastruktur yang terkait dengan jaringan VPN, sehingga perusahaan dapat mencapai efisiensi yang lebih tinggi.

Kata Kunci: DMVPN; VPN; IPsec.

Abstract

DMVPN (Dynamic Multipoint Virtual Private Network) is a VPN technology that can simplify the configuration process and improve network efficiency. The purpose of this research was conducted as a response to the obstacles experienced by companies in VPN network performance that did not meet expectations and reduced high operational and infrastructure costs related to the performance of the current VPN network. In addition, to determine the extent to which the use of DMVPN can improve the performance of VPN networks in companies. The method used is data collection through observation and interviews, and analysis of the data that has been collected. The results showed that the use of DMVPN can increase the efficiency of the VPN network in the company by reducing traffic load and speeding up the data transmission process. Therefore, DMVPN technology is highly recommended for companies that require complex VPN networks and need optimal network performance. The results of this research are expected to provide a better understanding of the potential and effectiveness of using DMVPN in optimizing the performance of VPN networks in companies. It is expected that the implementation of DMVPN can increase data transfer speed, reduce latency, and increase data security in VPN networks. In addition, it is also expected that the use of DMVPN can reduce the operational and infrastructure costs associated with VPN networks, so that companies can achieve higher efficiency.

Keyword: DMVPN; VPN; IPsec.

1. Pendahuluan

Dengan semakin majunya teknologi informasi, jaringan komputer menjadi infrastruktur vital dalam mendukung berbagai aspek kehidupan manusia, termasuk komunikasi, bisnis, dan pendidikan. Dalam lingkungan korporat dan organisasi besar, jaringan komputer sering kali kompleks dan terdiri dari berbagai cabang atau lokasi yang tersebar. Penggunaan jaringan pribadi virtual (VPN) telah menjadi solusi populer untuk menyediakan konektivitas yang aman dan terenkripsi bagi para pengguna, terutama di dalam jaringan.

Metode DMVPN (*Dyanamic Multipoint Virtual Private Network*) telah diusulkan sebagai alternatif untuk mengatasi masalah-masalah yang muncul dalam penggunaan VPN tradisional. Dengan menggunakan DMVPN kita dapat mengatasi masalah yang terjadi pada tradisional VPN, dengan memperkenalkan teknologi Multipoint GRE (mGRE) dan protokol NHRP(*Next Hop Resolution Protocol*)sehingga memungkinkan setiap site dapat terhubung secara langsung satu sama lain. Dengan demikian dapat mengurangi beban trafik dan meningkatkan efsiensi jaringan. Selain itu, kelebihan DMVPN juga dapat diatur untuk mengizinkan akses langsung ke internet, sehingga dapat mengurangi baiaya dan meingkatkan kecepatan.Selain itu juga, DMVPN memanfaatkan teknologi routing dinamis untuk membangun koneksi langsung antara cabang-cabang yang terhubung ke jaringan pusat, tanpa memerlukan jalur tetap yang khusus untuk setiap site yang ada di cabang. Keuntungan utama DMVPN adalah kemampuannya untuk mengoptimalkan penggunaan jalur yang ada dan secara otomatis menyusun jalur tercepat dan terbaik untuk mengirimkan paket data.

Terdapat beberapa sumber penelitian terdahulu yang relevan dengan topik implementasi DMVPN (*Dynamic Multipoint Virtual Private Network*) dan performansinya dengan menggunakan berbagai protokol routing. Iryani dan Andika (2021) telah mengimplementasikan DMVPN dengan dual hub [1]. Sebagai perbandingan, Claudia dan Rifqi (2021) menganalisis performansi DMVPN dengan protokol HSRP dan GLBP [2]. Selain itu, Masruroh *et al.* (2018) juga mengevaluasi performa DMVPN dengan protokol routing RIP, OSPF, dan EIGRP [3]. Marah *et al.* (2021) memfokuskan penelitian mereka pada performa DMVPN dengan routing dinamis dan enkripsi IPsec [4]. Selain itu, Misra dan Goswami (2017) menyajikan informasi tentang dasar-dasar routing jaringan [5].

