

# MODUL AJAR FASE F

# SISTEM KEAMANAN JARINGAN



TUJUAN  
PEMBELAJARAN



## Modul 4

**TP : VPN (virtual private network)**



Idiarso, S.Kom

SISTEM INFORMASI  
JARINGAN DAN APLIKASI



**MODUL AJAR 4**  
**VPN**  
**Konsentrasi Keahlian**  
**Sistem Informasi Jaringan Dan Aplikasi**

<b>Konsentrasi Keahlian</b>	<b>: Sistem Informatika Jaringan Dan Aplikasi</b>
<b>Mata Pelajaran</b>	<b>: Sistem Keamanan Jaringan</b>
<b>Fase</b>	<b>: F</b>
<b>Nama Penyusun</b>	<b>: Idiarso,S.Kom</b>
<b>Instansi</b>	<b>: SMK Negeri 1 Punggelan</b>
<b>Jumlah Jam</b>	<b>: 72 JP (18 x Pertemuan)</b>

## **1. TUJUAN PEMBELAJARAN**

1. Setelah mempelajari materi dari internet, peserta didik dapat menjelaskan konsep virtual private network dengan benar
2. Setelah mempelajari materi dari internet, peserta didik dapat menentukan cara konfigurasi virtual private network dengan tepat
3. Setelah mempelajari materi dari internet, peserta didik dapat melakukan konfigurasi virtual private network dengan baik
4. Setelah mempelajari materi dari internet, peserta didik dapat menguji hasil konfigurasi virtual private network dengan benar
5. Setelah mempelajari materi dari internet dan melakukan praktikum, peserta didik dapat membuat laporan konfigurasi virtual private network dengan baik

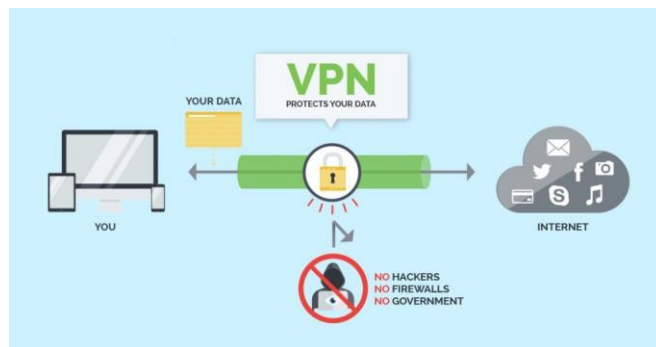
### **Indikator Ketercapaian Tujuan Pembelajaran**

- 3.1 Menjelaskan konsep virtual private network
- 3.2 Menentukan cara konfigurasi virtual private network Melakukan konfigurasi virtual private network
- 3.3 Menguji hasil konfigurasi virtual private network Membuat laporan konfigurasi virtual private network
- 3.4 Menentukan cara konfigurasi virtual private network
- 3.5 Melakukan konfigurasi virtual private network
- 3.6 Menguji hasil konfigurasi virtual private networkvirtual private network
- 3.7 Membuat laporan konfigurasi virtual private network

## LANGKAH PEMBELAJARAN

### Pertemuan 1 (4x45 menit)

- Pendahuluan** : 1) Apersepsi diberikan guru kepada peserta didik melalui pertanyaan pemantik yang disampaikan guru;
- Apa yang kalian ketahui tentang VPN ?
  - Alasan apa yang mendasari kita menggunakan VPN ?
- 2) Sebagai asesmen awal, peserta didik diminta untuk menjelaskan apa yang ada di benaknya ketika guru menayangkan gambar berikut;



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

Selanjutnya peserta didik diminta untuk

- Menjelaskan pengertian VPN
- Mendiskripsikan jenis-jenis dan cara kerja VPN

Inti

- :
- 1) Peserta didik memperhatikan tayangan-tayangan singkat di layar menggunakan *laptop* dan *infocus* lanjutan dari tayangan yang ditampilkan guru melalui Link  
<https://www.youtube.com/watch?v=CTkegOlywnI> dan [https://id.linkedin.com/learning/belajar-tentang-vpn/apa-itu-vpn?autoplay=true&trk=learning-course\\_tocItem&upsellOrderOrigin=default\\_guest\\_learning](https://id.linkedin.com/learning/belajar-tentang-vpn/apa-itu-vpn?autoplay=true&trk=learning-course_tocItem&upsellOrderOrigin=default_guest_learning)
  - 2) Peserta didik diminta untuk browsing materi tentang sejarah, pengertian, jenis, tipe, macam-macam, fungsi, prinsip dasar, dan mafaat VPN dalam mengamankan jaringan dengan menggunakan HP atau Komputer yang sudah disediakan di Lab .
  - 3) Peserta didik juga diarahkan untuk membuka google classroom untuk melihat materi yang guru sediakan sebagai bahan referensi.
  - 4) Peserta didik dibagi menjadi 8 kelompok diskusi sebagaimana tercantum pada LKPD 1 (**Dimensi P3 kreatif: Mengeksplorasi dan mengekspresikan pikiran dan/atau perasaannya dalam bentuk karya dan/atau tindakan, serta mengevaluasinya dan mempertimbangkan dampak dan risikonya bagi diri dan lingkungannya**)
  - 5) Hasil diskusi kelompok dituangkan dalam bentuk file presentasi kemudian diupload melalui Google classroom yang guru telah organisasikan di mana peserta didik dapat mengunjungi semua hasil karya kelompok lain dengan menyampaikan tanggapan dalam bentuk pertanyaan, masukan ataupun sanggahan
  - 6) Peserta didik membuat laporan hasil diskusi dengan menyertakan foto karya/hasil diskusi dalam bentuk deskripsi, PPT atau animasi, kemudian dipresentasikan

di depan kelas secara bergiliran sementara kelompok lain memberikan tanggapan.

- Penutup** :
- 1) Peserta didik diminta menyimpulkan keseluruhan materi dan guru memberikan penguatan dilanjutkan dengan penyampaian refleksi antar peserta didik dan kepada guru terkait penyampaian materi apakah menyenangkan, materi yang dibahas apakah mudah dipahami, apakah semua peserta didik paham, siapa saja yang belum paham adakah materi yang susah dipahami, materi mana yang perlu diperbaiki ?
  - 2) 2) Peserta didik mendengarkan pesan dari guru tentang materi yang harus disiapkan untuk pertemuan selanjutnya dan pembelajaran ditutup dengan doa.

