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

Laporan Sementara
Praktikum Jaringan Komputer

Tunneling, IP Security, Queue Tree dan Simple Tree, Trafik Bandwidth

Andrew Marlin - 5024231020

2025

1 Pendahuluan

1.1 Latar Belakang

Lalu lintas jaringan yang aman dan efisien menjadi jantung bagi perusahaan modern, terutama apabila memliki kantor cabang tersebar atau institusi pendidikan dengan kebutuhan internet cepat, di mana tantangan utamanya adalah menjamin keamanan transmisi data melalui internet yang tidak aman dan mengelola alokasi bandwidth terbatas secara optimal. Oleh karena itu, pembelajaran konfigurasi VPN menggunakan IPSec menjadi krusial untuk menciptakan terowongan komunikasi aman yang melindungi data sensitif, sementara implementasi mekanisme Quality of Service (QoS) seperti Queue Tree pada router penting untuk memastikan layanan kritis mendapatkan alokasi bandwidth memadai. Teknologi ini sangat relevan di dunia nyata, dengan perusahaan mengandalkan VPN untuk koneksi aman antar cabang dan akses jarak jauh, serta institusi pendidikan memanfaatkan QoS untuk kelancaran proses digital, sehingga penguasaan IPSec dan QoS menjadi kompetensi inti dalam administrasi jaringan dan keamanan siber seiring meningkatnya ketergantungan pada infrastruktur digital.

1.2 Dasar Teori

Secara teori, tunneling membungkus paket data dari satu protokol jaringan di dalam protokol lain, menciptakan sebuah "terowongan" virtual. Hal ini memungkinkan pengiriman data antar jaringan yang berbeda tipe atau untuk meningkatkan keamanan dengan enkapsulasi. Berbagai protokol tunneling seperti GRE, L2TP, dan PPTP memiliki mekanisme dan kegunaan spesifik dalam membangun koneksi ini.

IPSec (Internet Protocol Security) merupakan serangkaian protokol yang digunakan untuk mengamankan komunikasi melalui jaringan berbasis IP dengan menyediakan otentikasi, integritas, dan kerahasiaan data. Dasar teorinya melibatkan dua mode utama, yaitu mode transport yang hanya mengenkripsi payload data, dan mode tunnel yang mengenkripsi seluruh paket IP asli. IPSec menggunakan protokol seperti Authentication Header (AH) untuk integritas dan otentikasi, serta Encapsulating Security Payload (ESP) untuk kerahasiaan dan juga dapat menyediakan otentikasi.

Queue Tree dan Simple Queue adalah mekanisme manajemen bandwidth pada perangkat jaringan, khususnya router, untuk mengatur alokasi sumber daya jaringan kepada pengguna atau jenis trafik tertentu. Queue Tree menawarkan konfigurasi yang lebih kompleks dan hierarkis, memungkinkan pembagian bandwidth yang detail berdasarkan berbagai parameter seperti alamat IP, port, atau protokol. Sebaliknya, Simple Queue menyediakan metode yang lebih sederhana untuk membatasi kecepatan unggah dan unduh untuk target tertentu, seringkali berdasarkan alamat IP atau subnet. Keduanya bertujuan untuk memastikan kualitas layanan (QoS) dan mencegah monopoli bandwidth oleh satu pengguna atau aplikasi.

Trafik Bandwidth merujuk pada jumlah data yang dapat ditransfer melalui koneksi jaringan dalam satuan waktu tertentu, biasanya diukur dalam bit per detik (bps). Pemahaman trafik bandwidth penting untuk menganalisis kinerja jaringan, mengidentifikasi kemacetan, dan merencanakan kapasitas jaringan. Dasar teorinya melibatkan konsep seperti bandwidth maksimum (kapasitas teoritis), throughput (kecepatan transfer aktual), dan utilisasi (persentase bandwidth yang sedang digunakan). Analisis trafik bandwidth membantu administrator jaringan dalam mengoptimalkan penggunaan sumber daya dan memastikan pengalaman pengguna yang baik.