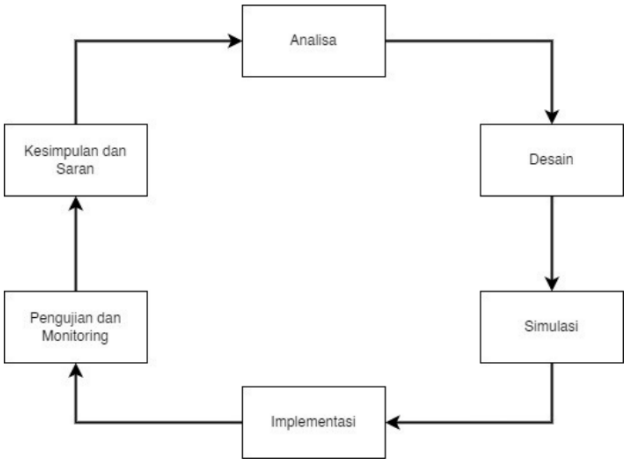
Selain penelitian terkait DMVPN, beberapa penelitian lain juga relevan. Dewi (2020) membahas keamanan jaringan menggunakan VPN dengan metode PPTP [6]. Umaroh dan Rifauddin (2020) mengimplementasikan VPN di perpustakaan universitas [7]. Suryani dan Honey (2007) membahas implementasi VPN dalam dunia bisnis [8]. Firmansyah *et al.* (2019) menganalisis performa Site-to-Site IP Security VPN dengan algoritma enkripsi ISAKMP [9]. Purnama Sari dan Kemala (2020) merancang jaringan VPN berbasis IP Security menggunakan router MikroTik [10]. Selain itu, Sudaryanto (2021) melakukan analisis konektivitas jaringan IPsec dan OpenVPN [12]. Novianto *et al.* (2022) mengimplementasikan keamanan akses terhadap website menggunakan Wireguard VPN di routerboard Mikrotik [13]. Madhadi dan Banowosari (2021) menganalisis performansi QoS VPN Encryption Protocol pada jaringan berbasis hybrid cloud [14]. Santoso *et al.* (2021) mengimplementasikan VPN Site-to-Site menggunakan protokol L2TP dan IPSec [15]. Niu *et al.* (2011) mengembangkan prosesor IPSec konfigurasi tinggi untuk jaringan keamanan [16]. Hauser *et al.* (2020) merancang P4-IPsec untuk VPN Site-to-Site dan Host-to-Site dengan SDN berbasis P4 [17].

Penelitian terdahulu mengenai implementasi DMVPN dan performansi jaringan VPN memberikan landasan yang kuat untuk mengeksplorasi keterkaitan dalam penelitian optimalisasi kinerja jaringan VPN dengan metode DMVPN. Sejumlah penelitian tersebut telah menguji DMVPN dengan berbagai konfigurasi, protokol routing, dan aspek keamanan, yang dapat menjadi rujukan penting dalam upaya untuk meningkatkan kinerja jaringan VPN menggunakan DMVPN. Dengan menggabungkan temuan-temuan dari penelitian-penelitian tersebut, penelitian ini dapat mengidentifikasi strategi dan langkah-langkah konkret untuk meningkatkan kinerja jaringan VPN dengan mengimplementasikan DMVPN dengan tepat, memilih protokol routing yang sesuai, dan mengoptimalkan aspek keamanan. Hal ini akan membantu organisasi atau individu dalam mencapai jaringan VPN yang lebih efisien dan andal.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1788-1798
DOI : https://doi.org/10.35870/jimik.v4i3.412

2. Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah metode NDLC (*Network Development Life Cycle)*. Metode NDLC terdiri dari bebrapa aspek merancang, mengimplementasikan, dan mengelola jaringan komputer. Berikut merupakan penjelasan dari masing-masing tahapannya.



