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

Laporan Sementara
Praktikum Jaringan Komputer

Tunneling, IP Security, dan Queueing

Rendy Lexxy Kurniawan - 5024231007

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital yang selalu berkembang, kebutuhan akan transmisi data yang aman, efisien, dan terorganisir melalui jaringan komputer menjadi semakin krusial. Perusahaan dan individu bergantung pada jaringan untuk melakukan berbagai aktivitas, mulai dari komunikasi dasar hingga transaksi bisnis yang kompleks dan akses ke sumber daya informasi. Seiring dengan meningkatnya volume dan sensitivitas data yang ditransmisikan, muncul pula tantangan terkait privasi, integritas data, dan pengelolaan lalu lintas jaringan yang optimal.

Tunneling hadir sebagai salah satu solusi untuk menciptakan jalur komunikasi privat dan aman di atas infrastruktur jaringan publik, seperti internet. Dengan membungkus paket data asli dalam header tambahan, tunneling memungkinkan data melintasi jaringan yang berbeda protokol atau kebijakan keamanan seolah-olah berada dalam satu koneksi langsung. Teknik ini menjadi dasar bagi implementasi *Virtual Private Network* (VPN) yang banyak digunakan untuk menghubungkan kantor cabang, pengguna jarak jauh, atau bahkan antar pusat data secara aman.

Namun, tunneling saja tidak selalu cukup untuk menjamin keamanan data. Oleh karena itu, *IP Security* (IPSec) memainkan peran vital dalam memberikan lapisan perlindungan tambahan. IPSec menyediakan mekanisme untuk autentikasi, enkripsi, dan integritas data pada level paket IP, sehingga memastikan bahwa data yang dikirim tidak hanya privat tetapi juga terlindungi dari modifikasi dan pemalsuan selama transit.

Di sisi lain, dengan semakin beragamnya jenis aplikasi dan layanan yang menggunakan jaringan, pengelolaan *bandwidth* dan kualitas layanan (*Quality of Service* - QoS) menjadi aspek penting. Teknik *queueing* atau antrian paket data memungkinkan administrator jaringan untuk mengatur prioritas lalu lintas, membatasi penggunaan bandwidth untuk aplikasi tertentu, dan memastikan bahwa aplikasi kritis mendapatkan alokasi sumber daya yang memadai. Tanpa mekanisme queueing yang efektif, jaringan dapat mengalami kongesti yang berakibat pada penurunan performa dan pengalaman pengguna yang buruk.

1.2 Dasar Teori

1.2.1 Tunneling

Tunneling adalah sebuah teknik dalam jaringan komputer yang memungkinkan transmisi data dari satu jaringan ke jaringan lain melalui jaringan perantara dengan cara membungkus (enkapsulasi) paket data protokol asli ke dalam paket data protokol lain. Paket yang telah dienkapsulasi ini kemudian dikirim melalui jalur virtual yang disebut tunnel. Tujuan utama tunneling adalah untuk menyediakan konektivitas antar jaringan yang mungkin memiliki arsitektur atau protokol yang berbeda, serta untuk menciptakan jalur komunikasi yang aman di atas jaringan publik.

- EoIP (Ethernet over IP) adalah protokol pada RouterOS MikroTik yang memungkinkan pembentukan tunnel Ethernet (Layer 2) di antara dua router melalui koneksi IP (Layer 3). Dengan EoIP, dua jaringan Ethernet yang terpisah secara geografis dapat dihubungkan seolah-olah berada dalam satu segmen LAN yang sama. Interface EoIP muncul sebagai interface Ethernet virtual pada router. Paket Ethernet dari satu sisi dienkapsulasi dalam header GRE/IP dan dikirim ke sisi lain, di mana header tersebut dilepas dan paket Ethernet asli diteruskan ke jaringan lokal.

Setiap tunnel EoIP diidentifikasi secara unik menggunakan `tunnel-id`. Keunggulan EoIP adalah kemampuannya untuk membawa semua jenis trafik Ethernet, termasuk protokol non-IP dan paket broadcast, sehingga cocok untuk bridging LAN.

