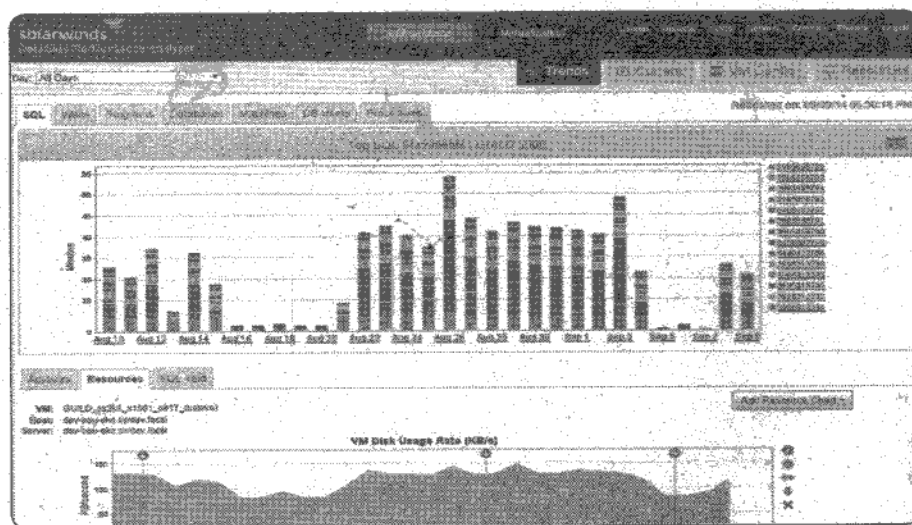


Perhatikan gambar dan teks berikut dengan saksama!



Sumber: <http://cbc1b481bf017626dad1-b47c988b54164eeced4913dd4c721a42.r70.cf1.rackcdn.com>, diakses 6 Oktober 2018, 08.45 WIB

Gambar 5.1 Monitoring kinerja server

Koneksi dari VPN bersifat virtual, karena jaringan *public* ini dibuat seakan-akan sebagai sebuah jaringan *private*, oleh sebab itu disebut dengan *Virtual Private*. VPN sering diimplementasikan untuk koneksi dari kantor cabang ke kantor pusat, sehingga jaringan kantor cabang dan kantor pusat bisa saling berkomunikasi seperti berada dalam satu jaringan lokal.

Dengan VPN ini kita seolah-olah membuat jaringan di dalam jaringan atau biasa disebut *tunnel* (terowongan). *Tunneling* adalah suatu cara membuat jalur privat dengan menggunakan infrastruktur pihak ketiga. VPN menggunakan salah satu dari tiga teknologi *tunneling* yang ada yaitu: PPTP, L2TP dan standar terbaru, *Internet Protocol Security* (biasa disingkat menjadi IPSec). VPN merupakan perpaduan antara teknologi *tunneling* dan enkripsi.

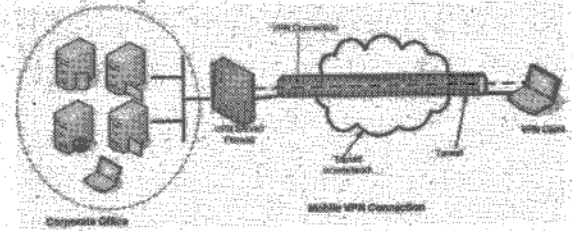
Untuk lebih memperdalam pengetahuanmu, pada pembelajaran ini kita akan membahas lebih dalam tentang VPN server. Untuk itu, bersungguh-sungguhlah dalam memahami materi berikut ini dengan saksama kamu lebih mudah memahami materi dan pengetahuan semakin bertambah.



A. Mengenal VPN Server

1. Pengertian VPN Server

VPN (*Virtual Private Network*) identik dengan sebuah teknologi yang memungkinkan dapat mengakses jaringan lokal melalui internet dengan teknologi *tunneling* sebagai koneksi *private* melalui *public* dengan mobilitas tinggi. Dengan VPN dapat membuat jaringan di dalam jaringan yang biasa disebut *tunnel*. Beberapa *software* dan teknik untuk membuat koneksi VPN, di antaranya PPTP dan OpenVPN. Penggunaan PPTP lebih praktis dan tidak memerlukan *software* khusus yang di-*install* di *client* tetapi kurang *secure*, karena enkripsi untuk koneksinya masih belum memadai. Sedangkan OpenVPN merupakan *software* untuk melakukan koneksi ke server VPN yang akan dienkripsi sedemikian rupa menggunakan *certificate* dan *key* yang berbeda untuk setiap *user*, sehingga keamanannya bisa dijamin. Selain proses konfigurasi yang agak panjang, OpenVPN memerlukan *software* khusus yang harus di-*install* di PC *client*, yaitu OpenVPN *client*.



Sumber: <https://idcloudhost.com>, diakses 8 Oktober 2018; 10.46 WIB

Gambar 5.2 VPN server

2. Fungsi Virtual Private Network (VPN)

Beberapa fungsi VPN antara lain sebagai berikut.

a. Menghubungkan Kantor-Kantor Cabang melalui Jaringan Publik

Perusahaan yang sudah menggunakan VPN, maka tidak perlu membangun jaringan sendiri. Perusahaan cukup terhubung dengan jaringan publik seperti internet, sebab hampir semua kantor perusahaan pasti memiliki akses internet. Dengan demikian, dapat menghemat anggaran koneksi untuk ke kantor cabang.

b. Mobile Working/Bekerja secara Remote

Perusahaan yang sudah menggunakan VPN, maka pegawai dapat terhubung langsung dengan jaringan kantor secara *private*. Setiap pegawai dapat melakukan pekerjaan yang biasa dilakukan dari depan komputer tanpa harus berada di kantor. Hal ini menjadi solusi *virtual office* di zaman mobilitas tinggi seperti sekarang.

c. Securing Your Network/Keamanan Jaringan

Saat ini beberapa vendor seperti Telkom memberikan solusi VPN untuk perusahaan-perusahaan. Namun solusi ini masih kurang aman, karena untuk terhubung dalam jaringan tidak memerlukan autentikasi. Sehingga, bila ada pengguna yang mengetahui setting VPN perusahaan tersebut maka dia dapat terhubung ke jaringan perusahaan tapi harus *login*. Misalnya pada telkomsel VPN hanya dengan mengganti nama VPN pada settingan *network* maka dia dapat langsung terhubung dengan jaringan dengan nama VPN tersebut. Dengan memasang VPN lagi di jaringan VPN semi publik tersebut maka jaringan akan lebih aman karena sebelum masuk jaringan kantor maka *user* harus membuat *tunnel* dulu dan *login* ke VPN server baru dapat terhubung dengan jaringan kantor.

d. Mengamankan Jaringan Wireless

Jaringan *wireless* merupakan jaringan publik yang dapat diakses oleh siapa saja yang berada di jangkauan *wireless* tersebut. Walaupun *wireless* juga memiliki pengamanan seperti WEP, WPA, dan WPA2 namun jaringan *wireless* masih saja dapat ditembus. Dengan menggunakan VPN maka *user* yang terhubung ke *wireless* harus membuat *tunnel* dulu dengan *login* ke VPN server baru dapat menggunakan *resource* jaringan seperti akses internet dan sebagainya.

3. Solusi Virtual Private Network

Beberapa solusi yang ada saat ini, solusi VPN dengan SSL merupakan yang paling banyak digunakan dengan OpenVPN sebagai aplikasinya. Selain gratis karena *open source* juga memiliki kemudahan dalam implementasi serta bersifat *multiplatform* dapat dijalankan pada Linux ataupun Windows. Beberapa solusi VPN yaitu sebagai berikut.



a. **IPSEC sebagai Solusi VPN via IP Secure Protocol**

Solusi yang sudah distandarisasi tapi paling susah dikonfigurasi. Tingkat keamanan yang cukup baik namun dalam implementasinya cukup rumit. Aplikasi yang digunakan yang berbasis *open source*, yaitu *Open/Free Swan*.

b. **PPPT sebagai Solusi VPN Versi Awal**

Solusi VPN dengan *feature* standar dimana jaringan dibangun dengan *point to point* seperti halnya anda melakukan *dial up* pada internet di rumah. Pada saat *dial up* ke *provider* internet ada maka akan dibangun *point to point tunnel* melalui jaringan telepon. Aplikasi *open source* yang menggunakan PPPT adalah *PopTop*.

c. **VPN with SSL**

VPN with SSL merupakan solusi VPN dengan menerapkan protocol *Secure Socket Layer (SSL)* pada enkripsi jaringan tunnel yang dibuat. Solusi ini diawali dengan aplikasi *OpenVPN*.

