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

Praktikum Jaringan Komputer

Modul 5 – VPN and QoS

I Gusti Ngurah Opaldi Partha Dwipayana – 5024221057

2025

1 Pendahuluan

1.1 Latarbelakang

Seiring dengan meningkatnya kebutuhan perusahaan dan lembaga pendidikan untuk terhubung secara aman melalui jaringan publik seperti internet, maka pengamanan data dan kontrol lalu lintas menjadi aspek yang sangat penting. VPN (Virtual Private Network) dengan protokol IPSec merupakan salah satu solusi yang memungkinkan dua jaringan berbeda—seperti kantor pusat dan cabang—terhubung secara aman melalui enkripsi data. Sementara itu, pada sisi manajemen bandwidth, penting untuk menerapkan Quality of Service (QoS) agar lalu lintas data dapat dibagi secara adil dan sesuai prioritas. Sebagai contoh, di lingkungan sekolah, kebutuhan bandwidth untuk e-learning dan akses guru perlu diprioritaskan dibanding aktivitas browsing siswa atau update sistem. Oleh karena itu, pemahaman mengenai konfigurasi VPN IPSec serta skema QoS seperti Queue Tree sangat penting dalam desain jaringan modern yang aman dan efisien.

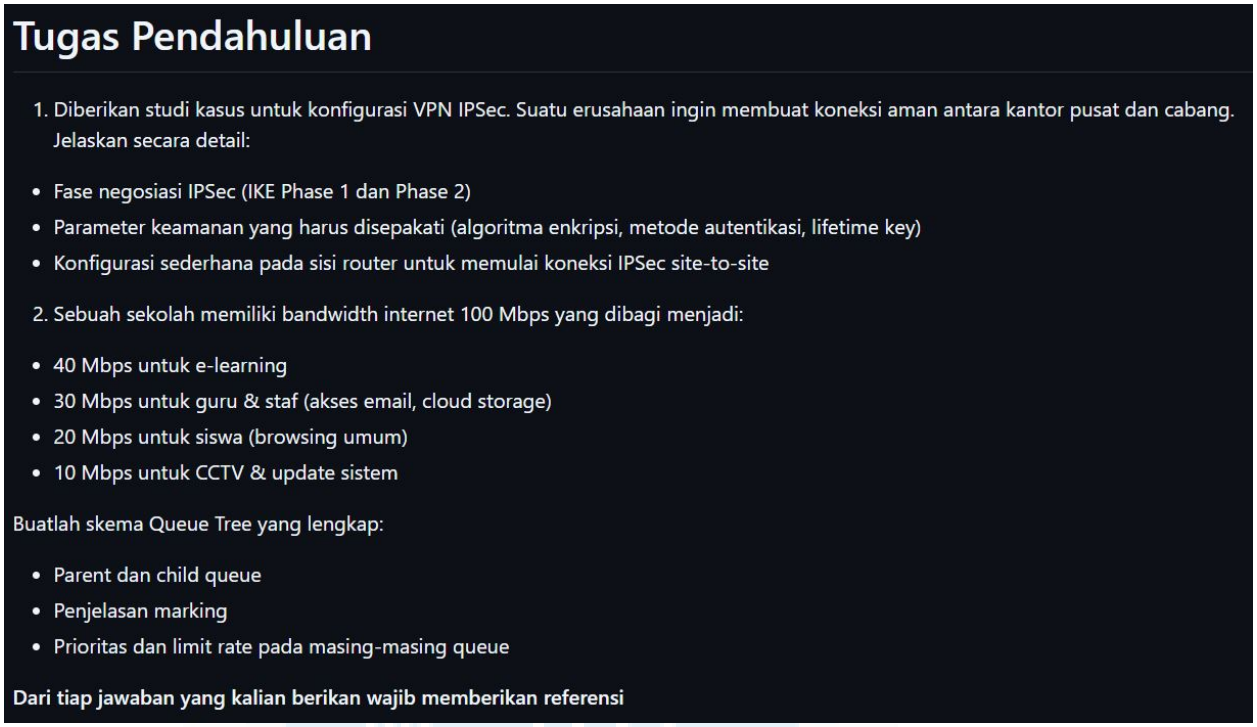
1.2 Tujuan

Virtual Private Network (VPN) adalah teknologi jaringan yang memungkinkan komunikasi data secara aman melalui jaringan publik dengan cara membuat "terowongan" terenkripsi antara dua titik. Salah satu protokol utama yang digunakan adalah **IPSec (Internet Protocol Security)**, yang bekerja di layer 3 OSI. IPSec menggunakan dua fase utama: IKE Phase 1 untuk membentuk jalur aman awal (IKE SA), dan IKE Phase 2 untuk mendefinisikan parameter enkripsi data (IPSec SA). IPSec mendukung berbagai algoritma enkripsi seperti AES dan metode autentikasi seperti Pre-Shared Key (PSK) atau sertifikat digital.