- IPIP (IP over IP) adalah protokol tunneling sederhana yang mengenkapsulasi paket IP di dalam paket IP lain. Artinya, header IP luar ditambahkan ke paket IP asli. Tunnel IPIP tidak menyediakan enkripsi atau otentikasi secara inheren, sehingga seringkali digunakan bersamaan dengan protokol keamanan lain jika diperlukan. Protokol ini bersifat stateless dan umumnya digunakan untuk menghubungkan dua jaringan IPv4 melalui jaringan IPv4 lainnya, atau untuk skenario di mana routing yang lebih kompleks diperlukan antar dua titik yang terhubung melalui IP. Karena hanya membawa trafik IP, IPIP tidak dapat digunakan untuk bridging Layer 2 seperti EoIP.
- PPTP (Point-to-Point Tunneling Protocol) adalah salah satu protokol VPN yang paling awal dan banyak diimplementasikan. PPTP bekerja dengan menciptakan tunnel melalui jaringan IP untuk mengirimkan paket PPP (Point-to-Point Protocol). Klien PPTP melakukan koneksi ke server PPTP, dan setelah otentikasi berhasil, sebuah tunnel akan terbentuk. PPTP menggunakan enkapsulasi GRE (Generic Routing Encapsulation) untuk membawa paket PPP. Meskipun mudah dikonfigurasi dan didukung secara luas, PPTP memiliki beberapa kelemahan keamanan yang telah diketahui, sehingga penggunaannya saat ini sering digantikan atau dilengkapi dengan protokol yang lebih aman.
- L2TP (Layer 2 Tunneling Protocol) adalah protokol tunneling VPN yang merupakan gabungan dari fitur terbaik PPTP (dari Microsoft) dan L2F (Layer 2 Forwarding Protocol dari Cisco). Seperti PPTP, L2TP juga menggunakan PPP untuk menyediakan layanan Layer 2 bagi pengguna. Namun, L2TP sendiri tidak menyediakan mekanisme enkripsi atau kerahasiaan data secara langsung. Oleh karena itu, L2TP sangat sering diimplementasikan bersama dengan IPSec (disebut L2TP/IPSec) untuk menyediakan otentikasi, integritas, dan enkripsi data yang kuat. L2TP dapat berjalan di atas berbagai jenis jaringan paket seperti IP, X.25, Frame Relay, atau ATM.

1.2.2 IP Security (IPSec)

IPSec adalah sebuah suite protokol standar yang dikembangkan oleh IETF (Internet Engineering Task Force) untuk mengamankan komunikasi pada lapisan IP (Layer 3). IPSec menyediakan kerangka kerja untuk memastikan kerahasiaan (confidentiality), integritas (integrity), dan otentikasi (authentication) data yang ditransmisikan melalui jaringan IP. IPSec dapat melindungi trafik antara dua host (host-to-host), dua gateway keamanan (network-to-network/site-to-site), atau antara gateway keamanan dan host (remote access). IPSec terdiri dari beberapa komponen utama, termasuk:

- **Authentication Header (AH)**: Menyediakan otentikasi sumber data dan integritas data, namun tidak menyediakan enkripsi.
- **Encapsulating Security Payload (ESP)**: Menyediakan otentikasi sumber data, integritas data, dan enkripsi (kerahasiaan). ESP lebih sering digunakan karena cakupan keamanannya yang lebih luas.
- **Security Associations (SA)**: Merupakan perjanjian satu arah antara dua entitas yang berkomunikasi, mendefinisikan bagaimana mereka akan menggunakan layanan keamanan untuk melindungi trafik.

- **Internet Key Exchange (IKE)**: Protokol yang digunakan untuk negosiasi parameter SA dan manajemen kunci secara dinamis.

IPSec sering digunakan sebagai mekanisme keamanan fundamental dalam implementasi VPN, terutama pada L2TP/IPSec dan VPN berbasis IKEv2.

1.2.3 Queueing (Manajemen Bandwidth)

Queueing adalah mekanisme yang digunakan dalam manajemen jaringan untuk mengontrol dan mengatur aliran paket data, dengan tujuan utama untuk mengelola penggunaan bandwidth dan meningkatkan kualitas layanan (QoS). Dengan queueing, administrator dapat memprioritaskan, membatasi, atau menjamin alokasi bandwidth untuk jenis trafik, pengguna, atau aplikasi tertentu. RouterOS MikroTik menyediakan dua metode utama untuk queueing: Simple Queue dan Queue Tree.