4. **Manfaat VPN (Virtual Private Network)**

Beberapa manfaat dari VPN (*Virtual Private Network*) sebagai berikut.

a. **Biaya lebih murah**

Pembangunan jaringan *leased line* khusus/pribadi memerlukan biaya yang sangat mahal. VPN dapat menjadi alternatif yang dapat digunakan untuk dapat mengatasi permasalahan tersebut. VPN dibangun dengan menggunakan jaringan internet milik publik tanpa perlu membangun jaringan pribadi. Dengan demikian, bila ingin menggunakan VPN hanya diperlukan koneksi internet.

b. **Fleksibilitas**

Sekarang ini internet semakin berkembang, dan makin banyak *user* yang menggunakannya membuat VPN juga ikut berkembang. Setiap *user* dapat tergabung dalam VPN yang telah dibangun tanpa terbatas jarak dan waktu. Fleksibilitas dapat dicapai apabila *user* tersebut terkoneksi dengan internet dan mendapat ijin menggunakan VPN.

c. **Kemudahan Pengaturan dan Administrasi**

Keseluruhan VPN dapat diatur dalam server VPN sendiri, dan untuk dapat digunakan oleh klien, maka perlu di-*install* aplikasi VPN pada klien. Hal ini tentu lebih mudah apabila dibandingkan dengan menggunakan *leased line* yang masih memonitor modem.

d. **Mengurangi Kerumitan Pengaturan dengan Teknologi Tunneling**

Tunneling (terowongan) merupakan kunci utama pada VPN. Koneksi pribadi dalam VPN dapat terjadi dimana saja selama terdapat *tunnel* yang menghubungkan pengirim dan penerima data. Dengan adanya *tunnel* ini, maka tidak diperlukan pengaturan-pengaturan lain yang ada di luar *tunnel* tersebut, asalkan sumber dari *tunnel* tersebut dapat menjangkau tujuannya.

5. **Implementasi VPN (Virtual Private Network)**

Beberapa implementasi dari VPN (*Virtual Private Network*) sebagai berikut.

a. **Intranet VPN**

Intranet merupakan koneksi VPN yang membuka jalur komunikasi pribadi menuju ke jaringan lokal yang bersifat pribadi melalui jaringan publik seperti internet. Melalui VPN jenis ini, *user* dapat langsung mengakses *file-file* kerja dengan leluasa tanpa terikat tempat dan waktu. Apabila dianalogikan pada sebuah perusahaan, koneksi ke kantor pusat dapat dilakukan dari mana saja, dari kantor pusat menuju ke kantor cabang dapat pula dibuat jalur komunikasi pribadi yang ekonomis.



b. Ekstranet VPN

Ekstranet VPN merupakan fasilitas VPN yang diperuntukkan bagi pihak-pihak dari luar anggota organisasi atau perusahaan, tetapi masih memiliki hak dan kepentingan untuk dapat mengakses data dalam kantor. Pada umumnya, *user* dari VPN dari jenis ini merupakan *customer*, *vendor*, *partner*, dan *supplier* dari suatu perusahaan.

c. Model Remote Access VPN

VPN merupakan sebuah proses *remote access* yang bertujuan mendapatkan koneksi ke jaringan *private* tujuannya. Proses *remote access* VPN tersebut dibedakan menjadi dua jenis berdasarkan oleh siapa proses *remote access* VPN tersebut dilakukan. Kedua jenis tersebut sebagai berikut.

1) Client-Initiated

Client-initiated merupakan pihak klien yang berinisiatif untuk melakukan sesuatu. Pada VPN jenis ini, ketika sebuah komputer ingin membangun koneksi VPN maka PC tersebut berusaha membangun *tunnel* dan melakukan proses enkripsi hingga mencapai tujuannya dengan aman. Namun, proses ini tetap mengandalkan jasa dari jaringan *Internet Service Provider* (ISP) yang dapat digunakan untuk umum. *Client-initiated* digunakan oleh komputer-komputer umum dengan mengandalkan *VPN server* atau *VPN concentrator* pada jaringan tujuannya.

2) Network Access Server-initiated

VPN merupakan jenis *network access server-initiated* ini tidak mengharuskan client untuk membuat *tunnel* dan melakukan enkripsi dan deskripsi sendiri berbeda dengan *client-initiated*. VPN jenis ini hanya mengharuskan *user* melakukan *dial-in* ke *Network Access Server* (NAS) dari ISP. Kemudian, NAS tersebut yang membangun *tunnel* menuju ke jaringan *private* yang dituju oleh klien tersebut. Dengan demikian, koneksi VPN dapat dibangun dan dipergunakan oleh banyak klien dari manapun, karena pada umumnya NAS milik ISP tersebut memang dibuka untuk umum. (Sumber: Patwiyanto, Sri Wahyuni, Sumari Agus Prasetyo, 2018)

Kegiatan 5.1

A. Judul Kegiatan : Menganalisis tentang VPN Server

B. Jenis Kegiatan : Kerja Mandiri

C. Tujuan Kegiatan : 1) Peserta didik dapat menjelaskan tentang VPN server dengan tepat. (KD 3)
2) Peserta didik dapat mengimplementasikan penerapan VPN server dalam kehidupan sehari-hari dengan terampil. (KD 4)

D. Langkah-Langkah Kegiatan:

1. Baca dan cermati cuplikan artikel tentang VPN server berikut ini!

Pengertian VPN, Manfaat, dan Cara Kerja VPN

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan local. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada di dalam LAN itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik.

Dari cara pandang jaringan, salah satu masalah jaringan internet (*IP public*) adalah tidak mempunyai dukungan yang baik terhadap keamanan. Sedangkan dari cara pandang perusahaan, IP adalah kebutuhan dasar untuk melakukan pertukaran data antara kantor cabang atau dengan rekanan perusahaan. VPN muncul untuk mengatasi persoalan tersebut. Sebuah jaringan perusahaan yang menggunakan infrastruktur IP untuk berhubungan dengan kantor cabangnya dengan cara pengalamatan secara *private* dengan melakukan pengamanan terhadap transmisi paket data.

Dikutip dari: <https://idcloudhost.com/panduan/pengertian-vpn-manfaat-dan-cara-kerja-vpn/>, diakses 27 September 2018; 10.00 WIB

Hasil Pengamatan:

2. Kumpulkanlah beberapa informasi tentang VPN server dari berbagai sumber yang dianggap relevan!

Hasil informasi yang diperoleh:

3. Lakukanlah analisis tentang VPN server meliputi:

- pengertian VPN server,
- fungsi VPN server,
- manfaat VPN server,
- cara kerja VPN server,
- kelebihan dan kekurangan *dedicated server*.

Hasil analisis:

-
-
-
-
-

4. Coba implementasikan penerapan VPN server dalam kehidupan sehari-hari! Kemudian buatlah laporan dari hasil percobaan yang telah kamu lakukan!

Hasil Percobaan:

Hasil Laporan:

5. Setelah selesai membuat laporan, kemukakan hasilnya secara lisan di hadapan guru dan temanmu sekelas! Jika ada tanggapan dan pertanyaan dari guru dan teman sekelas, tanggapilah secara responsif!

