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

Laporan Sementara
Praktikum Jaringan Komputer

VPN dan QoS

Kadek Candra Dwi Yanti - 5024231067

2025

1 Pendahuluan

1.1 Latar Belakang

Di dunia yang semakin terhubung ini, menjaga keamanan data dan pengaturan lalu lintas internet menjadi hal yang sangat penting. Saat ini, banyak perusahaan atau organisasi yang harus mengirimkan data antar cabang atau kantor pusat melalui jaringan yang lebih luas, yang sering kali rentan terhadap ancaman siber. Oleh karena itu, teknologi seperti VPN IPSec sangat dibutuhkan untuk mengamankan data yang dikirimkan agar tetap terlindungi melalui enkripsi dan autentikasi. Ini juga menjadi penting ketika perusahaan perlu menjaga kerahasiaan dan integritas informasi yang sensitif.

Selain itu, dengan semakin banyaknya perangkat yang terhubung ke jaringan, manajemen trafik menjadi isu utama. Setiap aplikasi memiliki kebutuhan bandwidth yang berbeda-beda. Tanpa pengaturan yang baik, bisa terjadi penurunan kualitas layanan, terutama pada aplikasi yang memerlukan koneksi stabil seperti video conference atau akses VPN. Oleh karena itu, pengelolaan bandwidth menggunakan Queue Tree menjadi penting agar tiap jenis trafik mendapatkan prioritas yang sesuai, sehingga layanan utama tetap berjalan lancar meski jaringan sedang padat.

Praktikum ini dilaksanakan untuk memberi pemahaman langsung tentang cara mengkonfigurasi VPN IPSec dan cara mengatur trafik jaringan dengan lebih efisien menggunakan Queue Tree. Pengetahuan ini sangat berguna, terutama di dunia profesional IT, di mana pengelolaan jaringan dan keamanannya sangat penting untuk mendukung kelancaran operasional dan melindungi data perusahaan.

1.2 Dasar Teori

1. VPN (Virtual Private Network) dan IPSec

   VPN adalah teknologi yang memungkinkan pengguna atau perangkat untuk terhubung ke jaringan lain secara aman melalui internet. Salah satu protokol yang digunakan dalam VPN adalah IPSec.

   Tunneling adalah proses pengiriman data melalui jalur yang aman, yang disebut "terowongan". Data yang dikirim akan dibungkus (encapsulated) sehingga bisa melintas di jaringan publik seperti internet tanpa mudah disadap.

   IPSec (Internet Protocol Security) adalah protokol yang digunakan untuk mengenkripsi dan mengautentikasi data yang dikirim melalui VPN. Dengan IPSec, data yang dikirim aman dari gangguan dan hanya bisa dibaca oleh pihak yang memiliki kunci enkripsi yang sesuai.

2. Fase IKE (Internet Key Exchange)

   Pada VPN, kedua perangkat yang ingin terhubung akan saling bertukar informasi yang diperlukan untuk membangun koneksi yang aman. Proses ini disebut IKE (Internet Key Exchange), yang terjadi dalam dua fase:

   - Fase 1: Digunakan untuk membangun koneksi yang aman antara perangkat, yaitu proses pertukaran kunci dan autentikasi
   - Fase 2: Setelah koneksi aman terjalin, fase ini digunakan untuk mengatur penggunaan kunci yang lebih spesifik untuk melindungi data yang dikirimkan

3. Queue Management (Manajemen Antrian)

   Manajemen antrian adalah teknik untuk mengatur aliran trafik di jaringan. Setiap aplikasi di jaringan mungkin membutuhkan kecepatan yang berbeda, sehingga tanpa pengaturan yang baik, jaringan bisa menjadi lambat atau tidak efisien. Ada dua metode utama yang digunakan dalam manajemen antrian jaringan:

   - Simple Queue: Merupakan cara paling sederhana untuk membatasi kecepatan data pada masing-masing IP atau pengguna. Misalnya, kita bisa membatasi kecepatan unduhan atau unggahan untuk tiap perangkat atau pengguna
   - Queue Tree: Pengaturan antrian yang lebih kompleks, di mana kita bisa membagi alokasi bandwidth berdasarkan prioritas. Misalnya, mengutamakan trafik video conference dibandingkan dengan trafik browsing

4. Mangle (Penandaan Paket)

   Pada konfigurasi Queue Tree, kita perlu memberi tanda pada paket data yang ada di jaringan. Fitur mangle pada MikroTik digunakan untuk menandai paket berdasarkan berbagai kriteria, seperti alamat IP, jenis aplikasi, atau jenis trafik (misalnya video, VoIP, browsing). Setelah paket diberi tanda, kita bisa memprioritaskan atau membatasi kecepatan pengirimannya menggunakan Queue Tree.