Gambar 1. Metode NDLC

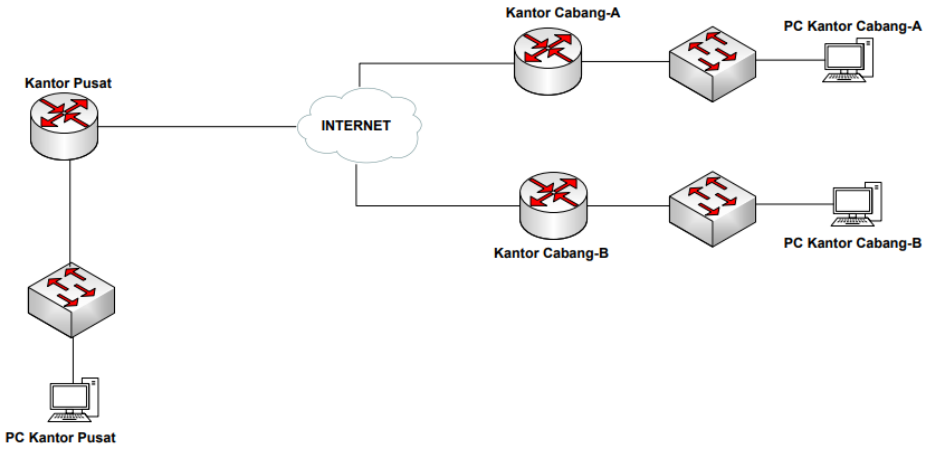
1) Analisa
   Pada tahap ini dimulai dengan menganalisa permasalahan yang muncul yaitu Bagaimana cara mengoptimalkan jaringan VPN dengan mengimplentasikan DMVPN dari Kantor Pusat dan Kantor Cabang menggunakan teknologi DMVPN.
2) *Desain*
   Pada tahap ini peneliti akan membuat suatu *design topologi* jaringan dari informasi atau data yang telah didapat sebelumnnya, dalam proses desain kita akan melakukan rancangan terhadap sebuah jaringan dimana jaringan tersebut akan memberikan gambaran seutuhnya dari kebutuhan yang ada.
3) Simulasi
   Pada tahap ini penulis akan melakukan simulasi sistem dan lingkungan *virtual* menggunakan GNS3 sesuai dengan sistem jaringan yang akan dibangun.
4) Implementasi
   Pada tahap ini penulis akan melakukan implementasi sesuai dengan analisa kebutuhan dan perancangan yang sudah dibuat untuk mengoptimalkan Jaringan VPN pada peruhsanaan menggunakan *teknologi* DMVPN dan melakukan pengujian unit system yang dibuat..
5) Pengujian dan *Monitoring*
   Pada tahap ini,penulis akan melakukan pengujian setelah implementasi selesai dilakukan. Tujuan dari pengujian tersebut untuk membuktikan hasil dari implementai yang dilakukan telah dibangun. Sementara untuk *monitoring* dilakukan untuk memastikan kinerja jaringan tetap optimal dan mengidentifikasi serta mengatasi masalah mungkin terjadi.
6) Kesimpulan
   Pada tahap ini, evaluasi terhadap hasil implementasi dan pengujian dilakukan. Kesimpulan berisi temuan penting saat penelitian dilakukan. Setelah menyimpulkan selanjutnya saran dari peneletian juga di sampaikan.

2.1 Analisa Topologi Jaringan

Topologi yang akan dibangun menggunakan lingkungan virtual GNS3, terdiri dari 3 *site*, di mana setiap site memiliki 1 *Router* yang terkoneksi ke internet. *Router* yang digunakan untuk simulasi dalam penelitian ini adalah *Router Cisco*, dimana masing-masing *Router* terkoneksi dengan jaringan

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1788-1798
DOI : https://doi.org/10.35870/jimik.v4i3.412

internet. Dan untuk client nya akan menggunakan VPCS(PC). Berikut merupakan rancangan topologi jaringan yang akan digunakan didalam penelitian ini.



Gambar 2. Topologi DMVPN

2.2 Parameter Pengujian

Pada Pada penelitian kali ini, parameter pengujian difokuskan pada tiga aspek Utama:

1) Pengujian protocol routing yang akan digunakan dalam jaringan DMVPN, seperti OSPF (*Open Shortest Path First*), EIGRP (*Enhanced Interior Gateway Routing Protocol*) atau RIP (*Routing Information Protocol*).
2) Menguji kemanan jaringan VPN dengan metode DMVPN dengan menggunakan fitur *IPSec* untuk melihat keunggulan dan kelemahan masing-masing.
3) Menguji *capability* dalam penggunaan DMVPN pada setiap *node* di *Router*, baik secara *CPU* maupun secara *Memory*.