Tanggapan:

Permasalahan dan Penyelesaian

Permasalahan 5.1:

VPN adalah singkatan dari "Virtual Private Network", merupakan suatu koneksi antara satu jaringan dengan jaringan lain secara pribadi melalui jaringan Internet (publik). Disebut dengan *Virtual Network* karena VPN menggunakan jaringan Internet sebagai media perantaranya alias koneksinya bukan secara langsung. Dan disebut *Private Network* karena VPN bersifat pribadi maksudnya hanya orang tertentu saja yang dapat mengaksesnya. Ada 3 jenis jaringan dari VPN yaitu intranet VPN, ekstranet VPN dan remote VPN? Apa perbedaan intranet VPN, ekstranet dan remote VPN?

Penyelesaian:

Ada 3 jenis jaringan antara lain:

Intranet adalah sebuah jaringan lokal yang dikhususkan kepada anggota suatu organisasi. Intranet bersifat *private* dan terjaga, di mana orang di luar organisasi tidak dapat mengaksesnya. Intranet berfungsi untuk

mempermudah anggota organisasi untuk membuat konten, berkomunikasi, berkolaborasi, *manage* tugas dan membangun kultur di dalam organisasi.

Ekstranet pada dasarnya adalah intranet yang memiliki jaringan "ekstra" di mana didalam ekstranet, suatu organisasi dapat berkomunikasi secara *private* dengan individu-individu penting di luar organisasi (*Client*, *Produsen*, *Partner*, *Vendor*, dll). Ekstranet sangat penting bagi suatu organisasi/perusahaan karena ekstranet dapat menyederhanakan proses bisnis, meningkatkan kepuasan konsumen dan dapat meningkatkan keamanan. *Vitual Private Network* (VPN) seperti namanya memiliki definisi yaitu sebuah jaringan *private virtual*. Dimana "virtual" memiliki arti bahwa jaringan *private* yang digunakan tidak memiliki bentuk fisik di dunia nyata sehingga VPN dapat digunakan untuk dikolaborasikan dengan jaringan-jaringan lainnya seperti ekstranet. Ketika kita menggunakan VPN saat mengakses internet, komputer kita bertindak seolah-olah berada di satu jaringan lokal yang sama dengan VPN tersebut. VPN dapat digunakan untuk melewati batas geografis suatu jaringan, dimana itu dapat menguntungkan apabila kita ingin mengakses hal-hal yang diblokir di daerah geografis kita. VPN juga dapat memberi keamanan lebih kepada kita karena pada saat kita menggunakan VPN, akses kita terenkripsi sehingga lebih sulit untuk dilacak.

Bagaimana pendapatmu (minimal 10 kata):

Apa alasannya (minimal 20 kata):

Permasalahan 5.2:

Pada umumnya implementasi VPN terdiri dari 2 macam. Pertama adalah *remote access* VPN, dan yang kedua adalah *site-to-site* VPN. *Remote access* yang biasa juga disebut *virtual private dial-up network* (VPDN), menghubungkan antara pengguna yang *mobile* dengan *local area network* (LAN). Berikan penjelasan tentang implementasi *remote access* VPN dan *site-to-site* VPN!

Penyelesaian:

Jenis VPN *remote access* digunakan oleh pegawai perusahaan yang ingin terhubung ke jaringan khusus perusahaannya dari berbagai lokasi yang jauh (*remote*) dari perusahaannya. Biasanya perusahaan yang ingin membuat jaringan VPN tipe ini akan bekerja sama dengan *enterprise service provider* (ESP). ESP akan memberikan suatu *network access server* (NAS) bagi perusahaan tersebut. ESP juga akan menyediakan *software* klien untuk komputer-komputer yang digunakan pegawai perusahaan tersebut. Untuk mengakses jaringan lokal perusahaan, pegawai tersebut harus terhubung ke NAS dengan *men-dial* nomor telepon yang sudah ditentukan. Kemudian dengan menggunakan *software* klien, pegawai tersebut dapat terhubung ke jaringan lokal perusahaan. Perusahaan yang memiliki pegawai yang ada di lapangan dalam jumlah besar dapat menggunakan *remote access* VPN untuk membangun WAN. VPN tipe ini akan memberikan keamanan, dengan mengenkripsi koneksi antara jaringan lokal perusahaan dengan pegawainya yang ada di lapangan. Pihak ketiga yang melakukan enkripsi ini adalah ISP.

Jenis implementasi VPN yang kedua adalah *site-to-site* VPN. Implementasi jenis ini menghubungkan antara 2 kantor atau lebih yang letaknya berjauhan, baik kantor yang dimiliki perusahaan itu sendiri maupun kantor perusahaan mitra kerjanya. VPN yang digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja, *supplier* atau pelanggan) disebut ekstranet. Sedangkan bila VPN digunakan untuk menghubungkan kantor pusat dengan kantor cabang, implementasi ini termasuk jenis intranet *site-to-site* VPN.

Bagaimana pendapatmu (minimal 10 kata):

Apa alasannya (minimal 20 kata):

B. Konfigurasi VPN Server (PPTP)

VPN merupakan server membutuhkan jaringan yang mengarah ke jaringan internet. Untuk jaringan internet, VPN server pun harus menggunakan *IP public* agar bisa diakses dari mana saja, tetapi untuk skala lokal dapat menggunakan *IP local* atau *private IP*. Sebuah VPN diciptakan untuk membangun koneksi *point-to-point* melalui penggunaan koneksi berdedikasi, protokol *tunneling* virtual, atau enkripsi lalu lintas data. PPTP (*Point-To-Point Protocol*) adalah metode untuk menerapkan jaringan pribadi virtual dengan menggunakan saluran kontrol atas TCP dan *tunnel* (terowongan) operasi GRE untuk merangkum paket PPP. Tujuan penggunaan protokol ini adalah untuk memberikan tingkat keamanan dan tingkat akses *remote* sebanding dengan produk khas VPN.

1. Langkah Konfigurasi

Konfigurasi untuk membuat VPN server dengan menggunakan PPTP dengan langkah-langkah sebagai berikut.

- a. Langkah pertama kali diawali dengan memberikan perintah sebagai berikut.

```
# apt-get install pptpd
```

Pada pertanyaan "*Do you want to continue? [Y/n]*", ketik huruf "Y" dan akhiri dengan menekan tombol *Enter*. Selanjutnya tunggu proses instalasi tahap pertama hingga selesai dengan baik.

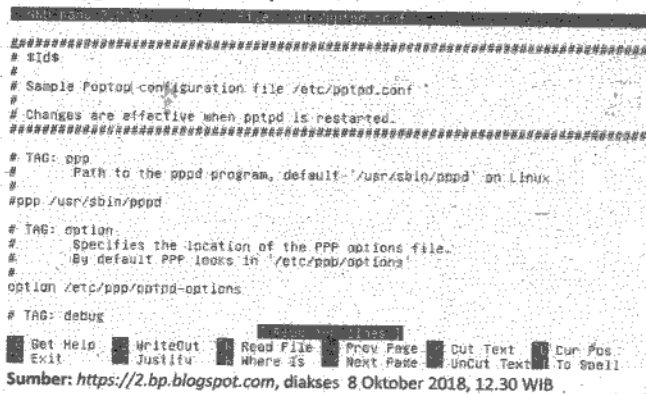
- b. Setelah proses instalasi awal selesai, pada tahap selanjutnya melakukan konfigurasi VPN dengan 3 buah *file* yang disediakan oleh Debian yaitu *file /etc/pptpd.conf*, *file /etc/ppp/pptpd-options*, dan *file /etc/ppp/chap-secrets*.

