Laboratorium
Multimedia dan Internet of Things
Departemen Teknik Komputer
Institut Teknologi Sepuluh Nopember

Laporan Sementara
Praktikum Jaringan Komputer

Tunneling dan IPsec (IP Security)

Farhan Abdurrahman Muthohhar - 5024221050

17 Mei 2025

1 Pendahuluan

1.1 Latar Belakang

Latar belakang dari tunneling adalah komunikasi antar perangkat melalui jaringan publik memiliki tingkat keamanan yang rendah, sehingga data yang dikirimkan rentan terhadap ancaman seperti penyadapan, hacking, atau pemalsuan data. Oleh karena itu, dibutuhkan mekanisme untuk memastikan keamanan dan kerahasiaan data dalam transmisi. Tunneling adalah Salah satu teknologi penting yang digunakan untuk mengatasi permasalahan tersebut. cara kerja tunneling yaitu proses membungkus atau encapsule paket data dalam protokol lain agar dapat dikirim secara aman melalui jaringan publik. Tunneling sering digunakan dalam implementasi VPN, yang memungkinkan komunikasi terenkripsi antar jaringan privat melalui internet.

Untuk menjamin integritas, otentikasi, dan kerahasiaan data, digunakan protokol IPsec (IP Security). IPsec adalah kumpulan protokol yang bekerja pada lapisan jaringan Network Layer dari model OSI. IPsec menyediakan dua mode utama, yaitu Transport Mode dan Tunnel Mode, dan menggunakan dua protokol utama, yaitu Authentication Header AH dan Encapsulating Security Payload ESP.

latar belakang praktikum ini, memberikan pengetahuan bagaimana proses tunneling dan IPsec bekerja dalam mengamankan komunikasi jaringan. Praktikum ini bertujuan untuk memberikan pemahaman praktis tentang konfigurasi dan analisis lalu lintas jaringan yang diamankan dengan IPsec, serta bagaimana tunneling digunakan dalam konteks VPN atau komunikasi antar jaringan secara aman.

1.2 Dasar Teori

Tunneling adalah teknik dalam jaringan komputer yang memungkinkan pengiriman data dari satu jaringan ke jaringan lain melalui jalur atau terowongan virtual. Proses ini dilakukan dengan membungkus atau encapsulation paket data asli ke dalam paket baru yang dapat melewati jaringan publik, seperti Internet. Tunneling sering digunakan dalam implementasi VPN untuk menjaga privasi dan keamanan koneksi antar titik yang terpisah secara geografis. Salah satu metode keamanan yang umum digunakan dalam tunneling adalah IPsec. IPsec adalah sebuah protokol keamanan jaringan yang beroperasi pada lapisan jaringan Layer 3 OSI untuk melindungi dan mengenkripsi paket IP. IPsec menyediakan mekanisme autentikasi, integritas, dan kerahasiaan data melalui dua mode utama, yaitu transport mode dan tunnel mode. Tunnel mode digunakan dalam VPN untuk mengamankan komunikasi antar gateway atau antara host dan gateway dengan cara mengenkripsi seluruh paket IP, sementara transport mode hanya mengenkripsi payload-nya. Dengan penerapan tunneling dan IPsec, data yang dikirim melalui jaringan publik dapat tetap terjaga keamanannya, terlindung dari ancaman penyadapan, manipulasi, dan hacking.

2 Tugas Pendahuluan

1. Diberikan studi kasus untuk konfigurasi VPN IPSec. Suatu perusahaan ingin membuat koneksi aman antara kantor pusat dan cabang. Jelaskan secara detail: Fase negosiasi IPSec (IKE Phase 1 dan Phase 2) Parameter keamanan yang harus disepakati (algoritma enkripsi, metode autentikasi, lifetime key) Konfigurasi sederhana pada sisi router untuk memulai koneksi IPSec site-to-site

Fase Negosiasi IPSec: IKE Phase 1 dan Phase 2

IPSec menggunakan protokol IKE (Internet Key Exchange) dalam membentuk koneksi aman antara dua jaringan. Proses ini terdiri dari dua fase utama.

IKE Phase 1 bertujuan untuk membentuk *Security Association (SA)* antara dua perangkat dengan menyepakati parameter keamanan seperti algoritma enkripsi, autentikasi, dan grup Diffie-Hellman. Proses ini dapat dilakukan dalam *Main Mode* (lebih aman) atau *Aggressive Mode* (lebih cepat, tetapi kurang aman).

