BAB II KERANGKA TEORITIS

A. Landasan Teori

1. Pengertian Jaringan Komputer

Jaringan Komputer adalah suatu sistem yang terdiri dari beberapa komputer yang saling terkoneksi satu dengan yang lain melalui sebuah media transmisi atau media komunikasi pertukaran data (Wagito, 2005). Tujuan dibangun sebuah jaringan komputer agar sebuah data dan atau sebuah informasi dapat ditransmisikan dari pengirim menuju ke penerima. Jaringan komputer digunakan untuk membagi sebuah sumber daya, untuk komunikasi dan akses informasi.

2. Jenis Jaringan Komputer

Beberapa jenis Jaringan Komputer (Mufadhol, 2008), sebagai berikut:

a. Local Area Network (LAN) LAN biasanya memiliki jarak jangkauan kurang lebih 10 km dan biasanya diterapkan pada jaringan komputer disebuah gedung, sekolahan, dan perkantoran.
b. Metropolitan Area Network (MAN) MAN memiliki jarak lebih luas dibanding LAN dengan jarak jangkauan 10–50 km dan biasanya diterapkan pada jaringan disebuah perkotaan. Contoh pengaplikasian MAN adalah adanya penyediaan layanan internet oleh Internet Service Provider di kota tersebut.
c. Wide Area Network (WAN) WAN memiliki jarak jangkauan yang sangat luas bahkan bisa dikatakan dapat mencakup jaringan komputer seluruh dunia. Media transmisi pada WAN dapat dihubungkan menggunakan satelit maupun menggunakan *fiber optic*.

3. Pengalamatan IP

IP versi 4 memiliki pengalamatan terstruktur, terdiri dari 32 bit yang ditulis dalam nilai – nilai desimal yang dibagi dalam 4 segment dan setiap segmen terdiri dari 8 bit. IP address dapat ditulis dalam 8 bit (octet) angka binari atau angka decimal (0-255) yang dipisahkan oleh tanda titik. Contoh penulisan IP address dalam bentuk binary 11000000.00010000.00001010.00000001 atau dalam bentuk desimalnya 192.16.10.1. Alamat IP terdiri dari dua bagian yaitu network ID dan host ID. Dimana network ID menentukan alamat jaringan dan host ID menetukan alamat host atau komputer. Untul menentukan alamat kelas IP, dilakukan dengan memeriksa 4 bit pertama (bit yang paling kiri) dari alamat IP.

Tabel 2. 1 Kelas IP

Kelas	4 Bit Pertama	Desimal
A	0xxx	1–126
B	10xx	128–191
C	110x	192–223
D	1110	224–239
E	1111	240–254

a. Kelas A

Bit pertama alamat IP kelas a adalah 0, network ID 8 bit dan panjang host ID 24 bit. Kelas A digunakan untuk jaringan yang berskala besar, terdapat 126 jaringan dan tiap jaringan dapat menampung hingga 16 juta host. Alamat IP kelas A dimulai dari 1.0.0.0 sampai dengan 126.255.255.255. alamat oktet awal 127 tidak boleh digunakan karena digunakan unutk mekanisme Inter-process Communication didalam perangkat jaringan yang bersangkutan.

b. Kelas B

Dua bit awal dari kelas B selalu diset 10 sehingga byte pertama kelas B bernilai antara 128-191. Network ID adalah 16 bit pertama dan host ID 16 bit sisanya. Kelas B digunakan untuk jaringan berskala menengah hingga besar, terdapat 16.384 jaringan dan tiap jaringan dapat menampung 65 ribu host. Alamat kelas B dimulai dari 128.0.0.0 sampai dengan 192.167.255.255.

c. Kelas C

Tiga bit awal dari kelas C selalu diset 110, sehingga byte pertama kelas C bernilai antara 192 – 223. Network ID adalah 24 bit dan host ID 8 bit sisanya. Kelas C biasa digunakan untuk jaringan kecil, terdapat 2.097.152 jaringan dan tiap jaringan dapat menampung 256 host. Alamat kelas C dimulai dari 192.168.0.0 sampai dengan 223.255.255.255.

d. Kelas D

Empat bit awal dari kelas D selalu diset 1110, sehingga byte pertama kelas D bernilai antara 224 – 239. Kelas D digunakan untuk keperluan multicast, yaitu suatu metode pengiriman yang digunakan bila suatu host ingin berkomunikasi dengan beberapa host sekaligus, dengan hanya mengirim satu datagram saja. Alamat dari kelass D adalah

224.0.0.0 sampai dengan 239.255.255.255. alokasi alamat tersebut ditujukan untuk keperluan sebuah grup, bukan untuk host seperti pada kelas A, B dan C.

e. Kelas E

Empat bit dari kelas E selalu diset 1111, sehingga byte pertama kelas E bernilai antara 240 – 254. Kelas E digunakan sebagai kelas eksperimental yang disiapkan untuk keperkuan di masa mendatang.

