Jurnal Infortech
Volume 2 No. 2 Desember 2020
E-ISSN: 2715-8160

OPTIMALISASI PERFORMA *SITE to SITE* IP *SECURITY* ISAKMP *VIRTUAL PRIVATE NETWORK* PADA XYZ

Ahmad Ulul Ilmi[1], Andry Maulana, M.Kom[2]

[1,2]Universitas Nusa Mandiri
ahmadululilmi105@gmail.com, andry.azy@nusamandiri.ac.id

Diterima _____ Direvisi _____ Disetujui _____

Abstrak - Kepolisian Negara Republik Indonesia memegang kendali terhadap terwujudnya kesejahteraan masyarakat Indonesia. Maka dari itu diperlukan suatu sistem jaringan yang dapat diandalkan untuk mendukung kesejahteraan masyarakat Indonesia khususnya di dalam Jaringan Komputer, salah satunya dengan menerapkan metode *Tunneling* menggunakan IPSec ISAKMP *Virtual Private Network*. Tujuan pengimplementasian *Site to Site* IP *Security Virtual Private Network With Algorithm Encryption* ISAKMP adalah untuk meningkatkan pelayanan yang diberikan oleh jaringan. Alasan utama untuk membuat *Site to Site* IP *Security Virtual Private Network With Algorithm Encryption* ISAKMP pada jaringan adalah penggunaan IPSec dapat meminimalisir dari serangan spying didalam jaringan dikarenakan IPSec melakukan enkripsi terhadap paket data didalam lalu lintas. Metode penelitian yang digunaan antara lain observasi, wawancara dan studi pustaka.

Kata Kunci: *Tunneling*, *Security*,Spying

PENDAHULUAN

Jaringan komputer adalah bagian penting dari sistem komunikasi didalam setiap aspek kehidupan kita. Tanpa kita sadari dengan adanya jaringan internet dapat menghambat beberapa aktivitas kita didalam melakukan sebuah bisnis dalam suatu perusahaan. Banyak perusahaan dan organisasi memerlukan layanan jaringan untuk mendukung operasional bisnis mereka. Oleh karena itu, layanan jaringan harus tersedia setiap saat, 24 jam sehari, guna memberikan dukungan yang berkelanjutan bisnis suatu perusahaan dan organisasinya. Untuk itu *Quality of Service* (QoS) di dalam layainan jaringan menjadi sebuah faktor terpenting(Azis, 2021).

Kepolisian Negara Republik Indonesia atau biasa disebut sebagai Polri merupakan salah satu alat atau institusi yang dimiliki oleh bangsa Indonesia untuk mewujudkan kesejahteraan masyarakat dan menjaga keharmonisan serta kedaulatan rakyat Indonesia(Hasibuan, 2021; Ilham et al., 2023). Kepolisian Negara Republik Indonesia memegang peran penting dalam keberlangsungan kehidupan masyarakat Indonesia. Kepolisian Negara Republik Indonesia memegang kendali terhadap terwujudnya kesejahteraan masyarakat Indonesia. Maka dari itu diperlukan suatu sistem jaringan yang dapat diandalkan untuk mendukung kesejahteraan masyarakat Indonesia khususnya di dalam Jaringan Komputer, salah satunya dengan menerapkan metode *Tunneling* menggunakan IPSec ISAKMP *Virtual Private Network*.

Menurut Firmansyah dkk Menyatakan bahwa, "Penggunaan IPSec dapat melindungi transfer data antara host *to* host, *network to network* hingga *network to* host dikarenakan melakukan pengenkripsi terhadap paket data yang ditransfer. Hasil pengujian dalam pengimplementasian jaringan *Site to Site* IP *Security Virtual Private Network With Algorithm Encryption* ISAKMP didapatkan pengurangan *hops* terhadap jaringan(Solikhah, 2021)." Sedangkan Menurut M. Ayub dkk Menyatakan bahwa "Salah satu keamanan yang digunakan dalam menggunakan perangkat berbasis internet adalah VPN dan *Firewall*. *Firewall* merupakan sebuah algoritma yang memungkinkan terjadinya kegiatan filterisasi, untuk menentukan pembatasan akses sebuah komputer, dimana dapat menggunakan akses jaringan publik dan komputer mana saja yang tidak dapat melewati akses jaringan publik, hal ini biasa disebut dengan filtering."(Ayub et al., 2021).