1) Konfigurasi *file /etc/pptpd.conf*

Konfigurasi *file /etc/pptpd.conf* dilakukan dengan memasukkan perintah:

```
# nano /etc/pptpd.conf
```

Sehingga muncul tampilan berikut.



```
#####
#
# Sample Poptod configuration file /etc/pptpd.conf
#
# Changes are effective when pptpd is restarted.
#####
# TAG: ppp
# Path to the pppd program, default '/usr/sbin/pppd' on Linux
#
#ppp /usr/sbin/pppd
#
# TAG: option
# Specifies the location of the PPP options file.
# By default PPP looks in '/etc/ppp/options'
#
option /etc/ppp/pptpd-options
#
# TAG: debug
#####
Get Help WriteOut Read File Prev Page Cut Text Cur Pos
Exit Justify Where Is Next Page UnCut Text To Spell
Sumber: https://2.bp.blogspot.com, diakses 8 Oktober 2018, 12.30 WIB
```

Gambar 5.3 Konfigurasi *file*

Pada bagian *localip* dan *remoteip* diganti sesuai dengan *IP address* komputer server yang digunakan. Maka di bagian paling bawah dari *file* konfigurasi, masukkan beberapa perintah sebagai berikut.

```
localip 192.168.100.2
remoteip 192.168.100.3-238,192.168.0.245
```

Perhatikan tampilan *text editor* nano sebagai berikut.

```
#####
#
# you must type 234-238 if you mean this.
#
# 4. If you give a single localIP, that's ok - all local IPs will
# be set to the given one. You MUST still give at least one remote
# IP for each simultaneous client.
#
# (Recommended)
#
#localip 192.168.100.2
#remoteip 192.168.100.3-238,192.168.0.245
#
# or
#localip 192.168.0.234-238,192.168.0.245
#remoteip 192.168.1.234-238,192.168.1.245
#####

Get Help WriteOut Read File Prev Page Cut Text Cur Pos
Exit Justify Where Is Next Page UnCut Text To Spell
```

Sumber: <https://1.bp.blogspot.com>, diakses 8 Oktober 2018, 12.40 WIB

Gambar 5.4 Text editor nano

Selanjutnya simpan dengan menekan tombol kombinasi CTRL+X, lalu jawab dengan menekan tombol Y, dan akhiri dengan menekan tombol *Enter*.

2) Konfigurasi file */etc/ppp/pptpd-options*

Konfigurasi file */etc/ppp/pptpd-options* dilakukan dengan memasukkan perintah sebagai berikut.

```
# nano /etc/ppp/pptpd-options
```

Sehingga muncul tampilan sebagai berikut:

```
#####
#
#####
#
#####
# Sample Poptop PPP options file /etc/ppp/pptpd-options
# Options used by PPP when a connection arrives from a client.
# This file is pointed to by /etc/pptpd.conf option keyword.
# Changes are effective on the next connection. See "man pppd".
#
# You are expected to change this file to suit your system. As
# packaged, it requires PPP 2.4.2 and the kernel MPPE module.
#####
# Authentication
# Name of the local system for authentication purposes
# (must match the second field in /etc/ppp/chap-secrets entries)
name pptpd
# Optional: domain name to use for authentication
#####
Get Help WriteOut Read File Prev Page Cut Text Cur Pos
Exit Justify Where Is Next Page UnCut Text To Spell
```

Sumber: <https://2.bp.blogspot.com>, diakses 8 Oktober 2018, 12.50 WIB

Gambar 5.5 Tampilan konfigurasi file */etc/ppp/pptpd-options*

Pada bagian paling bawah dari *file* konfigurasi, lakukan pencarian pada bagian *ms-dns* dengan menghilangkan tanda # dan mengganti alamat dns baru. Format yang digunakan adalah "*ms-dns->ip address server*". Perintah yang digunakan dapat dituliskan sebagai berikut.

```
ms-dns 192.168.100.2
nobsdcomp
noipx
mtu 1490
mru 1490
```


Perhatikan tampilan *text editor nano* sebagai berikut.

```

# (needed on some networks with Windows 9x/ME/XP clients; see posting to
# postop-server on 14th April 2005 by Pawel Rokryka and followups,
# http://macr.theimgroup.com/?t=1113431784000&sr=1&w=2 )
noip
noipccomp

# turn off logging to stderr, since this may be redirected to /dev/
# which may trigger a loopback
nologfd

# put plugins here
# (putting them higher up may cause them to sent messages to the tty)

ms-dns 192.168.100.2
nobdcomp
noipx
mtu 1490
mtu 1490

Get Help WriteOut Read File Prev Page Cut Text Cur Pos
Exit Justify Where Is Next Page UnCut Text To Spell

```

Sumber: <https://3.bp.blogspot.com>, diakses 8 Oktober 2018, 13.00 WIB

Gambar 5.6 Tampilan *text editor nano*

Selanjutnya simpan dengan menekan tombol kombinasi CTRL+X, kemudian jawab dengan menekan tombol Y, dan akhiri dengan menekan tombol *Enter*.

3) Konfigurasi *file /etc/ppp/chap-secrets*

Konfigurasi *file /etc/ppp/chap-secrets* dilakukan dengan memasukkan perintah sebagai berikut.

```
# nano /etc/ppp/chap-secrets
```

Berbeda dengan dua konfigurasi sebelumnya, *file* konfigurasi jenis ini bertujuan membuat *username* dan *password* yang digunakan untuk login VPN client dengan Windows OS atau Linux OS. Beberapa format standar yang digunakan dengan acuan dasar sebagai berikut.

Tabel 5.1 Format Standard

No.	Format	Keterangan
1.	<i>Client</i>	nama <i>user</i>
2.	<i>Secret</i>	<i>password</i> dari <i>user</i>
3.	<i>IP address</i>	<i>IP address</i> komputer <i>server</i>

Pada bagian paling bawah dari konfigurasi diberikan kode format *aku [tab] * [tab] aku [tab] **, sehingga tampak sebagai berikut.

```

# Secrets for authentication using CHAP
# client      server      secret      IP addresses
aku *        aku *

```

Sumber: <https://2.bp.blogspot.com>, diakses 8 Oktober 2018, 13.10 WIB

Gambar 5.7 Tampilan kode format *aku [tab] * [tab] aku [tab] **

Selanjutnya simpan dengan menekan tombol kombinasi CTRL+X, lalu jawab dengan menekan tombol Y, dan akhiri dengan menekan tombol *Enter*.

- c. Setelah proses instalasi selesai, lakukan *restart service pptpd* dengan perintah sebagai berikut.

```
# service pptpd restart  
atau  
# /etc/init.d/pptpd restart
```

Hingga muncul pernyataan sebagai berikut.

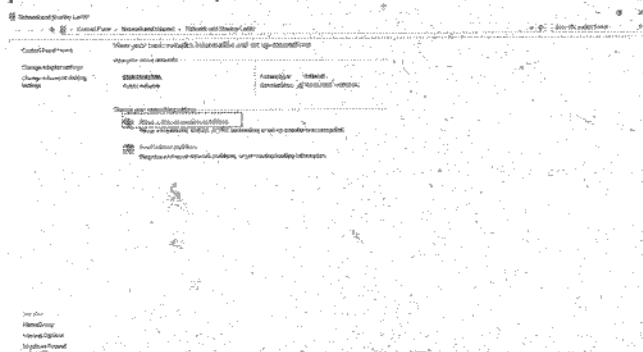
```
[ok] restarting pptpd (via systemctl): pptpd.service.
```

Tunggu hingga proses *restart* berjalan dengan baik.

2. Langkah Uji Coba

Setelah proses instalasi dan konfigurasi VPN server selesai, dilanjutkan dengan melakukan pengujian VPN server dengan VPN client, misalnya menggunakan sistem operasi Windows 10. Langkah-langkahnya sebagai berikut.