2.3 Alat penelitian

Alat-alat yang digunakan untuk mendukung penelitian ini meliputi hardware berupa laptop, dan juga aplikasi GNS-3 yang sudah terinstall didalamnya. Berikut adalah detail alat yang digunakan dalam penelitian ini.

Tabel 1. Spesifikasi Hardware

No	Jenis hardware	Spesifikasi
1	Laptop	Lenovo Thinkpad E14
2	CPU	Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz 2.10 GHz
3	RAM	8GB
4	HDD	8Gb

Tabel 2. Spesifikasi Software

No	Jeni Software	Spesifikasi
1	Windows 10 Enterprise	Lenovo Thinkpad E14
2	GNS-3	Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz 2.10 GHz
3	VM	8GB
4	HDD	8Gb

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1788-1798
DOI : https://doi.org/10.35870/jimik.v4i3.412

3. Hasil dan Pembahasan

Setelah melakukan tahapan implementasi, selanjutnya akan dilakukan pengujian. Berikut merupakan pengujian yang akan dilakukan pada penelitian kali ini.

3.1 Pengujian *Routing Protocol* OSPF pada DMVPN

Pengujian ini bertujuan untuk memeriksa apakah kinerja DMVPN dapan menggunakan *routing protocol* OSPF untuk *koneksi Lan* pada jaringan DMVPN.

```
Kantor-Pusat#sh ip route ospf
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.168.12.2 to network 0.0.0.0

      2.0.0.0/32 is subnetted, 1 subnets
O        2.2.2.2 [110/1001] via 10.10.10.3, 00:43:49, Tunnel0
      3.0.0.0/32 is subnetted, 1 subnets
O        3.3.3.3 [110/1001] via 10.10.10.4, 00:43:49, Tunnel0
O     192.168.3.0/24 [110/1001] via 10.10.10.3, 00:43:49, Tunnel0
O     192.168.4.0/24 [110/1001] via 10.10.10.4, 00:43:49, Tunnel0
Kantor-Pusat#
```

Gambar 3. Show OSPF Kantor Pusat

```
Cabang-A#sh ip route ospf
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.168.13.2 to network 0.0.0.0

      1.0.0.0/32 is subnetted, 1 subnets
O        1.1.1.1 [110/1001] via 10.10.10.1, 00:42:55, Tunnel0
      3.0.0.0/32 is subnetted, 1 subnets
O        3.3.3.3 [110/1001] via 10.10.10.4, 00:42:55, Tunnel0
O     192.168.1.0/24 [110/1001] via 10.10.10.1, 00:42:55, Tunnel0
O     192.168.4.0/24 [110/1001] via 10.10.10.4, 00:42:55, Tunnel0
Cabang-A#
```

Gambar 4. Show OSPF Cabang-A

```
Cabang-B#sh ip route ospf
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.168.14.2 to network 0.0.0.0

      1.0.0.0/32 is subnetted, 1 subnets
O        1.1.1.1 [110/1001] via 10.10.10.1, 00:44:40, Tunnel0
      2.0.0.0/32 is subnetted, 1 subnets
O        2.2.2.2 [110/1001] via 10.10.10.3, 00:44:30, Tunnel0
O     192.168.1.0/24 [110/1001] via 10.10.10.1, 00:44:40, Tunnel0
O     192.168.3.0/24 [110/1001] via 10.10.10.3, 00:44:30, Tunnel0
Cabang-B#
```

Gambar 5. Show OSPF Cabang-B

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1788-1798
DOI : https://doi.org/10.35870/jimik.v4i3.412

```
Cabang-A#traceroute 10.10.10.4
Type escape sequence to abort.
Tracing the route to 10.10.10.4
VRF info: (vrf in name/id, vrf out name/id)
  1 10.10.10.1 144 msec 68 msec 76 msec
  2 10.10.10.4 156 msec 60 msec 60 msec
Cabang-A#traceroute 10.10.10.4
Type escape sequence to abort.
Tracing the route to 10.10.10.4
VRF info: (vrf in name/id, vrf out name/id)
  1 10.10.10.4 72 msec 56 msec 60 msec
Cabang-A#
```