4. Pengertian IP Adress Private dan Public

a. IP Address Private

Hampir seluruh alamat pada IPv4 merupakan alamat public yang dapat digunakan pada jaringan internet, namun terdapat juga blok alamat yang digunakan untuk keperluan terbatas atau tidak terhubung dengan internet. Alamat tersebut disebut sebagai alamat private. Range alamat private adalah:

1. 10.0.0.0 – 10.255.255.255
2. 172.16.0.0 – 172.31.255.255
3. 192.168.0.0 – 192.168.255.255

Host – host yang tidak memerlukan akses ke internet dapat menggunakan alamat private sebanyak apapun. Namun, jaringan internal tetap harus didesain dengan pengalamatan yang baik dan terstruktur sehingga alamat yang digunakan tetap unik untuk network internal tersebut.

Host yang berada di jaringan yang berbeda dapat menggunakan alamat private yang sama. Paket yang menggunakan alamat tersebut sebagai source dan destination tidak akan muncul di jaringan internet. Router atau firewall yang terletak di ujung jaringan tersebut harus memblok atau menterjemahkan alamat – alamat tersebut.

b. IP Address Public

Umumnya alamat IPv4 merupakan alamat publik. Alamat tersebut didesain untuk digunakan pada host yang dapat diakses oleh host lain melalui internet (Aldwin Nayoan, 2020).

5. Pengertian Algoritma Routing

Algoritma routing (Tanenbaum, 2004, p264) adalah bagian dari perangkat lunak *network layer* yang bertanggung jawab untuk memutuskan jalur *output* pada paket yang telah ditransmisikan padanya. Algoritma routing

dibagi menjadi dua kelas utama, *adaptive* dan *nonadaptive*. *Adaptive algorithm* merubah keputusan routing mereka sebagai cerminan perubahan yang terjadi dalam topologi, dan biasanya *traffic* juga. Adaptive algorithm berbeda dimana mereka mendapatkan informasi mereka (misal: dari router yang berdekatan), ketika mereka mengganti router (misal: ketika topologi berubah), dan metric yg digunakan untuk optimisasi (misal: jumlah hop). *Non-Adaptive algorithm* keputusan routing tidak berdasarkan pada pengukuran atau perkiraan *traffic* dan *topology*.sebagai gantinya, pemilihan route di-*input* secara manual oleh *administrator* ke dalam *router* ketika jaringan sedang *boot*. Prosedur ini sering disebut *static routing*.

6. Pengertian Virtual Private Network

Menurut (http://computer.howstuffworks.com/VPN.htm 23 Oktober 2012) teknologi virtual private network adalah sebuah private network yang bekerja menggunakan public network atau internet untuk menghubungkan user secara bersama-sama. VPN ini dibuat dengan tujuan dapat menghubungkan antar jaringan computer private secara aman dan dapat diandalkan melalui internet. VPN boleh jadi termasuk ke dalam salah satu kandidat WAN (Sofana, 2012)

VPN memiliki kelebihan dan kekurangan, berikut adalah kelebihan dan kekurangan VPN:

Kelebihan:

1. Biaya relatif murah, karena tidak perlu membuat jalur pribadi hanya memanfaatkan jaringan internet publik.
2. Fleksibilitas, semakin berkembangnya internet dan banyaknya user yang menggunakannya membuat VPN juga berkembang.
3. Mengurangi kerumitan pengaturan dengan teknologi tunneling, tunneling merupakan kunci utama pada VPN. Koneksi pribadi dalam VPN dapat terjadi dimana saja selama terdapat tunnel yang menghubungkan pengirim dan penerima data.

Kekurangan:

1. VPN membutuhkan perhatian yang serius pada keamanan jaringan publik. Oleh karena itu diperlukan tindakan yang tepat untuk mencegah terjadinya hal-hal yang tidak diinginkan.
2. Ketersediaan dan performasi jaringan khusus perusahaan sangat tergantung pada faktor-faktor yang berada di luar kendali pihak perusahaan, karena teknologi VPN ini memanfaatkan media internet.

3. Ada kemungkinan perangkat pembangun teknologi jaringan VPN dari beberapa vendor yang berbeda tidak dapat digunakan secara bersama-sama.

   Jenis-Jenis VPN

   1. Site-to-site VPN : merupakan suatu jaringan yang memungkinkan kantor-kantor yang berada di tempat berbeda dapat saling terhubung dengan aman melalui public network atau internet. Site-to-site VPN ini sangat cocok bagi perusahaan yang memiliki lusinan kantor cabang yang tersebar di seluruh dunia.
   2. Remote-site VPN : mengizinkan user untuk melakukan hubungan yang aman dengan sebuah jaringan komputer. User tersebut dapat melakukan akses ke sumber-sumber data yang aman yang ada pada jaringan tersebut.VPN jenis ini memang cukup baik untuk user individual.