## Pertemuan 2 (4x45 menit)

**Pendahuluan** : 1) Peserta didik merespon apersepsi yang disampaikan guru dalam mengawali kegiatan pembelajaran dengan menjawab pertanyaan pemantik sekaligus asesmen awal;

- Apa yang kalian pahami tentang protokol VPN?
- Bagaimana cara kita memilih protokol mana yang sesuai dalam penggunaannya ?
- Apa saja pertimbangan dalam pemilihan VPN ?
- Apa perbedaan antara protokol VPN PPTP, L2TP, dan OpenVPN ?
- Apa kelebihan dan kekurangan dari protokol VPN yang paling umum digunakan?
- Apakah semua protokol VPN kompatibel dengan semua perangkat dan sistem operasi?

**Inti** : 1) Peserta didik memperhatikan tayangan-tayangan singkat di layar menggunakan *laptop* dan *infocus* lanjutan dari tayangan yang ditampilkan guru melalui Link [https://id.linkedin.com/learning/belajar-tentang-vpn/istilah-dan-dasar-dasar?autoplay=true&trk=learning-course\\_tocItem&upsellOrderOrigin=default\\_guest\\_learning](https://id.linkedin.com/learning/belajar-tentang-vpn/istilah-dan-dasar-dasar?autoplay=true&trk=learning-course_tocItem&upsellOrderOrigin=default_guest_learning)

2) Peserta didik diminta untuk browsing materi tentang

- PPTP (Point-to-Point Tunneling Protocol)
- L2TP (Layer 2 Tunneling Protocol)
- OpenVPN
- IPSec (Internet Protocol Security)

- SSTP (Secure Socket Tunneling Protocol)
  - WireGuard
  - IKEv2 (Internet Key Exchange version 2)
  - SSL/TLS (Secure Sockets Layer/Transport Layer Security)
  - Cisco VPN (Cisco's proprietary VPN protocol)
  - SoftEther VPN (Open-source multi-protocol VPN software)
- 3) Peserta didik juga diarahkan untuk membuka google classroom untuk melihat materi yang guru sediakan sebagai bahan referensi.
  - 4) Peserta didik dibagi menjadi 8 kelompok diskusi sebagaimana tercantum pada LKPD 2 (**Dimensi P3 kreatif: Mengeksplorasi dan mengekspresikan pikiran dan/atau perasaannya dalam bentuk karya dan/atau tindakan, serta mengevaluasinya dan mempertimbangkan dampak dan risikonya bagi diri dan lingkungannya**)
  - 5) Hasil diskusi kelompok dituangkan dalam bentuk file presentasi kemudian diupload melalui Google classroom yang guru telah organisasikan di mana peserta didik dapat mengunjungi semua hasil karya kelompok lain dengan menyampaikan tanggapan dalam bentuk pertanyaan, masukan ataupun sanggahan
  - 6) Peserta didik membuat laporan hasil diskusi dengan menyertakan foto karya/hasil diskusi dalam bentuk deskripsi, PPT atau animasi, kemudian dipresentasikan di depan kelas secara bergiliran sementara kelompok lain memberikan tanggapan.



**Penutup**

- :
- 1) Peserta didik diminta menyimpulkan keseluruhan materi dan guru memberikan penguatan dilanjutkan dengan penyampaian refleksi antar peserta didik dan kepada guru terkait penyampaian materi apakah menyenangkan, materi yang dibahas apakah mudah dipahami, apakah semua peserta didik paham, siapa saja yang belum paham adakah materi yang susah dipahami, materi mana yang perlu diperbaiki ?
  - 2) Peserta didik mendengarkan pesan dari guru tentang materi yang harus disiapkan untuk pertemuan selanjutnya dan pembelajaran ditutup dengan doa.

Pertemuan 3 (4x45 menit)	
Pendahuluan	<p>: 1) Peserta didik merespon apersepsi yang disampaikan guru dalam mengawali kegiatan pembelajaran dengan menjawab pertanyaan pemantik sekaligus asesmen awal;</p> <ol style="list-style-type: none"> <li>Apa yang kalian pahami tentang protokol VPN server dan client dari pertemuan kemarin ?</li> <li>Bagaimana cara kita menerapkannya di Sistem operasi yang kita gunakan ?</li> </ol>
Inti	<p>: 1) Peserta didik memperhatikan tayangan-tayangan singkat di layar menggunakan <i>laptop</i> dan <i>infocus</i> lanjutan dari tayangan yang ditampilkan guru melalui Link</p> <p><a href="https://www.youtube.com/watch?v=sHmLFjFYQhA">https://www.youtube.com/watch?v=sHmLFjFYQhA</a> dan <a href="https://www.youtube.com/watch?v=O1e2-fYZaV0">https://www.youtube.com/watch?v=O1e2-fYZaV0</a></p> <p>2) Peserta didik juga diarahkan untuk membuka google classroom untuk melihat materi yang guru sediakan sebagai bahan referensi.</p> <p>3) Guru menambahkan panduan penggunaan VPN di Sistem operasi Windows linux dan cara seting disisi Server seperti pada link</p> <p><a href="https://www.youtube.com/watch?v=z7mO9cQMfLs">https://www.youtube.com/watch?v=z7mO9cQMfLs</a> dan <a href="https://www.youtube.com/watch?v=XecLftQBNTk">https://www.youtube.com/watch?v=XecLftQBNTk</a></p> <p>4) Peserta didik diminta untuk mempraktikan menggunakan perangkat komputer mereka masing-masing.</p> <p>5) Peserta didik membuat laporan pembuatan VPN menggunakan sistem operasi Windows dan Linux dalam bentuk Video yang kemudian diupload kdalam youtube masing-masing.</p>

<b>Penutup</b>	:	<p>3) Peserta didik diminta menyimpulkan keseluruhan materi dan guru memberikan penguatan dilanjutkan dengan penyampaian refleksi antar peserta didik dan kepada guru terkait penyampaian materi apakah menyenangkan, materi yang dibahas apakah mudah dipahami, apakah semua peserta didik paham, siapa saja yang belum paham adakah materi yang susah dipahami, materi mana yang perlu diperbaiki ?</p> <p>4) Peserta didik mendengarkan pesan dari guru tentang materi yang harus disiapkan untuk pertemuan selanjutnya dan pembelajaran ditutup dengan doa.</p>
----------------	---	---

