JUTIS (Jurnal Teknik Informatika Unis)
Vol. 12 No. 1 Bulan April 2024 **p-ISSN: 2252-5351**
Program Studi Teknik Informatika – Fakultas Teknik **e-ISSN: 2656-0860**
Universitas Islam Syekh-Yusuf Tangerang

Perancangan Jaringan Vpn Dan Keamanan Data Menggunakan Tunelling Pada Laboratorium Komputer UIN Sunan Kalijaga Yogyakarta

Nurdi Afrianto[1], Dori Gusti Alex Candra[2*], Budi Permana Putra[3], Irzon Meiditra[4], Idir Fitriyanto[5], Bambang Sugiantoro[6]
[1,2,3,4,5] Fakultas Ilmu Komputer dan Teknik, Institut Teknologi Mitra Gama, Duri
[6] Program Studi Magister Informatika, Fakultas Sains dan Teknologi, UIN Sunan Kalijaga, Yogyakarta

nurdiafrianto1995@gmail.com[1] ,dorigustialexcandra@gmail.com [2*],
budipermanaputra96@gmail.com[3], meiditrairzon@gmail.com[4], idirfitriyanto45@gmail.com[5],
bambang.sugiantoro@uin-suka.ac.id[6]

Abstrak
Metode utama untuk mengamankan dan mengenkripsi transmisi data melalui jaringan internet adalah dengan meggunakan virtual private network (VPN) atau jaringan pribadi virtual. Saat ini Laboratorium UIN Sunan Kalijaga belum terkoneksi antara komputer server dan klien hal ini menyebabkan sulitnya transfer data atau sharing data dan juga dalam transfer data ini user masih menggunakan media internet seperti email karena banyak data-data penting yang terdapat didalamnya yang sangat rentan jika email itu sendiri diretas oleh pihak yang tidak bertanggung jawab, sehingga kampus belum dapat memastikan keamanan data yang dikirim. Karena permasalahan tersebut, maka dilakukan perancangan VPN yang merupakan sarana untuk berkomunikasi dan mentransfer data dengan aman dan menjaga keabsahan data. Penelitian yang dilakukan dilaboratorium UIN Sunan Kalija Yogyakarta ini bertujuan untuk membangun atau merancang sebuah sistem jaringan pribadi virtual (VPN), yang dimana sistem ini berguna untuk memberikan keamanan pada data yang di transferkan dari komputer server ke komputer klien atau sebaiknya melalui jaringan publik. Menggunakan dua router Mikrotik, VPN diimplementasikan menggunakan protokol tunneling point to point (PPTP). Hanya sedikit penyesuaian yang dilakukan pada konfigurasi jaringan komputer untuk mengurangi biaya dan waktu implementasi. Pengujian yang dilakukan untuk menerapkan keamanan data pada jaringan VPN dengan menggunakan software wireshark yang dimana pada software ini dapat di gunakan untuk memantau jalannya aktivitas pada saat data ditransferkan atau diambil. Temuan penelitian menunjukkan bahwa ada koneksi VPN antara klien dan server komputer laboratorium. Selain itu, koneksi terus menerus antara Either-1 dan Either-2 melalui jaringan VPN yang sedang digunakan sangat berbahaya untuk menjaga keamanan.

Kata kunci: *Jaringan pribadi virtual, VPN, Mikrotik, PPTP*

A. Pendahuluan

Data apa pun perlu ditangani dengan presisi, kecepatan, dan akurasi untuk menginformasikan upaya kegiatan manusia sehari-hari (Diana et al., 2021). Pesatnya kemajuan teknologi dan inovasi berbasis pengetahuan telah berdampak signifikan terhadap kehidupan manusia di berbagai bidang kehidupan, termasuk pengelolaan data informasi dalam konteks jaringan komputer (Wardana et al., 2022). Tidak dapat dipungkiri

bahwa keberadaan komputer telah memberikan dampak yang begitu signifikan pada zaman kita. Pekerjaan dilakukan secara manual sebelum komputer ditemukan, membutuhkan waktu lama untuk diselesaikan dan tidak selalu memastikan keakuratan data. Namun, tantangan tersebut sekarang dapat diatasi berkat komputer, karena mereka menawarkan begitu banyak keuntungan yang mendorong pengguna beralih dari proses manual ke komputerisasi. Ada beberapa dampak positif dari komputerisasi, terutama dalam hal efisiensi dan efektivitas pengguna (Nur et al., 2021).

Melalui penggunaan teknologi internet dan VPN (Virtual Private Network), manusia dapat mengakses jaringan lokal dari luar dengan mudah dan cepat (Dewi et al., 2020). Dengan menggunakan VPN, pengguna dapat mengakses subsistem lokal daya jaringan seperti server data dan menerima hak dan kewajiban yang sama seolah-olah mereka hadir secara fisik di lokasi tempat sumber daya jaringan lokal berada (Budimulya et al., 2022). Tujuan utama VPN adalah untuk melindungi informasi sensitif dari akses tidak sah saat dikirim melalui Internet. Akibatnya, setiap VPN selalu menyertakan dua fungsi paling mendasar: enkripsi dan tunneling (Sari et al., 2020). Sebagai hasil dari tersedianya beberapa opsi tunneling, termasuk Point to Point Tunneling Protocol, menggunakan jaringan publik dengan standar dan ketentuan yang sama seperti menggunakan jaringan pribadi adalah keuntungan tunggal menggunakan VPN PPTP (Ramdhani & Yusuf, 2022).