Dalam jaringan komputer, keamanan paket data sewaktu pengiriman dan penerimaan paket data sangatlah penting untuk menjamin bahwa paket data yang dikirimkan sampai pada pihak yang dituju, dan tidak jatuh pada pihak yang tidak berkepentingan. Permasalahan terhadap keamanan jaringan selalu dikembangkan sejalan dengan perkembangan teknologi informasi. Penggunaan IP *Security* (IPSec) merupakan sebuah metode enkripsi yang digunakan untuk melindungi kerahasiaan, dan keutuhan data pengguna layanan di jaringan internet(Prayogi Wicaksana et al., 2021; Suryantoro et al., 2021). IPSec merupakan skema keamanan end *to* end yang beroperasi didalam jaringan internet. Penggunaa IPSec dapat melindungi transfer data antara host *to* host, *network to network* atau diantara *network* dengan host. Penggunaan IPSec dapat meminimalisir dari serangan spying didalam jaringan dikarenakan IPSec melakukan enkripsi terhadap paket data didalam lalu lintas jaringan(Collins et al., 2021; Pratama, 2023).

Tujuan pengimplementasian *Site to Site* IP *Security Virtual Private Network With Algorithm Encryption* ISAKMP adalah untuk meningkatkan pelayanan yang diberikan oleh jaringan. Alasan utama untuk membuat *Site to Site* IP *Security Virtual Private Network With Algorithm Encryption* ISAKMP pada jaringan adalah penggunaan IPSec dapat meminimalisir dari serangan spying didalam jaringan dikarenakan IPSec melakukan enkripsi terhadap paket data didalam lalu lintas jaringan. Berdasarkan permasalahan diatas penulis mengambi(Madhadi & Banowosari, 2021; Prameswari & Marcus, 2024)l judul "Optimalisasi Performa *Site to Site* IP *Security* ISAKMP *Virtual* Provate *Network* Pada XYZ" sebagai judul skripsi..

Analisis masalah yang dihadapi membutuhkan batasan masalah atau ruang lingkup penelitian agar penyajian lebih terhubung dan terfokus. Batasan masalah yang akan didiskusikan adalah sebagai berikut: pertama, akan difokuskan pada implementasi *Site to Site* IP *Security* ISAKMP *Virtual Private Network*. Kedua, akan dilakukan pengujian sebelum dan sesudah pengimplementasian untuk mengevaluasi efektivitasnya.

METODE PENELITIAN

1. Metode Pengumpulan Data

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

a. Observasi

Penulis mengumpulkan data yang diperoleh dengan cara melakukan penelitian secara langsung ke perusahaan dengan melakukan riset selama kurang lebih 3 (tiga) bulan. Penulis melakukan peninjauan langsung tentang proses kerja dari jaringan komputer yang berada pada XYZ..

b. Wawancara

Penulis melakukan interaksi langsung dan terstruktur melalui sesi tanya jawab dengan pertanyaan yang relevan terkait dengan masalah yang sedang diteliti. Selain itu, penulis secara cermat mendengarkan penjelasan yang diberikan oleh narasumber, yaitu team IT operations dan IT *Network*, guna memastikan data dan informasi yang diperoleh akurat dan dapat dipercaya.

c. Studi Pustaka

Penulis melakukan pengamatan dengan membaca buku-buku dari beberapa referensi serta browsing melalui internet yang dapat dijadikan acuan dalam pencarian data serta penulis mencari beberapa referensi yang sesuai dengan pembahasan dari internet dan perpustakan Universitas Nusa Mandiri.

2. Analisa Penelitian

Ada beberapa tahap yang dilakukan penulis untuk menganalisa penelitian ini, diantaranya:

a. Analisa Kebutuhan

Analisa kebutuhan dilakukan untuk menghasilkan suatu perancangan jaringan komputer yang efisien, cepat dan tepat. Analisa kebutuhan dilakukan sebelum implementasi jaringan yang akan dirancang di XYZ, dengan menganalisa kebutuhan tersebut maka dapat mempermudah proses implementasi karena segala kebutuhan yang diperlukan untuk perancangan telah tersedia.

b. Merancang dan Membangun Sistem

Merupakan tahapan selanjutnya untuk melakukan desain dari rancangan jaringan usulan dengan menerapkan jaringan *Redudancy Hot Standby Router Protocol* dan *Access Control List*.

c. Implementasi

Tahap berikutnya setelah analisis adalah tahap desain. Pada tahap ini, tujuan sistem dilaksanakan menggunakan hasil pengamatan pada ar*Site*ktur jaringan komputer yang sudah berjalan di XYZ. Untuk itu, dibutuhkan perancangan jaringan yang sesuai dengan metode *Redudancy Hot Standby Router Protocol* dan *Access Control List* yang akan diterapkan.

d. Pengujian

Testing adalah proses melakukan pengujian terhadap QoS yang telah dirancang untuk mengevaluasi keberhasilan implementasi *Redudancy Hot Standby Router Protocol* dan *Access Control List*.

