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

Laporan Sementara
Praktikum Jaringan Komputer

Tunneling dan IPSec

Muhammad Panji Fathuroni - 5024231050

2025

1 Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi telah menjadikan internet sebagai infrastruktur vital yang menopang hampir seluruh aspek kehidupan modern, mulai dari bisnis hingga interaksi sosial. Namun, sebagai sebuah jaringan publik yang terbuka, internet secara inheren tidak aman dan membawa risiko signifikan terhadap privasi dan keamanan data. Informasi yang ditransmisikan rentan terhadap berbagai ancaman seperti penyadapan, modifikasi, dan pencurian oleh pihak yang tidak bertanggung jawab. Untuk menjawab tantangan keamanan ini, organisasi dan individu memerlukan metode untuk membangun jalur komunikasi yang aman dan privat di atas jaringan publik, sebuah konsep yang dikenal sebagai Virtual Private Network (VPN). Implementasi VPN secara fundamental mengandalkan dua teknologi inti yang saling melengkapi, yaitu Tunneling dan IPsec. Tunneling merupakan mekanisme yang menciptakan sebuah "terowongan" virtual melalui jaringan internet, yang bekerja dengan cara membungkus paket data asli ke dalam paket data lain. Proses enkapsulasi ini memungkinkan data untuk melintasi jaringan yang berbeda dan menyembunyikan alamat IP asli, namun mekanisme ini sendiri tidak menyediakan perlindungan keamanan. Untuk mengamankan data yang melewati terowongan tersebut, diperlukan sebuah kerangka kerja keamanan yang kuat. Di sinilah IPsec (Internet Protocol Security) memainkan peran sentral. IPsec adalah sebuah suite protokol yang dirancang untuk mengamankan komunikasi pada lapisan jaringan dengan menyediakan layanan esensial berupa kerahasiaan melalui enkripsi, integritas data melalui hashing, serta autentikasi untuk memverifikasi identitas pihak-pihak yang berkomunikasi. Oleh karena itu, praktikum ini menjadi sangat relevan karena memberikan pemahaman praktis tentang bagaimana mengonfigurasi dan menganalisis kolaborasi antara tunneling dan IPsec untuk membangun sebuah koneksi VPN yang aman dan andal, sebuah kompetensi yang krusial dalam dunia jaringan komputer dan keamanan siber. Dasar Teori

1.2 Dasar Teori

Tunneling adalah sebuah teknik jaringan di mana sebuah paket data dari protokol tertentu dibungkus atau dienkapsulasi di dalam header paket dari protokol lain sebelum dikirimkan. Proses ini dapat dianalogikan seperti memasukkan sebuah surat ke dalam amplop baru untuk dikirimkan melalui sistem pos yang berbeda. Router di titik awal tunnel akan menerima paket asli, menambahkan header baru, dan mengirimkannya melalui jaringan perantara. Di titik akhir, router penerima akan melepaskan header tambahan tersebut untuk mengekstrak paket asli dan meneruskannya ke tujuan akhir. Protokol tunneling yang umum digunakan adalah Generic Routing Encapsulation (GRE) yang sangat fleksibel karena mampu membungkus berbagai jenis protokol, namun tidak memiliki fitur keamanan bawaan. Untuk mengatasi kelemahan keamanan pada protokol tunneling dasar, digunakanlah IPsec (Internet Protocol Security). IPsec adalah sebuah kerangka kerja standar yang dikembangkan oleh IETF untuk menyediakan keamanan pada lapisan IP (Layer 3). IPsec menawarkan tiga pilar keamanan utama: kerahasiaan (confidentiality) yang dicapai melalui enkripsi data menggunakan algoritma seperti AES; integritas (integrity) yang menjamin data tidak diubah selama transmisi menggunakan fungsi hash seperti SHA; dan autentikasi (authentication) yang memverifikasi identitas pengirim dan penerima, biasanya menggunakan Pre-Shared Key (PSK) atau sertifikat digital. Arsitektur IPsec terdiri dari beberapa komponen utama. Dua protokol inti yang menyediakan keamanan adalah Authentication

Header (AH) dan Encapsulating Security Payload (ESP). AH menyediakan autentikasi dan integritas untuk keseluruhan paket IP, termasuk header-nya, namun tidak menyediakan enkripsi. Sementara itu, ESP adalah protokol yang lebih modern dan umum digunakan karena mampu menyediakan kerahasiaan (enkripsi), integritas, dan autentikasi untuk payload data, namun tidak untuk header IP terluar. Proses negosiasi parameter keamanan antara dua perangkat, seperti algoritma enkripsi dan kunci yang akan digunakan, dikelola oleh protokol Internet Key Exchange (IKE). IKE bekerja dalam dua fase: Fase 1 membangun saluran komunikasi yang aman untuk negosiasi, dan Fase 2 menggunakan saluran tersebut untuk menyepakati parameter spesifik untuk mengamankan data aktual. Dalam implementasinya, IPsec dapat beroperasi dalam dua mode yang berbeda: Mode Transport dan Mode Tunnel. Pada Mode Transport, IPsec hanya mengenkripsi dan/atau mengautentikasi payload (data) dari paket asli, sementara header IP asli tetap tidak berubah. Mode ini umumnya digunakan untuk komunikasi ujung ke ujung (end-to-end) antara dua host. Sebaliknya, Mode Tunnel mengenkapsulasi keseluruhan paket IP asli (baik header maupun payload) ke dalam sebuah paket IP yang baru dengan header IP yang baru pula. Mode Tunnel adalah mode yang paling umum digunakan untuk membangun VPN site-to-site, di mana gateway atau router di setiap lokasi bertindak sebagai titik akhir dari terowongan IPsec, mengamankan seluruh lalu lintas data antar jaringan privat.