5. Prioritas Trafik (Traffic Prioritization)

   Penting untuk memastikan aplikasi yang membutuhkan koneksi stabil mendapatkan prioritas lebih tinggi di jaringan. Misalnya, aplikasi yang digunakan untuk video call atau akses VPN kantor harus mendapat prioritas tinggi agar tidak terhambat meski jaringan sedang padat. Prioritas trafik memungkinkan pengaturan mana aplikasi yang lebih penting untuk didahulukan.

6. Enkripsi dan Keamanan

   Keamanan data sangat penting dalam pengiriman data melalui jaringan. Teknologi seperti enkripsi dan autentikasi digunakan untuk memastikan data yang dikirimkan tetap aman. Enkripsi mengacak data sehingga hanya pihak yang memiliki kunci yang tepat yang dapat membaca data tersebut. Sementara autentikasi memastikan bahwa data yang diterima berasal dari sumber yang sah dan tidak diubah selama perjalanan.

7. Firewall

   Firewall digunakan untuk memantau dan mengontrol aliran data masuk dan keluar dari jaringan. Dalam konteks VPN, firewall berfungsi untuk menambah lapisan perlindungan, memastikan hanya koneksi yang sah yang diizinkan untuk mengakses jaringan.

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:

   - 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

Jawaban:

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

- Fase 1 (ISAKMP Phase 1):
  - Tujuan: Fase pertama bertujuan untuk melakukan autentikasi mutual antara kedua router dan membangun saluran aman (tunnel) untuk komunikasi lebih lanjut. Pada jurnal "Key Exchange in IPSec" oleh Perlman dan Kaufman (2000), fase pertama ini bertanggung jawab untuk memastikan identitas kedua pihak dengan menggunakan pre-shared keys atau public
  - Proses: Kedua pihak akan bertukar informasi yang berisi kebijakan enkripsi dan autentikasi melalui ISAKMP (Internet Security Association and Key Management Protocol) untuk memulai pertukaran kunci.
    Proses ini juga melibatkan Diffie-Hellman exchange untuk menghasilkan kunci sesi yang digunakan di fase kedua. Hal ini sesuai dengan yang dituliskan pada jurnal Perlman dan Kaufman (2000), Halaman 51-52
- Fase 2 (IPSec Phase 2):
  - Tujuan: Fase kedua berfungsi untuk melindungi data yang dikirim melalui tunnel dengan membentuk Security Associations (SAs) yang melindungi data tersebut
  - Proses: Fase kedua ini menggunakan transform set untuk menyepakati algoritma enkripsi yang akan digunakan untuk melindungi data dan memastikan data tersebut tetap aman sepanjang pertukaran.
    Hal ini sesuai dengan yang dituliskan pada jurnal Perlman dan Kaufman (2000), Halaman 53-54

(b) Parameter Keamanan yang Harus Disepakati

Pada Fase 1 dan Fase 2, beberapa parameter keamanan yang harus disepakati antara kedua pihak adalah:

- Algoritma Enkripsi:
  Algoritma seperti AES (Advanced Encryption Standard) digunakan untuk menjaga kerahasiaan data yang dikirimkan.
  - IKE Phase 1: Algoritma enkripsi yang digunakan bisa DES (56-bit), 3DES (168-bit), atau AES (128-bit, 192-bit, 256-bit). Untuk keamanan yang lebih tinggi, AES direkomendasikan.
  - IPSec (Phase 2): Algoritma enkripsi yang digunakan adalah ESP dengan AES-128/192/256 atau 3DES untuk kompatibilitas mundur.

  Hal ini sesuai dengan yang dituliskan pada jurnal "Implementation of Site to Site IPsec VPN Tunnel between Routers", Halaman 164
- Metode Autentikasi:
  Pre-shared key (PSK) atau public key encryption digunakan untuk memastikan autentikasi mutual antara kedua pihak dalam koneksi.