HASIL DAN PEMBAHASAN

1. Konsep Penunjang Usulan

a. *Site to Site* IP *Security Virtual Private Network*

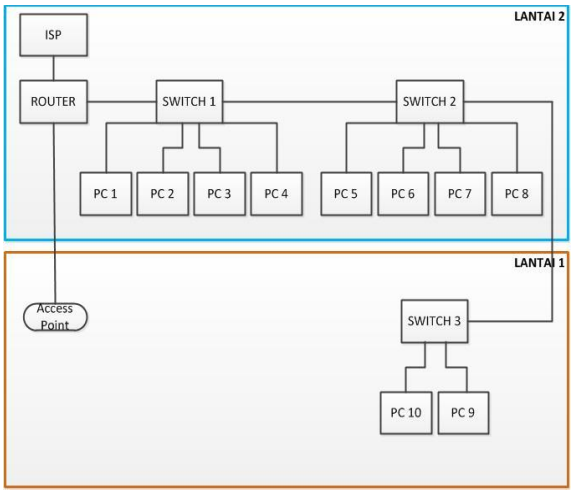
Saat implementasi ini digunakan, IPSec dapat meminimalisir dari serangan spying didalam jaringan dikarenakan IPSec melakukan enkripsi terhadap paket data didalam lalu lintas jaringan. Serta pengimplementasian IPSec mampu membuat jumlah *hops* yang dilalui maka semakin besar pula nilai *Time to Live* (TTL) yang didapatkanLoad Sharing

b. *Access Control List*

Access Control List diharapkan mampu memberikan batasan hak akses terhadap seluruh client yang terhubung didalam jaringan berjalan dengan menentukan alokasi IP *Address* mana yang di izinkan dan ditolak untuk melakukan akses kedalam tujuan tertentu.

2. Skema Jaringan Awal

Pada Divisi Sumber Daya Manusia XYZ terdapat skema jaringan yang terdiri dari blok diagram dan skema jaringan komputer.



Sumber: Hasil Penelitian

Gambar 1. Topologi Jaringan

Keterangan topologi jaringan komputer yang berada pada LPSE POLRI sebagai berikut:

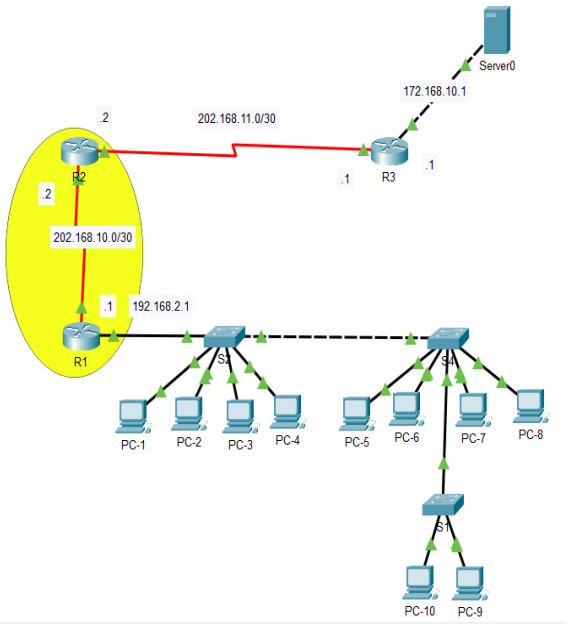
a. Internet *Service Provide*r (ISP) yang digunakan adalah Speedy dengan bandwidth 20 Mbps. *Router*board mikrotik pada jaringan komputer Divisi Sumber Daya Manusia XYZ berfungsi sebagai pusat kontrol jaringan komputer Divisi Sumber Daya Manusia XYZ.
b. Wireless *Access* Point berfungsi untuk membuat jaringan WLAN di kantor Divisi Sumber Daya Manusia XYZ.
c. Terminal yang digunakan berupa *switch* D-*LINK* 8 Port [DES-1008A].
d. *Client* terdiri dari 10 PC dan beberapa laptop karyawan.
e. Media transmisi yang digunakan kabel UTP Cat 5e.