2 Tugas Pendahuluan

1. **Studi Kasus Konfigurasi VPN IPsec Site-to-Site**

   Sebuah perusahaan ingin membuat koneksi aman antara kantor pusat dan cabang. Berikut adalah penjelasan detailnya.

   a. Fase Negosiasi IPsec (IKE Phase 1 dan Phase 2)

   Proses negosiasi IPsec dikelola oleh protokol IKE (*Internet Key Exchange*) dan dibagi menjadi dua fase utama untuk membangun koneksi yang aman.

   - **IKE Phase 1 (Fase Pembangunan Terowongan Manajemen):** Tujuannya adalah untuk mengautentikasi kedua perangkat dan membuat saluran komunikasi yang aman untuk melindungi negosiasi selanjutnya. Proses ini diringkas dengan akronim **HAGLE**: Hashing, Authentication, Diffie-Hellman Group, Lifetime, dan Encryption.
   - **IKE Phase 2 (Fase Pembangunan Terowongan Data):** Tujuannya adalah menegosiasikan parameter keamanan untuk terowongan yang akan dilewati oleh data pengguna sebenarnya. Negosiasi ini terjadi di dalam saluran aman yang telah dibuat oleh Fase 1 dan akan menyepakati protokol (ESP), algoritma, mode tunnel, dan lifetime untuk sesi data.

   b. Parameter Keamanan yang Harus Disepakati

   Agar koneksi berhasil, kedua router harus dikonfigurasi dengan parameter yang identik. Tabel berikut merangkum parameter krusial tersebut.

Tabel 1: Parameter Keamanan Esensial pada IPsec

Parameter	Deskripsi dan Contoh Rekomendasi
Algoritma Enkripsi	Menentukan tingkat kerahasiaan data. **Contoh:** AES-256 (paling aman).
Metode Autentikasi	Memverifikasi identitas router lawan. **Contoh:** Pre-Shared Key (PSK).
Algoritma Hash	Menjamin integritas data. **Contoh:** SHA-256.
DH Group	Digunakan untuk pertukaran kunci yang aman. **Contoh:** Group 14 atau lebih tinggi.
Lifetime Key	Durasi validitas kunci. **Contoh:** 86400 detik (Phase 1) dan 3600 detik (Phase 2).

c. Konfigurasi Sederhana pada Sisi Router

Berikut adalah contoh konfigurasi pada router MikroTik di kantor pusat (IP Publik `1.1.1.1`) yang terhubung ke kantor cabang (IP Publik `2.2.2.2`).

```
# Langkah 1: Konfigurasi Peer
/ip ipsec peer
add address=2.2.2.2 name=ke-cabang secret="RahasiaKantorPusat123"

# Langkah 2: Konfigurasi Proposal
/ip ipsec proposal
set [find default=yes] auth-algorithms=sha256 enc-algorithms=aes-256-cbc

# Langkah 3: Konfigurasi Policy (Traffic Selector)
/ip ipsec policy
add dst-address=192.168.20.0/24 src-address=192.168.10.0/24 \
tunnel=yes proposal=default sa-dst-address=2.2.2.2 sa-src-address=1.1.1.1

# Langkah 4: Aturan NAT Bypass
/ip firewall nat
add action=accept chain=srcnat dst-address=192.168.20.0/24 \
src-address=192.168.10.0/24
```

2. **Skema Queue Tree untuk Manajemen Bandwidth Sekolah**

   Untuk alokasi bandwidth 100 Mbps, diperlukan penandaan paket (Mangle) dan pembuatan struktur Queue Tree.

a. Konfigurasi Penandaan Paket (Firewall Mangle)

Langkah pertama adalah menandai koneksi dan paket untuk setiap grup pengguna agar dapat diidentifikasi oleh Queue Tree.

```
/ip firewall mangle
# Mark koneksi untuk setiap grup
add chain=prerouting src-address-list=guru_staf action=mark-connection \
new-connection-mark=conn_guru passthrough=yes
# ... (ulangi untuk e-learning, siswa, cctv)

# Mark paket berdasarkan koneksi
add chain=prerouting connection-mark=conn_guru action=mark-packet \
new-packet-mark=paket_guru passthrough=no
add chain=postrouting connection-mark=conn_guru action=mark-packet \
new-packet-mark=paket_guru passthrough=no
# ... (ulangi untuk e-learning, siswa, cctv)
```

b. Skema dan Struktur Queue Tree

Setelah paket ditandai, struktur pohon berikut diimplementasikan.

```
Total_Bandwidth (max-limit: 100M)
  |-- Queue_CCTV (priority: 1)
  |-- Queue_E-Learning (priority: 2)
  |-- Queue_Guru_Staf (priority: 4)
  `-- Queue_Siswa (priority: 8)
```

Gambar 1: Struktur Hirarki Queue Tree

c. Tabel Detail Konfigurasi Queue Tree

Tabel berikut merangkum parameter yang diterapkan pada setiap antrian.

Nama Queue	Packet Mark	Prioritas	Limit-at	Max-limit
Queue_CCTV	paket_cctv	1	10M	10M
Queue_E-Learning	paket_elearning	2	40M	100M
Queue_Guru_Staf	paket_guru	4	30M	100M
Queue_Siswa	paket_siswa	8	20M	80M

3. **Referensi**

- https://translate.google.com/translate?u=https://support.perimeter81.com/docs/ipsec-tunnel&hl=id&sl=en&tl=id&client=wa
- https://translate.google.com/translate?u=https://www.goodaccess.com/blog/ipsec-vpn&hl=id&sl=en&tl=id&client=srp
- https://citraweb.com/artikel/273/