2 Tugas Pendahuluan

1. **Studi Kasus**

   a. Fase Negosiasi IPsec (IKE Phase 1 dan Phase 2)

   - **IKE Phase 1 (ISAKMP SA):**
     - Tujuan: Membangun kanal komunikasi yang aman dan terotentikasi antara dua peer IPsec (gateway).
     - Proses Utama: Negosiasi proposal kebijakan keamanan IKE (enkripsi, hash, grup Diffie-Hellman, autentikasi, lifetime), pertukaran kunci Diffie-Hellman untuk menghasilkan kunci sesi bersama, dan autentikasi peer.
     - Hasil: Terbentuknya ISAKMP Security Association (SA) atau IKE SA, yang melindungi negosiasi pada Phase 2.
   - **IKE Phase 2 (IPsec SA):**
     - Tujuan: Negosiasi parameter keamanan untuk melindungi data pengguna yang akan dilewatkan melalui tunnel IPsec.
     - Proses Utama: Menggunakan kanal aman yang sudah terbentuk di Phase 1, peer menegosiasikan proposal IPsec (protokol IPsec AH/ESP, algoritma enkripsi dan autentikasi untuk data, lifetime SA).
     - Hasil: Terbentuknya minimal dua IPsec SA (satu inbound, satu outbound) untuk setiap protokol (AH/ESP) yang digunakan. SA ini digunakan untuk enkapsulasi dan dekapsulasi lalu lintas data aktual.

   b. Parameter Keamanan yang Harus Disepakati

   - **Algoritma Enkripsi:** Menentukan metode untuk mengubah data menjadi tidak terbaca tanpa kunci yang benar. Contoh:
     - AES (Advanced Encryption Standard): 128-bit, 192-bit, 256-bit (paling umum dan aman).
     - 3DES (Triple Data Encryption Standard): Lebih tua, kurang aman dibandingkan AES.
   - **Metode Autentikasi (pada IKE Phase 1):** Memverifikasi identitas peer.
     - *Pre-Shared Keys (PSK):* Kunci rahasia yang sama dikonfigurasikan manual pada kedua peer. Cocok untuk jumlah peer terbatas.
     - *Digital Signatures (RSA/DSA):* Menggunakan infrastruktur kunci publik (PKI) dan sertifikat digital. Lebih scalable dan aman untuk jaringan besar.
   - **Algoritma Hash (Integritas):** Memastikan data tidak diubah selama transmisi.
     - SHA (Secure Hash Algorithm): SHA-256, SHA-384, SHA-512 (lebih kuat).
     - MD5 (Message Digest 5): Dianggap kurang aman untuk integritas saat ini.
   - **Grup Diffie-Hellman (DH):** Menentukan kekuatan kunci sesi yang dihasilkan. Grup yang lebih tinggi memberikan keamanan lebih baik tetapi membutuhkan lebih banyak sumber daya komputasi. Contoh: Group 14, 19, 20, 21.
   - **Lifetime Key:**

- *IKE SA Lifetime (Phase 1):* Durasi waktu atau volume data sebelum IKE SA harus dinegosiasikan ulang. Contoh: 86400 detik (24 jam).
- *IPsec SA Lifetime (Phase 2):* Durasi waktu atau volume data sebelum IPsec SA (untuk data pengguna) harus dinegosiasikan ulang. Contoh: 3600 detik (1 jam) atau 4608000 kilobytes. Rekeying periodik meningkatkan keamanan.

Semua parameter ini harus cocok pada kedua sisi router agar koneksi IPsec berhasil terbentuk.

c. Konfigurasi Sederhana pada Sisi Router untuk Memulai Koneksi Site-to-Site Konfigurasi dasar biasanya melibatkan langkah-langkah berikut (sintaks spesifik tergantung vendor router, misal Cisco, Mikrotik):

(a) **Definisi Kebijakan ISAKMP/IKE (Phase 1):**
- Tentukan prioritas kebijakan.
- Pilih algoritma enkripsi (misalnya, AES).
- Pilih fungsi hash (misalnya, SHA256).
- Pilih metode autentikasi (misalnya, pre-shared-key).
- Tentukan grup Diffie-Hellman (misalnya, group 14).
- Atur lifetime.