Protokol tunneling point-to-point (PPTP) akan digunakan untuk mengimplementasikan jaringan VPN. Untuk meningkatkan keamanan data komunikasi sensitif, jaringan pribadi virtual (VPN), protokol tunneling point-to-point (PPTP), dan router VPN sering digunakan (Andriani et al., 2022). Awalnya, VPN hanyalah jaringan komunikasi virtual aman yang dilakukan secara pribadi. VPN ini dapat digunakan sebagai sarana komunikasi data pribadi yang aman melalui jaringan internet publik (Febrianti et al., 2021).

Tujuan dari teknologi tunneling adalah untuk mengembangkan dan menyediakan koneksi point-to-point dari sumber ke tujuan (Christo & Mulyono, 2022). Teknik ini dikenal sebagai tunneling karena koneksi point-to-point biasanya dibuat dengan memotong jaringan publik yang terbuka, tetapi mereka tidak cukup menangani paket data milik orang lain yang juga menggunakan jaringan publik untuk memotong jaringan terbuka, karena koneksi hanya berfungsi untuk mentransfer data dari satu sumber ke sumber lainnya. Meskipun koneksi titik-ke-titik ini tampaknya tidak ada, tampaknya data yang dikirim melaluinya sebenarnya dikirim melalui koneksi titik-ke-titik yang aman (Putra et al., 2018).

Berdasarkarkan penelitian yang telah dilakukan oleh (Syarif & Sobari, 2022) dengan judul "Implementasi Virtual Private Network (VPN) menggunakan Metode PPTP pada PT. Sinar Quality Internusa" bahwa jaringan lokal dari PT.Sinar Quality Internusa dan PT. Hoco Asian Industri telah berhasil terhubung satu sama lain atau sebalik nya dengan baik dengan menggunakan VPN metode PPTP, dan dapat bertukar informasi mengirim atau menerima data satu sama lain secara langsung, Lalu dengan sudah terhubung nya jaringan antar kedua site, dan melakukan konfigurasi sharing folder, user dari kedua site sudah bisa saling bertukar data tanpa lagi menggunakan layanan chat.

Adapun penelitian yang telah dilakukan oleh (Andriani et al., 2022) dengan judul "Implementasi VPN Menggunakan Metode Point to Point Tunneling Protocol" dengan adanya penerapan VPN dengan metode PPTP, memudahkan karyawan Kantor XYZ yang sedang bekerja dari rumah atau work from home dapat saling berkomunikasi, sehingga pekerjaan dan pertukaran informasi akan menjadi semakin fleksibel dan semakin cepat. Serta pengujian keamanan terhadap jaringan di kantor XYZ sebelum menggunakan VPN Server membuktikan bahwa penyadap masih bisa memperoleh data berupa informasi login website, login mikrotik, maupun melihat isi data ketika melakukan pertukaran data. Sedangkan ketika user mengkoneksikan VPN Server penyadap tidak dapat melihat isi data yang terdapat di dalamnya.

Penelitian selanjutnya dilakukan oleh S. Dewi (2020), Penelitian ini bertujuan agar pertukaran data dari kantor kabupaten ke kantor desa dapat dilakukan secara aman dan terkendali, kemudian disebutkan bahwa metode tunneling protocol PPTP *(Point to Point Tunneling Protocol)* yang diterapkan pada Kantor Desa Kertaharja berdampak sangat positif karena dengan adanya penerapan metode tunneling tersebut jaringan komputer antara kantor dapat saling terhubung dan berkomunikasi, dengan itu pekerjaan dan pertukaran informasi akan menjadi semakin fleksibel dan semakin cepat, dan juga administrator jaringan tidak perlu repot-repot melakukan kunjungan untuk memonitoring jaringan yang sedang berjalan pada masing-masing kantor (Dewi et al., 2020).

Adapun perbedaan penelitian yang akan dilakukan terletak pada objek yang akan diteliti yaitu Laboratorium UIN Sunan Kalijaga dengan mengembangkan kembali peracangan jaringan VPN menggunakan metede PPTP dengan Permasalahan yang ada pada Laboratorium UIN Sunan Kalijaga yaitu belum terkoneksi antara komputer server dan komputer klien hal ini menyebabkan sulitnya transfer data atau sharing data dan juga dalam transfer data ini user masih menggunakan media internet seperti email karena banyak data-data penting yang terdapat didalamnya yang sangat rentan jika email itu sendiri diretas oleh pihak yang tidak bertanggung jawab

Masalah-masalah ini mendorong penulis untuk mengembangkan solusi dengan mempertimbangkan aspek ekonomi dan keamanan data jaringan, serta kemajuan teknologi yang cepat dalam hal fitur, fungsi, dan implementasi yang memungkinkan untuk terhubung dan berkomunikasi dengan perangkat lain, dengan platform yang berbeda (Ekawati & Irwan, 2021). Untuk menerapkan pengamanan pada data komputer dengan menggunakan ekstensi atau format enkripsi tertentu agar data tidak mudah dicuri atau disadap oleh orang yang tidak bertanggung jawab, maka Virtual Private Network (VPN) dengan metode tunneling dapat membuat koneksi pada jaringan publik (internet) dengan hak dan pengaturan yang mirip dengan jaringan lokal (Supriyanto & Suharyanto, 2019).