7. Pengertian IPSec

IPSec (Forouzan, 2007, p841) adalah framework terbuka yang merinci aturan untuk komunikasi yang aman. Keamanan yang IPSec mampu sediakan melalui kombinasi dari protokol enkripsi dan mekanisme keamanan. IPSec memungkinkan sistem untuk memilih protokol keamanan yang diperlukan, memilih algoritma enkripsi yang diinginkan untuk digunakan dengan protokol yang dipilih dan menghasilkan kunci enkripsi apapun yang diperlukan untuk menyediaknan layanan yang diminta. IPSec menyediakan layanan enkripsi untuk keamanan transmisi data. IPSec bekerja pada network layer, melindungi, dan mengotentikasi paket IP yang sedang berkomunikasi.

Framework IPSec terdiri dari lima blok:

1. Protokol IPSec, meliputi AH dan ESP.
2. Jenis kerahasiaan yang diimplementasikan menggunakan algoritma enkripsi seperti DES, 3DES, AES. Pilihan penggunaan tergantung pada tingkat keamanan yang dibutuhkan.
3. Integritas yang dapat diimplementasikan baik menggunakan MD5 atau SHA.
4. Bagaimana shared secret key dibentuk. Kedua metode tersebu adalah pre-shared atau digitally signed (tandatangan digital) menggunakan RSA.
5. Merupakan kelompok algoritma Diffie-Hellman (DH). Ada empat algoritma pertukaran kunci yang terpisah yaitu DH kelompok 1 (DH1),

DH kelompok 2 (DH2), DH kelompok 5 (DH5), DH kelompok 7 (DH7). Jenis kelompok yang dipilih tergantung pada kebutuhan tertentu.

IPSec dapat mengamankan jalur antara sepasang gateway, sepasang host, gateway dan host. Dengan menggunakan framework IPSec, IPSec menyediakan fungsi-fungsi keamanan penting sebagai berikut:

1. Confidentiality (kerahasiaan), untuk meyakinkan bahwa sulit untuk orang lain tetapi dapat dimengerti oleh penerima yang sah bahwa data telah dikirimkan. Contoh: Kita tidak ingin tahu seseorang dapat melihat password kerika login ke remote server.
2. Integrity (integritas), untuk menjamin bahwa data tidak berubah dalam perjalanan menuju tujuan.
3. Authenticity (otentikasi), untuk menandai bahwa data yang dikirimkan memang berasal dari pengiriman yang benar.
4. Secure key exchange, IPSec menggunakan algoritma DH untuk menyediakan metode pertukaran kunci public antara dua rekan untuk membentuk sebuah kunci rahasia bersama.

8. Pengertian L2TP

L2TP adalah sebuah tunneling protocol yang memadukan dan mengombinasikan dua buah tunneling protocol yang bersifat proprietary, yait u L2F (Layer 2 Forwarding) milik Cisco Systems dengan PPTP (Point-to-PointTunnelingProtocol) milik Microsoft (Sofana, 2009). Namun, teknologi tunneling ini tidak memiliki mekanisme untuk menyediakan fasilitas enkripsi karena memang benar-benar murni hanya membentuk jaringan tunnel. Selain itu, apa yang lalu-lalang di dalam tunnel ini dapat ditangkap dan dimonitor dengan menggunakan protocolanalizer. L2TP dikembangkan oleh Microsoft dan Cisco. Bisa mengenkapsulasi data dalam IP, ATM, Frame Relay dan X.25.

9. Pengertian Algortima RSA

Algoritma RSA merupakan salah satu algoritma public key yang populer dipakai dan bahkan masih dipakai hingga saat ini. Kekuatan algoritma ini terletak pada proses eksponensial, dan pemfaktoran bilangan menjadi 2 bilangan prima yang hingga kini perlu waktu yang lama untuk melakukan pemfaktorannya. Algoritma ini dinamakan sesuai dengan nama penemunya, Ron Rivest, Adi Shamir dan Adleman(Rivest-Shamir-Adleman) yang

dipublikasikan pada tahun 1977 di MIT, menjawab tantangan yang diberikan algoritma pertukaran kunci Diffie Hellman.

Algoritma RSA mengikuti skema Block Cipher, yaitu sebelum dilakukan enkripsi, plainteks yang ada dibagi ke dalam blok-blok yang sama panjang dimana plainteks dan cipherteksnya berupa integer antara 1 sampai n dengan n biasanya berukuran 2048 bit dan panjang bloknya berukuran tidak lebih dari log (n) + 1 dengan basis 2.

Menurut (Ir. Rinaldi Munir, M.T, 2004), mengungkapkan rumus pembentukan algoritma RSA didasarkan pada persamaan matematika dan didasarkan pada teorema Euler sehingga didapat rumus untuk enkripsi. Fungsi enkripsi dan dekripsi algoritma RSA adalah sebagai berikut.