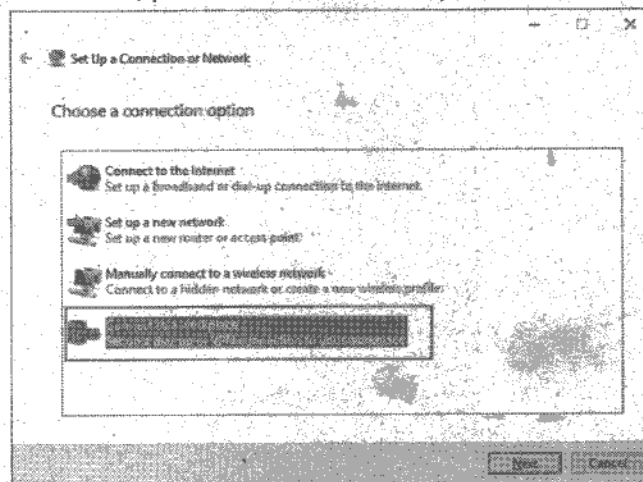
- Untuk membuat *network VPN client* dapat dilakukan melalui menu Control Panel. Langkah ini dilakukan dengan cara menekan *Windows+R* lalu ketikkan *Control Panel*.
- Kemudian pilih "*Network and Internet*" → klik "*Network and Sharing Center*" → dan selanjutnya pilih menu "*Set Up New Connections or Network*"



Sumber: <https://4.bp.blogspot.com>, diakses 8 Oktober 2018, 14.00 WIB

Gambar 5.7 Tampilan *Set Up New Connections or Network*

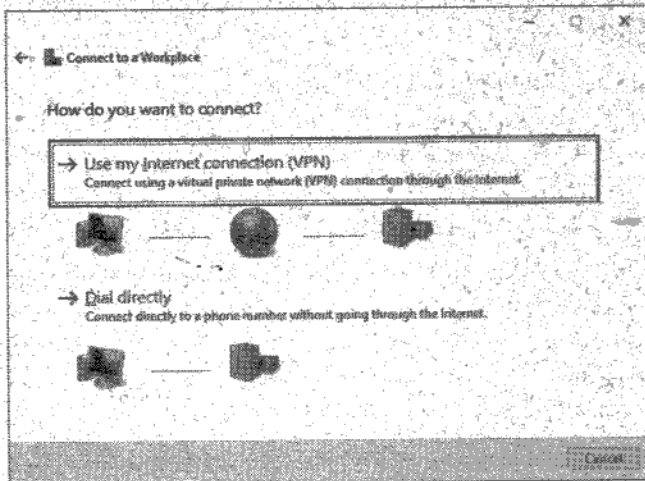
- Setelah itu, pilih "*Connect to a Workplace*".



Sumber: <https://2.bp.blogspot.com>, diakses 8 Oktober 2018, 14.10 WIB

Gambar 5.8 Tampilan *Connect to a Workplace*

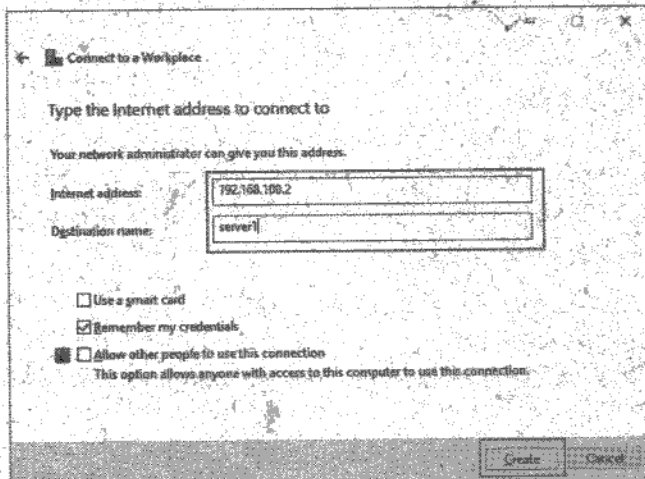
d. Pilih "Use My Internet Connections".



Sumber: <https://4.bp.blogspot.com>, diakses 8 Oktober 2018, 14.20 WIB

Gambar 5.9 Tampilan Use My Internet Connections

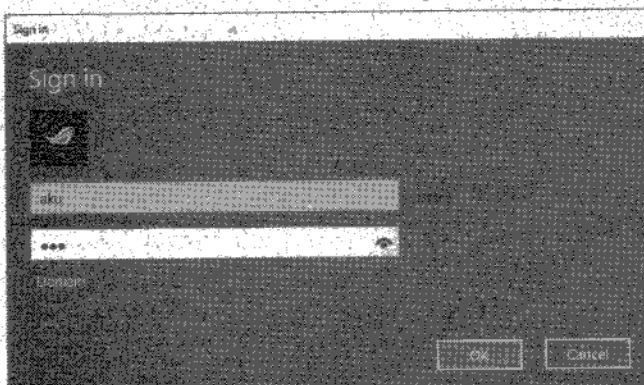
e. Setelah itu, dalam menu *Internet Address*, masukkan *IP server* atau *DNS server* setelah diisi, kemudian klik *Create*.



Sumber: <https://2.bp.blogspot.com>, diakses 8 Oktober 2018, 14.30 WIB

Gambar 5.10 Memasukkan IP server

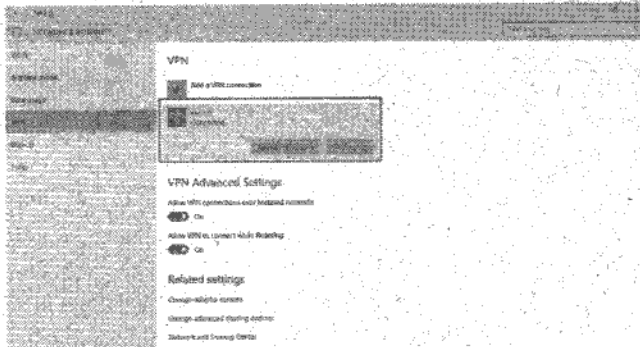
f. Masukkan *username* dan *password*-nya yang telah kita konfigurasi di server tadi, kemudian klik *OK*.



Sumber: <https://1.bp.blogspot.com>, diakses 8 Oktober 2018, 14.40 WIB

Gambar 5.11 Memasukkan username dan password

- g. Kemudian masuk pada proses verifikasi ke VPN server dan apabila komputer *client* sudah terhubung ke komputer server, maka pengujian VPN *Debian Server* telah berhasil.



Sumber: <https://1.bp.blogspot.com>, diakses 8 Oktober 2018, 14.50 WIB

Gambar 5.11 Komputer *client* sudah terhubung ke komputer *server*

(Sumber: Patwiyanto, Sri Wahyuni, Sumari Agus Prasetyo, 2018)

Kegiatan 5.2

- A. **Judul Kegiatan** : Memahami Konfigurasi VPN Server (PPTP)
- B. **Jenis Kegiatan** : Praktikum Kelompok
- C. **Tempat** : Laboratorium Komputer/Ruang Kelas
- D. **Tujuan Kegiatan** : 1) Peserta didik dapat mengetahui dan memahami cara melakukan konfigurasi VPN server (PPTP) dengan tepat. (KD 3)
2) Peserta didik dapat melakukan konfigurasi VPN server (PPTP) dengan terampil. (KD 4)
- E. **Alat dan Bahan**: Koneksi internet, laptop/PC, dan server.
- F. **Langkah-Langkah Praktikum**
1. Bentuklah kelompok regu dengan membagi jumlah peserta didik dalam kelasmu menjadi 5 kelompok. Lalu siapkan alat dan bahan yang diperlukan dalam melakukan konfigurasi VPN server (PPTP)!
 2. Setelah semua peralatan dan bahan siap, maka mulai melakukan praktik, meliputi:
 - a. Konfigurasi VPN server (PPTP).
 - b. Uji coba hasil instalasi dan konfigurasi VPN server (PPTP).
 3. Praktikkan langkah demi langkah dalam konfigurasi VPN server (PPTP) seperti pada pembahasan materi di atas dengan runtut!
 4. Setelah berhasil melakukan praktik di atas, selanjutnya buatlah laporan hasil kerja dalam kolom yang sudah disediakan di bawah ini!

G. **Laporan Praktikum**

.....

.....

.....



Permasalahan dan Penyelesaian

Permasalahan 5.3:

Teknologi jaringan VPN menggunakan internet sebagai media transmisi data ke tempat yang dituju. Oleh karena itu pengamanan transmisi data melalui internet menjadi hal yang sangat substansial untuk diperhatikan agar diperoleh komunikasi yang aman. Apa saja metode pengamanan data yang dapat dilakukan pada teknologi jaringan VPN?

Penyelesaian:

Beberapa metode pengamanan data yang dapat dilakukan pada teknologi jaringan VPN antara lain dengan menggunakan firewall. Pengamanan dapat juga dilakukan dengan melakukan enkripsi pada data yang akan dikirim melalui internet. Selain itu, data dapat juga dikirim menggunakan protokol khusus yang aman untuk transmisi data melalui internet (IPSec). Alternatif lain pengendalian keamanan jaringan VPN adalah dengan menggunakan metode AAA server yang akan memeriksa autentikasi, otorisasi, dan merekam segala sesuatu yang dilakukan pengguna pada suatu jaringan.