#### Pertemuan 4 (8x45 menit)

<b>Pendahuluan</b>	:	<p>1) Peserta didik merespon apersepsi yang disampaikan guru dalam mengawali kegiatan pembelajaran dengan menjawab pertanyaan pemantik sekaligus asesmen awal;</p> <p>a. Bagaimana kalian menerapkan VPN dalam suatu jaringan yang lebih kompleks ?</p> <p>b. Apakah mikrotik menyediakan VPN yang bervariasi seperti yang sudah pernah kita lakukan pada pertemuan sebelumnya ?</p>
<b>Inti</b>	:	<p>1) Peserta didik memperhatikan tayangan-tayangan singkat di layar menggunakan <i>laptop</i> dan <i>infocus</i> lanjutan dari tayangan yang ditampilkan guru melalui Link <a href="https://www.youtube.com/watch?v=MGRy-H-NmFA">https://www.youtube.com/watch?v=MGRy-H-NmFA</a></p> <p>2) Peserta didik juga diarahkan untuk membuka google classroom untuk melihat materi yang guru sediakan sebagai bahan referensi.</p> <p>3) Guru menambahkan panduan penggunaan VPN menggunakan Mikrotik.</p> <p>4) Peserta didik diminta untuk mempraktikkan menggunakan perangkat komputer mereka</p>

		masing-masing.
		5) Peserta didik membuat laporan pembuatan VPN menggunakan Mikrotik
		6) Peserta didik mendokumentasikan langkah-langkah dalam suatu file presentasi ataupun video yang nantinya dijadikan bahan evaluasi dan diskusi bersama
<b>Penutup</b>	:	<p>1) Peserta didik diminta menyimpulkan keseluruhan materi dan guru memberikan penguatan dilanjutkan dengan penyampaian refleksi antar peserta didik dan kepada guru terkait penyampaian materi apakah menyenangkan, materi yang dibahas apakah mudah dipahami, apakah semua peserta didik paham, siapa saja yang belum paham adakah materi yang susah dipahami, materi mana yang perlu diperbaiki ?</p> <p>2) Peserta didik mendengarkan pesan dari guru tentang materi yang harus disiapkan untuk pertemuan selanjutnya dan pembelajaran ditutup dengan doa.</p>

<b>Pertemuan 5 (8x45 menit)</b>		
<b>Pendahuluan</b>	:	<p>1) Peserta didik merespon apersepsi yang disampaikan guru dalam mengawali kegiatan pembelajaran dengan menjawab pertanyaan pemantik sekaligus asesmen awal;</p> <p>a. Apa perbedaan antara VPN dan SSH dalam konteks jaringan?</p> <p>b. Mengapa kita perlu menghubungkan VPN dan SSH?</p> <p>c. Bagaimana cara menghubungkan ke server SSH melalui koneksi VPN?</p> <p>d. Apa manfaat menggunakan SSH melalui VPN daripada langsung menggunakan SSH?</p>

<p><b>Inti</b></p>	<p>:</p> <ol style="list-style-type: none"> <li>7) Peserta didik memperhatikan tayangan-tayangan singkat di layar menggunakan <i>laptop</i> dan <i>infocus</i> lanjutan dari tayangan yang ditampilkan guru melalui Link <a href="https://id.linkedin.com/learning/belajar-tentang-vpn/mengonfigurasi-server-ssh?autoplay=true&amp;trk=learning-course_tocItem&amp;upsellOrderOrigin=default_guest_learning">https://id.linkedin.com/learning/belajar-tentang-vpn/mengonfigurasi-server-ssh?autoplay=true&amp;trk=learning-course_tocItem&amp;upsellOrderOrigin=default_guest_learning</a></li> <li>8) Peserta didik juga diarahkan untuk membuka google classroom untuk melihat materi yang guru sediakan sebagai bahan referensi.</li> <li>9) Guru menambahkan panduan penggunaan VPN dan SSH melalui router Mikrotik.</li> <li>10) Peserta didik dibagi menjadi 8 kelompok untuk berdiskusi sebagaimana tercantum pada LKPD 5</li> <li>11) Peserta didik diminta untuk mempraktikkan menggunakan perangkat komputer mereka masing-masing</li> <li>12) Peserta didik membuat laporan pembuatan VPN dan SSH sebagi remot menggunakan Mikrotik</li> <li>13) Peserta didik mendokumentasikan langkah-langkah dalam suatu file presentasi ataupun video yang nantinya dijadikan bahan evaluasi dan diskusi bersama</li> </ol>
<p><b>Penutup</b></p>	<p>:</p> <ol style="list-style-type: none"> <li>1) Peserta didik diminta menyimpulkan keseluruhan materi dan guru memberikan penguatan dilanjutkan dengan penyampaian refleksi antar peserta didik dan kepada guru terkait penyampaian materi apakah menyenangkan, materi yang dibahas apakah mudah dipahami, apakah semua peserta didik paham, siapa saja yang belum paham adakah materi yang susah dipahami, materi mana yang perlu diperbaiki ?</li> <li>2) Peserta didik mendengarkan pesan dari guru tentang materi yang harus disiapkan untuk pertemuan selanjutnya dan pembelajaran ditutup dengan doa.</li> </ol>

Pertemuan 6 (8x45 menit)	
<b>Pendahuluan</b>	<p>: 1) Peserta didik merespon apersepsi yang disampaikan guru dalam mengawali kegiatan pembelajaran dengan menjawab pertanyaan pemantik sekaligus asesmen awal;</p> <p>a. Bagaimana kalian menerapkan VPN dalam suatu jaringan yang lebih kompleks ?</p> <p>b. Apakah mikrotik menyediakan VPN yang bervariasi seperti yang sudah pernah kita lakukan pada pertemuan sebelumnya ?</p>
<b>Inti</b>	<p>: 1) Peserta didik memperhatikan tayangan-tayangan singkat di layar menggunakan <i>laptop</i> dan <i>infocus</i> lanjutan dari tayangan yang ditampilkan guru melalui Link <a href="https://www.youtube.com/watch?v=MGRy-H-NmFA">https://www.youtube.com/watch?v=MGRy-H-NmFA</a></p> <p>2) Peserta didik juga diarahkan untuk membuka google classroom untuk melihat materi yang guru sediakan sebagai bahan referensi.</p> <p>3) Peserta didik secara mandiri mengerjakan Praktik interkoneksi jaringan sebagaimana tercantum di LKPD 6</p> <p>4) Peserta didik diminta untuk mempraktikkan menggunakan perangkat komputer mereka masing-masing</p> <p>5) Peserta didik membuat laporan pembuatan interkoneksi jaringan menggunakan Mikrotik</p> <p>6) Peserta didik mendokumentasikan langkah-langkah dalam suatu file presentasi ataupun video yang nantinya dijadikan bahan evaluasi dan diskusi bersama</p>