Fungsi Enkripsi: C = Me mod n

Fungsi Dekripsi: M = Cd mod n

Ket:

C = Cipherteks

M = Message (plainteks)

e = Kunci public

d = kunci private

Penggunaan algoritma RSA harus memenuhi kriteria-kriteria sebagai berikut.

a. Memungkinkan untuk mencari nilai e, d, dan n dimana Med mod n = M untuk semua M < n.
b. Relative mudah untuk menghitung nilai Me mod n dan Cd mod n untuk semua nilai M < n. Tidak memungkinkan mencari nilai d jika diberikan nilai n dan e. Syarat nilai e dan d: gcd(d, e) = 1

Langkah langkah menentukan RSA :

a. Langkah 1 : Pilih 2 bilangan prima secara acak untuk nilai p & q. Dengan syarat nilai p > q sebagai sample, kita akan ambil nilai p = 61, & q = 53
b. Langkah 2 : Hitung N. N adalah p*q, 61 * 53 = 3233
c. Langkah 3 : Hitung φ (baca:phi).

   φ = (p-1)*(q-1)

   φ = (61-1) * (53-1)

   φ = 60 * 52

   φ = 3120
d. Langkah 4 :

Pilih nilai e dengan syarat e > 1, dan GCD(e,3120) = 1 sebagai sample, nilai e yang akan kita ambil adalah 17.

Sebelumnya, sesuai persyaratan, kita tes dulu apakah GCD(17,3120) = 1 ?

3120 mod 17 = 9

17 mod 9 = 8

9 mod 8 = 1

8 mod 1 = 0

Ternyata benar GCD(17,3120) = 1 (1 didapat dari angka yang saya beri warna biru). Berarti kita dapat menggunakan angka 17 sebagai nilai e.

e. Langkah 5 :

Pilih nilai d, dengan syarat (d.e) mod φ = 1

sebagai sample, nilai d yang akan kita ambil adalah 2753.

Sebelumnya sesuai persyaratan kita tes dulu apakah (2753*17) mod 3120 = 1 ?

(2753*17) mod 3120 = 1

= 46801 mod 3120

= 1

Ternyata benar (2753*17) mod 3120 = 1. Berarti persyaratan terpenuhi & 2753 sudah bisa dipastikan dapat mengisi nilai d

Dengan demikian, kita dapat menyimpulkan bahwa :

Private key RSA nya adalah :

n = 3233

d = 2753

Public key RSA nya adalah :

n = 3233

e = 17

B. Tinjauan Studi

Penelitian rujukan merupakan acuan yang dibutuhkan seorang peneliti untuk melakukan penelitian. Penelitian rujukan pada penelitian ini diambil berdasarkan kesamaan metode yang digunakan yaitu Penerapan Algoritma RSA Pada IPSec untuk Router dalam Perluasan Jaringan. Banyak penelitian yang menggunakan metode ini dalam berbagai kasus. Antara lain:

1. **Analisis Performa Site to Site IP Security Virtual Private Network (VPN) Menggunakan Algoritma Enkripsi ISAKMP** (Firmansyah, Mochamad Wahyudi, Rachmat Adi Purnama, STMIK Nusa Mandiri Jakarta, 2019)

   Pada penelitian tersebut permasalahana yang dibahas adalah bahwa penggunaan penggunaan Site to Site VPN mampu meminimalisir

penggunaan bandwith pada jaringan internet. Pengimplementasian IPSec dan enkripsi ISAKMP mampu menjaga keaslian terhadap paket data saat terjadi transfer paket data. Selain itu, pengimlementasian *tunnel* VPN mampu meminimalisir terjadinya kebocoran paket data dan Site to Site VPN mampu meringkas hops yang dilalui didalam jaringan internet dengan menggunakan TTL 126.

Perbandingan dengan penelitian yang sedang disusun adalah pengimplementasian IPSec dan enkripsi dengan metode algoritma RSA.

2. **Analisis Dan Implementasi Ipsec (Ip Security) Dalam Proses Pengamanan Layer Dua Tunneling Protokol** (Septian Prima Putra, Fazmah Arief Yulianto, Tri Brotoharsono, Universitas Telkom, 2011)

   Pada penelitian tersebut permasalahan yang dibahas adalah analisis dan performa jaringan menggunakan L2TP IPsec. Penggunaan L2TP dan L2TP/IPsec dalam hubungan nilai performansi jaringan didapat bahwa dengan menggunakan L2TP nilai troughput merupakan nilai yang baik daripada L2TP/IPsec.

   Perbandingan dengan penelitian yang sedang disusun adalah perluasan jaringan dengan implementasi L2TP/IPSec.

3. **Analisis VPN IPSec Dalam Segi Keamanan dan Efisiensi Bisnis Pada Perusahaan PT XYZ** (Dede Fadhilah, Iwan Krisnadi, Universitas Mercubuana, 2017)

   Pada penelitian tersebut permasalahan yang dibahas adalah VPN IPsec dapat melindungi data perusahaan dan meningkatkan efisiensi perusahaan. perusahaan yang mempunyai kantor pusat dan kantor cabang yang secara geografis letaknya berjauhan dapat terhubung dengan adanya teknologi VPN IPSec, dan menghasilkan jalur lintas komunikasi proses pertukaran data yang aman dan terpercaya (secure and reliable). Dengan adanya jalur VPN IPSec, perusahaan dapat menghemat biaya pengeluaran antara kantor cabang dengan kantor pusat dan dapat terhubung secara real time.

