RENCANA PELAKSANAAN PEMBELAJARAN

Nama Sekolah	:	SMK Bhakti Praja Adiwerna
Kompetensi Keahlian	:	Teknik Komputer dan Jaringan
Mata Pelajaran	:	Administrasi Sistem Jaringan
Kelas / Semester	:	XII/ Gasal
Tahun Ajaran	:	2020/2021
Alokasi Waktu	:	6 x 45 Menit (1 x Pertemuan)

A. Kompetensi Inti

KI 3. Pengetahuan

Memahami, menerapkan, menganalisis, dan mengevaluasi tentang pengetahuan faktual, konseptual, operasional dasar, dan metakognitif sesuai dengan bidang dan lingkup kerja Teknik Komputer dan Jaringan pada tingkat teknis, spesifik, detil, dan kompleks, berkenaan dengan ilmu pengetahuan, teknologi, seni, budaya, dan humaniora dalam konteks pengembangan potensi diri sebagai bagian dari keluarga, sekolah, dunia kerja, warga masyarakat nasional, regional, dan internasional.

KI 4. Katerampilan

Melaksanakan tugas spesifik dengan menggunakan alat, informasi, dan prosedur kerja yang lazim dilakukan serta memecahkan masalah sesuai dengan bidang kerja Teknik Komputer dan Jaringan. Menampilkan kinerja di bawah bimbingan dengan mutu dan kuantitas yang terukur sesuai dengan standar kompetensi kerja.

Menunjukkan keterampilan menalar, mengolah, dan menyaji secara efektif, kreatif, produktif, kritis, mandiri, kolaboratif, komunikatif, dan solutif dalam ranah abstrak terkait dengan pengembangan dari yang dipelajarinya di sekolah, serta mampu melaksanakan tugas spesifik di bawah pengawasan langsung.

Menunjukkan keterampilan mempersepsi, kesiapan, meniru, membiasakan, gerak mahir, menjadikan gerak alami dalam ranah konkret terkait dengan pengembangan dari yang dipelajarinya di sekolah, serta mampu melaksanakan tugas spesifik di bawah pengawasan langsung.

B. Kopetensi Dasar dan Indikator Pencapaian Kopetensi

Kopetensi Dasar	**Indikator Pencapaian Kopetensi**
3.13 Mengevaluasi VPN Server	3.13.4 Menentukan cara konfigurasi *VPN Server*
4.13 Mengkonfigurasi VPN Server	4.13.1 Menguji hasil konfigurasi *VPN Server*

C. Tujuan Pembelajaran

1. Setelah berdiskusi dan menggali informasi, peserta didik akan dapat :
   a. Menganalisis penggunaan VPN Server dengan benar dan tepat
   b. Mengetahui cara konfigurasi VPN Server dengan benar dan tepat

D. Materi Pembelajaran

1. Konfigurasi VPN Server
2. Menguji hasil konfigurasi *VPN Server*

E. Pendekatan, Model dan Metode Pembelajaran

Pendekatan berfikir : Sientific learning
Strategi : Cooperatif Learning
Model Pembelajaran : Project Based Learning
Metode Pembelajaran : Diskusi dan tanya jawab online, Penugasan

F. Kegiatan Pembelajaran

Kegiatan	Langkah – langkah Pembejalaran	Alokasi Waktu
Kegiatan Pendahuluan	**Melalui Grub Kelas WhatsApp :** 1. Guru mengajak peserta didik bergabung di Grub Kelas WhatsApp 2. Guru mengucapkan salam 3. Guru menyapa kondisi peserta didik 4. Guru mengingatkan Peserta Didik untuk selalu mematuhi protokol kesehatan yang ada 5. Guru mengajak peserta didik untuk berdo'a sebelum memulai pembelajaran 6. Peserta didik diminta mengisi presensi hadir di Google Form 7. Guru mengulas materi sebelumnya mengenai cara konfigurasi VPN Server 8. Guru menyampaikan ke peserta didik materi yang akan dipelajari pada pertemuan ini mengenai Menguji hasil konfigurasi *VPN* Server 9. Guru menyampaikan tujuan pembelajaran	10 Menit
Kegiatan Inti	**Mengamati (Stimulation)**	
	Melalui Google Classroom • Guru 1. Mempresentasikan menguji hasil konfigurasi VPN Server melalui modul • Peserta didik 1. Secara mandiri membuka modul tentang menguji hasil konfigurasi VPN Server di Google Classroom	
	Menanya (Problem Statement)	
	Melalui Google Classroom 1. Membagi peserta didik menjadi beberapa kelompok 2. Memberikan pertanyaan terkait cara menguji hasil konfigurasi VPN Server	