<b>Penutup</b>	:	<p>1) Peserta didik diminta menyimpulkan keseluruhan materi dan guru memberikan penguatan dilanjutkan dengan penyampaian refleksi antar peserta didik dan kepada guru terkait penyampaian materi apakah menyenangkan, materi yang dibahas apakah mudah dipahami, apakah semua peserta didik paham, siapa saja yang belum paham adakah materi yang susah dipahami, materi mana yang perlu diperbaiki ?</p> <p>2) Peserta didik mendengarkan pesan dari guru tentang materi yang harus disiapkan untuk pertemuan selanjutnya dan pembelajaran ditutup dengan doa.</p>
----------------	---	---

### **LEMBAR KERJA PESERTA DIDIK (LKPD)**

#### **LEMBAR KERJA PESERTA DIDIK (LKPD) 1**

1. Berkelompoklah menjadi 8 (delapan) kemudian tulis nama dan nomor absen peserta didik di kelompokmu
2. Carilah materi di internet tentang sejarah singkat, pengertian, prinsip dasar, jenis/ type, fungsi, dan manfaat VPN
3. Diskusikan Bersama kelompokmu
  - a. Pengertian VPN
  - b. Jenis-jenis VPN
  - c. VPN gratis dan berbayar
  - d. Perbedaan dengan Proxy
  - e. Penggunaan umum VPN
  - f. Manfaat penggunaan VPN
  - g. Pengalaman menggunakan VPN

#### **LEMBAR KERJA PESERTA DIDIK (LKPD) 2**

- 1) Jelaskan masing masing Protokol VPN sbb :

- PPTP (Point-to-Point Tunneling Protocol)
- L2TP (Layer 2 Tunneling Protocol)
- OpenVPN

- IPSec (Internet Protocol Security)
  - SSTP (Secure Socket Tunneling Protocol)
  - WireGuard
  - IKEv2 (Internet Key Exchange version 2)
  - SSL/TLS (Secure Sockets Layer/Transport Layer Security)
  - Cisco VPN (Cisco's proprietary VPN protocol)
  - SoftEther VPN (Open-source multi-protocol VPN software)
- 2) Apa perbedaan antara protokol VPN PPTP, L2TP, dan OpenVPN ?
  - 3) Apa kelebihan dan kekurangan dari protokol VPN yang paling umum digunakan?
  - 4) Apakah semua protokol VPN kompatibel dengan semua perangkat dan sistem operasi?

#### JAWABAN LKPD 2

1. Berikut adalah beberapa jenis protokol VPN yang umum digunakan:
  1. PPTP (Point-to-Point Tunneling Protocol): Protokol yang relatif mudah dikonfigurasi dan umum digunakan untuk koneksi VPN. Namun, keamanannya bisa dipertanyakan.
  2. L2TP/IPsec (Layer 2 Tunneling Protocol with IPsec): Protokol gabungan yang menggabungkan L2TP untuk pembentukan terowongan dan IPsec untuk keamanan. Lebih aman daripada PPTP.
  3. OpenVPN: Protokol open-source yang sangat fleksibel dan aman. Mendukung enkripsi yang kuat dan dapat berjalan di berbagai platform.
  4. SSTP (Secure Socket Tunneling Protocol): Protokol yang dikembangkan oleh Microsoft dan berjalan melalui port TCP 443, sehingga seringkali dapat melewati firewall dengan mudah.
  5. IKEv2 (Internet Key Exchange version 2): Protokol yang kuat dan stabil, sering digunakan untuk koneksi VPN di perangkat mobile. Dikombinasikan dengan IPsec untuk keamanan.
  6. WireGuard: Protokol VPN yang relatif baru dan didesain dengan fokus pada kecepatan, keamanan, dan efisiensi. Tersedia untuk berbagai platform.
  7. IPSec (Internet Protocol Security): Protokol yang sering digunakan bersama L2TP/IPsec atau IKEv2. Menawarkan enkripsi yang kuat dan dukungan yang luas.
  8. Cisco VPN: Protokol VPN propietari yang dikembangkan oleh Cisco Systems.



Digunakan khususnya untuk koneksi VPN di perangkat dan jaringan Cisco.

9. SSL/TLS (Secure Sockets Layer/Transport Layer Security): Protokol yang sering digunakan dalam VPN SSL, yang menggunakan web browser sebagai klien VPN.

Umumnya digunakan untuk mengamankan koneksi web.

10. SoftEther VPN: Protokol VPN open-source yang serbaguna dan mendukung berbagai fitur seperti keamanan, fleksibilitas jaringan, dan skalabilitas.

2. Perbedaan antara protokol VPN PPTP, L2TP, dan OpenVPN adalah sebagai berikut:

- PPTP (Point-to-Point Tunneling Protocol): PPTP adalah protokol yang lebih tua dan relatif mudah dikonfigurasi. Namun, keamanannya kurang dibandingkan dengan protokol lainnya. PPTP menggunakan enkripsi yang lebih lemah dan dapat rentan terhadap serangan.

- L2TP (Layer 2 Tunneling Protocol): L2TP adalah protokol yang lebih aman daripada PPTP. Protokol ini menggabungkan L2TP untuk pembentukan terowongan dan IPsec untuk keamanan. L2TP/IPsec sering digunakan di lingkungan perusahaan karena keamanan yang lebih baik.

- OpenVPN: OpenVPN adalah protokol yang sangat fleksibel dan aman. Protokol ini open-source, mendukung enkripsi yang kuat, dan dapat berjalan di berbagai platform termasuk Windows, macOS, Linux, Android, dan iOS. OpenVPN dapat menggunakan protokol UDP atau TCP, dan memiliki kemampuan untuk menyesuaikan pengaturan enkripsi dan otentikasi.

3. Kelebihan dan kekurangan dari protokol VPN yang umum digunakan adalah sebagai berikut:

- PPTP:

- Kelebihan: Mudah dikonfigurasi, umum didukung oleh banyak perangkat dan sistem operasi.