Jaringan pada Divisi Sumber Daya Manusia XYZ menggunakan dua layanan ISP yang berbeda dimana layanan ISP tersebut yang berada pada kantor pusat menggunakan ISP Biznet Metronet sedangkan untuk kantor cabang menggunakan ISP Telkom, alasan perbedaan ISP tersebut dikarenakan cakupan area layanan Biznet belum mencangkup sampai pada kantor cabang. Disetiap kantor terdapat *router* sebagai pintu gerbang dari jaringan publik ke jaringan lokal dan juga berfungsi sebagai pemberi alamat IP kepada setiap pengguna. Pada setiap kantor juga memiliki 1 *switch* yang terhubung ke masing-masing perangkat jaringan wireless ataupun jaringan LAN yang terpasang pada setiap perangkat komputer karyawan(Hegia Theodosius *Site*pu, Miftahul Ilmi, 2024).

Router yang digunakan adalah cisco 2901. Untuk terminal yang menghubungkan setiap perangkat pada jaringan Divisi Sumber Daya Manusia XYZ menggunakan satu buah *switch*. Dimana *switch* utama tersebut terhubung kepada *switch* masing-masing lantai, dan *router*. Sedangkan *switch* yang berada di masing-masing lantai berjumlah 24 port menghubungkan 10 *client*, *printer*, *switch* utama, dan *access point*. Kabel jaringan yang digunakan Divisi Sumber Daya Manusia XYZ adalah kabel UTP (*Unshield Twisted Pair*) cat 6e dengan konektor RJ-45.

Pengalokasian IP *Address* yang digunakan pada Divisi Sumber Daya Manusia XYZ menggunakan IP *Address* kelas C, yaitu 192.168.10.XXX dengan *default* subnet *mask* kelas C yaitu 255.255.255.0 atau *prefiks* / 24 dengan *protokol TCP/IP*. Pemberian IP *Address* pada Divisi Sumber Daya Manusia XYZ diberikan secara *static* dan *dynamic*, dimana setiap *client* mendapat IP secara otomatis dari *router*

Router yang digunakan adalah *cisco* 2901. Untuk terminal yang menghubungkan setiap perangkat pada jaringan Divisi Sumber Daya Manusia XYZ menggunakan satu buah *switch*. Dimana *switch* utama tersebut terhubung kepada *switch* masing-masing lantai, dan *router*. Sedangkan *switch* yang berada di masing-masing lantai berjumlah 24 port menghubungkan 10 *client*, printer, *switch* utama, dan *access* point. Kabel jaringan yang digunakan Divisi Sumber Daya Manusia XYZ adalah kabel UTP (Unshield Twisted Pair) cat 6e dengan konektor RJ-45.



Sumber: Hasil Penelitian

Gambar 2. Skema Jaringan Awal

merupakan skema jaringan komputer yang digunakan pada Divisi Sumber Daya Manusia XYZ dengan menggunakan satu buah *router* cisco 2901 dan menggunakan ISP Biznet 20Mbps, serta perangkat tambahan seperti switch untuk menghubungkan jaringan LAN di setiap lantai guna menunjang pelayanan akses jaringan komputer.

2. Spesifikasi *Hardware*.

Spesifikasi perangkat keras yang digunakan pada jaringan komputer di Divisi Sumber Daya Manusia XYZ adalah menggunakan perangkat keras seperti pada tabel berikut:

a. Server

Server merupakan sistem komputer yang menyediakan jenis layanan atau *service* tertentu dalam sebuah jaringan komputer. Komputer yang digunakan untuk server harus memiliki spesifikasi yang lebih bagus daripada *client*. Karena komputer server memiliki tugas yang lebih komplek, yaitu sebagai pusat pengolahan data dalam suatu jaringan. Berikut spesifikasi komputer server yang digunakan pada Divisi Sumber Daya Manusia XYZ:

Tabel 1 Spefisikasi Komputer Server

No.	Komponen	Spesifikasi
1	*Processor*	*Intel Xeon*
2	*MotherBoard*	HP *Blade gen* 8 BL 4C
3	*Hard Disk*	5000 GB
4	RAM	512 GB
5	*Optical Disk*	DVD RW
6	NIC	10G

Sumber: Hasil Penelitian

Berdasarkan hasil analisa spesifikasi perangkat keras server, seperti yang tertera pada tabel 1, penulis menyimpulkan bahwa perangkat keras yang digunakan pada server sudah cukup memenuhi standar.

b. *Client*

Dalam sebuah jaringan tidak hanya komputer server yang dibutuhkan tetapi juga perlu komputer sebagai *client*. Komputer *client* berfungsi sebagai user (pengguna) yang membutuhkan data dari komputer server. Komputer *client* juga memiliki peran yang penting dalam sebuah jaringan. Oleh karena itu spesifikasi komputer *client* juga harus diperhatikan. Berikut adalah spesifikasi komputer *client* pada Divisi Sumber Daya Manusia XYZ Indonesia.