	• Peserta didik 1. Menggali informasi dan menemukan mengenai cara menguji hasil konfigurasi VPN Server	40 Menit
	Mengeksplorasi (Data Collection)	
	Melalui Google Classroom • Guru 1. Mengamati Keaktifan peserta didik melalui kolom komentar pada materi yang dibagi di Google Classroom • Peserta didik 1. Menggali informasi mengenai menguji hasil konfigurasi VPN Server dari sumber internet, buku yang ada	
	Mengasosiasi (Verification)	
	Melalui Google Classroom • Guru 1. Mengamati Keaktifan peserta didik melalui kolom komentar pada materi yang dibagi di Google Classroom dan memberikan bimbingan serta arahan kepada peserta didik bila terjadi kesalahan 2. Bersama peserta didik berdiskusi menguji hasil konfigurasi VPN Server • Peserta didik 1. Berdiskusi dengan guru mengenai hasil Pekerjaan yang telah dilakukan 2. Menyampaikan hasil yang didapat dari mengeksplorasi menguji hasil konfigurasi VPN Server • Guru bersama peserta didik membuat kesimpulan dari pembelajaran yang dilakukan	
	Mengkomunikasikan (Generalization)	
	Melalui Google Classroom • Guru 1. Mengamati Keaktifan peserta didik dan memberikan penilaian kepada peserta didik • Peserta didik 1. Menyampaikan hasil mengeksplorasi menguji hasil konfigurasi VPN Server masing-masing kelompok di Google Classroom	
Penutup	**Melalui Grub Kelas WhatsApp :** 1. Guru memberikan penguatan terhadap materi yang telah dipelajari 2. Guru memberi motivasi kepada peserta didik untuk terus meningkatkan belajar 3. Guru menyampaikan agenda kegiatan dipertemuan berikutnya mengenai membuat laporan konfigurasi *VPN Server*	10 Menit

	4. Guru meminta salah satu siswa memimpin do'a penutup	

G. Penilaian Hasil Pembelajaran

1. Teknik Penilaian

No.	Aspek yang dinilai	Teknik Penilaian	Bentuk Penilaian	Waktu Penilaian
1.	Pengetahuan	Tertulis	Tes Tertulis dan pilihan ganda Melalui Google Classroom	Saat pembelajaran
2.	Keterampilan	Penugasan	Lembar penilaian tugas/ presentasi dan rubrik	Saat pembelajaran/ Setelah pembelajaran
3.	Sikap	Penilaian diri/Observasi	Lembar pengamatan dan observasi	Saat pembelajaran/ Setelah pembelajaran

H. Rencana Tindak Lanjut Hasil Penilaian

1. Analisis Hasil Penilaian
   - Analisis hasil penilaian diadakan setelah diadakan tes formatif
   - Hasil analisis penilaian menentukan perlu tidaknya diadakan remedial atau pengayaan
2. Pembelajaran Remedial dan Pengayaan
   - Bagi peserta didik yang memperoleh nilai kurang dari 75 diadakan remedi.
   - Apabila jumlah peserta didik yang remidi 75% atau lebih maka diadakan pembelajaran remedial.
   - Bagi peserta didik yang memperoleh nilai 75 atau lebih maka diadakan pengayaan.

I. Media, Bahan dan Sumber Pembelajaran

1. Media
   a. Power Point
   b. Google Classroom
   c. Google Form
   d. WhatsApp
   e. Youtube
2. Alat/Bahan
   a. Laptop
   b. Smartphone
   c. Komputer
   d. Koneksi Internet
3. Sumber Pembelajaran
   a. Buku :
      Administrasi Sistem Jaringan, Penerbit Andi
      Administrasi Sistem Jaringan, Penerbit Elangga
   b. Internet

c. Youtube

https://www.youtube.com/watch?v=b4H12IWF7fo

https://www.youtube.com/watch?v=GRP-2TuzdCQ

https://www.youtube.com/watch?v=a1uoDo57I_4

Adiwerna, Mei 2020

Mengetahui

Kepala SMK Bhakti Praja Adiwerna

Erfan Suparmono, S.Pd.,MA

NIPY. 850 980 153

Guru Mata Pelajaran,

Wiwit Kurniasih, S.Kom

NIPY. 850 016 597

LAMPIRAN

1. Instrumen Penilaian
   1) Pengetahuan

   Penilaian pengetahuan dengan tes tertulis

Pertanyaan	Bobot
1. Jaringan pribadi (bukan untuk akses umum) yang menggunakan medium nonpribadi (misalnya internet) untuk menghubungkan antar remote-site secara aman merupakan definisi dari... 2. Jelaskan konsep kerja VPN dalam jaringan public 3. Jelaskan apa saja protokol pada VPN! 4. Jelaskan apa saja kelebihan dan kekurangan VPN! 5. Pada VPN, apa yang dimaksud dengan Tunelling?	
Nilai Akhir (NA)	100

Kunci Jawaban

Jawaban
1. VPN 2. Melindungi pertukaran data yang Anda lakukan dari WiFi atau jaringan yang tidak dapat dipercaya. Ini akan membantu ketika menggunakan jaringan publik di kafe, bar, dan semacamnya. 3. Protokol VPN antara lain: a. Point to Point Tunneling Protocol (PPTP) b. Layer 2 Tunnelling Protocol (L2TP) c. IPsec (Internet Protocol Security) d. Secure Socket Layer 4. Kelebihan dan kekurangan VPN

KELEBIHAN	**KEKURANGAN**
Kerahasiaan data lebih aman.	Koneksi lebih lambat.
Bisa mengakses website terblok.	Koneksi tidak stabil.
Identitas IP asli tidak langsung diketahui.	Konfigurasi manual cukup rumit.
Akses jaringan dari lokasi yang berbeda.	Ada batasan penggunaan.