Bagaimana pendapatmu (minimal 10 kata):

.....

.....

Apa alasannya (minimal 20 kata):

.....

.....

Permasalahan 5.4:

PPTP merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari *remote client* (*client* yang berada jauh dari *server*) ke *server* pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP (Snader, 2005). Protokol ini dikembangkan oleh Microsoft dan Cisco. Teknologi jaringan PPTP merupakan pengembangan dari *remote access Point-to-Point protocol* yang dikeluarkan oleh *Internet Engineering Task Force* (IETF). PPTP merupakan protokol jaringan yang merubah paket PPP menjadi IP datagram agar dapat ditransmisikan melalui internet. PPTP juga dapat digunakan pada jaringan *private LAN-to-LAN*. PPTP terdapat sejak dalam sistem operasi Windows NT server dan Windows NT Workstation versi 4.0. Komputer yang berjalan dengan sistem operasi tersebut dapat menggunakan protokol PPTP dengan aman untuk terhubung dengan *private network* sebagai *client* dengan *remote access* melalui internet. PPTP juga dapat digunakan oleh komputer yang terhubung dengan LAN untuk membuat VPN melalui LAN. Fasilitas utama dari penggunaan PPTP adalah dapat digunakannya *public-switched telephone network* (PSTN) untuk membangun VPN. Pembangunan PPTP yang mudah dan berbiaya murah untuk digunakan secara luas menjadi solusi untuk *remote user* dan *mobile user*, karena PPTP memberikan keamanan dan enkripsi komunikasi melalui PSTN ataupun internet. Berikan contoh implementasi dari PPTP!

Penyelesaian:

PPTP merupakan *protocol* VPN pertama yang didukung oleh *Microsoft Dial-Up Networking*. Semua versi rilis *Microsoft Windows* sejak *Windows 95 OSR2* telah dilengkapi dengan aplikasi PPTP *client*, sedangkan PPTP server berada pada *Routing dan Remote Access Service* untuk *Microsoft Windows*. *Microsoft Windows Mobile* 2003 dan versi yang lebih tinggi juga telah didukung oleh *protocol* PPTP. PPTP yang mendukung *server-side* Linux disediakan oleh *PoPToP daemon*. *Mac OS X* (termasuk versi yang dinamakan ke iPhone) juga sudah dilengkapi dengan PPTP *client*. Begitu juga berbagai *gadget* dengan sistem operasi Android telah mendukung pemakaian PPTP dengan baik.

Bagaimana pendapatmu (minimal 10 kata):

.....

.....

Apa alasannya (minimal 20 kata):

.....

.....



HOTS (High Order Thinking Skills)

A. Pilihlah satu jawaban yang paling benar dengan cara memberi tanda silang (X) pada huruf A, B, C, D, atau E serta tuliskan alasannya!

1. PPTP (*Point-To-Point Protocol*) adalah metode untuk menerapkan jaringan pribadi virtual dengan menggunakan saluran kontrol atas TCP dan *tunnel* (terowongan) operasi GRE untuk merangkum paket PPP. Tujuan penggunaan protokol ini adalah untuk memberikan tingkat keamanan dan tingkat akses *remote* sebanding dengan produk khas VPN. Konfigurasi untuk membuat VPN server dengan menggunakan PPTP langkah pertama kali diawali dengan memberikan perintah: `# apt-get install pptpd`. Langkah selanjutnya yang harus dilakukan adalah
 - A. selanjutnya akan muncul pernyataan "*Do you want to continue? [Y/n]*", ketik huruf "n" dan akhiri dengan menekan tombol *Enter*. Kemudian tunggu proses instalasi tahap pertama hingga selesai dengan baik
 - B. selanjutnya akan muncul pernyataan "*Do you want to continue? [Y/n]*", ketik huruf "Y" dan akhiri dengan menekan tombol *Enter*. Kemudian tunggu proses instalasi tahap pertama hingga selesai dengan baik
 - C. selanjutnya akan muncul pernyataan "*Do you want to continue? [Y/n]*", ketik huruf "n" dan akhiri dengan menekan tombol *Enter*
 - D. selanjutnya akan muncul pernyataan "*Do you want to continue? [Y/n]*", ketik huruf "Y" dan akhiri dengan menekan tombol *Enter*
 - E. semua jawaban salah

Alasan:

2. Setelah proses instalasi awal selesai, pada tahap selanjutnya melakukan konfigurasi VPN dengan 3 buah *file* yang disediakan oleh Debian yaitu *file /etc/pptpd.conf*, *file /etc/ppp/pptpd-options*, dan *file /etc/ppp/chap-secrets*. Konfigurasi *file /etc/pptpd.conf* dilakukan dengan memasukkan perintah: `# nano /etc/pptpd.conf`. Pada bagian *localip* dan *remoteip* diganti sesuai dengan *IP address* komputer *server* yang digunakan. Maka di bagian paling bawah dari *file* konfigurasi, masukkan beberapa perintah *localip* 192.168.100.2 dan *remoteip* 192.168.100.3-238, 192.168.0.245. Setelah mengikuti langkah tersebut, langkah selanjutnya yang harus dilakukan adalah
 - A. selanjutnya simpan dengan menekan tombol kombinasi CTRL+X, jawab dengan menekan tombol Y, dan akhiri dengan menekan tombol *Enter*
 - B. selanjutnya simpan dengan menekan tombol kombinasi CTRL+X, jawab dengan menekan tombol n, dan akhiri dengan menekan tombol *Enter*
 - C. selanjutnya simpan dengan menekan tombol kombinasi CTRL+S, jawab dengan menekan tombol Y, dan akhiri dengan menekan tombol *Enter*
 - D. selanjutnya simpan dengan menekan tombol kombinasi CTRL+S, jawab dengan menekan tombol n, dan akhiri dengan menekan tombol *Enter*
 - E. semua jawaban salah

Alasan:

3. Konfigurasi *file /etc/ppp/pptpd-options* dilakukan dengan memasukkan perintah: `# nano /etc/ppp/pptpd-options`. Pada bagian paling bawah dari *file* konfigurasi, lakukan pencarian pada bagian *ms-dns* dengan menghilangkan tanda # dan mengganti alamat dns baru. Format yang digunakan adalah "*ms-dns-->ip address server*". Dengan demikian, perintah yang digunakan adalah
 - A. `localip 192.168.100.2`
`remoteip 192.168.100.3-238,192.168.0.245`
 - B. `ms-dns 192.168.100.2`
`nobsdcomp`
`noipx`
`mtu 1490`
`mru 1490`



- C. # nano /etc/ppp/chap-secrets
- D. # service pptpd restart atau # /etc/init.d/pptpd restart
- E. semua jawaban salah

Alasan:

4. Konfigurasi file */etc/ppp/chap-secrets* dilakukan dengan memasukkan perintah: # nano /etc/ppp/chap-secrets. Pada bagian paling bawah dari konfigurasi diberikan kode format *aku [tab] * [tab] aku [tab]* *. Selanjutnya simpan dengan menekan tombol kombinasi CTRL+X, jawab dengan menekan tombol Y, dan akhiri dengan menekan tombol *Enter*. Setelah proses instalasi selesai, lakukan *restart service pptpd*. Perintah yang digunakan untuk melakukan *restart service pptpd* adalah

- A. # service pptpd restart
- B. # /etc/init.d/pptpd restart
- C. # restarting pptpd
- D. jawaban a dan b benar
- E. semua jawaban benar

Alasan:

5. Masih berkaitan dengan soal nomor 4 di atas, setelah melakukan *restart service pptpd*, maka pernyataan yang akan muncul adalah

- A. muncul pernyataan: [ok] restarting pptpd
- B. muncul pernyataan: [ok] via systemctl): pptpd.service
- C. muncul pernyataan: [ok] restarting pptpd (via systemctl): pptpd.service
- D. muncul pernyataan: [ok] pptpd.service (via systemctl): restarting pptpd
- E. semua jawaban salah

Alasan:

B. Jawablah pertanyaan berikut dengan tepat!

1. VPN (*Virtual Private Network*) identik dengan sebuah teknologi yang memungkinkan dapat mengakses jaringan lokal melalui internet dengan teknologi *tunneling* sebagai koneksi *private* melalui *public* dengan mobilitas tinggi. Dengan VPN kita dapat membuat jaringan di dalam jaringan yang biasa disebut sebagai *tunnel*. Tuliskan yang kamu ketahui tentang fungsi VPN!