(b) **Konfigurasi Pre-Shared Key:**
- Masukkan pre-shared key dan alamat IP peer remote.

(c) **Definisi Transform Set (Phase 2):**
- Tentukan nama transform set.
- Pilih protokol IPsec (misalnya, ESP).
- Pilih algoritma enkripsi ESP (misalnya, AES).
- Pilih algoritma autentikasi ESP (misalnya, SHA-HMAC).
- Atur mode (tunnel).

(d) **Konfigurasi Crypto Map (atau setara):**
- Tentukan nama dan urutan crypto map.
- Tautkan dengan alamat IP peer remote.
- Tautkan dengan transform set yang telah dibuat.
- Tentukan *Access Control List (ACL)* atau *traffic selector* yang mendefinisikan lalu lintas mana yang akan dienkripsi (misalnya, lalu lintas antara LAN kantor pusat dan LAN kantor cabang).

(e) **Terapkan Crypto Map ke Interface WAN:**
- Terapkan crypto map yang telah dibuat ke interface router yang terhubung ke internet.

(f) **Konfigurasi ACL (Access Control List):**
- Buat ACL yang mendefinisikan lalu lintas "menarik" (interesting traffic) yang akan melewati tunnel VPN. Alamat sumber adalah jaringan lokal, dan alamat tujuan adalah jaringan remote (dan sebaliknya pada router remote).

- Pastikan ACL ini tidak memblokir lalu lintas IKE (UDP port 500 dan 4500 jika NAT Traversal digunakan) atau protokol IPsec (AH: protokol IP 51, ESP: protokol IP 50). Biasanya, lalu lintas IKE/IPsec diizinkan secara implisit atau tidak perlu didefinisikan dalam ACL "interesting traffic".

(g) **Pastikan Routing:**

- Pastikan router tahu cara mencapai jaringan remote melalui tunnel VPN.

2. **Skema Queue Tree** Asumsi menggunakan Mikrotik RouterOS sebagai contoh untuk terminologi Queue Tree.

   Skema Queue Tree

```
GLOBAL (Parent - Interface WAN - max-limit: 100M)
  |
  +-- Q_ELEARNING (Child of GLOBAL - limit-at: 40M, max-limit: 100M, priority: 1)
  |
  +-- Q_GURU_STAF (Child of GLOBAL - limit-at: 30M, max-limit: 100M, priority: 2)
  |
  +-- Q_SISWA (Child of GLOBAL - limit-at: 20M, max-limit: 80M, priority: 3)
  |
  +-- Q_CCTV_UPDATE (Child of GLOBAL - limit-at: 10M, max-limit: 20M, priority: 4)
```

   a. Parent dan Child Queue

   - **Parent Queue (GLOBAL):**
     - Diterapkan pada interface WAN fisik (misalnya, `ether1-gateway`).
     - `max-limit`: 100 Mbps (total bandwidth internet).
     - Queue ini menjadi induk bagi semua antrian lainnya.
   - **Child Queues:**
     - **Q_ELEARNING:** Parent: GLOBAL. Untuk lalu lintas e-learning.
     - **Q_GURU_STAF:** Parent: GLOBAL. Untuk lalu lintas guru dan staf.
     - **Q_SISWA:** Parent: GLOBAL. Untuk lalu lintas siswa.
     - **Q_CCTV_UPDATE:** Parent: GLOBAL. Untuk lalu lintas CCTV dan update sistem.

   b. Penjelasan Marking Packet marking adalah proses menandai paket data berdasarkan kriteria tertentu (misalnya, alamat IP sumber/tujuan, port, protokol, dll.) sehingga router dapat mengidentifikasi dan mengarahkan paket tersebut ke antrian (queue) yang sesuai.