5. Tunneling adalah cara di mana data ditransfer antara dua jaringan dengan aman. Semua data yang ditransfer difragmentasi menjadi paket atau bingkai yang lebih kecil dan kemudian melewati terowongan. Proses ini berbeda dari transfer data normal antar node.

Rubrik Penilaian Pengetahuan :

No.	Jawaban

1	• Skor 0 bila tidak menjawab • Skor 30 bila jawaban salah • Skor 50 bila jawaban kurang benar • Skor 75 bila jawaban mendekati benar • Skor 100 bila jawaban benar

2) Keterampilan

Penilaian ketrampilan dengan praktik tentang Konfigurasi *VPN Server*.

No.	Aspek	Rentang Skor
1.	Persiapan	20
2.	Proses	50
3.	Hasil	20
4.	Waktu	10
	Nilai Akhir (NA)	100

3) Sikap

Penilaian Sikap melalui Penilaian Diri

No.	Aspek Pengamatan	TP	KD	SR	SL
1.	Saya berdoa sebelum belajar				
2.	Saya bersemangat mengikuti pelajaran				
3.	Saya mengerjakan sendiri ulangan harian/tugas				
4.	Saya terlibat aktif dalam bekerja menyelesaikan tugas kelompok				

Keterangan :
1 = TP : Tidak pernah
2 = KD : Kadang – kadang
3 = SR : Sering
4 = SL : Selalu
Pedoman penilaian
Nilai Akhir :
3,51 – 4,00 : Sangat Baik (SB)
2,51 – 3,50 : Baik (B)
1,51 – 2,50 : Cukup (C)
1,00 – 1,50 : Kurang (K)

URAIAN MATERI

VPN Server

A. Pengertian

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.

B. Jenis-Jenis dari VPN

Ada 3 jenis jaringan antara lain:

1. Remote VPN

Jenis VPN ini ditujukan pada pengguna yang ingin mengakses jaringan pusat dari tempat yang berada di luar area pusat data dimana user dapat data perusahaan kapanpun dan dimanapun berada contohnya penyelia suatu perusahaan yang dilengkapi laptop untuk mengakses informasi di kantor pusat. Kunci dari jenis komunikasi ini adalah fleksibilitas dan biasanya bandwidth dan performance tidak menjadi isu yang begitu penting.

2.Intranet VPN

VPN jenis ini diimplementasikan pada infrastruktur jaringan diperusahaan yang memiliki beberapa lokasi gedung berbeda, biasanya digunakan untuk menghubungkan kantor kantor cabang dengan kantor pusat suatu perusahaan. Jenis VPN ini harus benar-benar aman dan memenuhi standar performansi dan kebutuhan bandwidth dengan persyaratan yang ketat.

3.Extranet VPN

Pada jenis komunikasi ini, VPN menggunakan Internet sebagai backbone utama. Biasanya VPN jenis ini ditujukan untuk skala komunikasi yang lebih luas melibatkan banyak pengguna dan kantor cabang yang tersebar.

C. Fungsi dari VPN

Berikut adalah fungsi dari VPN:

1. Kerahasiaan (Confidentially) : VPN merupakan terknologi yang menggunakan jaringan internet atau jaringan publik yang tentunya sangat rawan terhadap pencurian informasi atau data. Maka VPN memakai metode enkripsi untuk mengacak data yang lewat. Dengan menggunakan metode enskripsi itu, keamanan data akan cukup terjamin dari pencurian data. Walau ada pihak-pihak yang bisa menyadap data-data yang melewati jaringan internet maupun jalur dari VPN sendiri, akan tetapi belum tentu yang menyadap dapat membaca data tersebut sebab data tersebut sebelumnya telah teracak. Dapat disimpulkan dari fungsi confidentially ini maksudnya supaya data yang di transmisikan haya dapat diakses oleh orang yang memang berhak saja.

2. Keutuhan data (Data Integrity) : VPN mempunyai teknologi yang dapat menjaga keutuhan informasi atau data mulai dari data tersebut dikirim kan hingga data tersebut sampai di tempat yang di tujunya. Sehingga data saat di perjalanan dapat terhindar dari berbagai macam gangguan seperti data hilang, rusak, atau dimanipulasi oleh pihak-pihak yang tidak bertanggung jawab.

3. Autentikasi sumber (Origin Authentication) : VPN mempunyai kemampuan untuk melakukan autentifikasi terhadap sumber dari pengiriman data yang akan di terimanya. VPN dapat melakukan pemeriksaan kepada data yang masuk dan mengakses informasi dari sumbernya, lalu alamat dari sumber data

tersebut akan di setujui jika proses autentifikasi berhasil, dengan begitu VPN dapat menjamin semua data yang di kirimkan dan juga yang diterima berasal dari sumber yang memang benar-benar seharusnya, tidak ada informasi atau data yang dikirimkan oleh pihak lain dan data yang dipalsukan.

