11/21/2024

JARINGAN KOMPUTER LANJUT

PERTEMUAN X

NAMA: RIFANDY ARNAS

NIM/NPM: 232310001

KELAS: TI – 23 – PA (LAB 2)

Tugas Pertemuan Ke-10

TUNNELING

PEMBAHASAN

Github:
https://github.com/Rifandy232310001TeknologiInformasi/Jaringan_Komputer_Lanjut-Lab

Soal nomor 1

Tunneling:

Tunneling adalah proses pengiriman data antar jaringan melalui protokol tertentu yang membungkus data aslinya dalam format lain. Proses ini memungkinkan data melewati jaringan yang tidak mendukung protokol tersebut. Contohnya adalah encapsulation data TCP/IP dalam protokol lain seperti GRE atau IPsec.

VPN (Virtual Private Network):

VPN adalah teknologi yang memungkinkan pengguna untuk membuat koneksi jaringan yang aman dan terenkripsi melalui jaringan publik seperti internet. VPN menciptakan "jalur pribadi" antara perangkat pengguna dan server tujuan.

Pentingnya Teknologi Ini:

- ⇨ **Keamanan: Menjaga kerahasiaan data yang dikirimkan, terutama pada jaringan publik.**
- ⇨ **Fleksibilitas: Mendukung karyawan yang bekerja jarak jauh dengan akses aman ke jaringan perusahaan.**
- ⇨ **Konektivitas Global: Menghubungkan kantor-kantor cabang di berbagai lokasi secara efisien.**

Contoh Kasus:

- ⇨ Perusahaan multinasional menggunakan VPN untuk menghubungkan kantor pusat dengan cabang-cabang di berbagai negara.
- ⇨ Individu menggunakan VPN untuk mengakses konten yang dibatasi secara geografis.

Soal nomor 2

1. **PPTP (Point-to-Point Tunneling Protocol):**

- **Kelebihan:**
    - Mudah dikonfigurasi.
    - Kompatibel dengan berbagai perangkat.
- **Kekurangan:**
    - Keamanan relatif rendah karena enkripsi yang lemah.

2. **L2TP (Layer 2 Tunneling Protocol):**

- **Kelebihan:**
    - Mendukung enkripsi IPsec untuk keamanan lebih baik.
    - Cocok untuk koneksi dengan IP dinamis.
- **Kekurangan:**
    - Pengaturan lebih kompleks dibanding PPTP.

3. **EoIP (Ethernet over IP):**

- **Kelebihan:**
    - Menghubungkan jaringan Layer 2 melalui Layer 3 (IP).
    - Sangat fleksibel untuk bridging.

- **Kekurangan:**
    - Tidak memiliki enkripsi bawaan.

Soal nomor 3

1. **Keamanan:**

- PPTP: Keamanan rendah karena hanya menggunakan protokol MPPE (Microsoft Point-to-Point Encryption).
- L2TP: Lebih aman karena mendukung IPsec sebagai lapisan enkripsi tambahan.

2. **Kompatibilitas:**

- PPTP: Sangat kompatibel dengan berbagai perangkat dan sistem operasi.
- L2TP: Dapat bekerja dengan baik tetapi memerlukan konfigurasi tambahan untuk IPsec.

3. **Penggunaan di Jaringan dengan IP Dinamis:**

- PPTP: Mudah digunakan pada jaringan dengan IP dinamis tetapi kurang aman.
- L2TP: Lebih aman, tetapi memerlukan konfigurasi lebih untuk menangani perubahan IP.

Soal nomor 4

Peran EoIP:

EoIP memungkinkan penggabungan dua jaringan LAN yang secara fisik terpisah menjadi satu jaringan Layer 2 melalui koneksi IP.

Cara Kerja:

- EoIP membuat tunnel yang membungkus frame Ethernet ke dalam paket IP.
- Frame tersebut kemudian dikirim melalui jaringan IP ke tujuan, di mana data akan diekstrak kembali menjadi frame Ethernet.

Contoh Implementasi:

Perusahaan dengan dua kantor di kota berbeda dapat menggunakan EoIP untuk menghubungkan jaringan lokal mereka agar terlihat seperti satu jaringan LAN.

Soal nomor 5

Peningkatan Keamanan oleh IPsec:

IPsec mengenkripsi data pada tingkat jaringan, sehingga menjamin kerahasiaan dan integritas data yang dikirimkan.

Prinsip Kerja IPsec:

- **Enkripsi:** Data dienkripsi menggunakan algoritma seperti AES atau 3DES.
- **Autentikasi:** Memastikan hanya pengguna yang sah yang dapat mengakses data.

- **Integritas:** Melindungi data dari perubahan selama transmisi menggunakan protokol AH (Authentication Header) atau ESP (Encapsulating Security Payload).

Kombinasi L2TP/IPsec:

Kombinasi ini memberikan:

- **Keamanan Tinggi:** L2TP menangani tunneling sementara IPsec menyediakan enkripsi.
- **Kompatibilitas Luas:** Dukungan luas pada perangkat modern.