

Optimizing Secure Communication in Distributed Corporate Networks through PPTP and IPsec VPN Protocols

Wilona Angelina Azels¹, Theresia Ghozali^{2*}, Marsul Siregar³

^{1,2,3}Program Studi Teknik Elektro, Fakultas Teknik
Universitas Katolik Atma Jaya Indonesia, Jakarta 12930, Indonesia

Article Info	Abstract
<i>Article history:</i> Received 05 12 2023 Accepted 14 12 2023 <i>Keywords:</i> <i>iPerf, IPsec, Mikrotik CHR, PPTP, VirtualBox, VPN, Winbox,</i>	<i>In today's industry, company's activities are scattered in several locations and need internet for communication purposes. However, it will be dangerous if third-parties have access to their information. One of the solutions for securing information exchange is by using Virtual Private Network (VPN). The VPN protocols that will be used are Point-to-Point Tunneling Protocol (PPTP) with the help of Internet Protocol Security (IPsec). These protocols are simulated in VirtualBox that has been previously installed with two Mikrotik routers and two Windows 7 operating systems. The PPTP and IPsec protocols are configured in both routers through Winbox software. For the computers, the IP addresses are configured along with iPerf software for bandwidth analysis. In this VPN simulation, both computers can communicate with each other and have no problem in accessing the internet. In PPTP's network, the average bandwidth is 1.293 Mbits/sec. Meanwhile, in PPTP with IPsec's network, the average bandwidth is 0.853 Mbits/sec. There is a slight difference considering that in PPTP, the data packets are only encapsulated. On the other hand, the data packets in IPsec protocol are both encapsulated and encrypted.</i>

Info Artikel	Abstrak
<i>Histori Artikel:</i> Diterima: 05 12 2023 Disetujui: 14 12 2023 <i>Kata Kunci:</i> <i>iPerf, IPsec, Mikrotik CHR, PPTP, VirtualBox, VPN, Winbox,</i>	<i>Di era industri saat ini, aktivitas perusahaan yang tersebar di beberapa lokasi membutuhkan internet sebagai media komunikasi. Namun pertukaran informasi akan berbahaya jika dapat diakses oleh pihak ketiga. Salah satu cara untuk menjaga pertukaran informasi adalah menggunakan Virtual Private Network (VPN). Protokol VPN yang digunakan adalah Point-to-Point Tunneling Protocol (PPTP) dan dibantu dengan Internet Protocol Security (IPsec). Kedua protokol VPN tersebut disimulasikan pada VirtualBox yang sudah terdapat 2 router Mikrotik CHR dan 2 komputer dengan sistem operasi Windows 7. Konfigurasi pada router adalah protokol PPTP dan IPsec yang dilakukan melalui Winbox, sementara pada komputer Windows 7 adalah konfigurasi alamat IP dan software iPerf untuk pengambilan data bandwidth pada jaringan VPN. Hasil yang didapatkan pada jaringan VPN adalah kedua komputer Windows 7 mampu saling berkomunikasi dan mengakses internet. Pada jaringan PPTP, bandwidth rata-ratanya adalah 1,293 Mbits/sec. Sementara pada jaringan PPTP dengan IPsec, bandwidth rata-ratanya adalah 0,853 Mbits/sec. Hal ini dikarenakan PPTP hanya melakukan enkapsulasi paket data sementara pada IPsec terdapat enkapsulasi serta enkripsi paket data.</i>

1. PENDAHULUAN

Di era Industri saat ini, aktivitas perusahaan tidak hanya dilakukan di satu tempat saja, namun bisa tersebar di berbagai lokasi secara bersamaan. Salah satu media komunikasi yang dapat digunakan agar informasi perusahaan dapat selaras dan tidak bertolak belakang adalah dengan menggunakan internet. Dengan adanya internet, biaya dan waktu yang digunakan untuk bertukar informasi akan berkurang. Hal ini didukung dengan hasil survei oleh World Bank [1], bahwa sekitar 36% persen pengguna menggunakan internet untuk berkomunikasi. Oleh karena itu akan sangat berbahaya jika informasi perusahaan dapat diakses oleh pihak ketiga.

*Corresponding author. Theresia Ghozali
Email address: theresia.ghozali@atmajaya.ac.id

Terdapat berbagai cara untuk menjaga pertukaran informasi melalui internet, salah satunya adalah *Virtual Private Network* (VPN). Dengan menggunakan VPN, pengiriman akan dijaga keamanan dan keasliannya. Dari berbagai macam protokol VPN, *Point-to-Point Tunneling Protocol* (PPTP) adalah protokol VPN yang sudah ada sejak tahun 1999. Namun protokol PPTP ini hanya memiliki fitur enkapsulasi paket data saja, sehingga masih rentan diretas oleh pihak ketiga. Protokol VPN lainnya yang dapat membantu PPTP adalah *Internet Protocol Security* (IPSec) yang mampu memberikan proteksi enkripsi yang baik.