D. Manfaat dari VPN

Berikut adalah manfaat dari VPN:

1. Remote Access : Maksudnya dengan menggunakan VPN kita bisa mengakses komputer ataupun jaringan kantor, dari mana saja selama terhubung ke jaringan internet atau publik.

2. Keamanan : dengan menggunakan koneksi VPN kita bisa browsing, searching dengan aman saat mengakses dunia maya atau jaringan internet publik misalnya seperti hotspot atau internet yang ada di cafe-cafe.

3. Dapat menghemat biaya setup jaringan : VPN juga dapat dipakai sebagai cara alternatif untuk menghubungkan jaringan lokal yang cukup luas dengan biaya yang lebih rendah. Karena transmisi data yang digunakan pada VPN memakai media jaringan internet atau jaringan publik yang sebelumnya telah ada tanpa perlu membangun jaringan sendiri.

4. Pengamanan Data di Jaringan Publik

Manfaat VPN lainnya adalah melindungi pertukaran data yang Anda lakukan dari WiFi atau jaringan yang tidak dapat dipercaya. Ini akan membantu ketika menggunakan jaringan publik di kafe, bar, dan semacamnya.

E. Cara Kerja dan Penggunaan VPN

Cara kerja dan Penggunaan VPN antara lain:

VPN mendukung banyak protokol jaringan seperti PPTP, L2TP, IPSec dan SOCKS. Protokol ini membantu cara kerja VPN untuk memproses otentikasi.

VPN klien dapat membuat sambungan dan mengidentifikasi orang-orang yang diberi wewenang di jaringan.

Jaringan VPN juga dienkripsi akan meningkatkan fitur keamanan , hal ini juga berarti bahwa VPN biasanya tidak terlihat pada jaringan yang lebih besar.

Teknologi saat ini semakin banyak mendasarkan perkembangan VPN karena mobilitas yang disediakan dan saat ini Virtual Private Network juga membuka jalan untuk koneksi Wi-Fi dan jaringan nirkabel pribadi.

F. Kelebihan dan Kekurangan VPN

Selain untuk menyembunyikan identitas asli, VPN juga dapat membatasi riwayat penelusuran oleh ISP dan pemerintah. Akan tetapi, ada beberapa kekurangan dari penggunaan VPN, salah satunya adalah koneksi yang terkadang lebih lambat. Berikut ini adalah kelebihan dan kekurangan VPN.

KELEBIHAN	**KEKURANGAN**
Kerahasiaan data lebih aman.	Koneksi lebih lambat.
Bisa mengakses website terblok.	Koneksi tidak stabil.

Identitas IP asli tidak langsung diketahui.	Konfigurasi manual cukup rumit.
Akses jaringan dari lokasi yang berbeda.	Ada batasan penggunaan.

G. Protocol VPN Protocol yang bekerja pada jaringan VPN adalah sebagai berikut:

a. Point to Point Tunneling Protocol (PPTP)

PPTP merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari remote client ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP. PPTP merupakan protokol jaringan yang mengubah paket PPP menjadi IP datagram agar dapat ditransmisikan melalui internet.

b. Layer 2 Tunnelling Protocol (L2TP)

L2TP adalah tunneling protokol yang memadukan dua buah tunneling protokol yakni L2F (Layer 2 Forwading) milik cisco dan PPTP milik Microsoft. L2TP biasa digunakan dalam membuat Virtual Private Dial Network (VPDN) yang dapat bekerja membawa semua jenis protokol komunikasi di dalamnya.

c. IPsec (Internet Protocol Security)

IPsec merupakan suatu pengembangan dari protokol internet protocol (IP) yang bertujuan untuk menyediakan keamanan pada suatu IP dan layer yang berada di atasnya. IPsec merupakan metode yang memproteksi IP datagram ketika paket ditransmisikan pada traffic. IPsec bekerja pada layer tiga OSI yaitu network layer sehingga dapat mengamankan data dari layer yang berada atasnya.

d. Secure Socket Layer

Secure Socket Layer (SSL) dan Transport Layer Security (TLS) merupakan solusi protokol untuk VPN yang bekerja pada layer 4. Pengguna dapat mengakses VPN perusahaan melalui aplikasi browser karena protokol ini merupakan protokol kriptografi yang digunakan untuk mengamankan komunikasi melalui internet.

Cukup Amankah Menggunakan VPN?

Keamanan terkadang menjadi perdebatan antara karyawan dengan perusahaan IT.

VPN dapat membuat koneksi Anda sangat aman, tetapi itu juga tergantung dengan protokol (jalan) yang Anda gunakan untuk melakukan koneksi.

Keamanan menggunakan VPN masih terhalang dua faktor utama, yaitu:

a) Batasan Teknologi
   Limitasi teknologi yang digunakan untuk mengembangan VPN, seperti tipe protokol dan enkripsi yang digunakan.
b) Batasan Hukum

Batasan hukum dan kebijakan memengaruhi apa yang dapat dilakukan dengan teknologi itu. Begitu pula dengan undang-undang negara tempat server dan perusahaan menyediakan VPN berada. Terkadang kebijakan perusahaan sendiri mempengaruhi cara perusahaan menerapkan teknologi ini dalam layanan mereka.