Jawaban:

2. Beberapa solusi yang ada saat ini, solusi VPN dengan SSL merupakan yang paling banyak digunakan dengan OpenVPN sebagai aplikasinya. Selain gratis karena *open source* juga memiliki kemudahan dalam implementasi serta bersifat *multiplatform* dapat dijalankan pada Linux ataupun Windows. Sebutkan dan berikan penjelasan tentang solusi VPN yang kamu ketahui!

Jawaban:

3. Selain fungsi dan solusi, tentang VPN juga mempunyai manfaat tersendiri. Sebutkan dan jelaskan yang kamu ketahui tentang manfaat VPN!

Jawaban:

4. Uraikan yang kamu ketahui tentang langkah-langkah konfigurasi untuk membuat VPN server dengan menggunakan PPTP!

Jawaban:

5. Uraikan yang kamu ketahui tentang langkah-langkah pengujian hasil pembuatan VPN server dengan VPN client menggunakan sistem operasi Windows yang kamu miliki!

Jawaban:



Studi Kasus

I. Baca dan pahami teks berikut!

Virtual Private Network

VPN merupakan singkatan dari *Virtual Private Network*, yaitu sebuah koneksi *private* melalui jaringan publik (dalam hal ini internet). Ada 2 kata yang dapat kita garis bawah yaitu:

1. *Virtual network*, yang berarti jaringan yang terjadi hanya bersifat virtual. Tidak ada koneksi jaringan secara riil antara 2 titik yang akan berhubungan.
2. *Private*, jaringan yang terbentuk bersifat *private* dimana tidak semua orang bisa mengaksesnya. Data yang dikirimkan terenkripsi sehingga tetap rahasia meskipun melalui jaringan publik.

Dengan VPN ini kita seolah-olah membuat jaringan di dalam jaringan atau biasa disebut *tunnel* (terowongan). *Tunneling* adalah suatu cara membuat jalur privat dengan menggunakan infrastruktur pihak ketiga. VPN menggunakan salah satu dari tiga teknologi *tunneling* yang ada yaitu: PPTP, L2TP dan standar terbaru, *Internet Protocol Security* (biasa disingkat menjadi IPsec). VPN merupakan perpaduan antara teknologi *tunneling* dan enkripsi.

Gambar di samping adalah gambaran tentang koneksi VPN yang menggunakan protokol PPTP. PPTP (*Pont to Point Tunneling Protocol*) adalah sebuah protokol yang mengizinkan hubungan *Point-to Point Protocol* (PPP) melewati jaringan IP, dengan membuat *Virtual Private Network* (VPN).

Disarikan dari: http://ppg.spada.ristekdikti.go.id/pluginfile.php/5727/mod_resource/content/2/U/UM-TK12-KB3-PDF-.pdf, diakses 8 Oktober 2018

Dalam rangka memperdalam pemahamanmu mengenai materi VPN Server, kerjakan tugas berikut dengan menggunakan model pembelajaran *Discovery Learning*. Analisislah VPN Server yang telah kamu pelajari selama ini sesuai dengan teks di atas. Tuliskan hasil analisismu sesuai dengan tahapan berikut.

A. Rumusan Masalah

1.
2.

B. Kajian Pustaka

1.
2.

C. Pengumpulan Data dan Informasi

1.
2.

D. Analisis Data

1.
2.

E. Simpulan

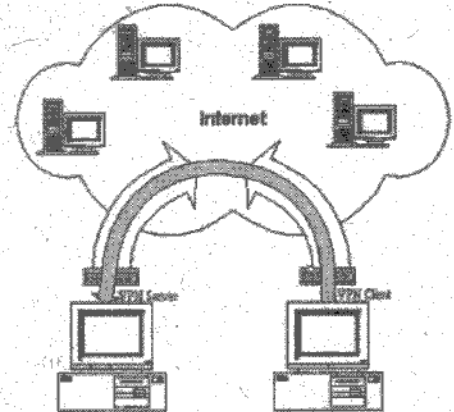
1.
2.

II. Cermati dan pahami teks berikut!

Cara Kerja VPN

Dari gambar di atas secara sederhana cara kerja VPN (dengan protokol PPTP) adalah sebagai berikut.

1. VPN membutuhkan sebuah server yang berfungsi sebagai penghubung antar PC, Server VPN ini bisa berupa komputer dengan aplikasi VPN Server atau sebuah Router, misalnya MikroTik RB 750.



Sumber: <http://3.bp.blogspot.com>, diakses 8 Oktober 2018, 15.30 WIB

Gambar 5.12 Koneksi VPN



2. Untuk memulai sebuah koneksi, komputer dengan aplikasi *VPN Client* mengontak *Server VPN*, *VPN Server* kemudian memverifikasi *username* dan *password* dan apabila berhasil maka *VPN Server* memberikan IP Address baru pada komputer *client* dan selanjutnya sebuah koneksi / *tunnel* akan terbentuk.
3. Untuk selanjutnya komputer *client* bisa digunakan untuk mengakses berbagai resource (komputer atau LAN) yang berada di belakang *VPN Server* misalnya melakukan transfer data, *print document*, *browsing* dengan *gateway* yang diberikan dari *VPN Server*, melakukan *remote desktop* dan lain sebagainya.

Disarikan dari: http://ppg-spada.ristekdikti.go.id/pluginfile.php/5727/mod_resource/content/2/UNM-TK12-KB3-PDF-.pdf, diakses 8 Oktober 2018

Teks di atas menjelaskan cara kerja VPN. Semua permasalahan yang sering terjadi pada VPN server akan dapat teratasi apabila mengetahui dan memahami prosedur dalam melakukan konfigurasi VPN server yang baik dan benar. Untuk mempertajam analisismu secara komprehensif mengenai VPN server seperti pada teks di atas, lakukan analisis masalah menggunakan model *Problem Based Learning* dengan melengkapi tahapan-tahapan berikut. Analisislah mengenai konfigurasi VPN server.

A. Rumusan Masalah

1.
2.

B. Aktivitas/Kegiatan Belajar untuk Menyelesaikan Masalah

No	Aktivitas Pembelajaran Penyelesaian Masalah	Hasil yang Dicapai
1.	Diskusi Kelompok	Simpulan hasil diskusi: 1. 2.
2.	Observasi	Hasil praktik: 1. 2.

C. Analisis Data

.....

.....

D. Simpulan Solusi Masalah secara Kelompok

.....

.....

III. Buatlah kelompok yang beranggotakan 4-5 orang! Bersama kelompokmu carilah informasi mengenai langkah-langkah melakukan konfigurasi VPN server! Setelah itu buatlah rancangan konfigurasi VPN server! Kerjakan tugas di bawah ini dengan menggunakan model *Project Based Learning*. Kemudian, lengkapilah langkah-langkah berikut.

- A. Judul Proyek:
- B. Jenis Tugas: Kelompok
- C. Jadwal Pelaksanaan

Tahapan	Tanggal Pelaksanaan	Jenis Kegiatan
1. Persiapan	1. Mencari referensi. 2. Mempersiapkan perlengkapan yang dibutuhkan. 3.