   Perbandingan dengan penelitian yang sedang disusun adalah menerapkan metode RSA sehingga manajemen jaringa jauh lebih aman.

4. **Rancang Bangun Keamanan Data Jaringan Komputer Dengan Menggunakan Metode Ipsec VPN** (Harun Sujadi, Amiq Burhanuddin, Universitas Majalengka, 2017).

Pada penelitian tersebut permasalahan yang dibahas adalah perusahaan tersebut memiliki masalah dalam pengiriman data keperusahaan cabang didaerah lain. Selain itu perusahaan tersebut juga menggunakan jaringan ke internet yang mempunyai kelemahan pada keamanan IP public. Alat yang digunakan yaitu menggunakan GNS3 dan menggunakan protokol IPSec. Dengan adanya IPSec VPN proses pengiriman data mengirim data dengan nyaman tanpa adanya ganguan dari pihak ketiga karena data yang telah dikirim sudah terenkripsi dengan baik.

Perbandingan dengan penelitian yang sedang disusun adalah pada penelitian ini menggunakan algoritma RSA untuk keamanan dan perluasan jaringan.

5. **Analisis Perancangan Dan Implementasi Ipsecurity (Ipsec) Sebagai Protokol Keamananuntuk Virtual Private Network (Vpn) Pada Klien PT. XYZ** (M. BAGUS OKA G.W, UNIVERSITAS BAKRIE, 2016)

   Pada penelitian tersebut permasalahan yang dibahas adalah Keamanan jaringan merupakan faktor penting dalam suatu organisasi yang menggunakan teknologi informasi dalam kegiatannya. IPSec berjalan di atas VPN dan berfungsi untuk mengenkripsi setiap paket. Data yang keluar dan masuk dalam suatu jaringan. Penelitian ini bertujuan untuk menganalisis perancangan dan implementasi IPSec sebagai protokol keamanan jaringan klien PT. XYZ.

   Perbandingan dengan penelitian yang sedang disusun adalah menerapkan perluasan jaringan dengan otentikasi terlebih dahulu menggunakan algoritma RSA.

6. **Penerapan Metode Ipsec Untuk Optimalisasi Koneksi Jaringan di PT. OTO MULTIARTHA** (Prionggo Hendradi, Braja Santosa, Fakultas Teknik, Teknik Informatika, Universitas Satya Negara Indonesia, 2017)

   Pada penelitian tersebut permasalahan yang dibahas adalah jaringan public yang digunakan oleh PT. OTO Multiartha dalam transaksi data dan informasi antara head office dan cabang, akan menjamin tingkat keamanan baik disisi pengirim maupun penerima informasi. Dengan menggunakan metode IPSec komunikasi jaringan private yang melewati jaringan internet public akan lebih aman dibandingkan hanya menggunakan davice firewall.

Perbandingan dengan penelitian yang sedang disusun adalah dengan menggunakan algoritma RSA otorisasi lebih terjamin aman, sehingga tidak langsung mengakses pada ip publik.

7. **Analisis Dan Optimalisasi Keamanan Jaringan Menggunakan Protokol IPSec** (Syarif Hidayatulloh,Universitas BSI, 2014)

   Pada penelitian tersebut permasalahan yang dibahas adalah keamanan akses jaringan data dengan menggunakan IP Publik dapat terenkripsi dengan baik. Keamanan pada jaringan komputer akan meningkat karena IPSec melakukan enkripsi terhadap data yang dikirim pada jaringan tersebut. Seandainya terjadi penyadapan data oleh pihak ketiga, maka data asli tidak dapat dilihat dengan mudah tanpa mengetahui kunci enkripsi yang digunakan.

   Perbandingan dengan penelitian yang sedang disusun adalah menerapkan metode RSA sehingga manajemen jaringan jauh lebih aman dengan adanya autentikasi.

8. **Metode Internet Protocol Security (IPSec) Dengan Virtual Private Network (VPN) Untuk Komunikasi Data** (Maryanto, Maisyaroh , Budi Santoso, STMIK Nusa Mandiri Jakarta, 2018)

   Pada penelitian tersebut permasalahan yang dibahas adalah membangun dan merancang jaringan komputer dengan tujuan keamanan, kehandalan, kecepatan, dan kehandalan teknologi yang digunakan. Dengan menggunakan jaringan VPN IPSec dapat menjadi solusi jaringan yang aman dan terintegrasi dengan baik karena data berjalan pada jaringan publik. Dengan keamanan jaringan dengan menggunakan sistem keamanan jaringan *firewall*, *Intrusion Prevention System (IPS)*, *McAfee Mail gateway* dan antivirus *McAfee Complete EndPoint Protection* akan sangat membantu dalam menangani gangguan keamanan jaringan pada Jaringan VPN.

   Perbandingan dengan penelitian yang sedang disusun adalah menerapkan metode RSA untuk autentikasi dan keamanan.

9. **Implementasi Virtual Private Network Openstack Terkoneksi Dengan Virtual Private Network Mikrotik Untuk Komunikasi Data Lebih Aman** (Cholifah Sulistin Angraeni, Hary Nugroho, Ega Dian Pramesta, Akademi Teknik Telekomunikasi Sandhy Putra Jakarta, 2017)

Pada penelitian tersebut permasalahan yang dibahas adalah VPN dapat terjadi antara dua PC atau lebih dengan menggunakan jaringan yang berbeda.

Sistem operasi perangkat lunak yang dapat digunakan untuk menjadikan PC sebagai router network yaitu MikroTik yang memiliki keamanan jaringan IPSec (Internet Protocol Security). Hasil yang di dapat dari penelitian ini yaitu nilai Bandwidth yang dihasilkan pada saat melakukan

Upload File memiliki hasil 0,267 Mbit/sec dan untuk hasil Download File bernilai 0,162 Mbit/sec. Sedangkan untuk hasil Packet Loss pada saat melakukan Upload File memiliki hasil yang bagus yaitu 0%, dan untuk nilai yang didapat pada saat mendownload yaitu 0%. Menurut standar TIPHON dan ITU-T nilai-nilai Packet Loss yang didapat memenuhi standar kategori degredasi, nilai yang sangat bagus adalah 0%, untuk kategori bagus memiliki nilai 3%, pada katagori sedang memiliki nilai 15%, dan untuk kategori jelek memilki nilai 25%.

Perbandingan dengan penelitian yang sedang disusun adalah menerapkan metode RSA untuk perluasan jaringan, bukan untuk menguji kecepatan jaringan dari VPN IPSec.

10. **Implementasi Remote Desktop Melalui VPN Berbasis IPSec pada Smartphone dengan Menggunakan Vyatta OS** (Kiki Agnia Maryam Larasati, Eddy Prasetyo Nugroho, Universitas Telkom, 2016)

    Pada penelitian tersebut permasalahan yang dibahas adalah remote user VPN dengan Vyatta OS dan pengamanan data saat proses tranmisi. Teknologi VPN berbasis IPSec yang dibangun berhasil menyediakan layanan akses data, resource monitoring dan trafik, dan remote desktop yang aman. Protokol keamanan IPSec berfungsi dengan baik dalam mengenkripsi data yang dikirim,sehingga sniffer tidak dapat membaca trafik protokol-protokol yang berjalan antara client dan web server maupun pada saat proses remote desktop.

    Perbandingan dengan penelitian yang sedang disusun adalah menerapkan metode RSA dan IPSec menggunakan mikrotik OS.

Tabel 2. 2 Tabel Tinjauan Pustaka

NO.	PENYUSUN	JUDUL	JURNAL SUMBER	KONTRIBUSI / KELEMAHAN
1	Firmansyah, Mochamad Wahyudi, Rachmat Adi Purnama, STMIK Nusa Mandiri (2019)	Analisis Performa Site to Site IP Security Virtual Private Network (VPN) Menggunakan Algoritma Enkripsi ISAKMP	JUITA: Jurnal Informatika e-ISSN: 2579-9801; Volume 7, Nomor 2, November 2019 https://doi.org/10.30595/juita.v7i2.4491	Pengimlementasian *tunnel* VPN mampu meminimalisir terjadinya kebocoran paket data dan Site to Site VPN mampu meringkas hops yang dilalui didalam jaringan internet dengan menggunakan TTL 126. Kontribusi : Pengimplementasian IPSec dan enkripsi dengan metode algoritma RSA
2	Septian Prima Putra, Fazmah Arief Yulianto, Tri Brotoharsono Universitas Telkom (2011)	Analisis Dan Implementasi Ipsec (Ip Security) Dalam Proses Pengamanan Layer Dua Tunneling Protokol	Jurnal Karya Ilmiah Klasifikasi No. 004 Tahun 2011 https://openlibrary.telkomuniversity.ac.id/pustaka/94815/analisis-dan-implementasi-ipsec-ip-security-dalam-proses-pengamanan-layer-dua-tunneling-protokol.html	Penggunaan L2TP dan L2TP/IPsec dalam hubungan nilai performansi jaringan didapat bahwa dengan menggunakan L2TP nilai troughput merupakan nilai yang baik

				daripada L2TP/IPsec Kontribusi : Perluasan jaringan dengan implementasi L2TP/IPSec.
3	Dede Fadhilah, Iwan Krisnadi	Analisis VPN IPSec Dalam Segi Keamanan dan Efisiensi Bisnis Pada Perusahaan PT XYZ	Jurnal Karya Ilmiah Tahun 2017 https://d1wqtxts1xzle7.cloudfront.net/58152201/Analisis_VPN_IPSec_Dalam_Segi_Keamanan_dan_Efisiensi_Bisnis_Pada_Perusahaan_PT_XYZ-libre.pdf?1547087027=&response-content-disposition=attachment%253B+filename%253DAnalisis_VPN_IPSec_Dalam_Segi_Keamanan_d.pdf	Dengan adanya jalur VPN IPSec, perusahaan dapat menghemat biaya pengeluaran antara kantor cabang dengan kantor pusat dan dapat terhubung secara real time Kontribusi : Menerapkan metode RSA sehingga manajemen jaringa jauh lebih aman.
4	Harun Sujadi, Amiq Burhanuddin, Universitas Majalengka (2017)	Rancang Bangun Keamanan Data Jaringan Komputer Dengan Menggunakan Metode Ipsec VPN	INFOTECH journal ISSN : 2460-1861 Tahun 2017 http://jurnal.unma.ac.id/index.php/infotech/article/download/691/639	Dengan adanya IPSec VPN proses pengiriman data mengirim data dengan nyaman tanpa adanya ganguan dari pihak ketiga karena data yang telah

				dikirim sudah terenkripsi dengan baik Kontribusi : Menggunakan algoritma RSA untuk keamanan dan perluasan jaringan.
5	M. BAGUS OKA G.W, UNIVERSITAS BAKRIE (2016)	Analisis Perancangan Dan Implementasi Ipsecurity (Ipsec) Sebagai Protokol Keamananuntuk Virtual Private Network (Vpn) Pada Klien PT. XYZ	Jurnal Tugas Akhir Tahun 2016 http://repository.bakrie.ac.id/446/1/00.%20Cover.pdf	Data yang keluar dan masuk dalam suatu jaringan. Penelitian ini bertujuan untuk menganalisis perancangan dan implementasi IPSec sebagai protokol keamanan jaringan klien PT. XYZ Kontribusi : Menerapkan perluasan jaringan dengan otentikasi terlebih dahulu menggunakan algoritma RSA.
6	Prionggo Hendradi, Braja Santosa, Fakultas	Penerapan Metode Ipsec Untuk Optimalisasi Koneksi	Jurnal Satya Informatika, Volume: 1, Nomor: 1, halaman 34-45 Tahun 2017	Dengan menggunakan metode IPSec komunikasi jaringan private

	Teknik, Teknik Informatika, Universitas Satya Negara Indonesia, (2017)	Jaringan di PT. OTO MULTIARTHA	https://lppm.usni.ac.id/jurnal/Prionggo-Hendradi,-Braja-Santosa.pdf	yang melewati jaringan internet public akan lebih aman dibandingkan hanya menggunakan davice firewall Kontribusi : Menggunakan algoritma RSA otorisasi lebih terjamin aman, sehingga tidak langsung mengakses pada ip publik.
7	Syarif Hidayatulloh, Universitas BSI, (2014)	Analisis Dan Optimalisasi Keamanan Jaringan Menggunakan Protokol IPSec	Jurnal Informatika. Vol. I No. 2 September 2014 https://doi.org/10.31311/ji.v1i2.47	Keamanan pada jaringan komputer akan meningkat karena IPSec melakukan enkripsi terhadap data yang dikirim pada jaringan tersebut. Seandainya terjadi penyadapan data oleh pihak ketiga, maka data asli tidak dapat dilihat dengan mudah tanpa

				mengetahui kunci enkripsi yang digunakan Kontribusi : Menerapkan metode RSA sehingga manajemen jaringan jauh lebih aman dengan adanya autentikasi.
8	Maryanto, Maisyaroh , Budi Santoso, STMIK Nusa Mandiri Jakarta, (2018)	Metode Internet Protocol Security (IPSec) Dengan Virtual Private Network (VPN) Untuk Komunikasi Data	Jurnal Penelitian Ilmu Komputer, System Embedded & Logic p-ISSN: 2303-3304,e-ISSN: 2620-35536 (2): 179 –188(September 2018) https://doi.org/10.33558/piksel.v6i2.1508	Dengan keamanan jaringan dengan menggunakan sistem keamanan jaringan *firewall*, *Intrusion Prevention System (IPS)*, *McAfee Mail gateway* dan antivirus *McAfee Complete EndPoint Protection* akan sangat membantu dalam menangani gangguan keamanan jaringan pada Jaringan VPN Kontribusi :

				Menerapkan metode RSA untuk autentikasi dan keamanan.
9	Cholifah Sulistin Angraeni, Hary Nugroho, Ega Dian Pramesta, Akademi Teknik Telekomunikasi Sandhy Putra Jakarta, (2017)	Implementasi Virtual Private Network Openstack Terkoneksi Dengan Virtual Private Network Mikrotik Untuk Komunikasi Data Lebih Aman	Jurnal ICT Akademi Telkom Jakarta, Vol.8 No.15, November 2017 http://ejournal.akademitelkom.ac.id/index.php/ictjurnal/article/download/122/100	Upload File memiliki hasil 0,267 Mbit/sec dan untuk hasil Download File bernilai 0,162 Mbit/sec. Sedangkan untuk hasil Packet Loss pada saat melakukan Upload File memiliki hasil yang bagus yaitu 0%, dan untuk nilai yang didapat pada saat mendownload yaitu 0%. Menurut standar TIPHON dan ITU-T nilai-nilai Packet Loss yang didapat memenuhi standar kategori degredasi, nilai yang sangat bagus adalah 0%, untuk