1. **Simple Queue** adalah cara termudah untuk melakukan manajemen bandwidth di RouterOS. Seperti namanya, konfigurasinya relatif sederhana dan biasanya digunakan untuk membatasi laju data (upload/download) untuk alamat IP atau subnet tertentu. Simple Queue bekerja secara sekuensial, artinya aturan yang berada di urutan atas akan diproses terlebih dahulu. Parameter utama dalam Simple Queue meliputi:

   - `Target`: Menentukan alamat IP, range IP, atau interface yang akan dikenai aturan queue.
   - `Max Limit (Upload/Download)`: Menentukan batas bandwidth maksimum yang dapat digunakan oleh target.
   - `Burst Limit, Burst Threshold, Burst Time`: Memungkinkan target untuk mendapatkan bandwidth lebih besar dari `Max Limit` untuk periode waktu tertentu.
   - `Limit At (CIR - Committed Information Rate)`: Menjamin bandwidth minimum yang akan selalu tersedia untuk target.

   Meskipun sederhana, Simple Queue efektif untuk skenario pembatasan bandwidth dasar.

2. **Queue Tree** adalah mekanisme manajemen bandwidth yang lebih canggih, fleksibel, dan hierarkis di RouterOS. Berbeda dengan Simple Queue yang memproses aturan secara sekuensial, Queue Tree bekerja berdasarkan paket yang telah ditandai (*marked packets*) menggunakan fitur Mangle di Firewall. Ini memungkinkan pembentukan struktur antrian berbentuk pohon, di mana bandwidth dapat dibagi dan diprioritaskan secara lebih granular dan kompleks. Queue Tree sangat berguna untuk skenario QoS yang rumit, di mana diperlukan pembagian bandwidth berdasarkan jenis layanan (misalnya, VoIP, Browse, download), departemen, atau grup pengguna dengan prioritas yang berbeda-beda. Setiap node dalam pohon antrian dapat memiliki tipe antrian (queue type) sendiri seperti PCQ (Per Connectiot-In, First-Out), yang mempengaruhi bagaimana paket diperlakukan dalam antrian tersebut.n Queue), RED (Random Early Detection), atau FIFO (Firs

2 Tugas Pendahuluan

Berikut adalah jawaban dari tugas pendahuluan yang telah dikerjakan, beserta penjelasan dari jawaban tersebut!

1. Konfigurasi VPN IPSec Site-to-Site

Koneksi VPN IPSec antar kantor pusat dan cabang memerlukan pemahaman mendalam mengenai beberapa aspek kunci untuk menjamin keamanan dan fungsionalitas.

1.1 Fase Negosiasi IPSec

Proses negosiasi IPSec terbagi dalam dua fase utama menggunakan protokol IKE (Internet Key Exchange):

A. IKE Phase 1: Membangun Saluran Manajemen (IKE SA)
Tujuan utama dari IKE Phase 1 adalah untuk membuat sebuah saluran komunikasi yang aman dan terautentikasi antara dua *peer* IPSec. Saluran ini disebut ISAKMP SA (Internet Security Association and Key Management Protocol Security Association) atau IKE SA. Fase ini melindungi negosiasi selanjutnya.

Proses utama dalam IKE Phase 1:

- **Autentikasi Peer:** Kedua perangkat saling memverifikasi identitas. Metode yang umum digunakan adalah:
  - *Pre-Shared Keys (PSK):* Kunci rahasia yang sama dikonfigurasikan secara manual pada kedua perangkat. Cocok untuk skenario sederhana.
  - *Digital Signatures (RSA Signatures):* Menggunakan sertifikat digital yang diterbitkan oleh Certificate Authority (CA). Lebih aman dan skalabel.
- **Negosiasi Kebijakan IKE SA (ISAKMP Policy):** Kedua *peer* menyepakati parameter keamanan untuk IKE SA itu sendiri:
  - Algoritma Enkripsi (misalnya, AES, 3DES)
  - Algoritma Hash/Integritas (misalnya, SHA-256, MD5)
  - Metode Autentikasi (PSK atau RSA)
  - Grup Diffie-Hellman (DH) (misalnya, Grup 14, 19)
  - *Lifetime* IKE SA (berapa lama SA ini valid sebelum perlu dinegosiasikan ulang)
- **Pertukaran Kunci Diffie-Hellman (DH):** *Peer* menggunakan algoritma DH untuk secara aman menghasilkan material kunci rahasia bersama (*shared secret key*) melalui jaringan yang tidak aman. Kunci ini kemudian digunakan untuk mengenkripsi komunikasi IKE selanjutnya.