Quality of Service (QoS) dalam jaringan komputer merujuk pada mekanisme untuk menjamin performa lalu lintas data dengan membagi bandwidth sesuai kebutuhan dan prioritas. Salah satu implementasi populer dalam perangkat MikroTik adalah **Queue Tree**, yaitu sistem antrean berbasis hierarki yang terdiri dari parent dan child queue. Queue Tree bekerja dengan memanfaatkan marking pada paket data menggunakan fitur Mangle untuk mengidentifikasi jenis trafik, kemudian menetapkan batas maksimum (max-limit), minimum (limit-at), dan prioritas layanan. QoS sangat penting untuk menghindari kemacetan jaringan dan memastikan layanan penting tetap berjalan optimal meski bandwidth terbatas.

2 Tugas Pendahuluan

Soal :



Tugas Pendahuluan

1. Diberikan studi kasus untuk konfigurasi VPN IPSec. Suatu erusahaan 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

2. Sebuah sekolah memiliki bandwidth internet 100 Mbps yang dibagi menjadi:

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

Buatlah skema Queue Tree yang lengkap:

- Parent dan child queue
- Penjelasan marking
- Prioritas dan limit rate pada masing-masing queue

Dari tiap jawaban yang kalian berikan wajib memberikan referensi

Jawaban :

1. ### Konfigurasi VPN IPSec Site-to-Site

   ### Fase Negosiasi IPSec (IKE Phase 1 dan Phase 2)

   Protokol IPSec bekerja dalam dua fase utama untuk membentuk koneksi aman antara dua jaringan yang berbeda:

   - **IKE Phase 1 (Main Mode)**: Fase ini bertujuan untuk membangun jalur aman awal yang disebut *IKE SA (Security Association)*. Di sini terjadi proses autentikasi kedua router menggunakan *Pre-Shared Key (PSK)* atau sertifikat digital, dan negosiasi parameter keamanan seperti algoritma enkripsi (contoh: AES-256), algoritma hash (contoh: SHA-256), grup Diffie-Hellman (contoh: modp2048), serta lifetime tunnel (misal: 3600 detik).
   - **IKE Phase 2 (Quick Mode)**: Setelah jalur aman terbentuk, fase ini digunakan untuk membentuk *IPSec SA*, yaitu tunnel yang akan mengamankan lalu lintas data sebenarnya antar jaringan LAN di kedua sisi. Parameter yang dinegosiasikan meliputi metode enkripsi, hash, kebijakan lalu lintas (subnet yang diizinkan), dan lifetime koneksi.