Jadi bisa dibilang tidak sepenuhnya menggunakan VPN itu aman. Namun, paling tidak menggunakan VPN akan lebih aman dibandingkan menggunakan koneksi biasa.

Jadi, Kapan Harus Menggunakan VPN?

Ada beberapa alasan menarik untuk menggunakan teknologi ini:

- Membantu Anda mendapatkan koneksi yang lebih aman ketika menggunakan WiFi publik.
- Mengenkripsi aktivitas Anda di situs web.
- Menyembunyikan aktivitas Anda terhadap orang-orang yang ingin mencoba mengetahui secara diam-diam.
- Menyembunyikan lokasi, dan mengizinkan Anda mengakses geo-blocked content ‘konten-konten yang diblok berdasarkan wilayah geografis’.
- Memastikan Anda lebih anonim di dalam situs web.

Cara Mendapatkan VPN Gratis

Apa itu VPN Gratis? VPN Gratis adalah layanan yang menyediakan server VPN dan dapat Anda gunakan secara gratis.

Melalui situs-situs di bawah ini, Anda bisa mendapatkan akses VPN secara gratis. Ada beberapa situs penyedia VPN Gratis yang bisa Anda coba. Situs-situs penyedia VPN Gratis ini menyediakan layanan aplikasi VPN yang dapat digunakan di perangkat desktop. Sedangkan jika Anda ingin menggunakan VPN pada perangkat mobile maupun desktop dapat mencoba aplikasi seperti Hotspot Shield atau Tunnel Bear.

1) Hotspot Shield
   Hotspot Shield adalah penyedia layanan VPN yang cukup populer. Meskipun menyediakan layanan premium, tetapi Hotspot Shield juga menawarkan versi gratis yang dapat Anda coba.

   Versi ini dapat mencegah situs yang mengandung malware dan membawa Anda untuk terkoneksi dengan situs yang diblok. Namun, versi gratis hanya dapat mengkoneksikannya untuk satu perangkat saja.
2) TunnelBear
   TunnelBear adalah aplikasi VPN yang cukup sederhana tetapi powerful. TunnelBear memiliki tampilan yang menarik sehingga memudahkan pengguna untuk menggunakannya.

   TunnelBear adalah sebuah aplikasi VPN yang ramah untuk perangkat Anda. TunnelBear memiliki UI yang menarik dan sederhana sehingga memudahkan pengguna untuk menggunakannya.

   Versi yang ditawarkan juga ada dua, gratis dan berbayar. Versi gratis dapat Anda coba sampai dengan 500MB penggunaan.

3) Hide.me
   Hide.me merupakan aplikasi penyedia internet yang ada di Malaysia dan mempunyai puluhan server yang ada di dunia. Versi gratis dari aplikasi ini mengizinkan Anda untuk menggunakan sampai dengan 3GB setiap bulannya.

Kesimpulan

VPN dapat membantu Anda untuk mengamankan koneksi yang Anda lakukan, begitu pula dengan identitas dan data pribadi. Meskipun ada kekurangan, tetapi itu menjadi bagian yang tidak bisa dipisahkan di dalam sebuah aplikasi.

Ada beberapa pilihan aplikasi penyedia layanan Server VPN, tetapi Anda juga dapat membuat Server VPN sendiri di VPS atau perangkat komputer Anda.

Konfigurasi VPN Server :

Perlu diketahui terlebih dahulu, bahwasanya vpn server membutuhkan jaringan yang mengarah ke jaringan Internet. Untuk jaringan Internet, vpn serverpun harus menggunakan Ip Public, agar bisa diakses dari mana saja, tetapi kali ini hanya akan menggunakan ip local saja atau private ip , aplikasi untuk membuat vpn server ada beberapa seperti : openvpn ,pptp dll yang anda bisa cari sendiri di internet ,dalam konfigurasi kali ini saya akan mengunakan pptp untuk membuat vpn server .

Berikut langkah-langkahnya :

1. pertama-tama silahkan masukan perintah .

#apt-get install pptpd

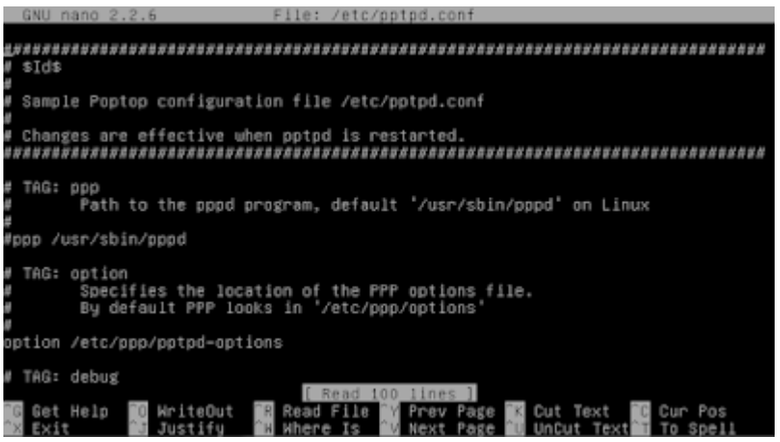
```
root@server1:/home/server1# apt-get install pptpd_
```

