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

Laporan Sementara
Praktikum Jaringan Komputer

VPN & Queue

Ahmad Akmal Defatra - 5024231005

2025

1 Pendahuluan

1.1 Latar Belakang

Di tengah pertumbuhan traffic data yang meningkat tajam dan mobilitas kerja yang kian tinggi, organisasi membutuhkan mekanisme yang mampu menjamin konektivitas antarsitus sekaligus menjaga kerahasiaan informasi. Virtual Private Network (VPN), khususnya implementasi IPSec pada lapisan jaringan, menawarkan terowongan terenkripsi yang memungkinkan pertukaran data melintasi internet publik tanpa mengorbankan kerahasiaan dan integritas paket. Teknologi ini menghadirkan skema keamanan terpadu yang dapat diadopsi baik oleh perusahaan besar maupun lembaga pendidikan untuk melindungi komunikasi internal dari intersepsi pihak luar.

Seiring dengan kebutuhan keamanan, muncul pula tuntutan kualitas layanan yang adil bagi beragam aplikasi seperti kelas daring, sistem administrasi, kamera pengawas, hingga pembaruan perangkat lunak yang berbagi satu jalur internet. MikroTik Queue Tree menyediakan kerangka hierarki antrean yang mampu mendistribusikan bandwidth sesuai prioritas, sekaligus membiarkan kapasitas tak terpakai dipinjam kelas lain secara dinamis. Pendekatan ini memastikan aplikasi kritis tetap responsif saat jaringan padat, tanpa perlu investasi infrastruktur tambahan yang mahal.

Modul 5 ini berfokus pada penerapan praktis kedua pilar tersebut yakni bagaimana merancang terowongan IPSec site-to-site agar segmen jaringan terpisah berkomunikasi secara aman, kemudian mengonfigurasi Queue Tree untuk membagi bandwith 100 Mbps menurut skenario layanan sekolah.

1.2 Dasar Teori

VPN adalah teknik encapsulation yang membungkus paket asli di dalam protokol tunneling sehingga traffic antar site tampak seolah-olah mengalir di jaringan privat. IPSec beroperasi di lapisan IP dengan menggunakan protokol ESP (Encapsulating Security Payload) dan AH (Authentication Header) untuk menyediakan kerahasiaan, autentikasi, dan integritas. Arsitektur IPSec diatur oleh dua pasang security association (SA): IKE SA sebagai kanal kontrol dan IPSec SA sebagai kanal data. Negosiasi IKE SA berlangsung melalui Internet Key Exchange (IKE) yakni versi terkini IKEv2 yang memanfaatkan Diffie–Hellman untuk pertukaran kunci, algoritma enkripsi simetris (AES-GCM atau AES-CBC) untuk kerahasiaan, serta fungsi hash (HMAC-SHA-256 atau SHA-2) guna memverifikasi integritas.

Mode tunnel melindungi keseluruhan paket IP header dan payload sehingga alamat privat tetap tersembunyi. mode transport hanya mengenkripsi payload, umum pada host-to-host. Parameter keamanan seperti jenis algoritma, grup DH, lifetime kunci, dan metode autentikasi (pre-shared key atau sertifikat X.509) harus identik di kedua ujung; ketidakcocokan mencegah SA terbentuk. Perfect Forward Secrecy (PFS) dapat diaktifkan agar kunci data tidak bergantung pada kunci lama, memperkecil dampak kompromi sesi. Ketika SA habis masa layan (rekey), IKE memulai negosiasi ulang transparan bagi pengguna.

Quality of Service memastikan traffic sensitif seperti video konferensi, aplikasi belajar daring—mendapat jatah bandwidth dan latensi terkontrol meski link sibuk. MikroTik RouterOS menyediakan dua kerangka antrean: Simple Queue dan Queue Tree. Simple Queue mengikat batas kecepatan langsung ke alamat atau antarmuka; cocok untuk pembatasan tunggal per host. Queue Tree bekerja pada rantai post-routing dengan hierarki parent/child sehingga beberapa kelas layanan berbagi alokasi dari parent yang sama.

Proses dimulai dengan packet marking di firewall mangle dimana paket diberi label (misalnya ele-

arn_pkt, guru_pkt) berdasarkan alamat, port, DSCP, atau VLAN. Label tersebut kemudian dipanggil oleh child queue, masing-masing memiliki parameter limit-at (garansi minimum), max-limit (batas tertinggi), dan priority (1 tertinggi, 8 terendah). MikroTik memanfaatkan algoritma Hierarchical Token Bucket (HTB) untuk membagi token bandwidth di antara child; saat link under-utilised, child dengan permintaan lebih besar dapat meminjam kapasitas yang tidak terpakai.

Queue Tree ditempatkan di satu titik global sehingga tidak perlu membuat antrean terpisah per antarmuka; hal ini memudahkan manajemen pada router gateway dengan banyak port. Karena eksekusi berada setelah NAT, antrean dapat diterapkan baik pada paket asli maupun paket yang telah di-translasi, tergantung titik mangle. Kombinasi packet marking yang tepat, prioritas, dan limit menjamin layanan kritis tetap responsif sembari menjaga keadilan distribusi bandwidth bagi pengguna umum.

