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

Laporan Sementara
Praktikum Jaringan Komputer

VPN & Queue

Mohammad Rizky Ibrahim Diswarin - 5024231055

2025

1 Pendahuluan

1.1 Latar Belakang

Dengan meningkatnya volume lalu lintas data dan mobilitas kerja, organisasi kini memerlukan solusi yang mampu menjamin koneksi antarlokasi yang aman dan stabil. Salah satu pendekatan yang umum digunakan adalah Virtual Private Network (VPN), khususnya dengan implementasi protokol IPSec pada layer jaringan. Teknologi ini menyediakan jalur komunikasi terenkripsi yang memungkinkan transmisi data melewati jaringan publik tanpa kehilangan integritas maupun kerahasiaan. IPSec merupakan pilihan tepat bagi perusahaan maupun institusi pendidikan untuk menjaga privasi komunikasi internal dari risiko penyadapan.

Di samping perlindungan data, kebutuhan akan manajemen bandwidth yang efisien juga semakin penting, mengingat berbagai aplikasi—seperti sistem pembelajaran daring, administrasi, pemantauan CCTV, dan pembaruan perangkat lunak—berbagi satu koneksi internet. MikroTik menyediakan fitur Queue Tree yang memungkinkan pembagian bandwidth berdasarkan prioritas layanan, serta memfasilitasi peminjaman kapasitas antar kelas layanan secara dinamis. Hal ini membantu menjaga performa layanan penting tetap optimal meskipun jaringan sedang padat, tanpa memerlukan investasi perangkat tambahan.

Modul kelima ini berfokus pada implementasi praktis dua teknologi utama, yaitu membangun koneksi VPN site-to-site menggunakan IPSec dan mengatur alokasi bandwidth 100 Mbps menggunakan Queue Tree sesuai skenario jaringan di lingkungan sekolah.

1.2 Dasar Teori

VPN merupakan mekanisme encapsulation yang membungkus paket asli ke dalam protokol tunneling, membuat lalu lintas jaringan terlihat seperti berada dalam jaringan privat. IPSec beroperasi pada lapisan IP dengan memanfaatkan protokol ESP (Encapsulating Security Payload) dan AH (Authentication Header) untuk menyediakan fungsi keamanan seperti enkripsi, autentikasi, dan integritas data. Dua entitas keamanan utama (Security Association) digunakan: IKE SA untuk kanal kontrol dan IPSec SA untuk kanal transmisi data.

Proses negosiasi kunci diawali dengan Internet Key Exchange (IKE), biasanya menggunakan versi IKEv2 yang mengimplementasikan algoritma Diffie–Hellman untuk pertukaran kunci, enkripsi simetris seperti AES-CBC atau AES-GCM untuk menjaga kerahasiaan, dan hash function (misalnya HMAC-SHA-256) untuk menjamin keutuhan data.

Mode tunnel IPSec mengenkripsi keseluruhan paket IP termasuk header-nya, sehingga informasi alamat jaringan internal tidak terlihat dari luar—umumnya digunakan untuk komunikasi antar situs (site-to-site). Sebaliknya, mode transport hanya mengenkripsi payload, dan biasa digunakan untuk koneksi antar host. Agar tunnel dapat terbentuk, kedua pihak harus sepakat atas parameter keamanan seperti jenis algoritma, grup DH, masa berlaku kunci (lifetime), serta metode autentikasi (pre-shared key atau sertifikat digital). Fitur Perfect Forward Secrecy (PFS) dapat diaktifkan untuk mencegah kompromi sesi lama berdampak pada sesi baru. Ketika masa aktif SA berakhir, proses negosiasi ulang dilakukan secara otomatis tanpa mengganggu koneksi.

Dalam manajemen Quality of Service (QoS), MikroTik RouterOS menyediakan dua mekanisme antrean: Simple Queue dan Queue Tree. Simple Queue digunakan untuk pembatasan bandwidth per host secara langsung. Sementara Queue Tree memungkinkan pembagian bandwidth berdasarkan

hierarki, dan lebih fleksibel karena dapat digunakan untuk berbagai jenis lalu lintas.

Konsep utama dalam Queue Tree adalah proses *packet marking* di firewall mangle. Paket diberi tanda berdasarkan karakteristik seperti alamat IP, port, VLAN, atau DSCP. Tanda ini digunakan oleh antrean anak (child queue) untuk mengalokasikan bandwidth sesuai parameter seperti *limit-at* (minimum bandwidth), *max-limit* (batas maksimum), dan *priority* (tingkat kepentingan). MikroTik menggunakan algoritma HTB (Hierarchical Token Bucket) untuk mendistribusikan bandwidth secara efisien. Karena diterapkan pada tahap post-routing, Queue Tree cukup dibuat satu kali di titik global dan berlaku lintas antarmuka, memudahkan manajemen pada router dengan banyak port.