- Phase 1: Menggunakan pre-shared key (PSK) atau RSA digital signatures untuk autentikasi. PSK lebih sederhana dan sering digunakan dalam koneksi site-to-site.
- Phase 2: Menggunakan HMAC-MD5 atau HMAC-SHA-1 untuk autentikasi data yang lebih aman dan memastikan integritas data yang dipertukarkan.

Hal ini sesuai dengan yang dituliskan pada jurnal "Implementation of Site to Site IPsec VPN Tunnel between Routers", Halaman 164-165

- Lifetime Key:
  Lifetime Key menentukan berapa lama kunci enkripsi yang digunakan akan bertahan sebelum perlu diperbarui untuk menjaga keamanan komunikasi dalam jangka panjang.
  - IKE SA Lifetime: Secara default, durasi IKE SA adalah 86400 detik (24 jam).
  - IPSec SA Lifetime: Durasi IPSec SA biasanya diatur selama 3600 detik (1 jam) sebelum harus diganti untuk menjaga keamanan sesi.

  Hal ini sesuai dengan yang dituliskan pada jurnal "Implementation of Site to Site IPsec VPN Tunnel between Routers", Halaman 165

(c) Konfigurasi sederhana pada sisi router untuk memulai koneksi IPSec site-to-site

Berdasarkan jurnal "Implementation of Site to Site IPsec VPN Tunnel between Routers" oleh Ei Ei Khaing et al. (2021), berikut adalah langkah-langkah konfigurasi dasar untuk membangun koneksi IPSec Site-to-Site pada router:

- Menambahkan Peer (Router Lawan)
  Tujuan: Menambahkan IP publik dari router lawan agar router bisa berkomunikasi secara aman.
  Konfigurasi:
  - Pada sisi kantor pusat, tambahkan peer dengan IP publik dari kantor cabang.
  - Gunakan mode Main untuk fase 1 dan pilih algoritma enkripsi dan autentikasi yang tepat.
  - Tentukan pre-shared key sebagai metode autentikasi.
- Membuat Proposal IPSec (Phase 2)
  Tujuan: Membuat proposal yang mendefinisikan algoritma enkripsi dan autentikasi yang akan digunakan selama fase pertukaran data.
  Konfigurasi:
  - Tentukan algoritma enkripsi yang digunakan untuk melindungi data, misalnya AES-256.
  - Tentukan algoritma autentikasi, seperti SHA-256.
  - Tentukan Lifetime untuk Security Associations (SAs), biasanya 1 jam untuk IPSec SA.
- Menambahkan Kebijakan IPSec (Policy)
  Tujuan: Menentukan jaringan mana yang akan terhubung melalui tunnel IPSec.
  Konfigurasi:
  - Tentukan ACL untuk Access Control List (ACL) yang mengizinkan lalu lintas antara kedua jaringan yang akan terkoneksi.
  - Policy menghubungkan proposal IPSec dengan kebijakan routing.

- Menambahkan Crypto Map
  Tujuan: Menyambungkan ISAKMP dan IPSec untuk mengonfigurasi tunnel yang aman.
  Konfigurasi:
  - Tentukan crypto map untuk mengonfigurasi opsi tunnel IPSec pada interface router
  - Tentukan group Diffie-Hellman yang sesuai untuk pengaturan key exchange
  - Atur SA lifetime sesuai dengan kebijakan keamanan yang disepakati
- Mengaktifkan Tunnel IPSec
  Tujuan: Aktifkan koneksi tunnel antara dua router.
  Konfigurasi:
  - Setel opsi tunnel=yes pada policy untuk memastikan tunnel IPSec dapat terhubung dan berfungsi
  - Pastikan static route ditambahkan untuk mengarahkan trafik antara kedua jaringan yang terhubung.