Tujuan dari penelitian ini adalah membuat simulasi jaringan VPN menggunakan protokol PPTP dan IPSec. Simulasi ini akan dilakukan pada *software* VirtualBox yang memiliki 2 *router* Mikrotik dan 2 komputer virtual dengan sistem operasi Windows 7. Dengan adanya penelitian ini, dapat dibandingkan jaringan VPN protokol PPTP saja dengan jaringan VPN protokol PPTP dan IPSec.

2. TEORI DASAR

2.1 *Virtual Private Network*

Virtual Private Network (VPN) adalah jaringan publik yang seolah-olah dibuat menjadi jaringan privat dan mampu mengamankan data serta alamat IP yang dikirim pada jaringan tersebut [1]. Jaringan VPN ini biasanya diimplementasikan pada *OSI layer* yang terdapat pada jaringan *Transmission Control Protocol / Internet Protocol* (TCP/IP). Protokol-protokol VPN yang dapat digunakan pada jaringan TCP/IP dapat dilihat pada Tabel 1.

Tabel 1. Protokol VPN

<i>OSI Layer</i> Jaringan TCP/IP	Protokol VPN
<i>Application Layer</i>	1. <i>Secure Socket Layer</i> (SSL).
<i>Transport Layer</i>	2. <i>Secure Shell</i> (SSH).
<i>Network Layer</i>	1. <i>Internet Protocol Security</i> (IPSec).
<i>Link Layer</i>	1. <i>Asynchronous Transfer Mode</i> (ATM) dan <i>Frame Relay Connections</i> . 2. <i>Multiprotocol Label Switching</i> (MPLS). 3. <i>Virtual Private Local Area Network Service</i> . 4. <i>Layer 2 Tunneling Protocol</i> (L2TP). 5. <i>Point to Point Tunneling Protocol</i> (PPTP).

2.2 *Point-to-Point Tunneling Protocol*

Cara kerja dari *Point to Point Tunneling Protocol* (PPTP) bergantung pada koneksi PPTP *server* dan PPTP *client* [3] seperti pada Gambar 1. Pada PPTP *server*, beberapa konfigurasi yang dapat diatur adalah jenis autentikasi yang diterima oleh *server*, ketersediaan PPTP *server*, dan jumlah paket data yang dapat diterima. Sementara pada PPTP *client*, beberapa konfigurasi yang dapat diatur adalah jenis autentikasi yang akan digunakan, alamat IP dari PPTP *server*, *user* dari PPTP *server*, dan *password* dari PPTP *server*.



Gambar 1. Struktur PPTP

2.3 Internet Protocol Security

Internet Protocol Security (IPSec) merupakan salah satu protokol selain PPTP yang mampu membangun jaringan VPN. Perbedaan keduanya adalah IPSec bekerja di lapisan ketiga pada *OSI Layer*, sedangkan PPTP bekerja di lapisan kedua pada *OSI layer*. IPSec menyediakan beberapa fitur, yaitu: enkapsulasi, enkripsi, dan autentikasi [3]. Fitur yang disediakan oleh IPSec akan dibantu dengan beberapa protokol, yaitu: *Encapsulating Security Protocol* untuk enkapsulasi, AES untuk enkripsi, serta SHA1 dan *pre shared key* untuk autentikasinya.

Internet Protocol Address (IP Address) adalah kumpulan 32 bit yang dibagi menjadi 4 oktet. Terdapat 2 bagian pada alamat IP, yaitu: *network ID* dan *host ID*. Fungsi dari *network ID* adalah menentukan alamat pada jaringan, sementara *host ID* berfungsi untuk menentukan alamat unik pada jaringan tersebut. Terdapat 2 jenis klasifikasi, yaitu: *classful* dan *classless* [3]. Pada penelitian ini, klasifikasi yang akan digunakan adalah *classful IP Address*.

Pada klasifikasi *classful*, alamat IP dibagi menjadi 5 class, yaitu: *A*, *B*, *C*, *D*, dan *E*. Umumnya, alamat IP yang sering digunakan adalah *class A* hingga *class C*. *Class D* dikhususkan untuk *multicast* sementara *class E* khusus untuk eksperimen atau penelitian. Perbedaan mendasar dari *class* ini adalah jumlah *host* yang mampu ditampung. *classful* pada alamat IP dapat dilihat pada Tabel 2.

Tabel 2. Alamat IP pada klasifikasi *classful*

<i>Class</i>	<i>Range of IP Address</i>	<i>Subnet Mask</i>
A	1.0.0.0 – 127.0.0.0	255.0.0.0
B	128.0.0.0 – 191.255.0.0	255.255.0.0
C	192.0.0.0 – 223.255.255.0	255.255.255.0
D	224.0.0.0 – 239.255.255.255	-
E	240.0.0.0 – 255.255.255.255	-

2.4 Network Address Translation

Terdapat 2 jenis alamat IP pada umumnya, yaitu: *public address* dan *private address*. *Private address* digunakan untuk keperluan internal pada jaringan dan dapat digunakan oleh semua orang. Kekurangan dari *private address* adalah tidak dapat digunakan untuk berkomunikasi dengan internet, berbeda dengan *public address* yang dapat berkomunikasi dengan internet. Oleh karena itu dibutuhkan *Network Address Translation* (NAT) yang mampu mengubah *private address* menjadi *public address*. Terdapat 2 jenis NAT, yaitu: *source NAT* (*srcnat*) dan *destination NAT* (*dstnat*) [7]. *Source NAT* yang digunakan pada penelitian ini bertugas pada paket data yang berasal dari jaringan NAT. Cara kerja dari *source NAT* adalah mengganti *private address* dari sumber dengan *public address* saat melewati *router*.