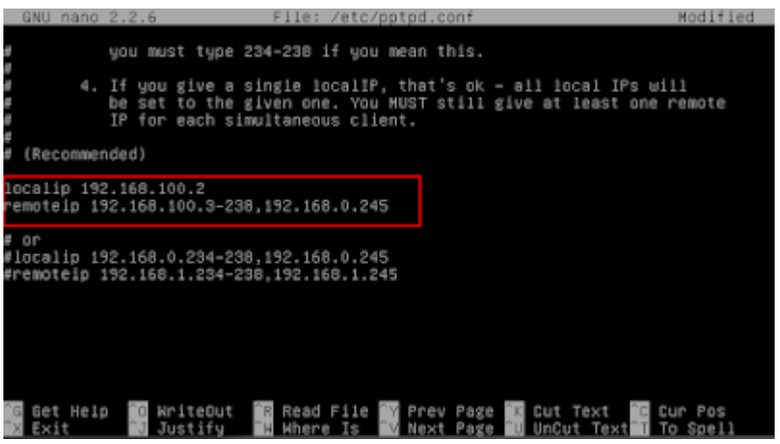
6. Selanjutnya anda harus mengkonfigurasi vpn anda, ada 3 buah file yang harus anda konfigurasikan yaitu “/etc/pptpd.conf”, “/etc/ppp/pptpd-options”, dan “/etc/ppp/chap-secrets" pertama masukan perintah berikut untuk mengkonfigurasi file /etc/pptpd.conf

```
root@server1:/home/server1# nano /etc/pptpd.conf _
```

Pada akhir file konfigurasi atau yang terbawah tambahkan beberapa baris berikut ini

localip 192.168.100.2
remoteip 192.168.100.3-238,192.168.0.245





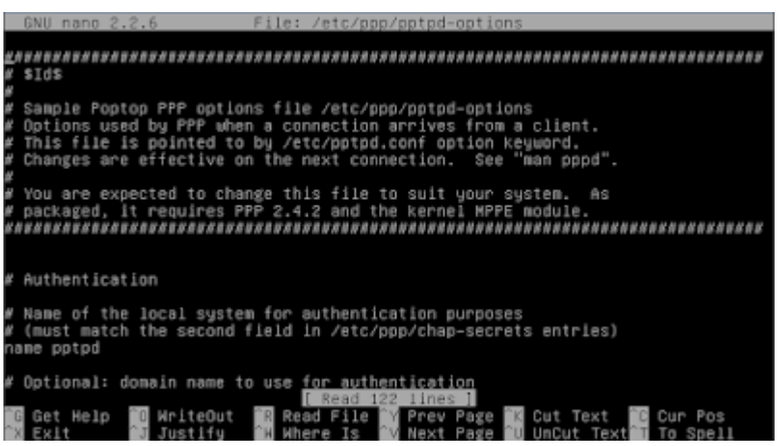
Simpan dengan menekan Ctrl+X => Y => Enter

3. Kemudian masukan perintah :

#nano /etc/ppp/pptpd-options

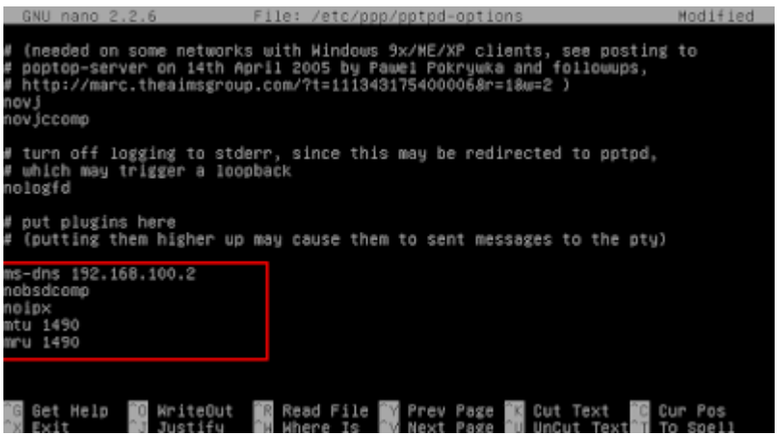
```
root@server1:/home/server1# nano /etc/ppp/pptpd-options
```