- Kekurangan: Keamanan yang lemah, rentan terhadap serangan, tidak disarankan untuk kebutuhan keamanan yang tinggi.

- L2TP/IPsec:

- Kelebihan: Lebih aman daripada PPTP, dukungan luas di banyak perangkat dan sistem operasi.

- Kekurangan: Kinerja sedikit lebih lambat dibandingkan PPTP, beberapa firewall dapat memblokir L2TP/IPsec.

- OpenVPN:

Kelebihan: Sangat fleksibel, aman dengan enkripsi yang kuat, mendukung banyak platform, dapat melewati firewall, dapat mengatasi perubahan jaringan dengan baik.

Kekurangan: Memerlukan perangkat lunak tambahan untuk diinstal, konfigurasi awal yang sedikit lebih rumit.

4. Tidak semua protokol VPN kompatibel dengan semua perangkat dan sistem operasi. Kompatibilitas protokol VPN tergantung pada dukungan yang diberikan oleh perangkat keras dan sistem operasi yang digunakan. Sebagian besar perangkat dan sistem operasi mendukung PPTP, L2TP/IPsec, dan OpenVPN. Namun, beberapa protokol mungkin tidak didukung oleh perangkat atau sistem operasi tertentu. Sebelum memilih protokol VPN, penting untuk memastikan bahwa protokol tersebut didukung oleh perangkat dan sistem operasi yang Anda gunakan.

### LEMBAR KERJA PESERTA DIDIK (LKPD) 3

1. Buatlah Langkah-langkah instalasi dan penggunaan VPN menggunakan sistem Operasi yang kalian Gunakan
2. Tuangkan Hasil pekerjaan kedalam file presentasi yang diupload di form google classroom dan video diupload ke akun youtube kalian masing-masing

### JAWABAN LKPD 2

Berikut adalah langkah-langkah umum untuk menginstal VPN di Windows:

1. Langkah pertama adalah memilih penyedia VPN dan mendaftar untuk mendapatkan akun VPN. Setiap penyedia VPN akan memberikan instruksi dan informasi yang diperlukan untuk menginstal dan mengonfigurasi VPN mereka.
2. Setelah Anda memiliki akun VPN, unduh perangkat lunak VPN dari penyedia tersebut. Mereka biasanya menyediakan perangkat lunak khusus yang kompatibel dengan Windows.
3. Setelah selesai mengunduh, buka file instalasi perangkat lunak VPN. Ikuti petunjuk instalasi yang diberikan oleh penyedia untuk menginstal perangkat lunak VPN.
4. Setelah instalasi selesai, buka perangkat lunak VPN yang baru diinstal. Biasanya, Anda akan melihat ikon atau shortcut perangkat lunak di desktop atau di bilah tugas Windows.
5. Saat pertama kali membuka perangkat lunak VPN, Anda akan diminta untuk masuk menggunakan akun VPN yang telah Anda buat sebelumnya. Masukkan kredensial yang diperlukan untuk masuk ke akun VPN.
6. Setelah masuk, Anda akan melihat antarmuka perangkat lunak VPN, di mana Anda dapat memilih server VPN yang ingin Anda gunakan. Biasanya, Anda dapat memilih server berdasarkan lokasi geografis atau negara.
7. Setelah memilih server, klik tombol "Connect" atau serupa untuk menghubungkan VPN. Tunggu beberapa saat hingga koneksi VPN berhasil terhubung.
8. Setelah terhubung, Anda dapat memverifikasi bahwa VPN berfungsi dengan memeriksa alamat IP publik Anda untuk memastikan bahwa alamat IP yang ditampilkan adalah alamat IP dari server VPN, bukan alamat IP asli Anda.

#### LEMBAR KERJA PESERTA DIDIK (LKPD) 4

1. Buatlah Langkah-langkah instalasi dan penggunaan VPN menggunakan sistem Operasi Mikrotik sebagai server dan contoh penerapannya pada sisi client
2. Tuangkan Hasil pekerjaan kedalam file presentasi yang diupload di form google classroom dan video diupload ke akun youtube kalian masing-masing

#### LEMBAR KERJA PESERTA DIDIK (LKPD) 5

1. Bagaimana langkah-langkah konfigurasi VPN di perangkat MikroTik?
2. Apa saja opsi-opsi konfigurasi yang perlu diatur dalam VPN di MikroTik?
3. Bagaimana cara mengonfigurasi protokol VPN tertentu (misalnya, PPTP atau L2TP) di MikroTik?
4. Apa yang perlu diatur untuk memastikan keamanan koneksi VPN di MikroTik?
5. Bagaimana cara menguji koneksi VPN yang dikonfigurasi di MikroTik untuk memastikan keterhubungannya?
6. Apa langkah-langkah konfigurasi yang perlu dilakukan di sisi client untuk menghubungkan ke VPN MikroTik?
7. Bagaimana cara menggunakan aplikasi SSH di sisi client untuk terhubung ke server tujuan?
8. Apa yang perlu diatur dalam aplikasi SSH untuk mengkonfigurasi otentikasi dan enkripsi yang aman?
9. Bagaimana cara mengatasi masalah umum saat mengkonfigurasi VPN di MikroTik dan SSH di sisi client?
10. Apakah ada perbedaan konfigurasi antara menggunakan SSH melalui koneksi VPN dengan menggunakan SSH langsung tanpa VPN?

#### Jawaban

1. Langkah-langkah konfigurasi VPN di perangkat MikroTik meliputi:
  - Menyiapkan antarmuka (interface) untuk koneksi VPN.

- Mengonfigurasi protokol VPN yang diinginkan (misalnya, PPTP, L2TP, atau OpenVPN) di bagian "IP" atau "PPP" pada MikroTik.
- Mengatur pengguna (user) dan kata sandi (password) untuk otentikasi VPN.
- Mengatur aturan firewall yang memperbolehkan lalu lintas VPN.
- Mengaktifkan layanan VPN dan menyediakan pengaturan tambahan seperti enkripsi, autentikasi, dan parameter lain sesuai kebutuhan.

2. Opsi-opsi konfigurasi yang perlu diatur dalam VPN di MikroTik mencakup:

- Pengaturan protokol VPN yang digunakan.
- Konfigurasi antarmuka dan alamat IP yang terkait dengan koneksi VPN.
- Opsi autentikasi dan enkripsi yang dipilih.
- Pengaturan routing untuk mengarahkan lalu lintas melalui koneksi VPN.
- Pembatasan akses dan izin untuk pengguna VPN.