Gambar 6. Traceroute Cabang-A

```
Cabang-B#traceroute 10.10.10.3
Type escape sequence to abort.
Tracing the route to 10.10.10.3
VRF info: (vrf in name/id, vrf out name/id)
  1 10.10.10.3 60 msec 36 msec 44 msec
Cabang-B#
```

Gambar 7. Traceroute Cabang-B

Dari gambar diatas dapat kita simpulkan bahwa *traffic* untuk *tunneling* pada saat melakukan *traceroute*, hop pertama kali ke Cabang-B akan ke kantor pusat terlebih dahulu, tetapi untuk selanjutnya ketika Cabang-A mengirim packet ke Cabang-B akan secara langsung ke site tersebut, tanpa harus packet tersebut transit ke kantor pusat. Dengan demikian dapat disimpulkan beban traffic yang ada pada kantor pusat akan lebih kecil,karena koneksi tunnel ke site lain bisa secara langsung seolah *directly connected*.

3.2 Pengujian Jaringan DMVPN menggunakan IPsec

pada pengujian kali ini kita bertujuan untuk memeriksa apakah koneksi tunneling yang dibangung antara kantor pusat dan cabang sudah ter-enkripsi dengan baik,sesuai fungsinya ipsec untuk memastikan agar koneksi tunneling yang digunakan dapat ter-enkripsi.

```
Kantor-Pusat#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.168.13.1    172.168.12.1    QM_IDLE           1002 ACTIVE
```

Gambar 8. Verify IPSec Kantor Pusat

```
Cabang-A#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.168.12.1    172.168.13.1    QM_IDLE           1001 ACTIVE
```

Gambar 9. Verify IPSec Cabang-A

```
Cabang-A#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/34/80 ms
Cabang-A#
```

Gambar 10. Ping Cabang-A ke Kantor Pusat

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1788-1798
DOI : https://doi.org/10.35870/jimik.v4i3.412

```
Kantor-Pusat#ping 10.10.10.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/43/48 ms
```