Dengan menggunakan VPN, dimungkinkan untuk membuat jaringan area lokal di luar jaringan terhubung ke jaringan lokal tertentu secara virtual sedangkan jaringan area lokal di bagian dalam jaringan terhubung secara fisik. Hanya pengguna VPN yang dapat mengakses data karena penggunaan protokol PPTP meningkatkan keamanan data. Dengan bantuan VPN, perangkat apa pun di luar jaringan lokal dapat terhubung secara

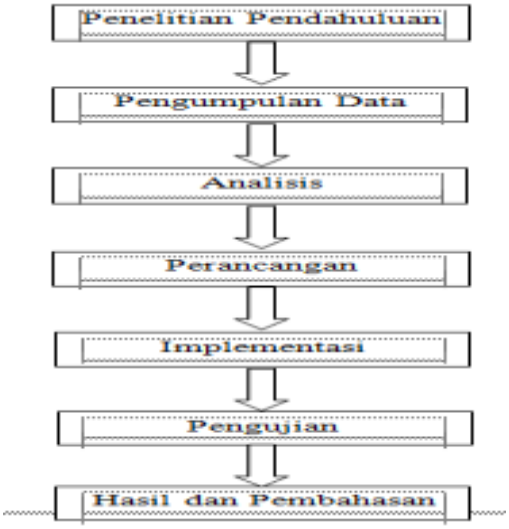
p-ISSN: 2252-5351
e-ISSN: 2656-0860

fisik ke perangkat apa pun di dalam jaringan lokal. Menggunakan protokol PPTP semakin meningkatkan keamanan data, membatasi akses ke data yang relevan hanya untuk pengguna VPN (Phang & Setyaningsih, 2021).

.

B. Metode

Metode yang digunakan dalam penelitian ini adalah penelitian dan pengembangan atau study and development. Menurut Borg dan Gall (1983: 772), proses mengembangkan dan memvalidasi barang atau produk pendidikan dikenal sebagai penelitian dan pengembangan alur kehidupan sistem informasi. Penulis akan melakukan penelitian berdasarkan hukum dan bahasa yang akan ditemui saat melakukan kajian untuk penerapan jaringan VPN dan keamanan data dengan metode tunneling di lab komputer Universitas Islam Sunan Kalijaga Yogyakarta (Pamungkas et al., 2021). Tahapan tersebut dibuat secara sistematis sehingga dapat digunakan untuk menghasilkan dokumentasi yang mudah dipahami dan mudah digunakan untuk mengatasi setiap potensi masalah. Untuk lebih jelasnya dapat dilihat pada Gambar 1.



Gambar 1. Kerangka Penelitian

Tahapan penelitian ini menjabarkan prosedur pengumpulan data dan menyusun sejumlah laporan yang diperlukan sebagai rekomendasi penelitian ini (Wicaksana et al., 2021):

1. **Penelitian Pendahuluan**
   Tujuan dari pendahuluan penelitian adalah untuk menata kembali alur penelitian yang semula. Pendahuluan penelitian dilakukan karena topik dan metode penelitian lainnya masih belum jelas bagi peneliti. Fokus studi dalam proposal dapat bervariasi sebagai hasil dari penelitian sebelumnya. Beberapa instrumen yang digunakan dalam studi utama dapat diuji dalam studi percontohan.
2. **Pengumpulan Data**
   Saat ini dilakukan pendataan dengan mencari informasi tambahan yang akan digunakan untuk mengatasi permasalahan proses internal laboratorium UIN Sunan Kalijaga Yogyakarta. Wawancara, observasi, tinjauan pustaka, dan analisis

laboratorium adalah metode yang digunakan dalam proses pengumpulan data untuk mendapatkan informasi tentang keamanan jaringan.

3. **Analisis**
   Analisis data adalah metode untuk melakukan analisis terhadap data yang diperlukan untuk pengembangan perancangan sistem yang akan datang. Dalam hal ini peneliti mengumpulkan data dari Laboratorium UIN Sunan Kalijaga Yogyakarta, dimana informasi tersebut perlu diverifikasi lebih teliti karena diperoleh melalui hasil wawancara. Belakangan, informasi yang ditemukan itu disampaikan ke Laboratorium UIN Sunan Kalijaga Yogyakarta.
4. **Perancangan**
   Perancangan merupakan tahap dimana segala kebutuhan sudah diketahui kemudian dilakukan perancangan atau desain sistem sesuai kebutuhan dari permasalahan yang ada pada penelitian untuk memeberikan solusi. Adapun membuat desain atau perancangan topologi yang kedepannya digunakan oleh laboratorium UIN Sunan Kalijaga dalam penelitian ini menggunakan Cisco.
5. **Implementasi**
   Implementasi merupakan tahap untuk mengetahui bagaimana aplikasi yang akan digunakan memberikan manfaat dan apakah sesuai dengan yang telah diharapkan sebelumnya.
6. **Pengujian**
   Pengujian sistem merupakan salah satu tahapan dalam pengujian yang digunakan untuk mengidentifikasi kelemahan sistem. Satu-satunya faktor terpenting dalam pengembangan VPN adalah biayanya yang relatif rendah, portabel, dan menjadi semakin populer di kalangan pengguna sebagai hasil dari peningkatan penggunaannya di internet. Adapaun pengujian dilakukan dengan menggunakan Wireshark adalah salah satu dari sekian banyak tool Network Analyzer yang banyak digunakan oleh Network Administrator untuk menganalisa kinerja jaringannya dan mengontrol lalu lintas data di jaringan yang Anda kelola. Wireshark menggunakan interface yang menggunakan Graphical User Interface (GUI).
7. **Hasil dan Pembahasan**
   Hasil dan pembahasan merupakan tahap akhir dalam penelitian dengan menyajikan data dalam bentuk laporan berdasar tahapan-tahapn yang sudah dilakukan dalam sebuah penelitian sehingga dapat menjadi acuan bagi peneliti selanjutnya.

C. Hasil dan Pembahasan

1. Analisa Kebutuhan

Saat ini sedang dilakukan kajian teknis terhadap permasalahan yang ada di laboratorium UIN Sunan Kalijaga. Analisis dilakukan dengan metode wawancara dengan bantuan staf laboratorium dan staf pendukung teknis. Selain itu, analisis dilakukan dengan menginventarisasi kondisi komputer laboratorium, baik dari segi desain dan konfigurasinya maupun perangkat kerasnya, untuk memastikan bahwa solusi yang ditawarkan tidak akan menghasilkan perubahan yang signifikan. kondisi tersebut. Ini

diperlukan karena, semakin banyak pekerjaan yang dilakukan, semakin banyak uang yang harus dibayarkan dalam proyek latihan saat ini.

Untuk menyelesaikan tugas ini, diperlukan sejumlah alat atau peralatan, termasuk perangkat keras dan perangkat lunak komputer. Tabel 1 berisi daftar alat yang diperlukan untuk tugas ini.

Tabel 1.
Peralatan Penelitian

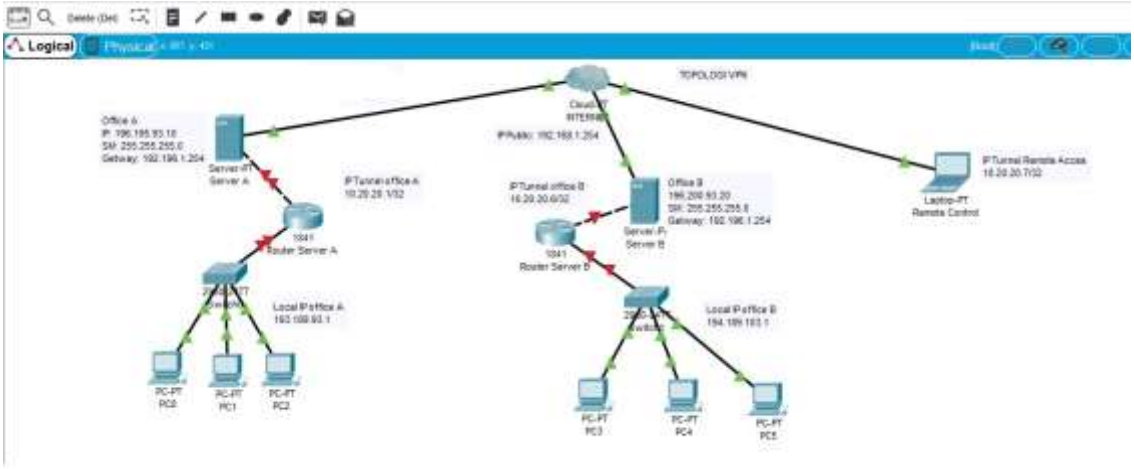
No	Nama	Jumlah	Keterangan
1	Laptop	1	Untuk melakukan Konfigurasi
2	PC	2	Untuk alat menjadi Server dan Client
3	Router Mikrotik RB 450G	1	Untuk aktivitas konfigurasi jaringan VPN server
4	Router Mikrotik RB 750	1	Untuk melakukan konfigurasi jaringan VPN client
5	Winbox	1	Untuk melakukan konfigurasi miktorik
6	Cisco	1	Untuk merancang dan mendesain topologi
7	Wireshark	1	Untuk melakukan pemantauan keamanan pada jaringan

Spesifikasi minimum untuk menjalankan sistem disini penulis menggunakan software aplikasi wiresharke v3.2.3 dalam melakukan pemantauan keamanan pada pada jaringan vpn. spesifikasi minimum dalam menjalankan wiresharke v3.2.3 adalah Windows 64-bit versi XP, Vista, Windows 7, Windows 8, dan Windows 10. Penulis menggunakan spesifikasi sebagai berikut:

a. Laptop HP AC002TU Series
b. Processor Intel Celeron-N3050
c. Memory 2GB DDR3
d. HDD 500GB

2. Perancangan

Perancangan arsitektur/topologi jaringan menggunakan laboratorium UIN Sunan Kalijaga yang akan dihubungkan dengan computer server dengan menggunakan jaringan VPN. Pemrosesan praktik ini dan juga memberikan dampak baik pada jaringan maupun keamanan data melalui jaringan vpn dan kami akan berusaha menerapkan sesuai dengan ketentuan dan izin dapi pimpinan laboratorium atau teknisi. Rancangan arsitektur/topologi jaringan yang akan dibuat dapat dilihat pada gambar 2.



Gambar 2. Rancangan Topologi VPN

Sampai saat ini, Laboratorium UIN Sunan Kalijaga masih menggunakan internet provider atau yang dikenal dengan internet service provider (ISP). Kemudian dibuatlah VPN dengan membuat "terowongan" (terowongan) antara komputer server ke komputer client sehingga semua data dari komputer client ke komputer server akan ditransfer melalui "terowongan" yang sudah dibuat. Untuk tujuan membuat VPN, komputer klien dan server keduanya memiliki router yang terhubung ke internet pada level yang sesuai. Pada Gambar 2, router-router yang digunakan memberikan catatan. Router Office A merupakan router yang terpasang pada komputer server, dan Router Office B merupakan router yang terpasang pada komputer client. Meskipun tersedia router lain, seperti yang dibuat oleh Cisco atau vendor lain, dalam pelaksanaan proyek ini, router Mikrotik dipilih karena kinerjanya yang baik dan biaya yang cukup rendah.

Implementasi Racangan Arsitektur Topologi Jaringan telah dimulai. Pada saat implementasi, jaringan komputer yang sudah ada hanya mengalami sedikit perubahan. Ini dilakukan dengan maksud meminimalkan biaya yang diperlukan. Area yang paling membutuhkan konfigurasi adalah setting router, baik itu di komputer client maupun server. Konfigurasi yang akan dibuat meliputi konfigurasi alamat IP (konfigurasi ini akan menetapkan alamat IP untuk setiap klien pada salah satu-2, Baik-1 atau Baik-2), konfigurasi gateway, konfigurasi DNS, konfigurasi NAT, konfigurasi perutean, dan konfigurasi PPTP.

Tabel 2.
Hasil Uji Coba

No	Nama PC	IP-Address	Hasil
1	Server A (Sebagai IP Tunnel OfficeA)	10.20.20.1	Terhubung sesuai dengan hasil konfigusasi pada router A
2	Server B (Sebagai IP Tunnel Office B)	10.20.20.6	Terhubung sesuai dengan hasil konfigusasi pada router B
3	Laptop-HP (Remote Access)	10.20.20.7	Terhubung pada jaringan vpn
4	Client-1	10.20.20.2	Terhubung pada jaringan vpn antara server A dengan server B

5	Client-2	10.20.20.3	Terhubung pada jaringan vpn antara server A dengan server B
6	Client-3	10.20.20.4	Terhubung pada jaringan vpn antara server A dengan server B
7	Client-4	10.20.20.5	Terhubung pada jaringan vpn antara server A dengan server B

3. Implementasi dan Pengujian Jaringan VPN

Proses implementasi dimulai ketika desain arsitektur/topologi jaringan telah dibuat. Dengan maksud untuk menekan biaya, maka dicoba untuk menggunakan jaringan komputer yang ada selama tahap implementasi hanya dengan sedikit perubahan. Konfigurasi router yang diterapkan di lab adalah komponen yang paling banyak berubah. Konfigurasi yang akan dilakukan terdiri dari konfigurasi IP address (pada konfigurasi ini akan ditentukan alamat IP setiap client pada Ether-1 dan Ether-2), konfigurasi getway, konfigurasi DNS, konfigurasi NAT, konfigurasi routing, dan konfigurasi PPTP.

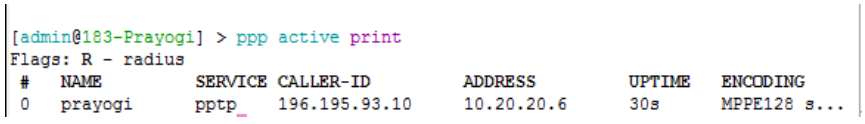
Pengujian jaringan VPN yang dibuat sedang dilakukan saat ini. Beberapa tes dilakukan untuk melihat apakah semua jaringan VPN operasional bebas dari kesalahan dan bekerja dengan baik. Beberapa pengujian teknis yang dilakukan pada langkah ini antara lain pengujian ping, pengujian rute IP, evaluasi fungsi server router A, pengujian konektivitas antar router yang terpasang, dan pengujian keamanan.

3.1 Hasil Konektivitas Router

Investigasi pertama adalah pencarian konektivitas antar router. Ketika Router A dan Router B berhasil terhubung, Router A akan secara otomatis mengembangkan alamat IP dinamis. Alamat ini adalah 10.20.20.1 dan digunakan untuk membuat terowongan VPN, sedangkan jaringan 10.20.20.0 dan 10.20.20.7 adalah alamat jarak jauh yang menghubungkan router ke router selama pembuatan VPN.

3.2 Hasil Konfigurasi VPN Menggunakan Metode PPTP

Setelah dipastikan router A dan B terhubung, langkah selanjutnya adalah konfirmasi bahwa konfigurasi VPN site-to-site yang sebelumnya dibuat menggunakan metode PPTP telah berhasil diselesaikan. Anda dapat melihat hasil konfigurasi dengan membuka Gambar 3 dan memilih baris yang sesuai.



Gambar 3. PPP aktif pada Router A

Pada gambar 3, perhatikan bahwa router A, bertindak sebagai server PPTP, telah terhubung ke router B, bertindak sebagai klien PPTP, yang diparkir. Jika setiap port terhubung ke server PPTP router A, maka either-1 dengan nama prayogi yang berfungsi sebagai alamat VP router B akan muncul.

3.3 Hasil Pengujian IP route

Adapun hasil pengujian IP route pada router A dapat dilihat pada Gambar 4.

```
[admin@183-Prayogi] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADC  10.20.20.1/32      10.20.20.6      pptp-out1                 0
 1 ADC  10.20.20.6/32      10.20.20.1      <pptp-prayogi>            0
 2 ADC  196.195.93.8/29    196.195.93.10   office_A                  0
                                           ether3
 3 A S  196.195.93.11/32                   <pptp-prayogi>            1
 4   S  196.195.93.11/32                   ether3                    1
 5 ADC  196.200.93.16/29   196.200.93.20   office_B                  0
```

Gambar 4. Hasil penngujian IP Route server pada router A

Gambar 4 menunjukkan alamat IP dari server PPTP yang menghubungkan router klien atau router B dengan alamat 10.20.20.1. Ada juga alamat IP lokal yang telah terhubung ke koneksi VPN menggunakan gateway office A selain alamat IP, menunjukkan bahwa itu telah terhubung ke router B.

3.4 Hasil Pengujian *PING*

a. Hasil pengujian ping koneksi dari *office_A* ke server.
Berdasarkan hasil pengujian PING antara office A dengan server yang ditunjukkan pada Gambar 5, office A mampu melakukan koneksi ke server yang telah dipastikan terhubung ke server menggunakan terowongan VPN.

```
[admin@183-Prayogi] > ping 196.195.93.10
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 196.195.93.10                              56  64 0ms
    1 196.195.93.10                              56  64 0ms
    2 196.195.93.10                              56  64 0ms
    3 196.195.93.10                              56  64 0ms
    4 196.195.93.10                              56  64 0ms
    5 196.195.93.10                              56  64 0ms
    6 196.195.93.10                              56  64 0ms
    sent=7 received=7 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

Gambar 5. Tampilan hasil pengujian ping koneksi *Office_A* ke server

b. Hasil pengujian ping koneksi dari *office_B* ke server.
Hasil pengujian PING antara office B dengan server seperti terlihat pada Gambar 6 menunjukkan bahwa Office B mampu melakukan koneksi ping ke server yang telah dipastikan terhubung ke server menggunakan tunnel VPN.