Referensi:

Perlman, R., & Kaufman, C. (2000). "Key Exchange in IPSec: Analysis of IKE". IEEE Internet Computing, November-December 2000, halaman 50-56

Link Referensi

Khaing, Ei Ei, et al. "Implementation of Site to Site IPsec VPN Tunnel between Routers", International Journal of Scientific Research in Science, Engineering and Technology, Volume 8 Issue 1, 2021, Pages 164-169

Lnk Referensi

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

   Jawaban:

   Skema Queue Tree untuk Pembagian Bandwidth

   (a) Parent Queue:
   - Nama Queue: parent-queue
   - Limit Rate: 100 Mbps (Total bandwidth yang tersedia)
   - Prioritas: Default (Karena ini adalah antrian utama untuk seluruh jaringan)

Hal ini sesuai dengan yang dijelaskan pada file "Implementasi Manajemen Bandwidth Menggunakan Queue Tree Router Mikrotik", Halaman 33

(b) Child Queues:

Setiap jenis trafik akan memiliki child queue masing-masing yang mengatur limit rate dan prioritas berdasarkan kebutuhan masing-masing.

i. Queue untuk E-learning:
   - Nama Queue: queue-elearning
   - Parent: parent-queue
   - Limit Rate: 40 Mbps (Untuk kebutuhan e-learning)
   - Prioritas: 1 (Prioritas tertinggi agar layanan e-learning tetap stabil tanpa gangguan)
   - Marking: Menggunakan mangle untuk menandai trafik yang berkaitan dengan aplikasi e-learning.

   Hal ini sesuai dengan yang dijelaskan pada file "Implementasi Manajemen Bandwidth Menggunakan Queue Tree Router Mikrotik", Halaman 34

ii. Queue untuk Guru dan Staf:
   - Nama Queue: queue-guru-staf
   - Parent: parent-queue
   - Prioritas: 2 (Prioritas menengah, lebih rendah dari e-learning)
   - Marking: Menggunakan mangle untuk menandai trafik terkait guru dan staf

   Hal ini sesuai dengan yang dijelaskan pada file "Implementasi Manajemen Bandwidth Menggunakan Queue Tree Router Mikrotik", Halaman 34-35

iii. Queue untuk Siswa (Browsing Umum):
   - Nama Queue: queue-siswa
   - Parent: parent-queue
   - Limit Rate: 20 Mbps (Untuk kebutuhan browsing umum)
   - Prioritas: 3 (Prioritas lebih rendah, agar tidak mengganggu layanan kritis lainnya)
   - Marking: Menggunakan mangle untuk menandai trafik yang berasal dari pengguna siswa.

   Hal ini sesuai dengan yang dijelaskan pada file "Implementasi Manajemen Bandwidth Menggunakan Queue Tree Router Mikrotik", Halaman 35lin+(32-39).

iv. Queue untuk CCTV & Update Sistem:
   - Nama Queue: queue-cctv-update
   - Parent: parent-queue
   - Limit Rate: 10 Mbps (Untuk kebutuhan CCTV dan update sistem)
   - Marking: Menggunakan mangle untuk menandai trafik CCTV dan update.

   Hal ini sesuai dengan yang dijelaskan pada file "Implementasi Manajemen Bandwidth Menggunakan Queue Tree Router Mikrotik", Halaman 35

Penjelasan Marking dan Prioritas

- Marking digunakan untuk menandai jenis trafik agar bisa diprioritaskan di Queue Tree. Di sini, mangle digunakan untuk memisahkan dan menandai trafik berdasarkan sumber (misalnya, IP) atau jenis aplikasi (misalnya, e-learning, akses email).

- Prioritas ditetapkan berdasarkan pentingnya aplikasi tersebut. Misalnya, e-learning mendapatkan prioritas tertinggi (1), sehingga walaupun trafik lain padat, e-learning akan tetap lancar. Sebaliknya, CCTV memiliki prioritas terendah (4), karena dianggap tidak kritis dibandingkan layanan lainnya.

Limit Rate pada Masing-Masing Queue

- E-learning: Diberikan 40 Mbps untuk memastikan proses pembelajaran daring berjalan lancar tanpa gangguan dari trafik lain.
- Guru & Staf: Diberikan 30 Mbps untuk kebutuhan mereka dalam mengakses email dan cloud storage.
- Siswa: Diberikan 20 Mbps untuk browsing umum, dengan prioritas lebih rendah.
- CCTV & Update Sistem: Diberikan 10 Mbps dengan prioritas paling rendah.

Referensi:

Iin Marlina & Andreas Perdana (2022), Implementasi Manajemen Bandwidth Menggunakan Queue Tree Router Mikrotik, Halaman 33-35

Link Referensi

Didi Susianto (2016), Implementasi Queue Tree untuk Manajemen Bandwidth Menggunakan Router Board Mikrotik, Halaman 33

Link Referensi