Gambar 11. Ping Kantor Pusat Ke Kantor Cabang-A

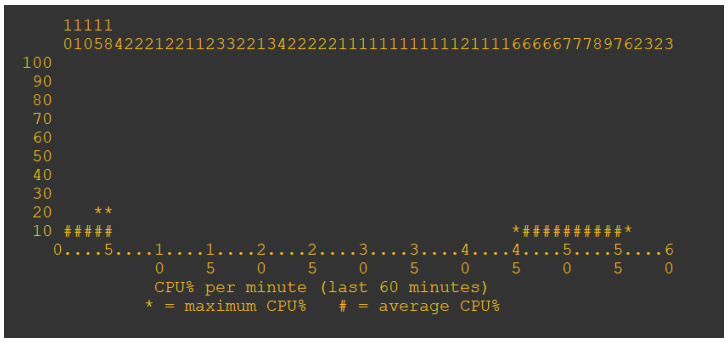
```
Cabang-B#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Cabang-B#ping 10.10.10.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Gambar 12. Ping kantor Cabang-B

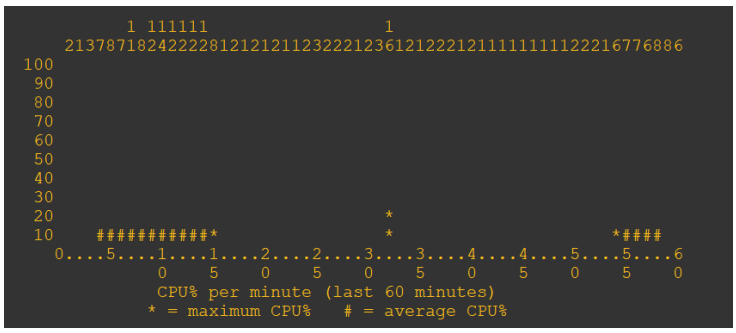
Dari Gambar diatas dapat disimpulkan hanya Router yang ada di kantor Cabang-B tidak dapat berkomunikasi dengan Router Kantor Pusat dan Router Cabang-A sedangkan router yang berada di Kantor Pusat dan Router Cabang-A dapat berkomunikasi satu sama lain, hal ini dikarenakan router Cabang-B tidak menjalankan Ipsec, sehingga tidak dapat berkomunikasi dengan router lainnya dan yang menjalankan Ipsec hanya router kantor pusat dan router Cabang-A oleh karena itu kedua site tersebut bisa saling berkomunikasi.

3.3 Pengujian Utilization Memory dan CPU

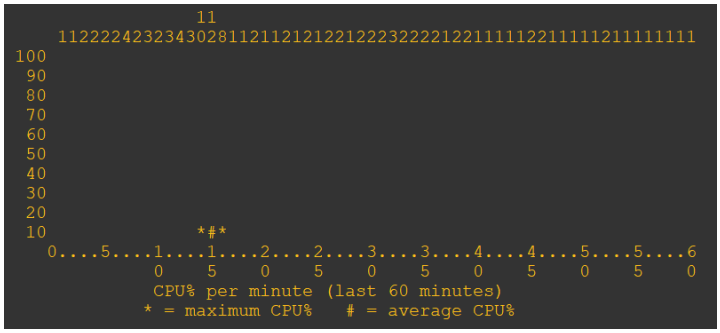
pada pengujian kali ini kita bertujuan untuk memeriksa apakah utilization pada perangkat setelah menggunakan fitur dmvpn bertambah secara signifikan baik utilization pada CPU maupun utilization pada Memory.



Gambar 13. CPU Kantor Pusat



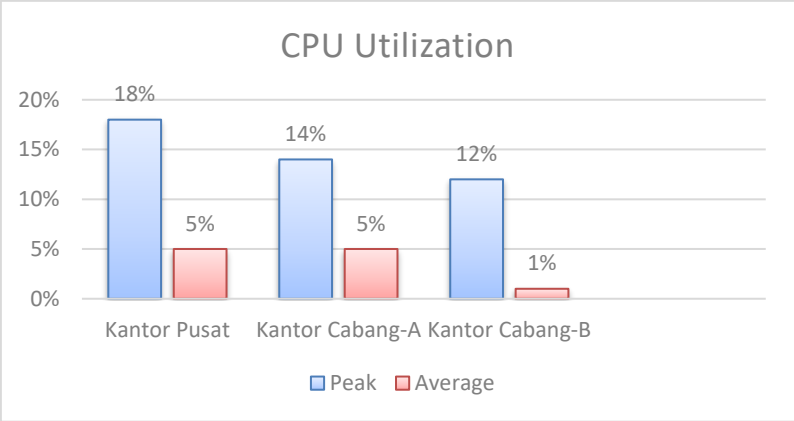
Gambar 14. CPU Kantor Cabang –A



Gambar 15. CPU Kantor Cabang-B

Table 3. CPU Utilization

Hostname	Peak	Average
Kantor Pusat	18%	5%
Kantor Cabang-A	14%	5%
Kantor Cabang-B	12%	1%



Gambar 16. CPU Utilization

Berdasarkan informasi dari 60 minutes terakhir dari data pada table diatas,secara rata-rata utilization tersebut dalam kondisi low. Terlihat dari keseluruhan perangkat peak paling tinggi tidak kurang dari 20%, dari data tersebut dapat disimpulkan bahwa penggunaan traffic pada DMVPN cukup baik.