3. Cara mengonfigurasi protokol VPN tertentu di MikroTik bervariasi tergantung pada protokol yang dipilih. Misalnya, untuk mengonfigurasi PPTP, Anda perlu menyiapkan antarmuka PPTP, membuat pengguna PPTP, dan mengaktifkan layanan PPTP. Untuk L2TP, Anda perlu membuat profil L2TP dan mengatur pengguna L2TP. Untuk OpenVPN, Anda perlu mengimpor konfigurasi OpenVPN yang valid dan mengaktifkan layanan OpenVPN.

4. Untuk memastikan keamanan koneksi VPN di MikroTik, perlu mengatur opsi enkripsi yang kuat, seperti menggunakan enkripsi AES-256, dan memastikan penggunaan protokol keamanan seperti IPsec atau SSL/TLS. Selain itu, konfigurasi firewall MikroTik untuk membatasi akses hanya pada port dan protokol yang diperlukan untuk koneksi VPN.

5. Untuk menguji koneksi VPN di MikroTik, Anda dapat menggunakan perangkat client yang mendukung protokol VPN yang sama dengan konfigurasi MikroTik. Anda dapat mencoba untuk terhubung menggunakan kredensial yang valid dan memverifikasi apakah koneksi berhasil terbentuk dan lalu lintas dapat berjalan melalui VPN.

6. Langkah-langkah konfigurasi di sisi client untuk menghubungkan ke VPN MikroTik meliputi mengatur koneksi VPN di perangkat client, seperti memasukkan alamat IP atau

nama domain server MikroTik, memasukkan pengguna dan kata sandi yang benar, serta mengatur opsi keamanan dan enkripsi sesuai dengan konfigurasi MikroTik.

7. Untuk menggunakan aplikasi SSH di sisi client, Anda perlu mengunduh dan menginstal aplikasi SSH yang sesuai dengan sistem operasi client Anda, seperti PuTTY untuk Windows atau OpenSSH untuk Linux atau macOS.

8. Dalam aplikasi SSH, Anda perlu mengonfigurasi alamat IP atau nama domain server tujuan, port

SSH yang digunakan (biasanya port 22), dan opsi keamanan seperti pemilihan metode otentikasi dan pengaturan kunci publik/privat.

9. Masalah umum saat mengkonfigurasi VPN di MikroTik dan SSH di sisi client dapat termasuk masalah koneksi, masalah otentikasi yang salah, atau konfigurasi yang tidak benar pada MikroTik atau perangkat client. Pengecekan kembali konfigurasi, penggunaan kredensial yang benar, dan pemecahan masalah secara bertahap dapat membantu mengatasi masalah ini.

10. Ada perbedaan konfigurasi antara menggunakan SSH melalui koneksi VPN dengan menggunakan SSH langsung tanpa VPN. Saat menggunakan SSH melalui koneksi VPN, Anda perlu mengonfigurasi koneksi VPN terlebih dahulu, dan kemudian menggunakan aplikasi SSH untuk terhubung ke alamat IP internal atau nama domain dari server tujuan yang terhubung melalui VPN. Sementara itu, saat menggunakan SSH langsung tanpa VPN, Anda dapat langsung menggunakan aplikasi SSH untuk terhubung ke alamat IP publik atau nama domain server tujuan.

#### LEMBAR KERJA PESERTA DIDIK (LKPD) 6

1. Buatlah Langkah-langkah instalasi dan penggunaan VPN dengan menggunakan sistem Interkoneksi Jaringan IP Tunnel supaya antara 2 jaringan jarak jauh bisa berkomunikasi seolah berada di jaringan lokal.
2. Tuangkan Hasil pekerjaan kedalam file presentasi yang diupload di form google classroom dan video diupload ke akun youtube kalian masing-masing

## ASESMEN PEMBELAJARAN, REMEDIAL DAN PENGAYAAN

### RUBRIK PENILAIAN

#### Teknik penilaian

- a. Sikap Prilaku Karakter : Observasi (Format Penilaian Sikap)
- b. Sikap Sosial : Observasi (Format Penilaian Sikap)
- c. Produk : Ujian Tulis (Uraian dan Pilihan Ganda)
- d. Proses : Tes Lisan (Format Assesmen Kinerja Proses)
- e. Keterampilan : Praktikum (Format Assesmen Kinerja Keterampilan)

#### 2. Instrumen penilaian

- a. Lembar Penilaian 1 : Sikap Perilaku Karakter
- b. Lembar Penilaian 2 : Sikap Sosial
- c. Lembar Penilaian 3 : Produk dilengkapi kunci jawaban
- d. Lembar Penilaian 4 : Proses
- e. Lembar Penilaian 5 : Keterampilan

#### 3. Pembelajaran remedial dan pengayaan

##### a) Remedial

Remedial dilaksanakan setelah diadakan penilaian pengetahuan bagi peserta didik yang mendapat nilai di bawah KKM dengan memberi tugas berupa:

- Mengulang Pendalaman Materi terkait rincian materi yang sulit
- Memanfaatkan peserta didik yang nilainya paling baik dan mempunyai kemampuan lebih untuk melakukan tutor sebaya
- Mengulang Melakukan Evaluasi dengan materi yang sama

##### b) Pengayaan

Peserta didik yang mendapat nilai di atas KKM diberikan pengayaan berupa:

- Memberikan tugas baru yang sepadan
- Mengembangkan materi yang sudah dikuasai dan membandingkan dari berbagai sumber belajar.