2.5 VirtualBox

VirtualBox adalah perangkat lunak *open-source* yang dikembangkan oleh Oracle [7]. Pada VirtualBox, salah satu pengaturan yang penting adalah *network adapter* yang akan digunakan pada *virtual machine*. Terdapat beberapa *network adapter* yang dapat digunakan pada VirtualBox, yaitu: *not attached*, *network address translation* (NAT), *bridged networking*, *internal networking*, *host-only networking*, dan *generic networking*. Pada penelitian ini, *network adapter* yang akan digunakan adalah *host-only networking* dan *internal networking*. Perbandingan dari semua jenis *network adapter* dapat dilihat pada Tabel 3.

Tabel 3. Perbandingan network adapter pada VirtualBox

<i>Network adapter</i>	<i>Virtual machine ke virtual machine</i>	<i>Virtual machine ke host</i>	<i>Host ke virtual machine</i>
<i>Not attached</i>	Tidak bisa	Tidak bisa	Tidak bisa
NAT	Tidak bisa	bisa	<i>Port Forward</i>
<i>Bridged networking</i>	Bisa	Bisa	Bisa
<i>Internal networking</i>	bisa	Tidak bisa	Tidak bisa
<i>Host-only networking</i>	bisa	bisa	bisa

2.6 Mikrotik

Mikrotik adalah sebuah perusahaan di Latvia yang berdiri pada tahun 1996 yang mengembangkan *router* dan sistem *wireless ISP*. Pada penelitian ini, Mikrotik *Cloud Hostes Router* (Mikrotik CHR) akan digunakan sebagai *router* pada simulasi jaringan VPN. Mikrotik CHR adalah RouterOS yang dirancang untuk dijalankan secara virtual pada *virtual machine* [5]. Mikrotik CHR ini memiliki fitur yang sama dengan RouterOS, namun yang berbeda adalah lisensinya. Jenis lisensi yang akan digunakan pada penelitian ini adalah lisensi gratis dan pengguna perlu mengunduh *disk image file* dan melakukan *install* pada *virtual machine*.

Untuk konfigurasi *router* Mikrotik, akan dibantu dengan *software* tambahan, yaitu: Winbox. Winbox adalah perangkat lunak open-source yang digunakan untuk mengkonfigurasi dan menyetel *router* Mikrotik menggunakan *MAC Address* ataupun *IP Address* [12]. Penggunaan *Software* Winbox ini mampu membantu pengguna mempercepat pekerjaan dalam melakukan penyetelan dan konfigurasi pada *router* Mikrotik karena telah menggunakan *Graphical Unit Interface* (GUI).

2.7 IPerf

IPerf adalah perangkat lunak *open- source* yang mampu mengukur *maximum bandwidth* pada jaringan IP [5]. *Software* iPerf ini mampu mengukur pada protokol *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP). Beberapa fitur dari *software* iPerf, yaitu: sudah dapat digunakan pada banyak sistem operasi, mampu digunakan untuk alamat IPv4 maupun IPv6, dan server dapat digunakan dalam berbagai koneksi.

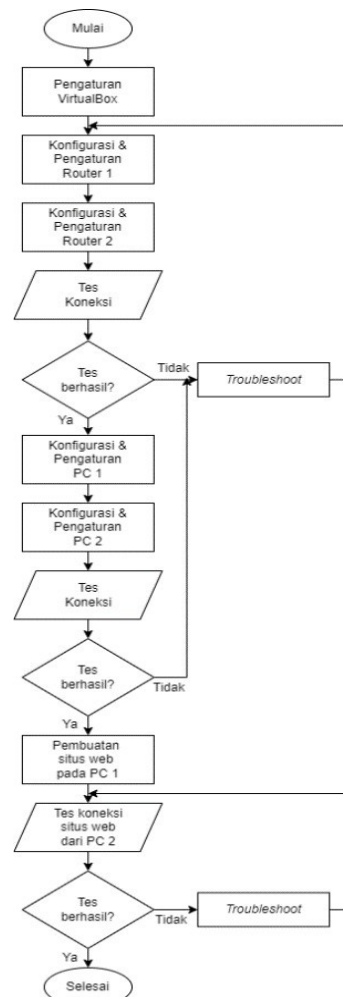
3. PERANCANGAN SISTEM

3.1 Perangkat Jaringan VPN

Perangkat-perangkat yang akan dikonfigurasi dan/atau diatur pada simulasi ini adalah VirtualBox, 2 *router* Mikrotik, dan 2 komputer virtual. Diagram alir untuk perancangan simulasi jaringan VPN dapat dilihat pada Gambar 4. Konfigurasi Alamat IP dan *interface* yang digunakan pada perangkat akan menggunakan *addressing table* pada Tabel 4.