lalu akan muncul tampilan seperti dibawah ini



Pada bagian paling bawah tambahkan baris berikut

ms-dns 192.168.100.2
nobsdcomp
noipx
mtu 1490
mru 1490



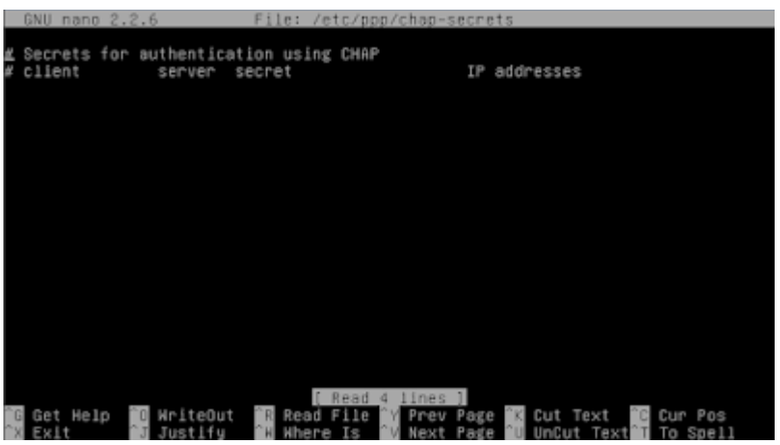
Simpan dengan menekan Ctrl+X => Y => Enter

4. kemudian edit file /etc/ppp/chap-secrets dengan perintah

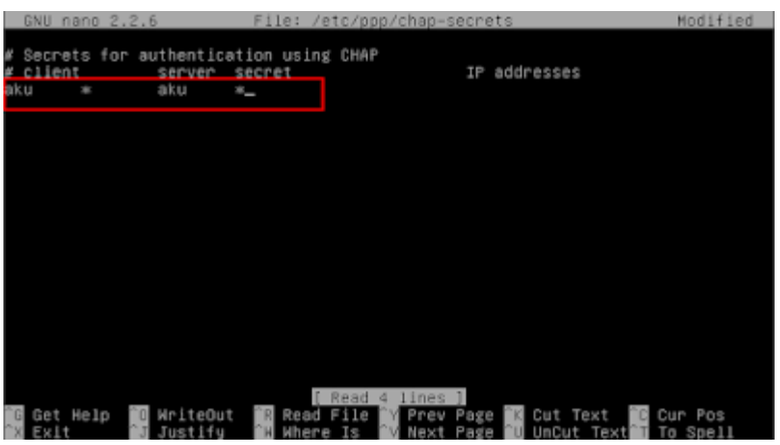
#nano /etc/ppp/chap-secrets

Pada file konfigurasi ini adalah untuk membuat username dan password untuk login vpn client pada windows atau linux tambahkan beberapa baris berikut ke bagian palingbawah file konfigurasi :

aku * aku *



Formatnya aku [tab] * [tab] aku [tab] * ,maka akan seperti dibawah ini



Setelah itu simpan, tekan Ctrl+x => Y => Enter

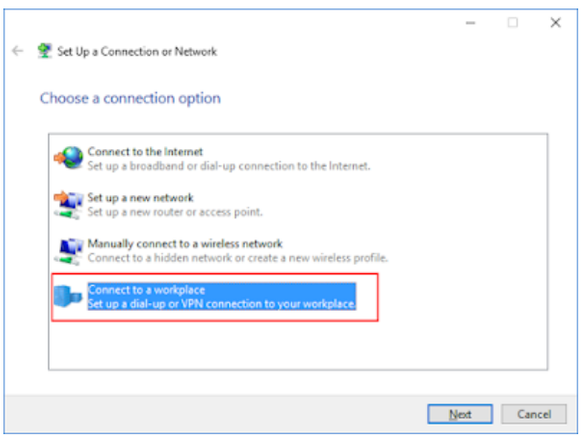
5. Kemudian restart service pptpd dengan perintah

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

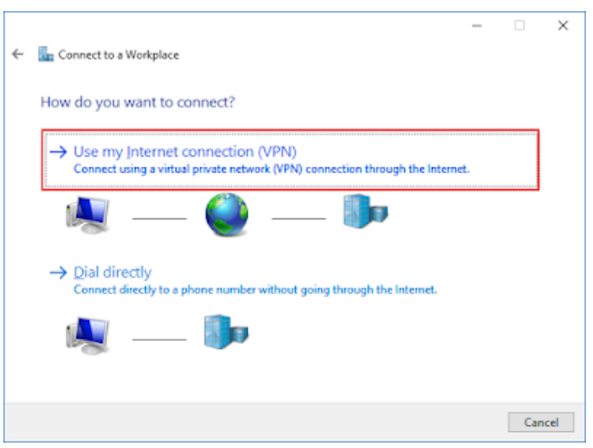
```
root@server1:/home/server1# /etc/init.d/pptpd restart
[ ok ] Restarting pptpd (via systemctl): pptpd.service.
root@server1:/home/server1# _
```

6. Sekarang coba pada Client, masuk ke Control Panel => Klik Set Up a New connection or Network .

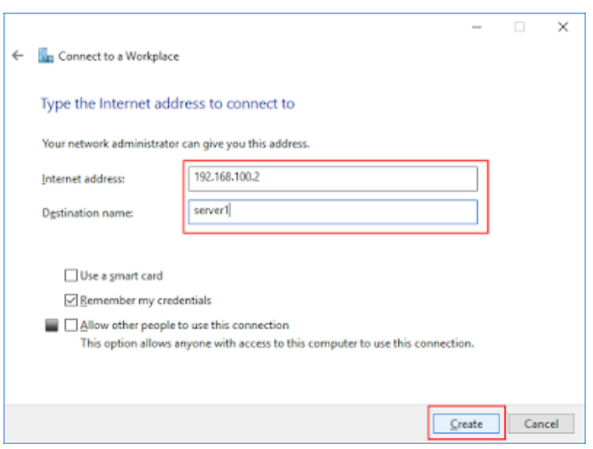
7. Maka akan muncul jendela baru seperti gambar dibawah, Pilih Connect to a WorkPlace => Next .