Mengetahui  
Kepala SMK Negeri 1 Punggelan

Banjarnegara, 19 Juni 2023  
Guru Mata Pelajaran,

**Drs. Supriyadi**  
**NIP. 19660128 199302 1 002**

**Idiarso, S.Kom**  
**NIP.19830804 202221 1 006**

**Asesmen Proses**

No	Kelompok	Keterbacaan Materi		Karya berupa Peta Konsep		Kreativitas		Laporan Diskusi		Presentasi	
		Ya	Tdk	Ya	Tdk	Ya	Tdk	Ya	Tdk	Ya	Tdk

**Asesmen Akhir : (Nama)**

Nama Siswa:				
No	Kreteria Ketuntasan	KETERCAPAIAN		
		Kurang kompeten (1)	Cukup Kompeten (2)	Kompeten (3)
1	Menjelaskan Pengertian VPN		v	
2	Mengidentifikasi Jenis-jenis VPN			v
3	Mengidentifikasi manfaat penggunaan VPN		v	
4	Menerapkan VPN server dan tunnel		v	
5	Menerapkan SSH server sebagai remot access	v		
6	Menerapkan interkoneksi Wan seolah berada di Lanatau lokal area network		v	

**KKTP:**

0 – 40 %	Belum tuntas, remidi pada seluruh materi
41 – 60 %	Belum tuntas, remidi pada materi yang belum dikuasai
61 – 80 %	Sudah tuntas, tetapi tanpa pengayaan
81 – 100%	Sudah tuntas, perlu pengayaan atau tantangan lebih



## Profil Pelajar Pancasila

No	Dimensi <b>Kreatif</b> -Sub Elemen	Terlihat maks	Terlihat sedikit	Belum terlihat
1	Mengeksplorasi dan mengekspresikan pikiran dan/atau perasaannya dalam bentuk karya dan/atau tindakan, serta mengevaluasinya dan mempertimbangkan dampak dan risikonya bagi diri dan lingkungannya			
2	Menghasilkan gagasan yang beragam untuk mengekspresikan pikiran dan/atau perasaannya, menilai gagasannya, serta memikirkan segala risikonya dengan mempertimbangkan banyak perspektif seperti etika dan nilai kemanusiaan ketika gagasannya direalisasikan			

### Alat dan Sumber Belajar

1. Media : *Google Classroom, Google Meet*
2. Alat : Smartphone atau Laptop
3. Bahan : Kuota, Lembar kerja, File Dokumen materi.
4. Sumber Belajar : Internet, Ebook, youtube

## PENILAIAN

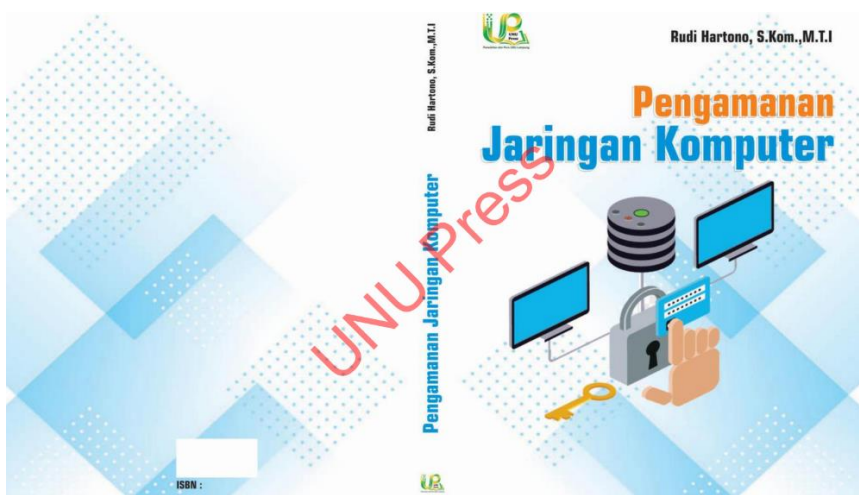
No	Aspek yang dinilai	Teknik	Penilaian	Waktu Penilaian
1	<u>Sikap / Afektif</u>		<u>Pengamatan</u>	Selama pembelajaran pada google classroom
2	Pengetahuan / Kognitif		Tes Tertulis	Penyelesaian tugas diskusi pada google classroom
3	<u>Ketrampilan/Psikomotorik</u>		<u>Unjuk Kerja</u>	Selama pembelajaran pada google classroom

## BAHAN BACAAN

Sistem Keamanan Jaringan.

	
LINK:	<a href="https://idiuptocode.blogspot.com/2022/07/sistem-keamanan-jaringan.html">https://idiuptocode.blogspot.com/2022/07/sistem-keamanan-jaringan.html</a>

Buku Pengamanan Jaringan Komputer

	
LINK:	<a href="https://drive.google.com/drive/u/0/search?fbclid=IwAR3ikp4fZw-myJQH1He4bo_ay_U_i9SZ23pG2mT9SWmaiKA0wsynEfKmtQQ&amp;q=jaringan">https://drive.google.com/drive/u/0/search?fbclid=IwAR3ikp4fZw-myJQH1He4bo_ay_U_i9SZ23pG2mT9SWmaiKA0wsynEfKmtQQ&amp;q=jaringan</a>

## Buku Jaringan Komputer

	
LINK:	<a href="https://drive.google.com/drive/u/0/search?fbclid=IwAR3ikp4fZw-myJQH1He4bo_ay_U_i9SZ23pG2mT9SWmaiKA0wsynEfKmtQQ&amp;q=jaringan">https://drive.google.com/drive/u/0/search?fbclid=IwAR3ikp4fZw-myJQH1He4bo_ay_U_i9SZ23pG2mT9SWmaiKA0wsynEfKmtQQ&amp;q=jaringan</a>

## Ebook Desain Keamanan Jaringan

	
LINK:	<a href="https://drive.google.com/drive/u/0/search?fbclid=IwAR3ikp4fZw-myJQH1He4bo_ay_U_i9SZ23pG2mT9SWmaiKA0wsynEfKmtQQ&amp;q=jaringan">https://drive.google.com/drive/u/0/search?fbclid=IwAR3ikp4fZw-myJQH1He4bo_ay_U_i9SZ23pG2mT9SWmaiKA0wsynEfKmtQQ&amp;q=jaringan</a>

## **Glosarium**

**VPN (Virtual Private Network):** Jaringan pribadi virtual yang memungkinkan pengguna untuk mengirim dan menerima data melalui koneksi internet dengan aman dan terenkripsi.

**Server VPN:** Server yang bertugas mengelola koneksi VPN dan memberikan akses ke jaringan pribadi melalui tunneling data yang aman.

**Tunneling:** Proses mengirim data melalui jaringan publik (seperti internet) dengan cara mengemasnya dalam paket data terenkripsi yang aman.

**Protokol VPN:** Standar komunikasi yang digunakan dalam mengatur koneksi VPN, seperti OpenVPN, IPsec, PPTP, L2TP, dan SSTP.

**Enkripsi:** Proses mengubah data menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang, sehingga melindungi kerahasiaan dan integritas data.

**Dekripsi:** Proses mengembalikan data yang telah dienkripsi menjadi bentuk aslinya setelah diterima oleh penerima yang berwenang.