```
Kantor-Pusat#sh processes memory
Processor Pool Total:  396826796 Used:   53907568 Free:  342919228
      I/O Pool Total:   33554432 Used:   10424832 Free:   23129600
Transient Pool Total:   16777216 Used:      10152 Free:   16767064
```

Gambar 17. Memory Utilization Kantor Pusat

```
Cabang-A#sh processes memory
Processor Pool Total:  396826796 Used:   53883788 Free:  342943008
      I/O Pool Total:   33554432 Used:   10426368 Free:   23128064
Transient Pool Total:   16777216 Used:      15252 Free:   16761964
```

Gambar 18. Memory Utilization Cabang-A

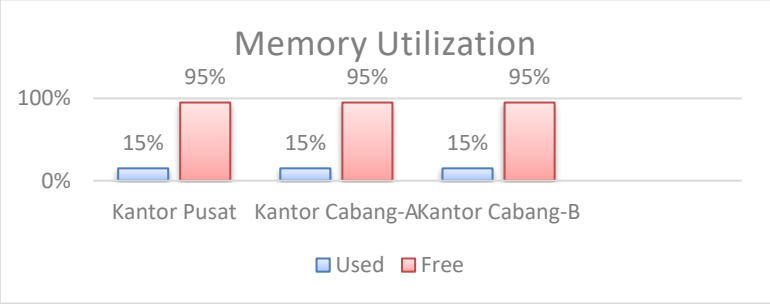
Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1788-1798
DOI : https://doi.org/10.35870/jimik.v4i3.412