Tabel 2 Spesifikasi komputer *client*

No.	Komponen	Spesifikasi
1	*Processor*	Core i7
2	*MotherBoard*	HP 8600
3	*Hard Disk*	1000 GB
4	RAM	16GB
5	*Optical Disk*	DVD RW
6	NIC	10/1000

Sumber: Hasil Penelitian

Berdasarkan hasil analisa spesifikasi perangkat keras *client*, seperti yang tertera pada tabel 2, penulis menyimpulkan bahwa perangkat keras yang digunakan pada *client* sudah cukup memenuhi standar.

c. Jaringan

Perangkat keras jaringan komputer merupakan peralatan-peralatan yang digunakan untuk menghubungkan komputer dengan komputer lainnya, dengan tujuan berbagi data, informasi dan peripheral dalam sebuah jaringan komputer. Berikut adalah spesifikasi perangkat keras pada Divisi Sumber Daya Manusia XYZ.

Tabel 3 Spesifikasi perangkat keras jaringan

No.	Perangkat	Spesifikasi
1	*Router*	*Cisco* 2901
2	*Switch*	*Cisco* 2960X
3	*Modem*	TP-*LINK*
4	Kabel	UTP cat 6e *Fiber Optic*
5	*Printer*	FUJI Xerox
6	*Wireless Access Point*	WiNG Motorola RFS6000

Sumber: Hasil Penelitian

Berdasarkan hasil analisa spesifikasi perangkat keras jaringan yang digunakan seperti yang tertera pada tabel 3, penulis menyimpulkan bahwa perangkat keras jaringan yang digunakan pada Divisi Sumber Daya Manusia XYZ sudah cukup memenuhi standar dan mampu melakukan tugasnya masing-masing dengan baik.

3. Alternatif Pemecahan Masalah

Berdasarkan hasil riset pada jaringan Divisi Sumber Daya Manusia (SDM) XYZ, ditemukan permasalahan berupa tingginya jumlah *hop count* dari client menuju data center, yang berdampak pada meningkatnya latensi dan penggunaan bandwidth yang tidak efisien. Untuk mengatasi hal tersebut, diusulkan penerapan *Virtual Private Network* (VPN) sebagai solusi peningkatan efisiensi dan keamanan jaringan.

VPN berfungsi membentuk jalur komunikasi terenkripsi sehingga transfer data menjadi lebih aman dan stabil. Metode *Site*-to-*Site* VPN dengan protokol IPSec *Tunneling* direkomendasikan karena mampu menghubungkan beberapa lokasi jaringan menjadi satu kesatuan sistem yang aman. Melalui enkripsi dan autentikasi pada setiap paket data, IPSec dapat melindungi komunikasi antar jaringan serta mengurangi *hop count* yang dilalui data.

Dengan penerapan *Site*-to-*Site* IPSec VPN, diharapkan kinerja jaringan Divisi SDM XYZ menjadi lebih efisien, aman, dan stabil dalam mendukung aktivitas pertukaran data antar lokasi.

