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

Laporan Sementara
Praktikum Jaringan Komputer

VPN

Muhammad Rifqi Abdillah - 5024231082

2025

1 Pendahuluan

1.1 Latar Belakang

Konektivitas jaringan yang aman dan efisien merupakan fondasi esensial bagi operasional organisasi modern. Hal ini terutama berlaku bagi perusahaan dengan kantor cabang yang tersebar secara geografis atau institusi pendidikan dengan kebutuhan akses internet yang beragam dan masif. Permasalahan utama yang sering dihadapi adalah bagaimana menjamin kerahasiaan, integritas, dan ketersediaan data yang ditransmisikan antar lokasi melalui jaringan publik seperti internet, yang pada dasarnya tidak aman. Selain itu, tantangan signifikan lainnya adalah pengelolaan alokasi bandwidth internet yang seringkali terbatas, agar dapat didistribusikan secara adil dan optimal untuk berbagai jenis layanan dan kelompok pengguna dengan tingkat prioritas yang berbeda-beda.

Pembelajaran dan praktik mengenai konfigurasi VPN (Virtual Private Network) menggunakan protokol IPSec (Internet Protocol Security) menjadi sangat krusial. IPSec memungkinkan pembentukan terowongan komunikasi yang aman di atas jaringan publik, sehingga melindungi data sensitif dari potensi penyadapan atau modifikasi oleh pihak yang tidak berwenang. Di sisi lain, pemahaman dan implementasi mekanisme Quality of Service (QoS), khususnya menggunakan metode seperti Queue Tree pada perangkat router, menjadi sangat penting. QoS bertujuan untuk memastikan bahwa layanan-layanan kritis, seperti aplikasi e-learning, layanan video conference untuk rapat penting, atau akses prioritas untuk staf operasional, mendapatkan alokasi bandwidth yang memadai dan terjamin. Hal ini secara langsung berdampak pada peningkatan produktivitas, efisiensi operasional, dan pengalaman pengguna secara keseluruhan.

Keterkaitan topik-topik ini dengan aplikasi di dunia nyata sangatlah erat. Perusahaan dari berbagai skala mengandalkan teknologi VPN untuk mengamankan koneksi site-to-site antar cabang, koneksi remote access bagi karyawan yang bekerja dari jarak jauh, serta koneksi ke layanan cloud. Institusi pendidikan, mulai dari sekolah hingga universitas, memanfaatkan QoS untuk menjamin kelancaran proses belajar-mengajar digital, ujian online, akses ke sumber daya perpustakaan digital, serta untuk mendukung aktivitas administratif dan operasional lainnya. Oleh karena itu, penguasaan teknologi IPSec dan QoS merupakan kompetensi inti dalam bidang administrasi jaringan dan keamanan siber saat ini, yang terus berkembang seiring dengan meningkatnya ketergantungan pada infrastruktur digital.

1.2 Dasar Teori

IPSec (Internet Protocol Security) adalah serangkaian protokol yang dikembangkan oleh Internet Engineering Task Force (IETF) untuk mengamankan komunikasi pada lapisan Internet Protocol (IP) melalui autentikasi dan enkripsi setiap paket IP dalam sebuah sesi komunikasi. IPSec dapat melindungi data antara dua host, dua gateway keamanan (seperti router atau firewall), atau antara gateway keamanan dan host. Tujuan utama dari IPSec meliputi: menjaga kerahasiaan (confidentiality) dengan mencegah data dibaca oleh pihak tidak berwenang melalui enkripsi; menjamin integritas data (data integrity) agar tidak terjadi perubahan selama transmisi; melakukan autentikasi sumber data (data origin authentication) guna memverifikasi identitas pengirim; serta menyediakan perlindungan anti-replay untuk mencegah penyerang mengirim ulang paket yang telah ditangkap sebelumnya.

Salah satu komponen penting dalam IPSec adalah IKE (Internet Key Exchange), protokol yang digunakan untuk menegosiasikan parameter keamanan atau Security Associations (SA) dan meng-

hasilkan kunci enkripsi bersama secara dinamis. Proses negosiasi IKE terdiri dari dua fase. Fase pertama (IKE Phase 1), yang dapat berjalan dalam mode Main atau Aggressive, bertujuan membentuk saluran komunikasi yang aman dan terautentikasi antara dua peer, yang disebut ISAKMP SA atau IKE SA. Dalam fase ini dilakukan pertukaran proposal keamanan (seperti algoritma enkripsi, fungsi hash, metode autentikasi, grup Diffie-Hellman, dan lifetime SA), pertukaran kunci Diffie-Hellman untuk menghasilkan kunci sesi secara rahasia, serta autentikasi antar peer menggunakan metode seperti Pre-Shared Key (PSK) atau sertifikat digital. Setelah IKE SA terbentuk, dilanjutkan ke fase kedua (IKE Phase 2 atau Quick Mode), yang bertujuan untuk menegosiasikan IPSec SA guna mengamankan lalu lintas data aktual. Dalam fase ini dilakukan pertukaran proposal keamanan IPSec, opsional pertukaran kunci DH baru jika fitur Perfect Forward Secrecy (PFS) diaktifkan, dan pembentukan dua IPSec SA yang bersifat unidirectional (masuk dan keluar). Parameter keamanan utama IPSec yang harus disepakati dalam proses ini meliputi algoritma enkripsi (seperti AES-128, AES-256, atau 3DES), metode autentikasi (PSK atau sertifikat digital RSA), fungsi hash untuk integritas data (misalnya SHA-1, SHA-256, atau MD5), grup Diffie-Hellman (seperti Group 2, 5, 14, 19, 21), lifetime key untuk IKE SA dan IPSec SA, protokol IPSec (AH atau ESP), serta mode enkapsulasi (Tunnel Mode atau Transport Mode).

Sementara itu, manajemen bandwidth dengan Queue Tree merupakan salah satu metode dalam implementasi Quality of Service (QoS), yang merujuk pada kemampuan jaringan untuk memberikan layanan prioritas terhadap jenis lalu lintas tertentu, guna mencapai performa jaringan yang optimal terutama saat jaringan sibuk atau terbatas. Queue Tree biasanya diterapkan di router (seperti MikroTik RouterOS) dan memungkinkan pembuatan struktur antrian hierarkis. Konsep utamanya meliputi proses packet marking menggunakan fitur mangle pada firewall untuk menandai paket berdasarkan kriteria seperti IP sumber/tujuan, port, protokol, atau konten. Struktur Queue Tree terdiri dari parent queue dan child queue, di mana parent menentukan batas bandwidth total dan child membagi bandwidth tersebut sesuai kebutuhannya. Setiap antrian dapat diberi nilai prioritas dari 1 hingga 8 (dengan 1 sebagai prioritas tertinggi) untuk mengatur siapa yang dilayani lebih dulu saat terjadi kongesti. Dua parameter penting lainnya adalah limit-at (CIR - Committed Information Rate), yaitu bandwidth minimum yang dijamin untuk antrian tertentu, serta max-limit (MIR - Maximum Information Rate), yaitu batas maksimum bandwidth yang bisa digunakan antrian tersebut. Untuk membagi bandwidth secara adil antar pengguna, digunakan tipe antrian khusus bernama PCQ (Per Connection Queue), yang akan membagi bandwidth tersedia secara merata pada setiap koneksi aktif. Queue Tree biasanya diterapkan pada lalu lintas keluar (output) dari interface WAN atau interface internal, tergantung pada arah lalu lintas yang ingin dikendalikan.

2 Tugas Pendahuluan

1. Jawaban:

   Negosiasi IPSec adalah proses di mana dua perangkat (peer) menyepakati parameter untuk membuat koneksi yang aman. Proses ini dikelola oleh Internet Key Exchange (IKE) dan dibagi menjadi dua fase utama:

   IKE Phase 1 (Main Mode atau Aggressive Mode) Tujuan utama dari IKE Phase 1 adalah untuk membuat saluran komunikasi yang aman dan terautentikasi antara dua *peer*. Saluran ini disebut ISAKMP SA (Internet Security Association and Key Management Protocol Security

Association) atau IKE SA. Langkah-langkah utama dalam IKE Phase 1 (menggunakan Main Mode yang lebih aman):

- **Pertukaran Proposal Keamanan (Security Proposal Exchange):** Kedua *peer* saling bertukar proposal kebijakan keamanan yang berisi:
  - Algoritma Enkripsi (Contoh: AES, 3DES) untuk kerahasiaan IKE.
  - Fungsi Hash (Contoh: SHA-256, MD5) untuk integritas pesan IKE.
  - Metode Autentikasi (Contoh: Pre-Shared Keys (PSK), Sertifikat Digital).
  - Grup Diffie-Hellman (DH) (Contoh: Group 14, 19) untuk pertukaran kunci aman.
  - Lifetime SA: Durasi validitas IKE SA (misalnya, 86400 detik).
- **Pertukaran Kunci Diffie-Hellman:** *Peer* menggunakan grup DH yang disepakati untuk menghasilkan kunci sesi bersama secara rahasia. Kunci ini digunakan untuk mengenkripsi komunikasi IKE selanjutnya.
- **Autentikasi:** Kedua *peer* saling mengautentikasi identitasnya menggunakan metode yang telah disepakati (PSK atau sertifikat).

Hasil dari IKE Phase 1 adalah IKE SA yang aman, di mana kedua *peer* telah saling mengautentikasi dan memiliki material kunci bersama.

IKE Phase 2 (Quick Mode) Setelah IKE SA terbentuk, IKE Phase 2 bertujuan untuk menegosiasikan IPSec SA. IPSec SA ini digunakan untuk mengamankan lalu lintas data aktual yang akan melewati VPN tunnel. Langkah-langkah utama dalam IKE Phase 2:

- **Pertukaran Proposal Keamanan IPSec:** *Peer* bertukar proposal untuk IPSec SA, meliputi:
  - Protokol IPSec: AH (Authentication Header) atau ESP (Encapsulating Security Payload). ESP lebih umum karena menyediakan enkripsi dan autentikasi.
  - Algoritma Enkripsi (untuk ESP): (Contoh: AES-256, AES-128).
  - Algoritma Autentikasi (untuk ESP atau AH): (Contoh: HMAC-SHA256, HMAC-MD5).
  - Mode Enkapsulasi IPSec: Tunnel Mode (seluruh paket IP asli dienkapsulasi) atau Transport Mode (hanya payload IP yang diamankan). Tunnel mode umum untuk site-to-site VPN.
  - Lifetime IPSec SA: Durasi validitas IPSec SA (misalnya, 3600 detik) dan/atau berdasarkan volume data.
  - (Opsional) Perfect Forward Secrecy (PFS): Jika diaktifkan, dilakukan pertukaran kunci DH baru untuk IPSec SA, meningkatkan keamanan.
- **Pertukaran Material Kunci:** Material kunci untuk IPSec SA diturunkan dari material kunci IKE Phase 1 (atau dari DH baru jika PFS digunakan).
- **Pembentukan IPSec SA:** Dua IPSec SA *unidirectional* dibuat (satu untuk lalu lintas masuk, satu untuk keluar).

Hasil dari IKE Phase 2 adalah IPSec SA yang siap digunakan untuk mengamankan data.

Parameter Keamanan yang Harus Disepakati (Konsisten di Kedua Sisi):

- **Parameter IKE Phase 1:**

  - Metode Autentikasi (PSK harus identik, atau sertifikat yang valid).
  - Algoritma Enkripsi.
  - Fungsi Hash.
  - Grup Diffie-Hellman.
  - Lifetime Key IKE SA.
- **Parameter IKE Phase 2:**
  - Protokol (ESP atau AH).
  - Algoritma Enkripsi (untuk ESP).
  - Algoritma Autentikasi.
  - Mode Enkapsulasi (Tunnel Mode untuk site-to-site).
  - Perfect Forward Secrecy (PFS) dan grup DH-nya jika digunakan.
  - Lifetime Key IPSec SA.
- **Identitas Peer:** Alamat IP publik dari masing-masing router.
- **Jaringan Lokal (Local Network) dan Jaringan Remote (Remote Network):** Subnet IP yang lalu lintasnya akan dilewatkan melalui tunnel VPN (sering disebut *traffic selectors* atau *proxy IDs*).

2. **Jawaban:**

   Penjelasan: Sebuah sekolah dengan bandwidth internet 100 Mbps ingin membaginya sebagai berikut:

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

   Berikut adalah skema Queue Tree yang dapat diterapkan (misalnya pada MikroTik RouterOS):

   Langkah 1: Packet Marking (Mangle) Sebelum membuat antrian, paket data harus ditandai terlebih dahulu di `IP > Firewall > Mangle`.

   - **Marking E-learning:** Tandai koneksi dan paket berdasarkan IP server e-learning atau port spesifik.

   Listing 1: Marking E-learning Connection Packet

```
/ip firewall mangle
add action=mark-connection chain=prerouting \
    dst-address=IP_SERVER_ELEARNING new-connection-mark=elearning_conn
   passthrough=yes \
    comment="Mark E-learning Connection"
add action=mark-packet chain=prerouting connection-mark=elearning_conn \
    new-packet-mark=elearning_pkt passthrough=no

```

   - **Marking Guru & Staf:** Tandai berdasarkan rentang IP Address guru/staf (misal `192.168.10.0/24`).

Listing 2: Marking Guru-Staf Connection Packet

```
/ip firewall mangle
add action=mark-connection chain=prerouting src-address=192.168.10.0/24 \
    new-connection-mark=guru_staf_conn passthrough=yes \
    comment="Mark Guru-Staf Connection"
add action=mark-packet chain=prerouting connection-mark=guru_staf_conn \
    new-packet-mark=guru_staf_pkt passthrough=no

```

- **Marking Siswa:** Tandai berdasarkan rentang IP Address siswa (misal `192.168.20.0/23`).

Listing 3: Marking Siswa Connection Packet

```
/ip firewall mangle
add action=mark-connection chain=prerouting src-address=192.168.20.0/23 \
    new-connection-mark=siswa_conn passthrough=yes comment="Mark Siswa
    Connection"
add action=mark-packet chain=prerouting connection-mark=siswa_conn \
    new-packet-mark=siswa_pkt passthrough=no

```

- **Marking CCTV & Update Sistem:** Tandai berdasarkan IP perangkat CCTV/server update atau port.

Listing 4: Marking CCTV-System Connection Packet

```
/ip firewall mangle
add action=mark-connection chain=prerouting src-address=
    IP_CCTV_OR_UPDATE_SERVER \
    new-connection-mark=cctv_system_conn passthrough=yes \
    comment="Mark CCTV-System Connection"
add action=mark-packet chain=prerouting connection-mark=cctv_system_conn \
    new-packet-mark=cctv_system_pkt passthrough=no

```

(Catatan: Aturan mangle di atas adalah untuk lalu lintas download. Untuk manajemen upload, diperlukan aturan mangle tambahan yang menandai paket berdasarkan `dst-address` untuk jaringan lokal atau menggunakan interface keluar yang berbeda untuk `chain=postrouting`)

Langkah 2: Konfigurasi Queue Tree (di `Queues > Queue Tree`) Skema ini berfokus pada manajemen bandwidth download. Struktur serupa dapat dibuat untuk upload.

- **Parent Utama:** `Total_Sekolah_Download`
  - **Parent:** `ether1-gateway` (interface WAN yang terhubung ke internet)
  - **Packet Marks:** (kosong, atau spesifik jika ada parent global lain)
  - **Queue Type:** `default` (atau `default-small`)
  - **Priority:** 8 (prioritas terendah karena hanya sebagai container)
  - **Limit-at (CIR):** 0
  - **Max-limit (MIR):** `100M` (total bandwidth download)
- **Child 1:** `Queue_Elearning`
  - **Parent:** `Total_Sekolah_Download`

  - **Packet Marks:** `elearning_pkt`
  - **Queue Type:** `pcq-download-default` (atau custom PCQ untuk pembagian adil per pengguna e-learning)
  - **Priority: 1** (Prioritas tertinggi)
  - **Limit-at (CIR):** `30M` (jaminan minimal saat dibutuhkan, bisa disesuaikan)
  - **Max-limit (MIR):** `40M` (batas maksimal)
- **Child 2:** `Queue_Guru_Staf`
  - **Parent:** `Total_Sekolah_Download`
  - **Packet Marks:** `guru_staf_pkt`
  - **Queue Type:** `pcq-download-default` (atau custom PCQ)
  - **Priority: 2**
  - **Limit-at (CIR):** `20M`
  - **Max-limit (MIR):** `30M`
- **Child 3:** `Queue_Siswa`
  - **Parent:** `Total_Sekolah_Download`
  - **Packet Marks:** `siswa_pkt`
  - **Queue Type:** `pcq-download-default` (atau custom PCQ)
  - **Priority: 3**
  - **Limit-at (CIR):** `10M` (jaminan bisa dinaikkan jika sisa CIR memungkinkan)
  - **Max-limit (MIR):** `20M`
- **Child 4:** `Queue_CCTV_System`
  - **Parent:** `Total_Sekolah_Download`
  - **Packet Marks:** `cctv_system_pkt`
  - **Queue Type:** `default-small` (umumnya traffic CCTV stabil)
  - **Priority: 4**
  - **Limit-at (CIR):** `5M`
  - **Max-limit (MIR):** `10M`

Penjelasan Tambahan untuk Skema Queue Tree:

- **Total CIR dan MIR:** Total `Limit-at` (CIR) dari semua child (30+20+10+5 = 65 Mbps) tidak melebihi `Max-limit` parent (100 Mbps). Sisa 35 Mbps menjadi *burstable bandwidth* yang dapat digunakan oleh antrian sesuai prioritasnya hingga mencapai `Max-limit` masing-masing. Total `Max-limit` (40+30+20+10 = 100 Mbps) sesuai dengan total bandwidth yang tersedia.
- **Burst:** Konfigurasi burst dapat ditambahkan pada setiap child queue untuk memberikan fleksibilitas penggunaan bandwidth lebih tinggi dalam waktu singkat, jika tersedia.
- **PCQ (Per Connection Queue):** Penggunaan tipe antrian PCQ pada e-learning, guru, dan siswa sangat disarankan untuk memastikan pembagian bandwidth yang adil di antara pengguna individu dalam masing-masing kategori tersebut.

- **Manajemen Upload:** Skema serupa (dengan penandaan paket dan alokasi bandwidth yang sesuai) harus dibuat untuk lalu lintas upload jika diperlukan kontrol yang ketat, dengan parent queue `Total_Sekolah_Upload` yang terpisah.
- **Pengujian dan Penyesuaian:** Setelah implementasi, lakukan pengujian dan monitor penggunaan bandwidth untuk menyesuaikan nilai CIR, MIR, dan prioritas agar sesuai dengan kebutuhan aktual dan memberikan performa optimal.