```
Cabang-B#sh processes memory
Processor Pool Total:  396826796 Used:   53883652 Free:  342943144
      I/O Pool Total:   33554432 Used:   10426368 Free:   23128064
Transient Pool Total:   16777216 Used:      15252 Free:   16761964
```

Gambar 19. Memory Utilization Cabang-B

Table 4. Memory Utilization

Hostname	Used	Free
Kantor Pusat	15%	95%
Kantor Cabang-A	15%	95%
Kantor Cabang-B	15%	95%



Gambar 20. Memory Utilization

Berdasarkan informasi pada table diatas, terlihat bahwa rata-rata penggunaan *memory* dari keseluruhan perangkat masih dibawah 20%. Maka dari itu dapat disimpulkan bahwa penggunaan DMVPN tidak memakan resource memory cukup banyak, karena free memory masih cukup banyak, terlihat dari ketiga perangkat dari penggunaan *free memory*-nya sekitar 95%.

4. Kesimpulan

Berdasarkan hasil penelitian dan anilisis data yang telah dilakukan, dapat disimpulkan, bahwa teknologi DMVPN memiliki kinerja yang cukup baik, berikut aspek detail dari hasil penelitian yang telah dilakukan. Pertama,dalam hal routing DMVPN dapat juga di kombinasikan oleh routing protocol OSPF ,dimana routing OSPF memiliki skabilitas,konvergensi yang cepat sehingga sangat baik untuk routing yang *effisien* serta dapat diandalkan didalam jaringan VPN. Kedua,dari aspek keamanan DMVPN dapat menambahkan teknologi IPsec,sehingga *traffic* yang *outgoing* ataupun *incoming* akan lebih ter-enkripsi lagi dengan adanya IPsec tersebut. Ketiga, dengan menggunakan DMVPN *resource* yang terpakai tidak cukup banyak, sehingga masih banyak *resource* yang dapat digunakan untuk teknologi lainnya.

5. Daftar Pustaka

[1] Iryani, N., & Andika, D. D. (2021). Implementasi Dynamic Multipoint Virtual Private Network Dual Hub. *InComTech: Jurnal Telekomunikasi dan Komputer*, *11*(2), 118-129.DOI: 10.22441/incomtech.v11i2.10839.

[2] Claudia, M., & Rifqi, M. (2021). Analisa Perbandingan Performansi Hot Standby Router Protocol (HSRP) dengan Gateway Load Balancing Protocol (GLBP) Pada Router Spoke DMVPN. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *5*(2), 504-512. DOI: 10.30865/mib.v5i2.2846.

[3] Masruroh, S. U., Widya, K. H. P., Fiade, A., & Julia, I. R. (2018, August). Performance evaluation dmvpn using routing protocol rip, ospf, and eigrp. In 2018 6th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-6). IEEE. DOI: 10.1109/CITSM.2018.8674051.

[4] Marah, H. M., Khalil, J. R., Elarabi, A., & Ilyas, M. (2021, June). DMVPN Network Performance Based on Dynamic Routing Protocols and Basic IPsec Encryption. In *2021 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)* (pp. 1-5). IEEE. DOI: 10.1109/ICECCE52056.2021.9514142.

[5] Misra, S., & Goswami, S. (2017). Network routing: fundamentals, applications, and emerging technologies.

[6] Dewi, S. (2020). Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis. *EVOLUSI: Jurnal Sains dan Manajemen*, *8*(1).

[7] Umaroh, L., & Rifauddin, M. (2020). Implementasi Virtual Private Network (Vpn) Di Perpustakaan Universitas Islam Malang. *Jurnal Dokumentasi dan Informasi*, *42*(2), 193-201. Doi: 10.14203/j.baca.v41i2.531.

[8] Suryani, E., & Honey, S. N. R. (2007). Implementasi Virtual Private Network–WAN dalam Dunia Bisnis. *vol*, *6*, 31-38.

[9] Firmansyah, F., Wahyudi, M., & Purnama, R. A. (2019). Analisis Performa Site to Site IP Security Virtual Private Network (VPN) Menggunakan Algoritma Enkripsi ISAKMP. *Juita*, *7*(2), 129-135. DOI: 10.30595/juita.v7i2.4491.

[10] A. Purnama Sari and N. Kemala, "PERANCANGAN JARINGAN VIRTUAL PRIVATE NETWORK BERBASIS IP SECURITY MENGGUNAKAN ROUTER MIKROTIK," vol. 7, no. 2, 2020.

[11] Sulistiyono, S. (2020). Perancangan Jaringan Virtual Private Network Berbasis Ip Security Menggunakan Router Mikrotik. *PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer*, *7*(2), 150-164. DOI: https://doi.org/10.30656/prosisko.v7i2.2523.

[12] Sudaryanto, A. (2021). Analisa Konektivitas Jaringan IPSEC Dan OpenVPN Pada Jaringan Berbasis IP Dinamis. *Informatics, Electrical and Electronics Engineering (Infotron)*, *1*(2), 56-65.

[13] Novianto, D., Japriadi, Y. S., & Tommy, L. (2022). Implementasi Keamanan Akses Terhadap Website Menggunakan Wireguard VPN Di Routerboard Mikrotik. *Jurnal Ilmiah Informatika Global*, *13*(2). DOI: 10.36982/jiig.v13i2.2308.

[14] "Madhadi, T. E., & Banowosari, L. Y. (2021). Analisis Perbandingan Performasi QoS VPN Encryption Protocol Pada Jaringan Berbasis Hybrid Cloud: Array. *Jurnal Ilmiah Komputasi*, *20*(1), 69-82. DOI: 10.32409/jikstik.20.1.2695.

[15] Santoso, B., Sani, A., Husain, T., & Hendri, N. (2021). VPN Site To Site Implementation Using Protocol L2TP And IPSec. *TEKNOKOM*, *4*(1), 30-36. DOI: 10.31943/teknokom.v4i1.59.

[16] Niu, Y., Wu, L., Wang, L., Zhang, X., & Xu, J. (2011, December). A configurable IPSec processor for high performance in-line security network processor. In *2011 Seventh International Conference on Computational Intelligence and Security* (pp. 674-678). IEEE. DOI: 10.1109/CIS.2011.154.

[17] Hauser, F., Häberle, M., Schmidt, M., & Menth, M. (2020). P4-ipsec: Site-to-site and host-to-site vpn with ipsec in p4-based sdn. *IEEE Access*, *8*, 139567-139586. DOI: 10.1109/ACCESS.2020.3012738.

[18] "Understanding Dynamic and Static Routing | Engineering Education (EngEd) Program | Section." https://www.section.io/engineering-education/understanding-static-dynamic-routing/ (accessed May 23, 2023).

[19] "Dynamic Routing Protocols | Catchpoint." https://www.catchpoint.com/dynamic-routing-protocols (accessed May 23, 2023).

[20] "DMVPN Phases | DMVPN Phase 1 2 3." https://network--insight-net.translate.goog/2015/02/03/design-guide-dmvpn-phases/?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=wapp (accessed May 23, 2023).