IKE Phase 2 digunakan untuk membentuk *IPSec SA* yang berfungsi melindungi lalu lintas data. Fase ini menggunakan *Quick Mode* untuk pertukaran parameter enkripsi dan autentikasi data, seperti ESP (Encapsulating Security Payload) dan AH (Authentication Header).

Referensi:

- Wahyudi, A. (2017). *Keamanan Jaringan Komputer*. ANDI Yogyakarta.
- Lumbantoruan, R. (2021). *Jaringan Komputer Tingkat Lanjut*. Penerbit Deepublish.

Parameter Keamanan yang Harus Disepakati

Untuk membangun tunnel yang aman antara kantor pusat dan cabang, diperlukan kesepakatan parameter berikut:

- **Algoritma Enkripsi**: Contohnya adalah AES-256 atau 3DES.
- **Algoritma Hashing**: SHA-256 digunakan untuk menjaga integritas data.
- **Autentikasi**: Umumnya menggunakan *Pre-Shared Key* (PSK).
- **Diffie-Hellman Group**: Contoh grup 14 (2048-bit).
- **Key Lifetime**: Masa berlaku kunci, misalnya 3600 detik.

Referensi:

- Taufik, I. (2019). *Implementasi Keamanan Jaringan Menggunakan VPN IPSec Berbasis Mikrotik*, Jurnal INFOKAM, STMIK AMIK Riau.
- Kementerian Kominfo RI. (2020). *Modul Pelatihan Keamanan Jaringan Dasar*.

Contoh Konfigurasi Router (Cisco)

Topologi

- Kantor Pusat: IP Lokal `192.168.1.0/24`, IP Publik `203.0.113.1`
- Kantor Cabang: IP Lokal `192.168.2.0/24`, IP Publik `198.51.100.1`

Konfigurasi Router di Kantor Pusat

```
crypto isakmp policy 10
 encryption aes 256
 hash sha256
 authentication pre-share
 group 14
 lifetime 3600
```

```
crypto isakmp key kuncirahasia address 198.51.100.1

crypto ipsec transform-set VPNSET esp-aes esp-sha-hmac
 mode tunnel

crypto map VPNMAP 10 ipsec-isakmp
 set peer 198.51.100.1
 set transform-set VPNSET
 match address 100

interface GigabitEthernet0/0
 crypto map VPNMAP

access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Konfigurasi Router di Kantor Cabang

```
crypto isakmp policy 10
 encryption aes 256
 hash sha256
 authentication pre-share
 group 14
 lifetime 3600

crypto isakmp key kuncirahasia address 203.0.113.1

crypto ipsec transform-set VPNSET esp-aes esp-sha-hmac
 mode tunnel

crypto map VPNMAP 10 ipsec-isakmp
 set peer 203.0.113.1
 set transform-set VPNSET
 match address 100

