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

Laporan Sementara
Praktikum Jaringan Komputer

Tunneling

Abraham Napitupulu - 5024231048

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital saat ini, konektivitas jaringan yang handal dan aman menjadi tulang punggung operasional berbagai organisasi, mulai dari perusahaan hingga institusi pendidikan. Kebutuhan untuk menghubungkan jaringan-jaringan yang terpisah secara geografis atau yang memiliki arsitektur berbeda secara mulus menjadi tantangan tersendiri. Oleh karena itu, pemahaman mendalam mengenai teknik tunneling menjadi sangat relevan, memungkinkan pembuatan jalur komunikasi privat virtual melalui infrastruktur jaringan publik atau antar jaringan yang tidak kompatibel secara langsung, sehingga memfasilitasi integrasi sistem dan pertukaran data yang efisien. Seiring dengan meningkatnya interkoneksi jaringan, isu keamanan data juga menjadi perhatian utama. Transmisi informasi sensitif melalui jaringan, terutama internet yang bersifat publik, rentan terhadap berbagai ancaman siber seperti penyadapan, modifikasi data, atau pemalsuan identitas. Untuk mengatasi risiko ini, implementasi protokol keamanan yang kuat seperti IPSec (IP Security) menjadi standar industri. Kebutuhan untuk membangun Virtual Private Network (VPN) yang aman antar kantor pusat dan cabang, atau untuk mendukung akses jarak jauh yang terproteksi, mendorong pentingnya penguasaan konfigurasi dan mekanisme kerja IPSec guna menjamin kerahasiaan, integritas, dan keaslian data yang dikirimkan. Di sisi lain, ketersediaan bandwidth jaringan seringkali menjadi sumber daya yang terbatas dan harus dibagi secara adil dan efisien di antara berbagai pengguna dan aplikasi dengan kebutuhan yang beragam. Tanpa pengelolaan yang baik, layanan-layanan krusial dapat terganggu oleh aktivitas jaringan lain yang kurang penting namun mengonsumsi banyak bandwidth, yang pada akhirnya menurunkan produktivitas dan pengalaman pengguna. Oleh karena itu, manajemen bandwidth dan implementasi Quality of Service (QoS) melalui mekanisme antrian (seperti Simple Queue dan Queue Tree) serta pengaturan prioritas trafik menjadi sangat penting untuk memastikan bahwa aplikasi kritis mendapatkan alokasi sumber daya yang memadai dan kinerja jaringan tetap optimal.

1.2 Dasar Teori

Tunneling adalah teknik untuk mengirimkan data dari satu jaringan ke jaringan lain yang berbeda jenis dengan cara "membungkus" paket data asli (enkapsulasi) agar dapat melintasi jaringan perantara, lalu membuka kembali bungkusan tersebut (dekapsulasi) di tujuan. Metode ini memungkinkan komunikasi antar jaringan yang terisolasi seolah-olah berada dalam satu jaringan privat. Berbagai protokol seperti GRE, IP-in-IP, hingga VXLAN mendukung fungsionalitas tunneling ini Untuk mengamankan komunikasi data, terutama melalui jaringan publik seperti internet, digunakan IPSec (IP Security). IPSec merupakan serangkaian protokol yang menyediakan autentikasi, enkripsi, dan integritas data pada lapisan IP. Proses negosiasi keamanannya diatur oleh IKE (Internet Key Exchange) yang terdiri dari dua fase: Phase 1 untuk membangun saluran aman awal dan Phase 2 untuk menegosiasikan parameter terowongan data IPSec. IPSec dapat beroperasi dalam Tunnel Mode (membungkus seluruh paket IP asli, cocok untuk VPN site-to-site) atau Transport Mode (hanya mengamankan payload, untuk komunikasi end-to-end). Protokol inti di dalamnya adalah AH (autentikasi) dan ESP (enkripsi dan autentikasi). Manajemen bandwidth adalah proses optimalisasi penggunaan sumber daya jaringan dengan mengatur alokasi dan prioritas lalu lintas data. Pada perangkat MikroTik, ini dapat dilakukan melalui Simple Queue untuk pembatasan bandwidth per pengguna/IP secara mudah, atau Queue Tree untuk pengaturan yang lebih kompleks dan hierarkis. Queue Tree memanfaatkan penandaan

paket (mangle) untuk mengklasifikasikan trafik dan menerapkan kebijakan QoS yang lebih granural, termasuk prioritas trafik untuk layanan penting. Pengaturan limit-at (kecepatan terjamin) dan max-limit (kecepatan maksimum) menjadi kunci dalam pembagian bandwidth.

Tugas Pendahuluan: Tunneling, VPN IPSec, dan Manajemen Bandwidth

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

   - **Fase Negosiasi IPSec (IKE Phase 1 dan Phase 2)**

     IPSec menggunakan IKE untuk membangun koneksi aman melalui dua fase:

     IKE Phase 1 (ISAKMP SA) Fase ini bertujuan membangun saluran komunikasi awal yang aman dan terautentikasi antar peer VPN. Proses utamanya melibatkan pertukaran proposal kebijakan keamanan, pertukaran kunci Diffie-Hellman untuk menghasilkan kunci rahasia bersama, dan autentikasi identitas peer. Hasilnya adalah IKE SA yang melindungi negosiasi fase berikutnya.

     IKE Phase 2 (IPSec SA) Menggunakan saluran aman dari Phase 1, fase ini menegosiasikan parameter spesifik untuk terowongan data IPSec. Ini mencakup pemilihan protokol IPSec (AH atau ESP), algoritma enkripsi/autentikasi data, mode enkapsulasi (umumnya Tunnel untuk site-to-site), dan jika Perfect Forward Secrecy (PFS) diaktifkan, pertukaran kunci sesi baru. Hasilnya adalah sepasang IPSec SA (untuk trafik masuk dan keluar) yang siap melindungi data aktual.

   - **Parameter Keamanan yang Harus Disepakati**

     Kedua peer VPN harus menyepakati parameter keamanan yang identik agar koneksi berhasil terbangun. Berikut adalah parameter kunci untuk masing-masing fase:

     Parameter IKE Phase 1 (ISAKMP SA):

     – *Algoritma Enkripsi:* Bertugas mengamankan pertukaran informasi selama Phase 1. Contoh umum adalah AES (misalnya, AES-128, AES-256) atau 3DES.

     – *Algoritma Hash (Integritas):* Digunakan untuk memastikan integritas pesan IKE. Contoh umum adalah SHA (misalnya, SHA-256, SHA-512).

     – *Metode Autentikasi Peer:* Cara peer memverifikasi identitas satu sama lain. Pilihan utama:

       * Pre-Shared Keys (PSK): Kunci rahasia yang sama dikonfigurasi secara manual di kedua peer.
       * Sertifikat Digital (RSA Signatures): Menggunakan infrastruktur kunci publik (PKI) untuk autentikasi yang lebih scalable.

     – *Diffie-Hellman (DH) Group:* Menentukan kekuatan (panjang bit) dari kunci yang dihasilkan selama pertukaran kunci DH. Grup dengan nomor lebih tinggi umumnya lebih aman (misalnya, Group 14, 19, atau lebih tinggi).

     – *Lifetime (Masa Berlaku SA):* Durasi waktu sebelum IKE SA harus dinegosiasi ulang untuk menjaga keamanan (misalnya, 86400 detik atau 24 jam).

     Parameter IKE Phase 2 (IPSec SA):

- *Protokol IPSec:* Pilihan antara:
  - ESP (Encapsulating Security Payload): Menyediakan kerahasiaan (enkripsi), integritas data, dan autentikasi asal data. Ini adalah pilihan yang paling umum.
  - AH (Authentication Header): Hanya menyediakan integritas data dan autentikasi asal data, tanpa memberikan kerahasiaan (enkripsi).
- *Algoritma Enkripsi (jika menggunakan ESP):* Algoritma yang digunakan untuk mengenkripsi data aktual yang dikirim melalui terowongan. Contoh: AES (misalnya, AES-128, AES-256).
- *Algoritma Autentikasi (untuk ESP atau AH):* Algoritma untuk memastikan integritas dan autentikasi data aktual. Contoh: HMAC-SHA (misalnya, HMAC-SHA-256, HMAC-SHA-512).
- *Mode Enkapsulasi:* Menentukan bagaimana paket asli dibungkus oleh IPSec:
  - Tunnel Mode: Seluruh paket IP asli (termasuk header IP asli) dienkapsulasi dalam paket IPSec baru. Ini adalah mode yang digunakan untuk VPN site-to-site (antar gateway/router).
  - Transport Mode: Hanya payload lapisan transport dari paket asli yang dienkapsulasi; header IP asli tetap tidak berubah. Umumnya digunakan untuk komunikasi end-to-end antar host atau dari host ke gateway.
- *Perfect Forward Secrecy (PFS) DH Group (Opsional):* Jika diaktifkan, pertukaran kunci Diffie-Hellman baru dilakukan untuk setiap pembentukan IPSec SA. Ini memastikan bahwa kunci sesi data bersifat independen dari kunci IKE Phase 1, meningkatkan keamanan. Menggunakan DH Group yang spesifik (misalnya, Group 14).
- *Lifetime (Masa Berlaku SA):* Durasi waktu atau volume data sebelum IPSec SA harus dinegosiasi ulang. Contoh: 3600 detik (1 jam) atau berdasarkan total volume data yang ditransfer.