Tabel 4. Addressing table jaringan VPN

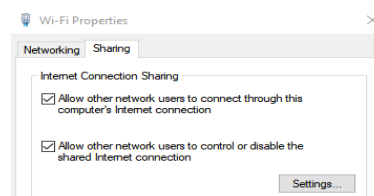
Perangkat	Interface	Alamat IP
<i>Router 1</i>	ether1	192.168.137.10
	ether2	192.168.10.1
	<pptp-pptp>	1.1.1.1
<i>Router 2</i>	ether1	192.168.137.20
	ether2	192.168.20.1
	pptp-out1	1.1.1.2
PC 1	-	192.168.10.4
PC 2	-	192.168.20.4



Gambar 2. Diagram alir simulasi jaringan VPN

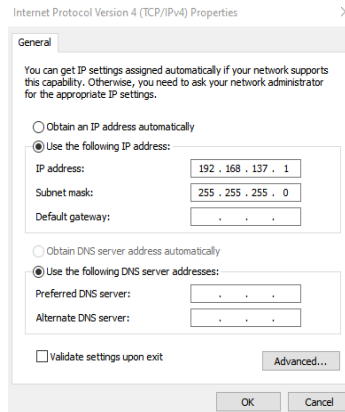
3.2 Pengaturan VirtualBox

Agar VirtualBox mampu menunjang pelaksanaan simulasi, maka *virtual machine* yang dibuat pada VirtualBox ini harus terhubung dengan komputer *host*. Oleh karena itu dibutuhkanlah pengaturan *sharing* koneksi internet. Tampilan *properties* dari koneksi internet dapat dilihat pada Gambar 5.

Gambar 3. Tampilan *Wi-Fi properties* pada komputer *host*

Pada tahap ini, koneksi internet sudah dibagikan dengan VirtualBox. Untuk melihat alamat IP yang akan digunakan pada VirtualBox, dapat dilihat dengan cara klik kanan pada *VirtualBox Host-Only Network* dan pilih *properties*. Kemudian klik dua kali pada pilihan 'Internet Protocol Version 4 (TCP/IPv4)'. Alamat IP yang tertera pada *properties* tersebut akan digunakan sebagai *gateway* pada

router agar dapat terkoneksi ke internet. Tampilan pengaturan alamat IPv4 pada *VirtualBox Host-Only Network* dapat dilihat pada Gambar 6.



Gambar 4. Alamat IP pada VirtualBox Host-Only Network

3.3 Konfigurasi Router

Pada jaringan VPN, akan terdapat 2 *router* yang akan digunakan. *Router* pertama akan bertindak sebagai *server*, dan *router* kedua akan bertindak sebagai *client*. Konfigurasi yang diperlukan pada penelitian ini adalah pengaturan *network adapter*, konfigurasi dasar *router*, konfigurasi PPTP, dan konfigurasi IPsec.

Terdapat 2 koneksi yang diperlukan pada *router*, yaitu: koneksi menuju internet dan koneksi menuju *router* lainnya. Untuk koneksi *router* menuju internet, akan menggunakan *Host-only Adapter*, sementara untuk koneksi *router* menuju *router* lainnya, akan menggunakan *internal network*. Pengaturan *network adapter* ini dapat diatur melalui pengaturan *virtual machine* pada VirtualBox. Penggunaan *network adapter* pada kedua *router* dapat dilihat pada Tabel 5.

Tabel 5. Network adapter pada router

Router	Adapter	Jenis Network Adapter	MAC Address
Router 1	Adapter 1	Host- only Adapter	08:00:27:A7:69:BD
	Adapter 2	Internal Network	-
Router 2	Adapter 1	Host- only Adapter	08:00:27:8B:8B:80
	Adapter 2	Internal Network	-

Seluruh konfigurasi *router* akan dilakukan menggunakan *software* Winbox. Cara untuk memasuki pengaturan *router* adalah memilih *MAC address router* yang diinginkan pada *software* Winbox. Untuk konfigurasi dasar, akan dilakukan konfigurasi alamat IP untuk masing-masing adapter pada *router* mengikuti *addressing table* pada Tabel 4. Konfigurasi dasar masing-masing *router* pada Adapter 1 dapat dilihat pada Tabel 6 dan untuk Adapter 2 dapat dilihat pada Tabel 7.