B. IKE Phase 2: Membangun Tunnel Data (IPSec SA)
Setelah IKE SA berhasil dibuat di Phase 1, IKE Phase 2 (juga dikenal sebagai *Quick Mode*) digunakan untuk menegosiasikan parameter keamanan untuk melindungi data pengguna yang sebenarnya. Negosiasi Phase 2 ini terjadi di dalam saluran aman yang telah dibuat oleh Phase 1.

Proses utama dalam IKE Phase 2:

- **Negosiasi Kebijakan IPSec SA (Transform Set):** Kedua *peer* menyepakati parameter untuk IPSec SA, yang akan mengamankan data aktual:

- Protokol IPSec:
  - **ESP (Encapsulating Security Payload):** Menyediakan kerahasiaan (enkripsi), integritas data, autentikasi data asal, dan perlindungan anti-replay.
  - **AH (Authentication Header):** Menyediakan integritas data, autentikasi data asal, dan perlindungan anti-replay. AH **tidak** menyediakan enkripsi.
- Algoritma Enkripsi untuk ESP (misalnya, AES-256)
- Algoritma Hash/Integritas untuk ESP atau AH (misalnya, SHA-256-HMAC)
- Mode Enkapsulasi:
  - **Tunnel Mode:** Seluruh paket IP asli (header dan payload) dienkapsulasi dalam paket IP baru. Digunakan untuk koneksi antar gateway (site-to-site VPN).
  - **Transport Mode:** Hanya payload IP yang dienkapsulasi; header IP asli tetap. Digunakan untuk koneksi antar host (end-to-end).
- *Lifetime* IPSec SA (berapa lama SA ini valid)
- (Opsional) Grup Diffie-Hellman untuk *Perfect Forward Secrecy (PFS)*. Jika PFS diaktifkan, kunci sesi baru akan dibuat untuk Phase 2 ini, independen dari material kunci Phase 1. Ini meningkatkan keamanan karena jika kunci Phase 1 terkompromi, kunci sesi Phase 2 tetap aman.

b. Parameter Keamanan yang Harus Disepakati

Untuk keberhasilan koneksi, kedua router harus menyepakati parameter berikut:

- **Algoritma Enkripsi:** Metode untuk menjaga kerahasiaan data (misalnya, AES-256, 3DES).
- **Algoritma Otentikasi/Integritas (Hash):** Metode untuk memastikan data tidak berubah dan sumbernya valid (misalnya, SHA-256, SHA-512).
- **Metode Otentikasi Peer:** Cara router saling verifikasi (misalnya, *Pre-Shared Key* atau Sertifikat Digital).
- **Grup Diffie-Hellman (DH Group):** Menentukan kekuatan pertukaran kunci (misalnya, Group 14 atau lebih tinggi).
- **Lifetime Kunci (SA Lifetime):** Durasi validitas SA sebelum negosiasi ulang.

c. Konfigurasi Router untuk memulai koneksi IPSec site-to-site (MikroTik RouterOS)

Langkah konseptual konfigurasi IPSec site-to-site pada MikroTik melibatkan pembuatan:

i. **IPSec Proposal:** Mendefinisikan set algoritma untuk IKE Phase 2 (misalnya, enkripsi AES-256, otentikasi SHA256).

ii. **IPSec Peer:** Mengatur parameter koneksi ke router lawan, termasuk alamat IP, metode otentikasi (PSK), dan parameter IKE Phase 1 (misalnya, enkripsi AES-256, DH Group 14).

iii. **IPSec Policy:** Menentukan trafik mana (berdasarkan alamat IP sumber dan tujuan LAN) yang akan diamankan menggunakan tunnel IPSec.

iv. **NAT Bypass (jika perlu):** Membuat aturan firewall NAT untuk memastikan trafik VPN tidak terkena NAT Masquerade.

2. Skema Queue Tree untuk Pembagian Bandwidth Sekolah

Pembagian bandwidth 100 Mbps di sekolah dapat diatur menggunakan Queue Tree pada MikroTik dengan langkah-langkah berikut:

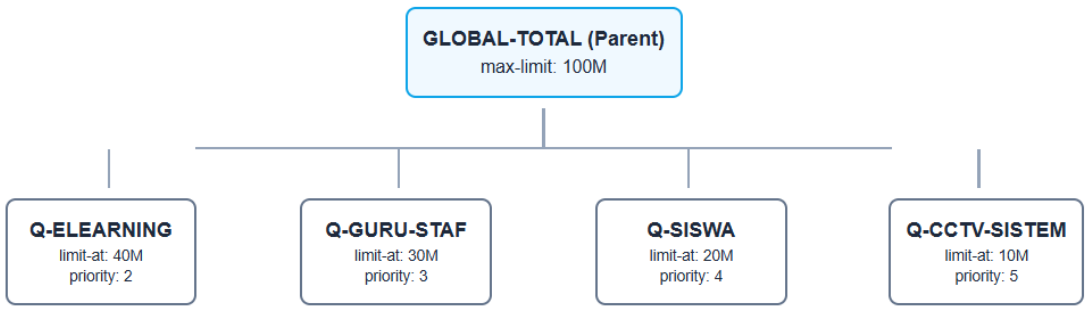
a. Penandaan Paket (Mangle)

Sebelum membuat antrian (queue), paket data harus ditandai terlebih dahulu menggunakan fitur Mangle di Firewall. Penandaan dilakukan berdasarkan kriteria spesifik untuk setiap kategori pengguna atau layanan:

TUJUAN	IDENTIFIER (CONTOH)	CONNECTION MARK	PACKET MARK
E-Learning	Port: 80, 443 ke IP Server E-learning	conn_elearning	pkt_elearning
Guru & Staf	Source IP: 192.168.1.0/25	conn_guru	pkt_guru
Siswa	Source IP: 192.168.10.0/24	conn_siswa	pkt_siswa
CCTV & Sistem	Port: 554 (RTSP), Source IP Server CCTV	conn_cctv	pkt_cctv

Gambar 1: Marking Paket (Mangle)

b. Struktur Queue Tree



Gambar 2: Queue Tree

Struktur antrian dibuat secara hierarkis:

i. **Parent Queues Global:** Dibuat satu parent queue utamauntuk `global_total` dengan `max-limit` 100 Mbps.

ii. **Child Queues per Kategori:** Pada parent queue `global_total`, dibuat child queue untuk masing-masing kategori paket yang telah ditandai, yaitu elearning, guru dan staff, siswa, dan cctv sistem.

c. Prioritas dan limit rate pada masing-masing queue

NAMA QUEUE	PARENT	PRIORITAS	LIMIT AT (CIR)	MAX LIMIT (MIR)
Q-ELEARNING	GLOBAL-TOTAL	2 (Tinggi)	40M	100M
Q-GURU-STAF	GLOBAL-TOTAL	3 (Medium)	30M	100M
Q-SISWA	GLOBAL-TOTAL	4	20M	100M
Q-CCTV-SISTEM	GLOBAL-TOTAL	5 (Adjustable)	10M	100M

Gambar 3: Marking Paket (Mangle)

- **E-Learning:**
  - `parent`: `global_total`
  - `packet-mark`: `pkt_elearning`
  - `limit-at` (jaminan): 40 Mbps
  - `max-limit` (batas atas): 100 Mbps
  - `priority`: 2 (Tinggi)
- **Guru & Staf:**
  - `parent`: `global_total`
  - `packet-mark`: `pkt_guru`
  - `limit-at`: 30 Mbps
  - `max-limit`: 100 Mbps
  - `priority`: 3 (Medium)
- **Siswa:**
  - `parent`: `global_total`
  - `packet-mark`: `pkt_siswa`
  - `limit-at`: 20 Mbps
  - `max-limit`: 100 Mbps
  - `priority`: 4
  - `queue-type`: PCQ (Per Connection Queue) untuk keadilan antar siswa.
- **CCTV & Update Sistem:**
  - `parent`: `global_total`
  - `packet-mark`: `pkt_cctv`
  - `limit-at`: 10 Mbps
  - `max-limit`: 100 Mbps
  - `priority`: 5 (atau disesuaikan)

Catatan: Prioritas yang lebih rendah angkanya berarti prioritas lebih tinggi. Penggunaan PCQ pada antrian siswa penting untuk distribusi bandwidth yang adil. Total `limit-at` dari semua child tidak boleh melebihi kapasitas parent agar

3. Sumber Referensi

- Kent, S., & Seo, K. (2005). RFC 4301: Security Architecture for the Internet Protocol. Internet Engineering Task Force (IETF).
- Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., & Kivinen, T. (2014). RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2). Internet Engineering Task Force (IETF).
- Kent, S. (2005). RFC 4303: IP Encapsulating Security Payload (ESP). Internet Engineering Task Force (IETF).
- Kent, S. (2005). RFC 4302: IP Authentication Header. Internet Engineering Task Force (IETF).
- Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson.