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

Laporan Sementara
Praktikum Jaringan Komputer

VPN

Ahmad Faiq Fawwaz - 5024231032

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam sistem jaringan yang terus berkembang, tantangan utama adalah menjamin keamanan komunikasi data serta mengelola trafik secara efisien agar setiap pengguna memperoleh alokasi bandwidth yang sesuai dengan kebutuhannya. Seiring meningkatnya ketergantungan masyarakat terhadap internet untuk berbagai aktivitas seperti perkantoran, pendidikan, hiburan, hingga layanan kesehatan, kebutuhan akan konektivitas yang aman dan stabil menjadi semakin mendesak. Untuk menjawab kebutuhan konektivitas antarlokasi yang aman melalui jaringan publik, teknologi tunneling seperti IPSec digunakan karena menyediakan komunikasi terenkripsi, menjaga integritas data, serta memastikan autentikasi antara pihak-pihak yang berkomunikasi. IPSec memungkinkan dua jaringan berbeda untuk saling terhubung secara privat meskipun menggunakan media komunikasi publik seperti internet, menjadikannya solusi penting dalam skenario seperti kantor pusat dan cabang atau akses jarak jauh oleh staf lapangan. Namun, keamanan saja tidak cukup. Lalu lintas jaringan yang tidak diatur dapat menyebabkan bottleneck, menurunkan performa, dan mengganggu kualitas layanan—terutama pada jaringan yang digunakan secara bersama-sama untuk aktivitas berat seperti video conference, streaming, cloud computing, hingga game online. Oleh karena itu, pengelolaan bandwidth menjadi aspek yang tidak kalah penting untuk dipahami. MikroTik sebagai perangkat jaringan yang banyak digunakan dalam skala kecil hingga menengah menawarkan fitur mangle dan Queue Tree yang sangat bermanfaat dalam pengaturan trafik jaringan. Fitur ini memungkinkan administrator jaringan untuk mengklasifikasikan, memprioritaskan, dan membatasi trafik berdasarkan jenis layanan, pengguna, alamat IP, atau port, sehingga alokasi bandwidth dapat lebih adil dan sesuai prioritas. Kombinasi antara tunneling yang aman dan pengelolaan bandwidth yang tepat menjadikan jaringan tidak hanya aman dari intersepsi data, tetapi juga efisien dalam pemanfaatan sumber daya jaringan. Dengan demikian, pengguna akhir dapat merasakan pengalaman jaringan yang stabil, responsif, dan andal. Modul ini memberikan landasan penting bagi mahasiswa untuk memahami penerapan nyata dari dua aspek krusial tersebut dalam dunia jaringan komputer modern, serta memberikan bekal keterampilan teknis dalam merancang dan mengelola jaringan yang optimal dari sisi keamanan maupun performa.

1.2 Dasar Teori

Tunneling adalah teknik encapsulation data yang memungkinkan suatu protokol jaringan dibungkus oleh protokol lainnya sehingga dapat melewati jaringan yang tidak mendukung protokol tersebut secara langsung. Metode ini sering digunakan untuk membentuk koneksi antar jaringan privat melalui jaringan publik seperti internet, dan dapat diterapkan pada berbagai skenario seperti site-to-site VPN, remote access VPN, hingga interkoneksi antar cabang perusahaan. Salah satu protokol yang banyak digunakan dalam tunneling adalah IPSec (Internet Protocol Security), yaitu sekumpulan protokol yang berfungsi untuk mengamankan komunikasi pada layer IP melalui mekanisme enkripsi, autentikasi, dan integritas data. IPSec bekerja melalui dua fase utama, yaitu IKE Phase 1 yang membentuk tunnel manajemen menggunakan ISAKMP SA dan IKE Phase 2 yang membentuk tunnel data menggunakan IPsec SA. Dalam konfigurasi praktikum, IPSec digunakan untuk membangun koneksi aman antara dua router yang merepresentasikan jaringan terpisah, seperti kantor pusat dan kantor cabang. Selain keamanan jaringan, pengelolaan trafik menjadi aspek penting dalam optimasi performa jaringan, terutama dalam lingkungan dengan keterbatasan bandwidth. Salah satu metode

yang digunakan adalah Queue Tree, yaitu teknik antrian bertingkat pada router MikroTik yang memungkinkan pembagian bandwidth secara proporsional dan berdasarkan prioritas trafik. Queue Tree bekerja dengan prinsip parent-child, di mana parent menentukan total bandwidth yang tersedia, dan child queue membagi bandwidth tersebut berdasarkan kriteria tertentu seperti protokol, alamat IP, atau port. Sebelum paket masuk ke dalam queue, diperlukan proses penandaan menggunakan fitur mangle di firewall MikroTik, yang berfungsi untuk mengidentifikasi jenis trafik berdasarkan parameter tertentu. Dengan kombinasi mangle dan Queue Tree, administrator jaringan dapat memprioritaskan trafik penting seperti akses e-learning, video conference, atau server internal agar tetap mendapatkan alokasi bandwidth yang stabil meskipun terjadi kemacetan jaringan. Penerapan teknik ini sangat penting untuk menjamin kualitas layanan (Quality of Service/QoS) pada jaringan institusi pendidikan, perkantoran, atau organisasi lainnya yang memiliki kebutuhan trafik yang beragam dan kritikal.

2 Tugas Pendahuluan

Bagian ini berisi jawaban dari tugas pendahuluan yang telah anda kerjakan, beserta penjelasan dari jawaban tersebut.

1. **Fase Negosiasi IPSec (IKE Phase 1 dan Phase 2)**

   IPSec menggunakan protokol IKE (Internet Key Exchange) untuk membangun tunnel VPN secara aman. Proses ini dibagi menjadi dua fase utama:

   - **IKE Phase 1** Fase ini bertujuan untuk membuat kanal komunikasi aman antara dua perangkat VPN (misal dua router). Ada dua mode: Main Mode (lebih aman) dan Aggressive Mode (lebih cepat). Hasil dari fase ini adalah terbentuknya *ISAKMP Security Association (SA)* dan pembuatan *shared secret key*.
     - Autentikasi: Pre-shared Key (PSK) atau digital certificate
     - Algoritma Enkripsi: AES, 3DES
     - Algoritma Hash: SHA-1, SHA-256
     - DH Group: Diffie-Hellman group (misalnya group 2, 14)
     - Lifetime: Waktu aktif SA (contoh: 86400 detik)
   - **IKE Phase 2 (Quick Mode)** Fase ini bertujuan membentuk IPSec SA, yaitu channel yang mengenkripsi data.
     - Negotiation of IPSec Protocol: ESP (Encapsulating Security Payload) atau AH (Authentication Header)
     - Algoritma Enkripsi: AES, 3DES
     - Algoritma Hash: SHA-1, SHA-256
     - Perfect Forward Secrecy (PFS): Opsional
     - Lifetime: Umumnya 3600 detik

   Referensi:

   - Cisco. *Understanding IKEv1 and IPsec.* `https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/217432-understand-ipsec-ikev1-protocol.html`

- NIST SP 800-77 Rev.1. *Guide to IPsec VPNs.* https://csrc.nist.gov/pubs/sp/800/77/r1/final

2. **Parameter Keamanan yang Harus Disepakati**

   Saat konfigurasi VPN IPSec, kedua pihak harus menyepakati parameter keamanan berikut:

   - **Algoritma Enkripsi:** AES 128/256-bit atau 3DES.
   - **Metode Autentikasi:** Pre-shared Key (PSK) atau sertifikat digital (X.509).
   - **Hash Function:** SHA-256 atau SHA-1.
   - **Diffie-Hellman Group:** Group 14 (2048-bit) atau lebih tinggi.
   - **Lifetime Key:** Umumnya 86400 detik (IKE Phase 1) dan 3600 detik (IKE Phase 2).

   Referensi:

   - Juniper Networks. *IPSec VPN Concepts.* https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/software/junos/vpn-ipsec/topics/topic-map/security-ipsec-vpn-overview.html
   - RFC 4306. *Internet Key Exchange (IKEv2).* https://www.rfc-editor.org/rfc/rfc4306.html

3. **Konfigurasi Sederhana Router IPSec Site-to-Site (Contoh Cisco IOS)**

```
crypto isakmp policy 10
 encr aes
 hash sha256
 authentication pre-share
 group 14
 lifetime 86400

crypto isakmp key MYSECRETKEY address 192.168.2.1

crypto ipsec transform-set TS esp-aes esp-sha-hmac

crypto map VPN-MAP 10 ipsec-isakmp
 set peer 192.168.2.1
 set transform-set TS
 match address 100

interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 crypto map VPN-MAP

access-list 100 permit ip 10.0.0.0 0.0.0.255 10.1.0.0 0.0.0.255
```

   Penjelasan:

   - `crypto isakmp policy`: Fase 1 - mendefinisikan algoritma dan metode autentikasi.
   - `crypto ipsec transform-set`: Fase 2 - mendefinisikan metode enkripsi dan hash.
   - `crypto map`: Menggabungkan kebijakan IKE dan IPSec.
   - `access-list`: Menentukan lalu lintas yang akan dienkripsi.

Referensi:

- Cisco. "Configure a LAN-to-LAN IPsec Tunnel Between Two Routers." https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/217432-understand-ipsec-ikev1-protocol.html

4. **Skema Queue Tree Bandwidth Sekolah**

   Dengan bandwidth total 100 Mbps, alokasi berdasarkan prioritas:

   - **Parent Queue:** total-bandwidth (100 Mbps)
     - Child: e-learning (40 Mbps, priority=1)
     - Child: guru-staf (30 Mbps, priority=2)
     - Child: siswa (20 Mbps, priority=3)
     - Child: CCTV-update (10 Mbps, priority=4)

   Penjelasan Queue Tree:

   - **Parent Queue:** Mengontrol seluruh bandwidth utama 100 Mbps
   - **Child Queue:** Membagi bandwidth berdasarkan fungsi dan prioritas.
   - **Marking:** Masing-masing trafik ditandai menggunakan firewall mangle rules:

```
/ip firewall mangle
add chain=forward src-address=192.168.1.0/24 action=mark-packet new-packet-mark=e-learning
add chain=forward src-address=192.168.2.0/24 action=mark-packet new-packet-mark=guru-staf
add chain=forward src-address=192.168.3.0/24 action=mark-packet new-packet-mark=siswa
add chain=forward src-address=192.168.4.0/24 action=mark-packet new-packet-mark=cctv
```

   - **Queue Tree Configuration (MikroTik):**

```
/queue tree
add name="parent" parent=global limit-at=100M max-limit=100M
add name="e-learning" parent=parent packet-mark=e-learning limit-at=40M priority=1
add name="guru-staf" parent=parent packet-mark=guru-staf limit-at=30M priority=2
add name="siswa" parent=parent packet-mark=siswa limit-at=20M priority=3
add name="cctv" parent=parent packet-mark=cctv limit-at=10M priority=4
```

   Referensi:

   - MikroTik Wiki. *Manual:Queue Tree.* https://wiki.mikrotik.com/Manual:Queue
   - MikroTik Documentation. *Queues.* https://help.mikrotik.com/docs/spaces/ROS/pages/328088/Queues