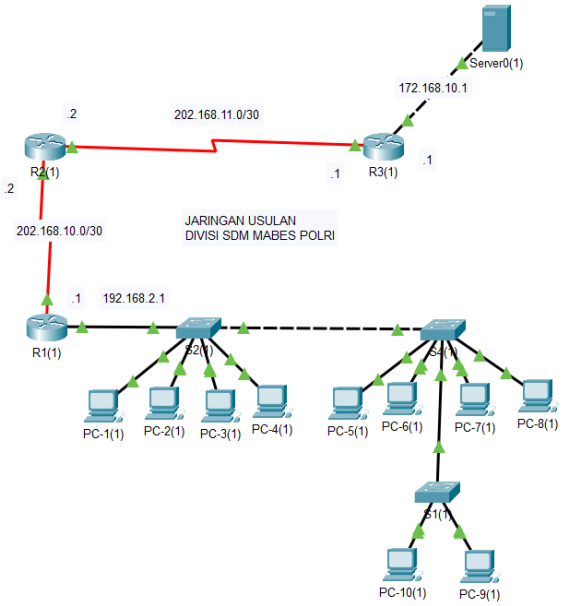
4. Jaringan Usulan

Jaringan yang penulis usulkan pada Divisi SDM XYZ adalah melakukan keamanan terhadap layanan jaringan menggunakan IP *Security* dan VPN. IP Sec berfungsi untuk melakukan enkripsi didalam melakukan transfer paket data dari asal ke tujuan. Serta pengimplementasia VPN *Site to Site* untuk mengoptimalkan *hop count* dengan melakukan *tunneling* dari sumber data ke tujuan data.

Topologi Jaringan

Dalam rancangan jaringan usulan yang penulis rancang untuk Divisi Sumber Daya Manusia XYZ tetap menggunakan topologi jaringan yang berjalan pada Divisi Sumber Daya Manusia XYZ. Dikarenakan topologi yang telah digunakan dapat berjalan cukup optimal secara keseluruhan serta tidak merubah total skema jaringan yang digunakan, penulis hanya saja mengimplementasikan jaringan usulan dengan menggunakan *Site to Site* IP *Security*

Virtual Private Network.



Sumber: Hasil Penelitian

Gambar 3. Skema Jaringan Usulan

Pada Gambar 3 merupakan skema jaringan usulan yang penulis usulkan pada Divisi SDM XYZ. Tidak terdapat penambahan perangkat jaringan namun penulis menambahkan metode keamanan terhadap layanan jaringan yang telah diimplementasikan sebelumnya. Keamanan jaringan yang akan digunakan pada Divisi SDM XYZ masih menggunakan keamanan jaringan yang sama, yaitu dengan menggunakan *firewall* dan antivirus kaspersky

Untuk melakukan pengimplementasian *Site to Site* IP *Security Virtual Private Network* didalam jaringan usulan terdapat beberapa konfigurasi yang harus dilakukan pada jaringan komputer.

a. Mengaktifkan *Security*

Langkah yang pertama dilakukan ialah mengaktifkan *security* technology package terhadap R1 dan R3.

R1(*config*)# license boot module c1900 technology-package *security*k9

R3(*config*)# license boot module c1900 technology-package *security*k9

b. Konfigurasi *Access Control List*

Setelah mengaktifkan technology package pada R1 dan R3, langkah selanjutnya ialah mengimplementasikan *Access Control List* (ACL) untuk menentukan *network* mana saja yang dapat melakukan akses didalam layanan jaringan. Implementasi ACL pada RI dengan konfigurasi

access-list 110 permit ip 192.168.2.0 0.0.0.255 172.168.10.0 0.0.0.255

Dan mengimplementasikan ACL pada R3 dengan perintah

access-list 110 permit ip 172.168.10.0 0.0.0.255 192.168.2.0 0.0.0.255

c. Konfigurasi Enkripsi ISAKMP

Langkah selanjutnya melakukan pembentukan enkripsi ISAKMP policy 10 terhadap R1 dan R3. Dengan perintah:

R1(*config*)# crypto isakmp policy 10
R1(*config*-isakmp)# *Encryption* aes 256
R1(*config*-isakmp)# authentication pre-share
R1(*config*-isakmp)# group 5
R1(*config*-isakmp)# exit
R1(*config*)# crypto isakmp key vpnpa55 *address* 202.168.11.1

R3(*config*)# crypto isakmp policy 10
R3(*config*-isakmp)# *Encryption* aes 256
R3(*config*-isakmp)# authentication pre-share
R3(*config*-isakmp)# group 5
R3(*config*-isakmp)# exit
R3(*config*)# crypto isakmp key vpnpa55 *address* 202.168.10.1

d. Konfigurasi IPSec

Setelah melakukan konfigurasi ISAKMP Policy, langkah selanjutnya melakukan pengimplementasian IPSec terhadap R1 dan R3. Dengan perintah:

R1(*config*)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R3(*config*)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac

5. Pengujian

Didalam pengimplementasian jaringan akhir, penulis membandingkan sebelum dan setelah pengimplementasian didalam rancangan jaringan. Terlihat hasil pengujian jaringan awal client memilik 4 *hops count* yang dilalui sedangkan setelah pengimplementasi jumlah *hops count* akan berkurang.

```
C:\>ping 172.168.10.254

Pinging 172.168.10.254 with 32 bytes of data:

Reply from 172.168.10.254: bytes=32 time=2ms TTL=125
Reply from 172.168.10.254: bytes=32 time=3ms TTL=125
Reply from 172.168.10.254: bytes=32 time=2ms TTL=125
Reply from 172.168.10.254: bytes=32 time=2ms TTL=125

Ping statistics for 172.168.10.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

Sumber: Hasil Penelitian

Gambar 4. Pengujian Jaringan Awal-1

Uji konektifitas yang pertama kali dilakukan adalah melakukan pengujian terhadap kinerja jaringan dengan melakukan perbandingan antara jaringan yang telah menggunakan *Tunneling* dengan sebelum *tunneling*. Pengujian *Tunnel* VPN dilakukan pada jaringan lokal R1 dengan IP *Address* 192.168.2.2 menuju jaringan lokal R3 dengan IP *Address* 172.168.10.254. Pengujian VPN *Tunnel* dapat dilakukan menggunakan perintah ping untuk melakukan pengiriman paket ICMP dan mendapatkan hasil traceroute seperti terlihat gambar 4 Terlihat nilai *Time to Live* (TTL) yang didapatkan

pada jaringan tanpa menggunakan *Tunnel* sebesar 125.

```
C:\>tracert 172.168.10.254

Tracing route to 172.168.10.254 over a maximum of 30 hops:

  1    0 ms      0 ms      10 ms     192.168.2.1
  2    2 ms      21 ms     0 ms      202.168.10.2
  3    3 ms      1 ms      0 ms      202.168.11.1
  4    1 ms      11 ms     0 ms      172.168.10.254

Trace complete.
```

Sumber: Hasil Penelitian

Gambar 5. Pengujian Jaringan Awal-2

Pengujian jaringan awal selanjutnya ialah dengan melihat jumlah *hops count* yang dilalui, pengujian dilakukan dengan skenario yang sama dengan menggunakan perintah tracert (alamat tujuan). Terlihat pada gambar 5 *hops count* yang dilalui sebanyak 4 *hops* untuk sampai pada alamat tujuan.

```
C:\>ping 172.168.10.254

Pinging 172.168.10.254 with 32 bytes of data:

Reply from 172.168.10.254: bytes=32 time=2ms TTL=126
Reply from 172.168.10.254: bytes=32 time=3ms TTL=126
Reply from 172.168.10.254: bytes=32 time=2ms TTL=126
Reply from 172.168.10.254: bytes=32 time=10ms TTL=126

Ping statistics for 172.168.10.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 10ms, Average = 4ms
```

Sumber: Hasil Penelitian

Gambar 6. Pengujian Jaringan Akhir-1

Pengujian pada jaringan akhir dilakukan untuk mendapatkan perbedaan sebelum maupun setelah konfigurasi didalam layanan jaringan. Jika melihat pada Gambar 6 TTL yang didapatkan sebelum pengimplementasian adalah TTL=125 sedangkan setalah pengimplementasian *Tunneling* menjadi TTL=126

```
C:\>tracert 172.168.10.254

Tracing route to 172.168.10.254 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.2.1
  2    28 ms     2 ms      1 ms      202.168.11.1
  3    16 ms     2 ms      20 ms     172.168.10.254

Trace complete.
```

Sumber: Hasil Penelitian

Gambar 7. Pengujian Jaringan Akhir-2

Terlihat pada gambar 7 *hops count* yang didapat setelah melakukan implementasi mengalami pengurangan dari sebelumnya 4 *hops count* menjadi 3 *hops count*.