**IP Address:** Alamat numerik yang unik diberikan kepada setiap perangkat yang terhubung ke jaringan, digunakan untuk mengidentifikasi dan mengarahkan paket data.

**Firewall:** Sistem keamanan yang digunakan untuk memantau dan mengontrol lalu lintas data yang masuk dan keluar dari jaringan, termasuk lalu lintas yang melalui VPN.

**Protokol Enkripsi:** Protokol khusus yang digunakan untuk mengamankan data yang dikirim melalui VPN, seperti AES (Advanced Encryption Standard), 3DES (Triple Data Encryption Standard), atau RSA (Rivest-Shamir-Adleman).

**Bandwidth:** Ukuran kapasitas maksimum yang dapat ditransfer melalui jaringan dalam periode waktu tertentu, biasanya diukur dalam bit per detik (bps).

**Log Aktivitas:** Rekaman yang berisi catatan kegiatan pengguna, seperti waktu dan durasi koneksi, alamat IP sumber dan tujuan, serta jenis data yang ditransfer melalui VPN.

**Double VPN:** Konfigurasi VPN di mana lalu lintas data melewati dua server VPN sebelum mencapai tujuan akhir, meningkatkan tingkat keamanan dan anonimitas.

**Kill Switch:** Fitur yang mematikan koneksi internet secara otomatis jika koneksi VPN terputus, untuk mencegah akses ke jaringan publik yang tidak aman.

**Split Tunneling:** Pengaturan di mana sebagian lalu lintas data dikirim melalui VPN, sementara sebagian lainnya langsung terhubung ke internet tanpa melalui VPN.

**Protokol PPTP (Point-to-Point Tunneling Protocol):** Protokol VPN yang umum digunakan untuk koneksi VPN yang lebih sederhana, namun memiliki tingkat keamanan yang lebih rendah dibandingkan protokol lainnya.

**Protokol L2TP/IPsec (Layer 2 Tunneling Protocol/Internet Protocol Security):** Protokol kombinasi yang menyediakan tingkat keamanan yang lebih tinggi dengan menggunakan enkripsi IPsec dan koneksi tunneling L2TP.

**Protokol OpenVPN:** Protokol open-source yang umum digunakan untuk koneksi VPN yang aman, menawarkan tingkat keamanan dan fleksibilitas yang tinggi.

**VPN Client:** Perangkat lunak atau aplikasi yang digunakan untuk mengatur dan mengelola koneksi VPN dari perangkat pengguna ke server VPN.

**VPN Gateway:** Titik masuk ke jaringan VPN yang berfungsi sebagai penghubung antara klien VPN dan server VPN.

**Anonimitas:** Kondisi di mana identitas pengguna atau lokasi fisiknya disembunyikan atau di rahasiakan, sehingga tidak dapat dilacak oleh pihak yang tidak berwenang.

**Split DNS:** Konfigurasi di mana pengguna VPN dapat mengakses domain dan layanan khusus melalui jaringan VPN, sementara domain dan layanan umum diakses melalui koneksi internet reguler.

**VPN Concentrator:** Perangkat keras khusus yang digunakan untuk mengelola dan menghubungkan banyak klien VPN ke server VPN secara efisien.

**Port Forwarding:** Proses mengarahkan lalu lintas jaringan yang masuk melalui port tertentu ke tujuan yang ditentukan, sering digunakan dalam pengaturan VPN untuk mengizinkan akses ke layanan internal yang dilindungi oleh VPN.

**VPNaaS (VPN as a Service):** Model layanan di mana penyedia layanan menyediakan infrastruktur VPN lengkap kepada pengguna, termasuk server, konektivitas, dan keamanan, tanpa memerlukan pengelolaan server VPN sendiri.

**VPN Client Compatibility:** Kemampuan VPN client untuk berintegrasi dan berfungsi dengan berbagai platform dan sistem operasi, seperti Windows, macOS, Linux, iOS, dan Android.

**VPN Gateway Compatibility:** Kemampuan VPN gateway untuk berintegrasi dan berkomunikasi dengan berbagai protokol VPN dan perangkat VPN lainnya.

**Remote Access VPN:** Jenis VPN yang digunakan untuk mengamankan koneksi jarak jauh pengguna ke jaringan pribadi, memungkinkan akses aman ke sumber daya jaringan dari luar lokasi fisik.

**Site-to-Site VPN:** Jenis VPN yang menghubungkan dua atau lebih jaringan lokal (site) yang terpisah secara geografis, menciptakan koneksi aman dan terenkripsi antara lokasi-lokasi tersebut.

**VPN Overhead:** Biaya tambahan yang terkait dengan penggunaan VPN, seperti

**pengurangan kecepatan koneksi dan penggunaan sumber daya tambahan yang diperlukan untuk mengenkripsi dan mendekripsi data.**

**VPN Load Balancing:** Proses mendistribusikan beban lalu lintas VPN secara merata di antara beberapa server VPN untuk meningkatkan kinerja dan ketersediaan.

**VPN Logging:** Praktik menyimpan catatan aktivitas dan data terkait penggunaan VPN, termasuk informasi seperti waktu dan durasi koneksi, alamat IP, dan jumlah data yang ditransfer.

**VPN Security Audit:** Proses evaluasi independen yang dilakukan untuk mengidentifikasi dan mengurangi potensi celah keamanan dalam konfigurasi dan implementasi VPN.

**VPN Bypass:** Praktik atau metode yang digunakan untuk menghindari atau melewati penggunaan VPN dalam mengakses atau mengirimkan lalu lintas ke tujuan tertentu.

**VPN Encryption Key:** Kunci kriptografi yang digunakan untuk mengenkripsi dan mendekripsi data yang dikirim melalui koneksi VPN, yang harus diketahui oleh kedua ujung koneksi.

**VPN Leakage:** Keadaan di mana data atau informasi yang seharusnya terlindungi oleh VPN bocor atau terungkap ke pihak yang tidak berwenang, bisa terjadi akibat konfigurasi yang salah atau kerentanan keamanan.

**VPN Policy:** Kebijakan yang ditetapkan oleh administrator jaringan

an atau penyedia VPN untuk mengatur penggunaan dan akses VPN, termasuk aturan keamanan dan batasan penggunaan.

Saya telah menambahkan beberapa istilah baru ke dalam glosarium VPN. Harapannya, tambahan ini akan membantu memperluas pemahaman Anda tentang konsep-konsep yang terkait dengan VPN.