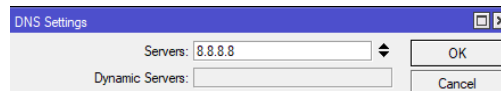
Tabel 6. Konfigurasi alamat IP Adapter 1

	Router 1	Router 2
Address	192.168.137.10/24	192.168.137.20/24
Network	192.168.137.0	192.168.137.0
Interface	ether1	ether1

Tabel 7. Konfigurasi alamat IP Adapter 2

	Router 1	Router 2
Address	192.168.10.1/24	192.168.20.1/24
Network	192.168.10.0	192.168.20.0
Interface	ether2	ether2

Setelah melakukan konfigurasi alamat IP, akan dilakukan konfigurasi *DNS server*. *DNS Server* yang akan digunakan pada kedua *router* adalah 8.8.8.8. Tampilan konfigurasi *DNS server* dapat dilihat pada Gambar 7.



Gambar 5. Konfigurasi DNS server

Setelah konfigurasi DNS, dilanjutkan dengan konfigurasi NAT. Konfigurasi NAT untuk kedua *router* dapat dilihat pada Tabel 8.

Tabel 8. Konfigurasi NAT

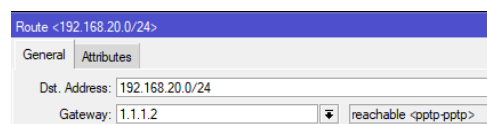
	Router 1	Router 2
Chain	scrnat	scrnat
Action	masquerade	masquerade

Konfigurasi PPTP *server* akan dilakukan pada *router* pertama. Untuk mengaktifkan PPTP *server* dapat dilakukan dengan cara menekan tombol PPTP *server* yang terdapat pada menu PPP pada Winbox dan klik pada *checkbox* dengan tulisan *enabled*. Setelah mengaktifkan PPTP *server*, Langkah berikutnya adalah membuat PPTP *secret*, yaitu nama dan *password* yang akan diperlukan oleh PPTP *client* untuk terhubung ke PPTP *server*. Pengaturan PPTP *secret* dapat dilihat pada Tabel 9.

Tabel 9. Pengaturan PPTP secret

Name	pptp
Password	pptp
Service	pptp
Profile	Default-encryption
Local Address	1.1.1.1
Remote Address	1.1.1.2

Langkah terakhir pada pengaturan PPTP pada *router* adalah penambahan *static routing*. Tampilan *static routing* untuk PPTP *server* dapat dilihat pada Gambar 8.



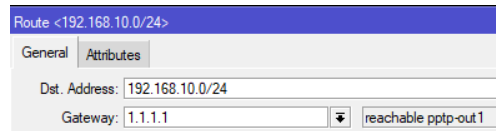
Gambar 6. Static routing PPTP server

Konfigurasi PPTP *client* akan dilakukan pada *router* kedua. Pengaktifkan PPTP *client* dapat dilakukan dengan cara menekan tombol PPTP *client* pada *dropdown menu* pada menu PPP dan memasukkan nama serta *password* yang telah diatur pada PPTP *server* sebelumnya. Pengaturan PPTP *client* dapat dilihat pada Tabel 10.

Tabel 10. Konfigurasi PPTP client

Name	pptp-out1
Connect to	192.168.137.10
User	pptp
Password	pptp
Profile	default-encryption

Langkah terakhir pada pengaturan PPTP pada *router* adalah penambahan *static routing*. Tampilan *static routing* untuk PPTP *client* dapat dilihat pada Gambar 9.



Gambar 7. Static routing PPTP client

Pengaturan IPsec pada kedua *router* harus sama agar dapat membangun koneksi IPsec. Karena IPsec akan digunakan bersamaan dengan PPTP, maka alamat IP yang akan digunakan dalam konfigurasi IPsec akan menggunakan alamat IP yang telah dikonfigurasi pada PPTP. Konfigurasi IPsec *peer* pada kedua *router* dapat dilihat pada Tabel 11.

Tabel 11. Konfigurasi IPsec Peer

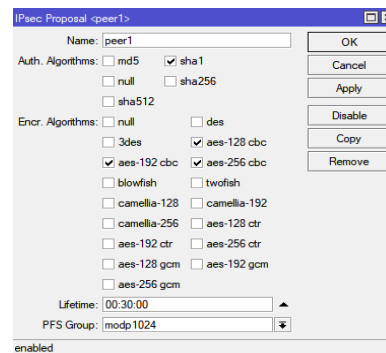
	Router 1	Router 2
Name	peer1	peer1
Address	1.1.1.2	1.1.1.1
Profile	peer1	peer1

Selain IPsec *peer*, konfigurasi yang diperlukan adalah IPsec *identity* untuk mengatur jenis autentikasi yang ingin digunakan. Konfigurasi IPsec *identity* dapat dilihat pada Tabel 12.

Tabel 12. Konfigurasi IPsec Identity

	Router 1	Router 2
Peer	peer1	peer1
Auth. Method	Pre shared key	Pre shared key
Secret	ipsec	ipsec

Langkah berikutnya adalah konfigurasi IPsec *proposal* untuk menentukan jenis autentikasi dan enkripsi yang ingin digunakan. Tampilan IPsec *proposal* dapat dilihat pada Gambar 10



Gambar 8. Tampilan IPsec proposal

Langkah terakhir adalah konfigurasi IPsec *policy* untuk menentukan jenis IPsec yang akan digunakan, protokol enkapsulasi, dan alamat IP pada jaringan IPsec. Konfigurasi IPsec *policy* pada kedua *router* dapat dilihat pada Tabel 13.

Tabel 13. Konfigurasi IPsec policy

	Router 1	Router 2
Peer	peer1	peer1
Tunnel	Yes	Yes
Source address	192.168.10.0 /24	192.168.20.0/24
Destination address	192.168.20.0 /24	192.168.10.0/24
IPsec protocol	ESP	ESP

<i>Proposal</i>	peer1	peer1
<i>SA source Address</i>	1.1.1.1	1.1.1.2
<i>SA destination Address</i>	1.1.1.2	1.1.1.1

3.4 Konfigurasi Komputer Virtual

Pada komputer virtual, pengaturan *network adapter* tetap diperlukan. Pengaturan *network adapter* dapat dilakukan melalui pengaturan *virtual machine* pada VirtualBox. *Network adapter* yang akan digunakan pada kedua komputer virtual adalah *internal network*. Setelah pengaturan *network adapter*, konfigurasi alamat IP akan dilakukan pada kedua router. Konfigurasi alamat IP pada komputer virtual dapat melalui *network connections*. Alamat IP yang akan digunakan pada kedua komputer virtual dapat dilihat pada Tabel 14.

Tabel 14. Konfigurasi alamat IP

	PC 1	PC 2
<i>IP Address</i>	192.168.10.4	192.168.20.4
<i>Subnet Mask</i>	255.255.255.0	255.255.255.0
<i>Default Gateway</i>	192.168.10.1	192.168.20.1
<i>Preferred DNS Server</i>	8.8.8.8	8.8.8.8

3.5 Pengaturan *Sharing Files*

Pengaturan *sharing files* akan dilakukan pada kedua komputer virtual agar dapat mengakses *file* pada komputer *host*. Fitur ini tersedia pada VirtualBox dengan cara melakukan *install* 'Insert Guest Additions CD image' pada *menubar* 'Device'. Setelah selesai melakukan pemasangan, Pengaturan *shared folder* akan dilakukan untuk mencari *path folder* dari *folder* yang ingin dibagikan dari komputer *host*. Fitur *sharing folder* ini akan digunakan untuk melakukan pemasangan *browser* Chrome, *software* iPerf, dan *software* XAMPP pada kedua komputer virtual.

3.6 Pembuatan Halaman Web

Pembuatan halaman web akan dilakukan pada komputer *host* terlebih dahulu untuk mempermudah pemrograman. Setelah web selesai dibuat, seluruh *file* web akan dipindahkan ke PC 1 yang akan bertindak sebagai *server*. Pada PC 1, *software* XAMPP akan dipasang dan *folder* berisikan *file* web akan dipindah ke *folder* 'htdocs' yang terdapat pada *folder* instalansi XAMPP.

4. PENGUJIAN SISTEM

4.1 Pengujian PPTP

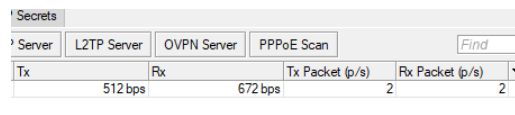
Pengujian PPTP pada jaringan VPN akan dilakukan dengan beberapa cara, yaitu: melalui *command prompt* dan *software* Winbox. Hasil pengujian menggunakan *ping* dapat dilihat pada Tabel 15.

Tabel 15. Hasil pengujian ping

Sumber	Tujuan	Hasil	Tracert
PC 1	PC 2	Berhasil	Melewati 1.1.1.2
PC 1	Google	Berhasil	-
PC 2	PC 1	Berhasil	Melewati 1.1.1.1
PC 2	Google	Berhasil	-

Dari pengujian pada Tabel 15, PPTP dapat berhasil dibuat. Hal ini dapat dibuktikan karena perangkat berhasil melakukan *ping* ke perangkat pada jaringan lain serta menggunakan alamat IP yang telah dibuat pada *tunnel* PPTP, yaitu: 1.1.1.1 dan 1.1.1.2. Selain itu, masing-masing perangkat masih dapat mengakses internet.

Untuk pengujian melalui Winbox, dapat dilihat pada *tab* 'interface' pada menu PPP. Jika terdapat koneksi PPTP, maka akan terlihat jumlah kecepatan *transfer* dan *receive* seperti pada Gambar 11.



Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
512 bps	672 bps	2	2

Gambar 9. Koneksi PPTP

4.2 Pengujian PPTP dan IPSec

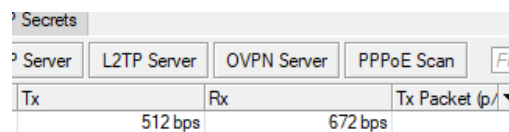
Pengujian PPTP dan IPSec akan dilakukan dengan cara yang sama seperti pengujian PPTP saja, yaitu: melalui *command prompt*, dan *software* Winbox. Hasil pengujian menggunakan *ping* dapat dilihat pada Tabel 16.

Tabel 16. Hasil pengujian ping

Sumber	Tujuan	Hasil	Tracert
PC 1	PC 2	Berhasil	Melewati 1.1.1.2
PC 1	Google	Berhasil	-
PC 2	PC 1	Berhasil	Melewati 1.1.1.1
PC 2	Google	Berhasil	-

Dari pengujian pada Tabel 16, Walaupun sudah terdapat koneksi IPSec, koneksi PPTP tetap berhasil dibuat. Hal ini dapat dibuktikan karena perangkat berhasil melakukan *ping* ke perangkat pada jaringan lain menggunakan alamat IP yang telah dibuat pada *tunnel* PPTP, yaitu: 1.1.1.1 dan 1.1.1.2. Selain itu, masing-masing perangkat masih dapat mengakses internet.

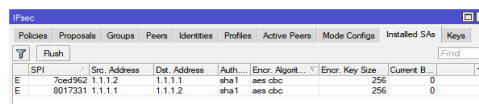
Untuk memastikan bahwa PPTP masih digunakan pada jaringan VPN, dilakukan pengujian melalui Winbox. Dengan cara yang sama seperti sebelumnya, koneksi PPTP dapat dilihat pada *tab* 'interface' pada menu PPP. Jika terdapat koneksi PPTP, maka akan terlihat jumlah kecepatan *transfer* dan *receive* seperti pada Gambar 12.



Tx	Rx	Tx Packet (p/s)
512 bps	672 bps	2

Gambar 10. Koneksi PPTP

Untuk pengujian IPSec dapat melalui *tab* 'installed SA' pada menu IPSec pada *software* Winbox. Jika IPSec berhasil dibuat pada jaringan, maka akan terdapat alamat IP yang digunakan beserta protokol yang digunakan pada IPSec, seperti pada Gambar 13.



SPI	Src Address	Dest Address	Auth...	Encr. Algorit...	Encr. Key Size	Current B...
1000962	1.1.1.2	1.1.1.1	sha1	aes cbc	256	0
8017331	1.1.1.1	1.1.1.2	sha1	aes cbc	256	0

Gambar 11. Koneksi IPSec

4.3 Pengujian iPerf

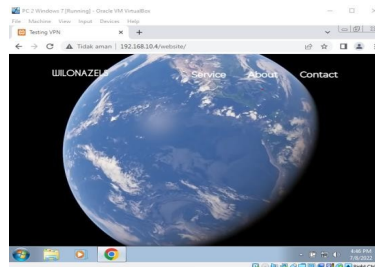
Pengujian *bandwidth* dengan *software* iPerf dilakukan pada kedua komputer virtual. PC 1 bertindak sebagai *server* dan PC 2 bertindak sebagai *client*. Pengujian dilakukan 2 kali, yaitu: untuk protokol PPTP dan untuk protokol PPTP dan IPSec. Hasil Pengujian iPerf dapat dilihat pada Tabel 17.

Tabel 17. Pengujian bandwidth pada jaringan VPN

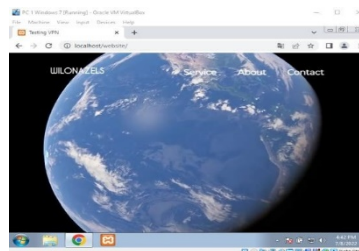
Interval	PPTP Dalam Mbits/sec	PPTP & IPSec Dalam Mbits/sec
1	1,77	1,61
2	0,92	0,88
3	0,92	0,87
4	0,92	0,91
5	0,92	0,86
6	0,93	0,91
7	0,92	0,88
8	0,92	0,89
Rata- Rata	1,03	0,98

4.4 Pengujian dengan web server

Pengujian dilakukan dari PC 2 dengan cara mengakses *server* yang terdapat pada PC 1. Tampilan halaman web pada *server* (PC 1) dapat dilihat pada Gambar 14 dan tampilan halaman web dari sisi *client* (PC 2) dapat dilihat pada Gambar 15.



Gambar 12. Tampilan Web pada sisi server



Gambar 13. Tampilan Web pada sisi client

Pada hasil pengujian menggunakan web *server*, tidak terlihat perbedaan tampilan halaman web pada jaringan PPTP dengan jaringan PPTP dan IPSec. Namun jika dilihat dari uji tes kecepatan internet menggunakan situs speedtest.net, terdapat perbedaan yang dapat dilihat pada Tabel 18.

Tabel 18. Perbandingan kecepatan internat jaringan VPN

	PPTP	PPTP & IPSec
Ping	15 ms	277 ms
Download	0,98 Mbps	0,78 Mbps
Upload	1,02 Mbps	1.00 Mbps

5. KESIMPULAN

Berdasarkan hasil simulasi jaringan VPN yang telah dilakukan, dapat disimpulkan bahwa protokol PPTP dapat digabungkan bersama dengan protokol IPSec sehingga memiliki tingkat keamanan yang lebih baik dibandingkan protokol PPTP saja. Namun jaringan PPTP dengan tambahan protokol IPSec

memiliki penurunan kecepatan internet dan *bandwidth*. Hal ini dikarenakan PPTP hanya melakukan enkapsulasi paket data sementara IPsec melakukan enkapsulasi serta enkripsi paket data.

Untuk pengembangan penelitian selanjutnya, dapat dilakukan perbandingan protokol PPTP/IPsec dengan protokol L2TP/IPsec. Hal ini dikarenakan protokol L2TP/IPsec sudah banyak digunakan pada jaringan VPN, namun belum ada perbandingan dengan protokol lainnya yang digunakan bersamaan dengan protokol IPsec.

DAFTAR PUSTAKA

- [1] M. A. Rizaty, "Masyarakat RI Paling Banyak Gunakan Internet untuk Berkomunikasi," Databoks, 29 7 2021. [Online]. Available: <https://databoks.katadata.co.id/datapublish/2021/07/29/masyarakat-ri-paling-banyak-gunakan-internet-untuk-berkomunikasi>. [Accessed 4 6 2022].
- [2] S. Frankel, K. Kent, R. Lewkowski, A. D. Orebaugh, R. W. Ritchey and S. R. Sharma, Guide to IPsec VPNs, Gaithersburg: National Institute of Standards and Technology, 2005.
- [3] A. K. Yoga, "Konfigurasi VPN PPTP pada Mikrotik," Citraweb, 10 1 2013. [Online]. Available: https://citraweb.com/artikel_lihat.php?id=43. [Accessed 4 6 2022].
- [4] Watchguard, "About IPsec Algorithms and Protocols," Watchguard, 2022. [Online]. Available: https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/mvvpn/general/ipsec_algorithms_protocols_c.html. [Accessed 4 6 2022].
- [5] S. Malik, Network Security Principles and Practice, Indianapolis: Cisco Press, 2002.
- [6] C. Bernstein and M. Cobb, "Advance Encryption Standard," Techtarget, 2022. [Online]. Available: <https://www.techtarget.com/searc hsecurity/definition/Advanced- Encryption-Standard>. [Accessed 4 6 2022].
- [7] T. E. Sinaga, "SHA 2 atau SHA-256? Revolusi Enkripsi Terbaik pada Website – SSL Indonesia," SSL Indonesia, 2022. [Online]. Available: <https://sslindonesia.com/sha-2-atau-sha-256-revolusi-enkripsi-terbaik-pada-website-ssl-indonesia/>. [Accessed 4 6 2022].
- [8] Computer Hope, "What is IP," Computer Hope, 2020. [Online]. Available: <https://www.computerhope.com/jargon/i/ip.htm>. [Accessed 4 6 2022].
- [9] S. Ulpada, "Perbedaan Srcnat & Dstnat Mikrotik beserta kegunaannya," Cyberdesu, 2021. [Online]. Available: <https://cyberdesu.com/perbedaan-src-nat-dengan-dst-nat-mikrotik/>. [Accessed 4 6 2022].
- [10] Á. Toledo, "Virtualbox," uptodown, 2019. [Online]. Available: <https://virtualbox.en.uptodown.com/windows>. [Accessed 4 6 2022].
- [11] D. Ninja, "Panduan Dasar Penggunaan Mikrotik CHR," DewaWeb, 9 3 2021. [Online]. Available: <https://www.dewaweb.com/blog/panduan-dasar-penggunaan-mikrotik-chr/>. [Accessed 4 6 2022].
- [12] A. Zaksa, "Download Winbox Mikrotik Terbaru 2022 (Free Download)," Nesabamedia, 2022. [Online]. Available: <https://www.nesabamedia.com/download-winbox/>. [Accessed 4 6 2022].
- [13] M. Zakaria, "Download Windows 7 Ultimate 32/64 Bit ISO (Official)," Nesabamedia, 2022. [Online]. Available: <https://www.nesabamedia.com/download-windows-7-iso/>. [Accessed 4 6 2022].
- [14] A. Faradilla, "Apa itu HTML? Fungsi dan Cara Kerja HTML," Hostinger, 2022. [Online]. Available: <https://www.hostinger.co.id/tutori al/apa-itu-html>. [Accessed 4 6 2022].
- [15] C. Ariata, "Apa Itu CSS? Pengertian, Fungsi, dan Cara Kerjanya," Hostinger Tutorial, 2021. [Online]. Available: <https://www.hostinger.co.id/tutori al/apa-itu-css>. [Accessed 4 6 2022].
- [16] M. R. Adani, "Memahami Konsep Penggunaan Xampp untuk Kebutuhan Development," Sekawan Media, 26 4 2021. [Online]. Available: <https://www.sekawanmedia.co.id/ blog/apa-itu-xampp/>. [Accessed 4 6 2022].
- [17] Filecatalyst, "What is iPerf and How to Use It," Filecatalyst, 2021. [Online]. Available: <https://www.filecatalyst.com/blog/what-is-iperf-and-how-to-use-it/>. [Accessed 4 6 2022].