2 Tugas Pendahuluan

1. **Diberikan studi kasus untuk konfigurasi VPN IPSec. Suatu erusahaan ingin membuat koneksi aman antara kantor pusat dan cabang. Jelaskan secara detail:**

   (a) **Fase negosiasi IPSec (IKE Phase 1 dan Phase 2**

   Phase 1 – IKE SA Establishment Tahap ini membangun terowongan kontrol (IKE SA) yang terenkripsi sehingga semua pertukaran selanjutnya berlangsung aman.

   1. **Exchange proposal.** Kedua jaringan bertukar daftar algoritma dan lifetime kunci yang mampu di eksekusi masing masing jaringan. Misalnya AES-256, SHA-256, DH Group 14
   2. **Diffie–Hellman key exchange.** Router menghitung key session bersama yang akan digunakan berdasarkan nilai publik DH yang dipertukarkan sebelumnya.
   3. **Peer authentication.** Identitas diverifikasi menggunakan pre-shared key atau sertifikat X.509. Namun jika cocok, proses berlanjut ke tahap selanjutnya.
   4. **IKE SA terbentuk.** Tunnel manajemen terenkripsi dan siap digunakan sebagai jalur negosiasi Phase 2.

   Phase 2 – IPSec SA (Quick Mode) Tahap ini membuat terowongan data yang mengenkripsi traffic antar-subnet.

   1. **Menentukan selector.** Setiap jaringan menentukan subnet sumber dan tujuan yang akan dilindungi, misalnya 10.10.10.0/24 10.20.20.0/24.
   2. **Negosiasi parameter ESP/AH.** Dipilih algoritma enkripsi (contoh AES-128 GCM), autentikasi (HMAC-SHA-256) dan opsi PFS yang cocok berdasarkan kemampuan yang sama antar jaringan pada phase 1
   3. **Pembuatan SA.** Dibentuk dua IPSec SA (inbound & outbound) lengkap dengan kunci baru serta lifetime.
   4. **Aliran data.** Paket yang cocok dengan selector kemudia dienkapsulasi ESP/AH lalu dikirim melalui tunnel traffic kini dienkripsi end-to-end.

Ringkasan hubungan fase

Phase 1 menyediakan kanal aman untuk negosiasi.

Phase 2 menggunakan kanal itu untuk mengenkripsi data.

Selama IKE SA masih valid, IPSec SA dapat diperbarui berkali-kali tanpa mengulang autentikasi.

(b) **Parameter keamanan yang harus disepakati**Keberhasilan pembentukan tunnel IPSec bergantung pada kesamaan tiga kelompok parameter di kedua sisi:

1. **Algoritma enkripsi**
   Yakni untuk menentukan cara data disandikan, pilihan umum nya adalah AES-128/192/256-CBC atau AES-256-GCM (mode GCM menyatukan enkripsi dan autentikasi).
2. **Metode autentikasi / integritas**
   Yakni untuk memastikan paket tidak diubah di tengah jalan, misalnya HMAC-SHA-256 atau HMAC-SHA-512.
3. **Diffie-Hellman group (PFS)**
   Yakni untuk memberi kekuatan pertukaran kunci dan kedua router harus memilih grup yang sama, misalnya grup 14 (2048-bit) atau Grup 16 (4096-bit)
4. **Lifetime kunci (SA lifetime)**
   Durasi sebelum kunci diganti otomatis. contohnya adalah 28 800 s (8 jam) untuk IKE SA dan 3 600 s (1 jam) untuk IPSec SA.
5. **Metode autentikasi peer**
   Pre-Shared Key (PSK) sederhana atau sertifikat X.509 untuk skala besar, kedua nilai harus identik di kedua endpoint.

Apabila salah satu parameter tidak cocok, proses negosiasi gagal dan tunnel tidak terbentuk.

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

(a) **Parent dan Child Queue**

Queue Tree bekerja berdasarkan hierarkis: satu parent sebagai "total" berguna untuk membatasi bandwidth 100 Mbps. Lalu empat child lain mengatur porsi e-learning, guru & staf, siswa, serta CCTV.

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

# child queues
```

```
/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) **Penjelasan Marking**

Queue Tree bekerja berdasarkan packet mark yang dibuat di firewall mangle. Setiap paket diberi label lalu dimasukkan ke child yang sesuai.

```
/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
```

Label `elearn_pkt`, `guru_pkt`, `siswa_pkt`, dan `cctv_pkt` selanjutnya dipanggil pada parameter `packet-mark` di setiap child queue.

(c) **Prioritas dan Limit Rate**

- **limit-at** menetapkan jatah minimum yang selalu tersedia, yakni:
  e-learning 40 Mbps,
  guru & staf 30 Mbps,
  siswa 20 Mbps,
  CCTV 10 Mbps.
- **max-limit** membatasi kecepatan agar total tidak melampaui 100 Mbps.
- **priority** menentukan urutan layanan bila trafik penuh (1 tertinggi, 8 terendah) dimana: E-learning diprioritaskan (1) → latensi rendah; guru (2), siswa (3), CCTV (4).

Dengan skema ini bandwidth terdistribusi sesuai aturan yang dibuat, dan saat koneksi tidak maksimal sisa kapasitas dapat dipinjam antar-queue karena semua child berada di bawah parent yang sama.

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. and Kam, J. (2018) Quality of Service Technologies for Wireless and Wired Networks. Singapore: Springer.

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