```
[admin@183-Prayogi] > ping 196.200.93.20
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 196.200.93.20                              56  64 5ms
    1 196.200.93.20                              56  64 0ms
    2 196.200.93.20                              56  64 0ms
    3 196.200.93.20                              56  64 0ms
    4 196.200.93.20                              56  64 0ms
    5 196.200.93.20                              56  64 0ms
    6 196.200.93.20                              56  64 0ms
    7 196.200.93.20                              56  64 0ms
    sent=8 received=8 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=5ms
```

Gambar 6. Tampilan hasil pengujian ping koneksi *Office_B* ke server

c. Hasil pengujian ping koneksi dari *office_B* ke *office_A atau sebaliknya*.
Terlihat dari hasil pengujian PING antara office B dan office A seperti terlihat pada Gambar 7, bahwa setup VPN tidak mengizinkan komunikasi antara kedua office tersebut; hal ini dilakukan demi menjaga keamanan. Hanya office B dengan server atau office A dengan server yang memenuhi syarat untuk koneksi VPN. Office B atau program serupa hanya terhubung ke server tanpa batas karena hal ini.

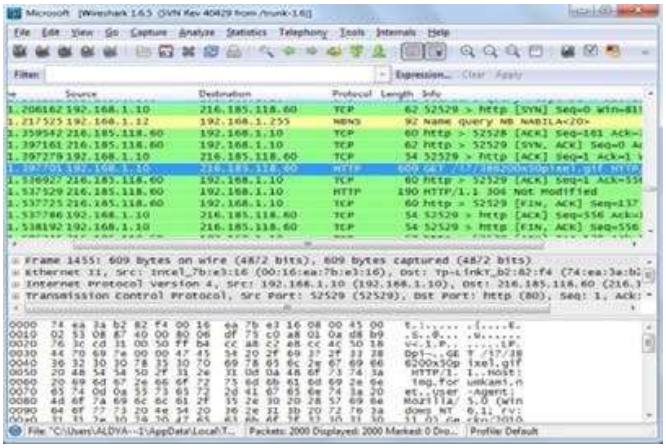
```
[admin@103-Prayogi] > ping 196.195.93.11
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 196.195.93.11                                           timeout
    1 196.195.93.11                                           timeout
    2 196.195.93.10                              84  64 971ms host unreachable
    3 196.195.93.11                                           timeout
    4 196.195.93.11                                           timeout
    5 196.195.93.10                              84  64 978ms host unreachable
    6 196.195.93.11                                           timeout
    7 196.195.93.11                                           timeout
    8 196.195.93.10                              84  64 978ms host unreachable
    9 196.195.93.11                                           timeout
    sent=10 received=0 packet-loss=100%
```

Gambar 7. Tampilan hasil pengujian ping koneksi *Office_B* ke *office_A*

3.5 Hasil Pengujian Keamanan Data

Aplikasi Wireshark secara khusus digunakan untuk melakukan metode pengujian keamanan pada penelitian ini:

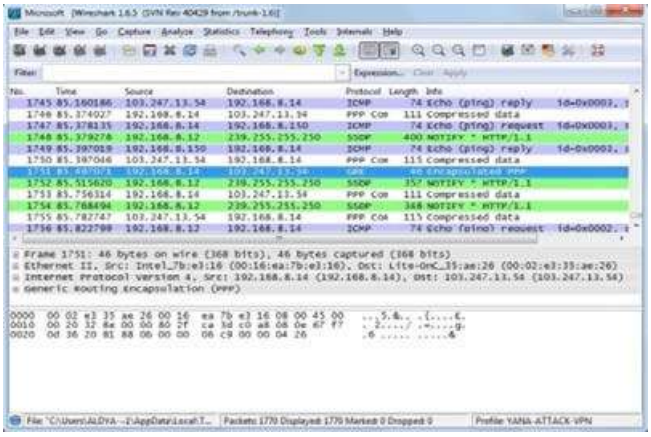
a. Eksperimen ini menggunakan program *Wireshark* untuk melakukan *sniffing* pada koneksi jaringan non-VPN di laboratorium.



Gambar 8. Jaringan Non VPN pada *Wireshark*

Gambar 8 menunjukkan telah terdeteksi beberapa penyadapan pada alamat IP 196.195.93.10 dengan memberikan informasi uploader file pixel.gif.

b. Eksperimen saat ini menggunakan perangkat lunak *Wireshark* untuk melakukan *sniffing* pada jaringan VPN di laboratorium.



Gambar 9. *Wireshark* pada jaringan VPN

Kolom info pada Gambar 9 yang bertuliskan "Encapsulated PPP and Compressed data" menunjukkan bahwa aktivitas VPN client dengan alamat IP 196.195.93.10 telah aktif pada jaringan VPN tunnel.

D. Kesimpulan

Setelah menyelesaikan setiap fase pelaksanaan proyek, yang mencakup segala hal mulai dari melakukan analisis kebutuhan hingga menulis hasil, kami dapat menarik kesimpulan sebagai berikut:

1. Ketika VPN dipasang di Laboratorium UIN Sunan Kalijaga Yogyakarta, metode PPTP dapat memberikan keamanan dengan menyertakan enkripsi di setiap tempat penyimpanan data dan dengan memberikan login dan kata sandi default untuk setiap cabang dan ether.
2. Perbandingan hasil evaluasi antara jaringan VPN dan non-VPN mengungkapkan bahwa aktivitas yang pertama lebih berhasil dari pada yang kedua karena aktivitas yang terakhir tidak diketahui orang lain.
3. Karena cacat desain, sistem ini masih rentan terhadap serangan pingflood yang menyebabkan serangan denial of service (DoS). Selain itu, jaringan VPN masih berisiko mengalami serangan intrusi jika sistem tidak menerapkan anti-flooding.

Ada beberapa kelemahan dalam penelitian ini, oleh karena itu dalam pengembangan kedepan anda harus memperhatikan saran berikut:

1. Meningkatkan keamanan server adalah jawaban atas masalah kerentanan di jaringan yang sudah menggunakan jaringan VPN.
2. Perlu dilakukan maintenance pada password manager dan security network. Solusinya adalah dengan cara dibuat dengan kombinasi huruf dan angka serta password-nya dibuat lebih dari 10 digit dan huruf dan angka tersebut, hal ini tujuannya untuk menyulitkan penyerangan terhadap aksi generate key oleh attacker.