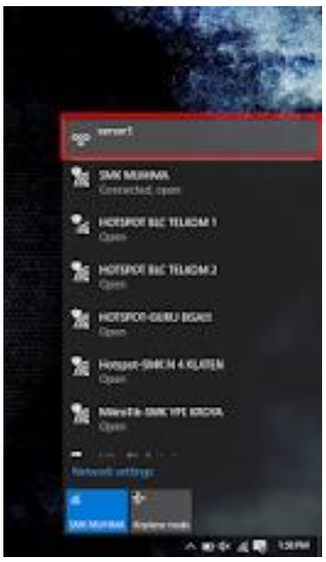
8. Pilih yang Use my Internet Connection (VPN) .



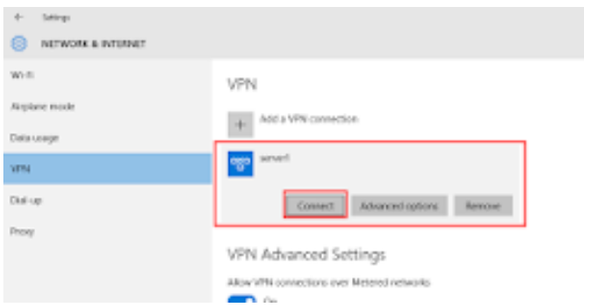
9. Masukkan nama Koneksi dan IP Server atau Domainnya => lalu Create .



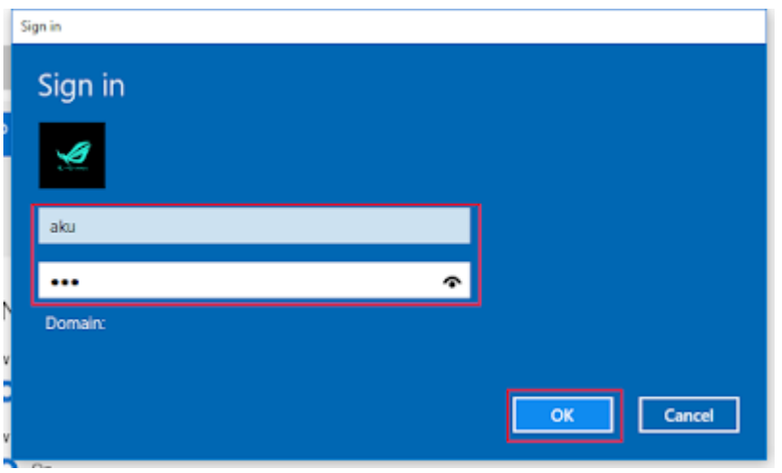
10. Klik Server1 (nama koneksi yang tadi dibuat) .



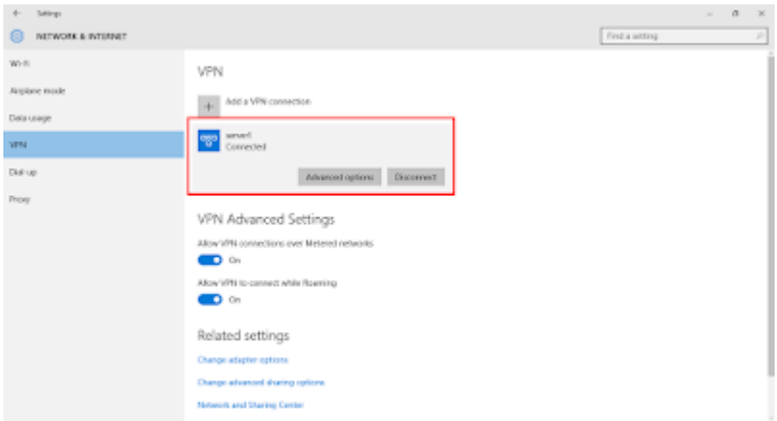
11. Kemudian akan muncul jendela baru, Klik Connect pada Server1 .



12. Lalu akan muncul jendela baru, anda diminta untuk memasukkan Username dan Password yang tadi dibuat .



13. Jika sudah Terkoneksi maka sudah Berhasil .


Settings
NETWORK & INTERNET
Find a setting
Wi-Fi
Airplane mode
Data usage
VPN
Dial-up
Proxy
VPN
Add a VPN connection
server1
Connected
Advanced options
Disconnect
VPN Advanced Settings
Allow VPN connections over Metered networks
On
Allow VPN to connect while Roaming
On
Related settings
Change adapter options
Change advanced sharing options
Network and Sharing Center