```
R1#sh crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 202.168.10.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (172.168.10.0/255.255.255.0/0/0)
   current_peer 202.168.11.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 0
   #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 0
```

Sumber: Hasil Penelitian

Gambar 8. Pengujian Jaringan Akhir-3

Terlihat pada gambar 8 merupakan hasil uji konektifitas terhadap jaringan IPSec *Tunnel* VPN. R1 menggunakan interface serial0/0/0 dengan alokasi IP *Address* 192.168.2.1 untuk dapat melakukan remote terhadap *network* 172.168.10.0/24. Penggunaan IPSec *Tunnel* VPN mampu melakukan pengenkripsian terhadap paket data yang dilaluinya. Terlihat pada gambar IV.6 *network* 192.168.2.0 melakukan pengiriman paket data menuju *network* 172.168.10.0/24 sebanyak 11 paket yang telah terenkripsi. Jumlah paket yang terenkripsi akan bertambah secara otomatis ketika terdapat transfer paket data didalam jaringan yang menggunakan *Tunnel* VPN.

KESIMPULAN

Penelitian ini berhasil menyimpulkan bahwa implementasi *Site to Site* VPN berbasis IP *Security* (IPSec) dan protokol ISAKMP merupakan solusi efektif dalam mengoptimalkan performa dan keamanan jaringan di lingkungan XYZ. Hasil pengujian secara kuantitatif menunjukkan peningkatan efisiensi jaringan, ditandai dengan penurunan *hop count* dari 4 menjadi 3 dalam jalur transmisi data, sekaligus peningkatan nilai *Time to Live* (TTL) yang berkontribusi pada stabilitas dan efisiensi koneksi. Lebih lanjut, penggunaan IPSec terbukti krusial dalam meningkatkan tingkat keamanan jaringan secara signifikan, karena mekanisme enkripsi yang diterapkan mampu melindungi paket data dari risiko penyadapan dan pencurian informasi. Secara komprehensif, penerapan teknologi ini telah berhasil meningkatkan performa, efektivitas, dan keamanan jaringan XYZ, menjadikannya lebih andal dalam mendukung pertukaran data yang aman dan efisien antar divisi.

REFERENSI

Ayub, M., Maulana, A., & Fauzi, A. (2021). Penerapan *Firewall* Dan Protokol IpSec/L2TP Sebagai Solusi Keamanan Akses Jaringan Publik. *Computer Science (CO-SCIENCE)*, *1*(2), 81–90. https://doi.org/10.31294/coscience.v1i2.435

Azis, S. (2021). *Secret of Keyboard Shortcut: Tombol-tombol Rahasia Untuk Bekerja Cepat Di Komputer*. https://books.google.co.id/books?id=HVnaCQAAQBAJ&dq=Aziz,+Sholechul.+(2021).+Secret+Of+Keyboard+Shortcut+Tombol-Tombol+Rahasia+Untuk+Bekerja+Cepat+Di+Komputer.+Jakarta:+Sealova+Media.&lr=&hl=id&source=gbs_navlinks_s

Collins, S. P., Storrow, A., Liu, D., Jenkins, C. A., Miller, K. F., Kampe, C., & Butler, J. (2021). *No Title 済無No Title No Title No Title*. *4*(11), 167–186.

Hasibuan, M. N. (2021). Peran Kepolisian Dalam Melakukan Pembinaan Keamanan Dan. *Jurnal*

Pro Justitia (Jpj), *2*(1), 76–88.

Hegia Theodosius *Site*pu, Miftahul Ilmi, Y. A. (2024). Jurnal Teknologi Digital dan Sistem Informasi. *Jurnal Teknologi Digital Dan Sistem Informasi*, *1*(2), 107–115.

Ilham, C. M., Rahman, A., & Rahman, A. (2023). *Praktik Penyelenggaraan Ketenteraman dan Ketertiban Umum*.

Madhadi, T. E., & Banowosari, L. Y. (2021). Analisis Perbandingan Performasi QoS VPN *Encryption Protocol* Pada Jaringan Berbasis Hybrid Cloud. *Jurnal Ilmiah Komputasi*, *20*(1), 69–82. https://doi.org/10.32409/jikstik.20.1.2695

Prameswari, A. D., & Marcus, R. D. (2024). Peningkatan Keamanan Jaringan *Virtual Private Network* Menggunakan Protokol IKE/IPSEC Berbasis Mikrotik. *J-Intech*, *12*(02), 371–382. https://doi.org/10.32664/j-intech.v12i02.1493

Pratama, R. (2023). Literature Review : *Network Security* Menggunakan *Virtual Private*. *Jurnal Jaringan Komputer Dan Keamanan*, *04*(03), 11–18.

Prayogi Wicaksana, Hadi, F., & Aulia Fitrul Hadi. (2021). Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan. *Jurnal KomtekInfo*, *8*(3), 169–175. https://doi.org/10.35134/komtekinfo.v8i3.128

Solikhah, M. (2021). *PROGRAM APLIKASI JASA ANGKUTAN PADA PT A DI KOTA CIREBON Mar'atus*. *3*(1), 23–27.

Suryantoro, H., Sopian, A., & Dartono. (2021). PENERAPAN TEKNOLOGI FORTIGATE DALAM PEMBANGUNAN JARINGAN VPN-IP BERBASIS IPSEC. *JURNAL ELEKTRO & INFORMATIKA SWADHARMA (JEIS)*, *01*, 1–7.