interface GigabitEthernet0/0
 crypto map VPNMAP

access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
```

Referensi:

- Maulana, A. (2020). *Implementasi VPN IPSec Site to Site Menggunakan Cisco Packet Tracer*, Jurnal SIMETRIS.
- Mulyana, A. (2021). *Panduan Konfigurasi VPN Cisco Router*, Politeknik Negeri Bandung.

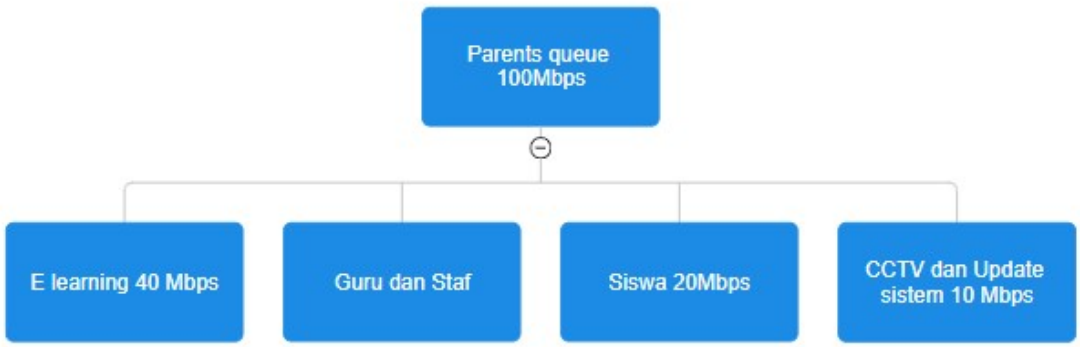
2. Sebuah sekolah memiliki bandwidth internet 100 Mbps yang dibagi menjadi: 40 Mbps untuk e-learning 30 Mbps untuk guru dan staf (akses email, cloud storage) 20 Mbps untuk siswa (browsing umum) 10 Mbps untuk CCTV dan update sistem Buatlah skema Queue Tree yang lengkap: Parent dan child queue Penjelasan marking Prioritas dan limit rate pada masing-masing queue

   Skema Queue Tree untuk Manajemen Bandwidth Sekolah

   Sebuah sekolah memiliki total bandwidth internet sebesar 100 Mbps yang harus dibagi ke beberapa layanan dengan alokasi sebagai berikut:

   - 40 Mbps untuk e-learning
   - 30 Mbps untuk guru dan staf (akses email, cloud storage)
   - 20 Mbps untuk siswa (browsing umum)
   - 10 Mbps untuk CCTV dan update sistem

   Skema Queue Tree



Gambar 1: Skema Queue Tree dengan Parent dan Child Queue

   - **Parent Queue**: Mengontrol keseluruhan bandwidth 100 Mbps pada interface utama yang terhubung ke internet.
   - **Child Queues**: Membagi bandwidth sesuai dengan kebutuhan masing-masing layanan.
     - E-learning: 40 Mbps
     - Guru dan staf: 30 Mbps
     - Siswa: 20 Mbps
     - CCTV dan update sistem: 10 Mbps

   Penjelasan Marking

   Marking paket digunakan untuk mengidentifikasi dan mengelompokkan jenis lalu lintas agar dapat diberikan perlakuan yang berbeda di dalam queue tree.

   - **Marking DSCP atau TOS**: Setiap jenis layanan diberi tanda (marking) berbeda, misalnya:

  - E-learning: DSCP 46 (Expedited Forwarding - prioritas tinggi)
  - Guru dan staf: DSCP 26 (Assured Forwarding)
  - Siswa: DSCP 10 (Best Effort)
  - CCTV dan update sistem: DSCP 18 (Low Priority)

Prioritas dan Limit Rate

Pengaturan prioritas dan limit rate dilakukan untuk menjamin kualitas layanan sesuai kebutuhan:

- **E-learning**
  - Prioritas *tinggi* agar aktivitas belajar online lancar tanpa gangguan.
  - Limit rate: **40 Mbps**
- **Guru dan Staf**
  - Prioritas *sedang*, akses email dan cloud harus stabil.
  - Limit rate: **30 Mbps**
- **Siswa**
  - Prioritas *rendah* untuk browsing umum.
  - Limit rate: **20 Mbps**
- **CCTV dan Update Sistem**
  - Prioritas *rendah* tetapi tetap harus ada bandwidth yang dijamin.
  - Limit rate: **10 Mbps**

Contoh Konfigurasi Queue Tree (MikroTik)

Berikut contoh konfigurasi sederhana menggunakan MikroTik RouterOS untuk Queue Tree:

```
/queue tree
add name=parent-queue max-limit=100M interface=ether1

add name=e-learning parent=parent-queue packet-mark=e-learning-mark
limit-at=40M max-limit=40M priority=1
add name=guru-staf parent=parent-queue packet-mark=guru-staf-mark
limit-at=30M max-limit=30M priority=2
add name=siswa parent=parent-queue packet-mark=siswa-mark limit-at=20M
max-limit=20M priority=3
add name=cctv-update parent=parent-queue packet-mark=cctv-mark limit-at=10M
max-limit=10M priority=4
```

Referensi

- Hariyanto, D. (2020). *Manajemen Bandwidth Menggunakan Queue Tree di MikroTik RouterOS*, Jurnal Teknologi Informasi dan Komunikasi.
- Kurniawan, A. (2019). *Pengaturan QoS dan Queue Tree untuk Optimasi Jaringan*, Modul Pelatihan Kominfo RI.
- MikroTik Documentation (2023). *Queue Tree*. https://wiki.mikrotik.com/wiki/Manual:Queue_Tree