2 Tugas Pendahuluan

1. **Studi Kasus VPN IPSec: Koneksi Aman Kantor Pusat dan Cabang**

   (a) **Tahapan Negosiasi IPSec (IKE Phase 1 dan Phase 2)**

   Fase 1 – Pembentukan IKE SA Tahap awal membentuk kanal kontrol terenkripsi untuk negosiasi berikutnya. Proses ini mencakup:

   1. Pertukaran proposal: kedua pihak mengirim daftar algoritma, grup DH, dan waktu aktif kunci yang didukung, contohnya AES-256, SHA-256, dan DH Group 14.
   2. Pertukaran kunci Diffie–Hellman: digunakan untuk menghasilkan shared session key berdasarkan nilai publik masing-masing.
   3. Autentikasi: menggunakan pre-shared key atau sertifikat digital untuk memverifikasi identitas.
   4. Pembentukan IKE SA: setelah semua parameter cocok dan berhasil diverifikasi, terbentuklah kanal kontrol terenkripsi untuk fase berikutnya.

   Fase 2 – Pembentukan IPSec SA (Quick Mode) Setelah IKE SA aktif, terowongan data (IPSec SA) dapat dibentuk:

   1. Menentukan selector: yaitu rentang IP sumber dan tujuan yang akan dienkripsi, misalnya 10.10.10.0/24 10.20.20.0/24.
   2. Negosiasi parameter ESP/AH: memilih enkripsi (misalnya AES-128-GCM), autentikasi (HMAC-SHA-256), serta PFS jika diaktifkan.
   3. Pembentukan SA: membuat dua SA (inbound dan outbound) lengkap dengan kunci dan waktu berlaku.
   4. Pertukaran data: paket yang cocok dengan selector akan dienkripsi dan dikirim melalui tunnel yang telah terbentuk.

   Hubungan antar fase:
   Fase 1 menyediakan jalur aman untuk negosiasi, sedangkan fase 2 menggunakan jalur tersebut untuk mengatur lalu lintas terenkripsi. Selama IKE SA valid, IPSec SA dapat diperbarui tanpa autentikasi ulang.

   (b) **Parameter Keamanan yang Harus Disepakati**
   Keberhasilan tunnel IPSec ditentukan oleh kesesuaian parameter berikut di kedua sisi:

1. Algoritma enkripsi: misalnya AES-128, AES-256-CBC, atau AES-256-GCM.
2. Fungsi hash untuk integritas: seperti HMAC-SHA-256 atau HMAC-SHA-512.
3. Grup Diffie–Hellman (PFS): seperti Group 14 (2048-bit) atau Group 16 (4096-bit).
4. Lifetime kunci: misalnya 28.800 detik untuk IKE SA dan 3.600 detik untuk IPSec SA.
5. Autentikasi antar perangkat: menggunakan PSK atau sertifikat X.509.

Jika ada ketidaksesuaian pada salah satu parameter, maka proses pembentukan tunnel akan gagal.

2. **Skema Queue Tree untuk Sekolah dengan Bandwidth 100 Mbps**

(a) **Struktur Queue: Parent dan Child**

Total bandwidth sebesar 100 Mbps dibagi ke empat jenis layanan menggunakan Queue Tree:

```
/queue tree add name=total parent=global max-limit=100M

/queue tree add name=elearning parent=total \
    limit-at=40M max-limit=40M priority=1 packet-mark=elearn_pkt

/queue tree add name=guru parent=total \
    limit-at=30M max-limit=30M priority=2 packet-mark=guru_pkt

/queue tree add name=siswa parent=total \
    limit-at=20M max-limit=20M priority=3 packet-mark=siswa_pkt

/queue tree add name=cctv parent=total \
    limit-at=10M max-limit=10M priority=4 packet-mark=cctv_pkt
```

(b) **Proses Packet Marking**

Marking dilakukan pada firewall mangle berdasarkan alamat IP tujuan:

```
/ip firewall mangle
  add chain=prerouting dst-address=192.168.10.0/24 \
      action=mark-packet new-packet-mark=elearn_pkt passthrough=yes

  add chain=prerouting dst-address=192.168.20.0/24 \
      action=mark-packet new-packet-mark=guru_pkt passthrough=yes

  add chain=prerouting dst-address=192.168.30.0/24 \
      action=mark-packet new-packet-mark=siswa_pkt passthrough=yes

  add chain=prerouting dst-address=192.168.40.0/24 \
      action=mark-packet new-packet-mark=cctv_pkt passthrough=yes
```

(c) **Konfigurasi Limit dan Prioritas**

- `limit-at`: alokasi minimum bandwidth yang dijamin untuk masing-masing layanan.
- `max-limit`: batas maksimal agar total bandwidth tidak melebihi 100 Mbps.
- `priority`: menentukan prioritas layanan saat bandwidth penuh (nilai lebih rendah berarti prioritas lebih tinggi).

Prioritas diberikan berdasarkan kebutuhan: e-learning (1), guru & staf (2), siswa (3), CCTV & sistem (4). Dengan struktur ini, bandwidth terbagi adil namun tetap fleksibel sesuai beban lalu lintas aktual.

2.1 Referensi

a) IETF (2005). RFC 4301 – *Security Architecture for the Internet Protocol*.

b) IETF (2016). RFC 7296 – *Internet Key Exchange Protocol Version 2 (IKEv2)*.

c) Stallings, W. (2022). *Network Security Essentials: Applications and Standards* (7th ed.). Boston: Pearson.

d) Jang, S., & Kam, J. (2018). *Quality of Service Technologies for Wireless and Wired Networks*. Singapore: Springer.

e) Chandra, R., & Shenoy, P. (2020). “Performance analysis of QoS queue scheduling on MikroTik RouterOS”, *International Journal of Advanced Computer Science and Applications*, 11(7), 120–127.