   (a) Buat `mangle rules` untuk menandai koneksi dan paket:

   - **Mark Connection:**
     - `mark-connection name=conn_elearning` untuk IP/port e-learning.
     - `mark-connection name=conn_guru_staf` untuk IP guru/staf.
     - `mark-connection name=conn_siswa` untuk IP siswa.
     - `mark-connection name=conn_cctv_update` untuk IP CCTV/port update.
   - **Mark Packet (berdasarkan connection mark):**

- `mark-packet name=pkt_elearning` jika `connection-mark=conn_elearning`.
- `mark-packet name=pkt_guru_staf` jika `connection-mark=conn_guru_staf`.
- `mark-packet name=pkt_siswa` jika `connection-mark=conn_siswa`.
- `mark-packet name=pkt_cctv_update` jika `connection-mark=conn_cctv_update`.

Penting untuk memastikan aturan mangle ditempatkan pada chain yang benar (`prerouting` atau `forward` tergantung topologi).

(b) Di setiap child queue, gunakan `packet-mark` yang sesuai untuk menangkap lalu lintas yang telah ditandai.

c. Prioritas dan Limit Rate untuk Masing-Masing Queue

- **Q_ELEARNING:**
  - `packet-mark`: pkt_elearning
  - `limit-at` (CIR - Committed Information Rate): 40 Mbps (jaminan bandwidth minimal)
  - `max-limit` (MIR - Maximum Information Rate): 100 Mbps (bisa menggunakan hingga total bandwidth jika tersedia dan prioritas memungkinkan)
  - `priority`: 1 (prioritas tertinggi)
- **Q_GURU_STAF:**
  - `packet-mark`: pkt_guru_staf
  - `limit-at`: 30 Mbps
  - `max-limit`: 100 Mbps
  - `priority`: 2
- **Q_SISWA:**
  - `packet-mark`: pkt_siswa
  - `limit-at`: 20 Mbps
  - `max-limit`: 80 Mbps (dibatasi agar tidak menghabiskan semua sisa bandwidth, memberikan ruang untuk burst layanan lain atau penyesuaian)
  - `priority`: 3
- **Q_CCTV_UPDATE:**
  - `packet-mark`: pkt_cctv_update
  - `limit-at`: 10 Mbps
  - `max-limit`: 20 Mbps (memberikan sedikit ruang untuk burst update penting)
  - `priority`: 4 (prioritas lebih rendah, namun tetap ada jaminan)

Catatan Penting untuk Queue Tree:

- Total `limit-at` dari semua child queue sebaiknya tidak melebihi `max-limit` parent queue (dalam kasus ini, $40 + 30 + 20 + 10 = 100$ Mbps, sesuai).
- Prioritas bekerja ketika terjadi kongesti. Queue dengan prioritas lebih tinggi (angka lebih kecil) akan didahulukan.
- `max-limit` pada child queue memungkinkan penggunaan bandwidth yang tidak terpakai oleh queue lain, hingga batas `max-limit` queue itu sendiri atau `max-limit` parent.

Referensi

(a) Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson.

(b) Kent, S., & Seo, K. (2005). *RFC 4301: Security Architecture for the Internet Protocol*. IETF.

(c) Cisco Systems. (n.d.). *IPsec Configuration Guide*. (Dokumentasi spesifik vendor, versi bisa bervariasi).

(d) Microsoft Docs. (n.d.). *IPsec*. (Dokumentasi untuk implementasi Windows).

(e) MikroTik Wiki. (n.d.). *Manual:Queue Tree*. Diakses dari `https://wiki.mikrotik.com/wiki/Manual:Qu`

(f) MikroTik Wiki. (n.d.). *Manual:Packet Flow*. Diakses dari `https://wiki.mikrotik.com/wiki/Manual:Pa` (atau versi relevan).

(g) Hart, B., & Kaven, G. (2019). *Learn RouterOS* (2nd ed.). (Buku panduan RouterOS).