Parameter Keamanan yang Harus Disepakati

Agar koneksi IPSec berhasil dibentuk, kedua perangkat harus memiliki parameter yang identik sebagai berikut:

Parameter	Contoh Nilai	Fungsi
Algoritma Enkripsi	AES-256, 3DES	Menyandikan data agar tidak dapat dibaca pihak ketiga
Algoritma Hash	SHA-256, SHA-1	Menjamin integritas dan keaslian data
Autentikasi	Pre-Shared Key (PSK)	Verifikasi identitas antar router
Diffie-Hellman Group	Group 14 (2048-bit)	Pertukaran kunci secara aman
Lifetime	3600 detik	Menentukan durasi validitas tunnel sebelum negosiasi ulang

Table 1: Contoh parameter keamanan IPSec

Konfigurasi Dasar IPSec Site-to-Site di MikroTik

Misalkan terdapat dua site sebagai berikut:

- Kantor Pusat: IP Publik 203.0.113.1, LAN 192.168.10.0/24
- Kantor Cabang: IP Publik 203.0.113.2, LAN 192.168.20.0/24

Berikut langkah konfigurasi di sisi MikroTik (kantor pusat):

```
/ip ipsec proposal
add name="my-proposal" auth-algorithms=sha256 enc-algorithms=aes-256-cbc \
    pfs-group=modp2048 lifetime=1h

/ip ipsec peer
add address=203.0.113.2/32 secret="vpnkey123" exchange-mode=main \
    send-initial-contact=yes

/ip ipsec policy
add src-address=192.168.10.0/24 dst-address=192.168.20.0/24 \
    sa-src-address=203.0.113.1 sa-dst-address=203.0.113.2 \
    tunnel=yes action=encrypt proposal=my-proposal

/ip firewall nat
add chain=srcnat src-address=192.168.10.0/24 dst-address=192.168.20.0/24 \
    action=accept place-before=0
```

References

[1] Cloudflare, *What is IPsec?*. [Online]. Tersedia: `https://www.cloudflare.com/learning/network-layer/what-is-ipsec/`

[2] MikroTik Wiki, *Manual:IP/IPsec*. [Online]. Tersedia: https://wiki.mikrotik.com/wiki/Manual:IP/IPsec

2. Skema Queue Tree

Sebuah sekolah memiliki bandwidth internet sebesar 100 Mbps yang dibagi menjadi:

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

Skema Queue Tree (Parent dan Child Queue)

Berikut ini contoh konfigurasi skema queue tree di MikroTik:

```
/queue tree
add name="Total-Bandwidth" parent=global max-limit=100M

add name="E-Learning" parent="Total-Bandwidth" packet-mark=
    ↪ e_learning \
    limit-at=10M max-limit=40M priority=1

add name="Guru-Staf" parent="Total-Bandwidth" packet-mark=
    ↪ guru_staf \
    limit-at=8M max-limit=30M priority=2

add name="Siswa" parent="Total-Bandwidth" packet-mark=siswa \
    limit-at=5M max-limit=20M priority=3

add name="CCTV-Update" parent="Total-Bandwidth" packet-mark=
    ↪ cctv_update \
    limit-at=2M max-limit=10M priority=4
```

Penjelasan Marking (Firewall Mangle)

Sebelum membuat queue, kita perlu melakukan **packet marking** dengan Mangle:

```
/ip firewall mangle
add chain=forward src-address=192.168.10.0/24 action=mark-
    ↪ packet new-packet-mark=e_learning passthrough=no
add chain=forward src-address=192.168.20.0/24 action=mark-
    ↪ packet new-packet-mark=guru_staf passthrough=no
add chain=forward src-address=192.168.30.0/24 action=mark-
    ↪ packet new-packet-mark=siswa passthrough=no
add chain=forward src-address=192.168.40.0/24 action=mark-
    ↪ packet new-packet-mark=cctv_update passthrough=no
```

Penjelasan Prioritas dan Limit Rate

- **Priority**: Nilai 1 (tertinggi) diberikan untuk layanan yang paling penting (e-learning), diikuti oleh guru & staf, siswa, dan terakhir CCTV.
- **Limit-at**: Bandwidth minimum yang dijamin.
- **Max-limit**: Bandwidth maksimum yang dapat digunakan jika tersedia.

Referensi

- MikroTik Wiki: *Queue Tree* dan *Mangle Rules*. `https://wiki.mikrotik.com`
- MikroTik RouterOS Documentation. `https://help.mikrotik.com`