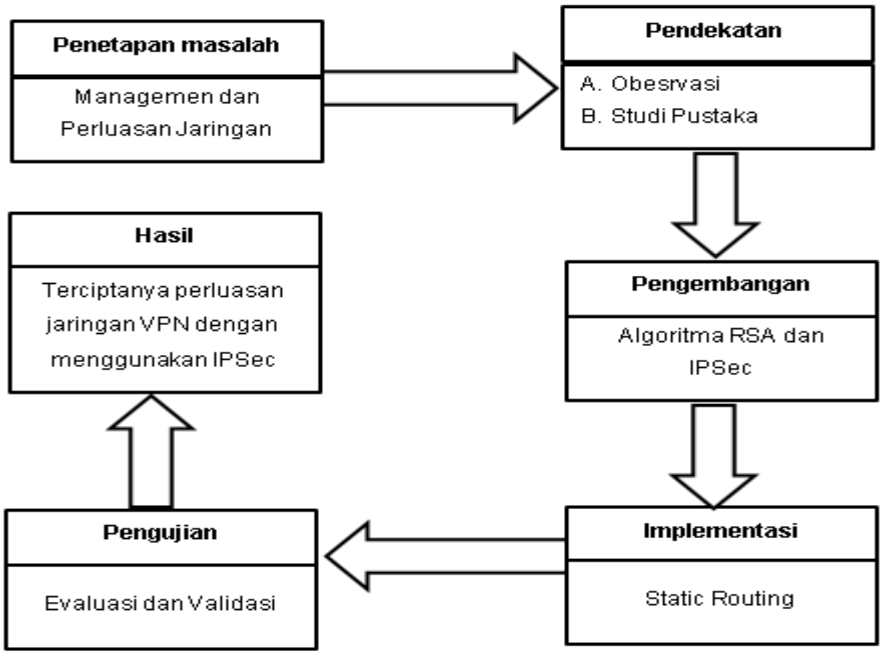
				kategori bagus memiliki nilai 3%, pada katagori sedang memiliki nilai 15%, dan untuk kategori jelek memilki nilai 25%. Perbedaan : Metode RSA untuk perluasan jaringan, bukan untuk menguji kecepatan jaringan dari VPN IPSec.
10	Kiki Agnia Maryam Larasati, Eddy Prasetyo Nugroho, Universitas Telkom, (2016)	Implementasi Remote Desktop Melalui VPN Berbasis IPSec pada Smartphone dengan Menggunakan Vyatta OS	Jurnal Teknik Informasi Vol 2 No 2 Tahun 2016 https://journals.telkomuniversity.ac.id/jti/article/view/502/377	Protokol keamanan IPSec berfungsi dengan baik dalam mengenkripsi data yang dikirim,sehingga sniffer tidak dapat membaca trafik protokol-protokol yang berjalan antara client dan web server maupun pada saat proses remote desktop Perbedaan dengan

				penelitian yang sedang disusun adalah menerapkan metode RSA dan IPSec menggunakan mikrotik OS.

C. Kerangka Pemikiran

Penjelasan tentang kerangka pemikiran pada penelitian ini adalah;

1. Penetapan masalah untuk menetapkan tujuan masalah
   Memanajemen perluasan jaringan dengan menggunakan algoritma RSA dan L2TP/IPSec.
2. Melakukan pendekatan dan mengetahui kebutuhan jaringan pada perusahaan
   Dengan mengadakan observasi dan mengetahui topologi jaringan yang sedang diterapkan dan mencari kelemahannya
3. Melakukan pengembangan IPSec pada VPN untuk perluasan jaringan intranet perusahaan. Pengembangan yang dilakukan dengan wilayah dan yang berbeda beda tergantung kepada perluasan area store yang ditentukan perusahaan.
4. Melakukan implementasi melalui tahap perancangan, tahap implementasi dan *static routing*
5. Pengujian yang dilakukan agar kebutuhan jaringan pada perusahan dapat termanagemen dengan tepat, dengan melakukan evaluasi dan validasi.
6. Melakukan evaluasi terhadap jaringan VPN. Evaluasi dilakukan apabila teridentifikasi kekurangan dalam prakteknya dan mencari solusi agar kekurangan tersebut dapat teratasi.



Gambar 2. 1 Kerangka Pemikiran

Berikut adalah gambar kerangka pemikiran untuk pemecahan masalah dalam penelitian ini yang digambarkan pada Gambar 2.1.