- A. *nature*
- B. *client*
- C. *secure*
- D. *tiap user*
- E. *enkripsi*

Alasan:

3. Kunci utama pada VPN adalah

- A. *tunneling*
- B. *publik*
- C. *labelling*
- D. *dial-in*
- E. *connecting*

Alasan:

4. Koneksi VPN yang membuka jalur komunikasi pribadi menuju ke jaringan lokal yang bersifat pribadi melalui jaringan publik disebut

- A. *ekstranet*
- B. *subnet*
- C. *data*
- D. *intranet*
- E. *private*

Alasan:

5. Pada VPN jenis *client-initiated*, ketika sebuah komputer ingin membangun koneksi VPN maka PC tersebut berusaha membangun *tunnel* dengan melakukan proses

- A. *deskripsi*
- B. *socket layer*
- C. *open source*
- D. *enkripsi*
- E. *IP secure protocol*

Alasan:

6. VPN jenis *network access server-initiated* hanya mengharuskan *user* melakukan *dial-in* ke *Network Access Server (NAS)* yang berasal dari

- A. *koneksi VPN*
- B. *ISP*
- C. *PPTP*
- D. *saluran kontrol*
- E. *operasi GRE*

Alasan:

7. Setelah memberikan perintah *apt-get install pptpd* maka akan muncul pertanyaan

- A. *Press any key to continue*
- B. *Do you want some help? [Y/n]*
- C. *Please save and continue*
- D. *Press CTRL+ALT+DEL to restart*
- E. *Do you want to continue? [Y/n]*

Alasan:

8. Untuk membuat *network VPN client* dapat dilakukan melalui menu

- A. *Network and Internet*
- B. *Network and Sharing Center*
- C. *Set Up New Connections or Network*
- D. *Connect to a Workplace*
- E. *Control Panel*

Alasan:

Perhatikan petunjuk berikut untuk dapat menyelesaikan soal nomor 9 dan 10!

Petunjuk:

- A. *Jika pernyataan benar, alasan benar, dan keduanya menunjukkan hubungan sebab-akibat.*
- B. *Jika pernyataan benar, alasan benar, tetapi keduanya tidak menunjukkan hubungan sebab-akibat.*
- C. *Jika pernyataan benar, alasan salah.*
- D. *Jika pernyataan salah, alasan benar.*
- E. *Jika pernyataan dan alasan salah.*

Pernyataan:

9. Perusahaan yang sudah menggunakan VPN, maka tidak perlu membangun jaringan sendiri. Perusahaan cukup terhubung dengan jaringan publik seperti internet.

Sebab

Hampir semua kantor perusahaan pasti memiliki akses internet. Dengan demikian dapat menghemat anggaran koneksi untuk ke cabang-cabang.

Jawaban:

Alasan:

10. Saat ini beberapa vendor seperti Telkom memberikan solusi VPN untuk perusahaan-perusahaan. Namun solusi ini masih kurang aman.

Sebab

Karena untuk terhubung tidak memerlukan autentikasi. Sehingga bila ada pengguna mengetahui settingan VPN perusahaan tersebut maka dia dapat terhubung ke jaringan perusahaan tapi harus *login*.

Jawaban:

Alasan:



Refleksi

Pada Bab V, peserta didik telah mempelajari tentang Mengevaluasi VPN Server. Materi yang telah dipahami maupun yang belum dipahami akan diberi tanda centang (✓) pada kolom di bawah ini. Peserta didik juga akan bertanya jika ada materi yang belum dipahami.

No.	Pernyataan	Keterangan	
		Paham	Belum Paham
1.	Menjelaskan dan memahami pengertian VPN server.
2.	Menjelaskan cara kerja VPN server.
3.	Melakukan konfigurasi VPN server.
4.	Menguji hasil konfigurasi VPN server.
....

Setelah mempelajari materi tentang mengevaluasi VPN server, kamu dapat mengambil refleksi sikap sebagai berikut.

1. Kritis dalam mengamati permasalahan-permasalahan nyata yang berkaitan dengan VPN server.
2.
3.
4.

Muatan Aktivitas Peserta Didik

(Berdasar Permendikbud Nomor 8 Tahun 2016)

A. Tugas Mandiri

1. Pelajarilah kembali materi tentang VTP server dengan saksama!
Hasil Pemahaman Materi:
.....
.....
2. Kumpulkanlah data informasi mengenai pengenalan VTP server beserta implementasinya!
Hasil Informasi yang Diperoleh:
.....
.....
3. Buatlah dalam bentuk makalah tentang pengenalan pengenalan VTP server beserta implementasinya di atas!
Hasil Makalah:
.....
.....
4. Susunlah makalah yang kamu buat ke dalam lembar kertas HVS ukuran A4 dengan spasi 1,5 serta cetak dengan menggunakan printer!
Hasil Penyusunan Makalah:
.....
.....
5. Serahkan tugas tersebut kepada gurumu dengan tepat waktu untuk mendapatkan penilaian!
Saya Mengumpulkan Tugas dengan:
.....
.....

B. Tugas Diskusi

1. Bentuklah kelompok yang beranggotakan 2-3 orang teman sekelasmu (terdiri atas laki-laki dan perempuan)!
Ketua kelompok :
Anggota I :
Anggota II :
2. Pelajarilah kembali materi tentang VPN server dengan saksama!
Hasil Pemahaman Materi:
.....
.....
3. Coba uraikan kembali informasi yang diperoleh tentang proses konfigurasi VPN server dan uji coba hasil konfigurasi VPN server!
Hasil Tugas:
.....
.....
4. Buatlah kesimpulan tentang masalah yang kamu hadapi dalam melakukan konfigurasi VPN server dan uji coba hasil konfigurasi VPN server, kemudian presentasikan!
Hasil Kesimpulan:
.....
.....
Hasil Presentasi:
.....
.....

C. Tugas Proyek

1. Bentuklah kelompok yang beranggotakan 2-3 orang teman sekelasmu (terdiri atas laki-laki dan perempuan)!
Ketua kelompok :
Anggota I :
Anggota II :
2. Setelah kelompok terbentuk, berdiskusilah untuk membuat perencanaan langkah-langkah pengujian VPN server dengan menggunakan VPN client pada sistem operasi Linux! Sumber-sumber data bisa diambil dari media cetak dan elektronik yang relevan.
Hasil Diskusi:
.....
.....
3. Siapkan alat dan bahan yang diperlukan untuk melakukan langkah-langkah pengujian VPN server dengan menggunakan VPN client pada sistem operasi Linux!
Alat :
Bahan :
Langkah Kerja:
a.
b.
c.
d. dst.

4. Lengkapilah konsep rancangan percobaan kalian dengan tabel rencana pelaksanaan proyek dan perkiraan waktunya!

Hasil Konsep Rancangan Percobaan:

.....

.....

5. Laksanakanlah percobaan berdasarkan konsep rancangan yang telah kamu buat!

Hasil Percobaan:

.....

.....

7. Kerjakan tugas ini dalam waktu satu minggu setelah guru memberikan perintah!

Saya Mengumpulkan Tugas dengan:

.....

.....

Interaksi Guru dan Orang Tua

Untuk mengisi form tabel interaksi guru dan orang tua, ikuti petunjuk gurumu!

Tabel 5.1 Form Interaksi Guru dan Orang Tua

Nama : NIS :

Kelas :

No.	Kompetensi	Keterangan Pencapaian Kompetensi			Paraf Guru	Paraf Orang Tua
		Baik	Cukup	Kurang		
1.	KI 1 Menghayati dan mengamalkan ajaran agama yang dianutnya.
2.	KI 2 Menghayati dan mengamalkan perilaku jujur, disiplin, santun, peduli (gotong royong, kerja sama, toleran, damai), bertanggung jawab, responsif, dan proaktif melalui keteladanan, pemberian nasehat, penguatan, pembiasaan, dan pengkondisian secara berkesinambungan serta menunjukkan sikap sebagai bagian dari solusi atas berbagai permasalahan dalam berinteraksi secara efektif dengan lingkungan sosial dan alam serta dalam menempatkan diri sebagai cerminan bangsa dalam pergaulan dunia.
3.	KD 3.14 Mengevaluasi VPN server.
4.	KD 4.14 Mengonfigurasi VPN server.

Keterangan: Berilah tanda centang (✓) sesuai dengan pencapaian kompetensi peserta didik.