3. Pengguna yang lebih suka menggunakan username dan password dengan jumlah digit yang sedikit perlu menyesuaikan karakter atau kebiasaannya karena hal tersebut membuat mereka menjadi sasaran penyadapan oleh pihak yang tidak diundang.

Daftar Pustaka

Andriani, R., Sa'di, A., & Putra, A. D. (2022). Implementasi VPN Menggunakan Metode Point to Point Tunneling Protocol. *Building of Informatics, Technology and Science (BITS)*, *4*(1), 184−190-184−190. https://doi.org/10.47065/bits.v4i1.1611

Budimulya, T., Safitri, M., & Faridi. (2022). PERANCANGAN VPN SEBAGAI PENDUKUNG SISTEM INFORMASI KEPEGAWAIAN PADA KANTOR KEMENTERIAN KESEHATAN RI. *JIKA (Jurnal Informatika)*, *6*(2), 197. https://doi.org/10.31000/jika.v6i2.6201

Christo, P., & Mulyono, H. (2022). PENERAPAN PRIVATE ACCESS MENGGUNAKAN METODE PPTP DAN OVPN DI YAYASAN UMMU'L QURO DEPOK JAKARTA. *JIKA (Jurnal Informatika)*, *6*(3), 256. https://doi.org/10.31000/jika.v6i3.5877

Dewi, S., Riyadi, F., Suwastitaratu, T., & Hikmah, N. (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), 128–139. https://doi.org/10.31294/evolusi.v8i1.7658

Diana, Gumiri, J. R., & Wandra, A. (2021). Optimasi Keamanan Virtual Private Network Untuk Komunikasi Data Di Pusat Informasi Pengembangan Pemukiman Dan Bangunan (PIP2B). *Pseudocode*, *8*(1), 76–89. https://doi.org/10.33369/pseudocode.8.1.76-89

Ekawati, I., & Irwan, D. (2021). Implementasi Virtual Private Network Menggunakan PPTP Berbasis Mikrotik. *JREC (Journal of Electrical and Electronics)*, *9*(1), 41–48. https://doi.org/10.33558/jrec.v9i1.3110

Febrianti, R., Sidik, Susafa'ati, Nainggolan, E. R., & Radiyah, U. (2021). Implementasi VPN Berbasis Point To Point Tunneling Protocol (PPTP) Menggunakan Mikrotik Router Board. *Jurnal Infortech*, *3*(1), 46–51. https://doi.org/10.31294/infortech.v3i1.10400

Nur, J., Raufun, L., & Afifa, M. (2021). SIMULASI VIRTUAL PRIVATE NETWORK (VPN) MENGGUNAKAN SECURE SOCKET TUNNELING PROTOCOL (SSTP) PADA JARINGAN KAMPUS UNIDAYAN BAUBAU. *Jurnal Informatika*, *10*(1), 85–92. https://doi.org/http://dx.doi.org/10.55340/jiu.v10i1.451

Pamungkas, A. P., Muhammad Reza Putra, & M. Hafizh. (2021). Analisis Jaringan VPN Menggunakan PPTP dan L2TP Berbasis Mikrotik pada Diskominfo Kabupaten Muko-muko. *Jurnal KomtekInfo*, *8*, 189–194. https://doi.org/10.35134/komtekinfo.v8i3.143

Phang, V., & Setyaningsih, E. (2021). Perancangan Virtual Private Network Dengan Protokol PPTP Menggunakan MikroTik Untuk Kebutuhan Remote Access. *Jurnal POLEKTRO: Jurnal Power Elektronik*, *10*(2), 68–71. https://doi.org/http://dx.doi.org/10.30591/polektro.v10i2.2573

Putra, J. L., Indriyani, L., & Angraini, Y. (2018). Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT. Asri Pancawarna. *IJCIT (Indonesian Journal on Computer and Information Technology*, *3*(2), 260–267. https://doi.org/https://doi.org/10.31294/ijcit.v3i2.4677

Ramdhani, R. F., & Yusuf, R. (2022). Implementasi Jaringan VPN untuk Mengurangi Biaya Komunikasi Menggunakan Metode EoIP Over PPTP: Studi Kasus House Printing. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *7*(3), 390. https://doi.org/10.26418/jp.v7i3.48171

Sari, A. P., Sulistiyono, & Kemala, N. (2020). PERANCANGAN JARINGAN VIRTUAL PRIVATE NETWORK BERBASIS IP SECURITY MENGGUNAKAN ROUTER MIKROTIK. *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, *7*(2), 150–164. https://doi.org/10.30656/prosisko.v7i2.2523

Supriyanto, B., & Suharyanto. (2019). Perancangan Jaringan VPN Menggunakan Metode Point To Point Tunneling Protocol. *Jurnal Teknik Komputer*, *5*(2), 235–240. https://doi.org/10.31294/jtk.v5i2.5452

Syarif, R. F., & Sobari, I. A. (2022). Implementasi Virtual Private Network (VPN) menggunakan Metode PPTP pada PT. Sinar Quality Internusa. *Jurnal Pendidikan Tambusai*, *6*(2), 15165–15184. https://doi.org/https://doi.org/10.31004/jptam.v6i2.4797

Wardana, M. A., Nusri, A. Z., & Juliandika. (2022). Jaringan Virtual Private Network (Vpn) Berbasis Mikrotik Pada Kantor Kecamatan Marioriawa Kabupaten Soppeng. *Jurnal Ilmiah Sistem Informasi Dan Teknik Informatika (JISTI)*, *5*(2), 107–116. https://doi.org/10.57093/jisti.v5i2.135

Wicaksana, P., Hadi, F., & Hadi, A. F. (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