- **Konfigurasi Sederhana pada Sisi Router untuk Memulai Koneksi IPSec Site-to-Site**

  Konfigurasi pada router umumnya melibatkan pendefinisian kebijakan ISAKMP (untuk IKE Phase 1), pengaturan transform set (untuk IKE Phase 2), pembuatan access control list (ACL) untuk menentukan lalu lintas mana yang akan melewati VPN, dan terakhir adalah crypto map yang mengikat semua elemen tersebut dan diterapkan pada interface WAN router.

  Contoh konseptual (mirip sintaks Cisco IOS) untuk router kantor pusat (dengan LAN `192.168.1.0/24`) yang terhubung ke kantor cabang (LAN `192.168.2.0/24`) dengan IP publik router cabang `[IP_PEER_CABANG]` dan Pre-Shared Key `KunciSangatRahasia`:

```
! Konfigurasi IKE Phase 1
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
 group 14
crypto isakmp key KunciSangatRahasia address [IP_PEER_CABANG]

! Konfigurasi IKE Phase 2
```

```
crypto ipsec transform-set SET_VPN esp-aes 256 esp-sha256-hmac
 mode tunnel

! ACL untuk menentukan traffic VPN
ip access-list extended TRAFFIC_VPN
 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

! Crypto Map
crypto map MAP_VPN 10 ipsec-isakmp
 set peer [IP_PEER_CABANG]
 set transform-set SET_VPN
 match address TRAFFIC_VPN

! Terapkan ke Interface WAN
interface GigabitEthernet0/0 ! Ganti sesuai interface WAN
 crypto map MAP_VPN
```

Konfigurasi yang serupa, dengan penyesuaian alamat IP, perlu diterapkan pada router di kantor cabang.

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 (Browse umum)
   - 10 Mbps untuk CCTV & update sistem

   Buatlah skema Queue Tree yang lengkap (diringkas):

   - **Parent dan Child Queue**

     Struktur hierarkis dibuat di MikroTik untuk mengelola total bandwidth 100 Mbps.

     Parent Queue: Diberi nama `Total_Bandwidth_Sekolah`, dengan `Max Limit` 100M/100M, diterapkan pada interface WAN.

     Child Queues (di bawah Parent Queue):
     - `Q_Elearning`: `Limit At` 40M, `Max Limit` 40M, Prioritas 1.
     - `Q_Guru_Staf`: `Limit At` 30M, `Max Limit` 30M, Prioritas 2.
     - `Q_Siswa`: `Limit At` 20M, `Max Limit` 20M, Prioritas 3.
     - `Q_CCTV_System`: `Limit At` 10M, `Max Limit` 10M, Prioritas 2.

   - **Penjelasan Marking (Mangle)**

     Paket data harus ditandai menggunakan Firewall Mangle sebelum diatur oleh Queue Tree. Proses ini umumnya melibatkan:

     (a) Penandaan koneksi (`mark-connection`) berdasarkan kriteria seperti IP address sumber/tujuan, address list, atau port layanan.

(b) Penandaan paket (`mark-packet`) berdasarkan tanda koneksi yang sudah ada. Tanda paket ini digunakan oleh Queue Tree.

Marking perlu dibedakan untuk lalu lintas download dan upload.

- **Prioritas dan Limit Rate pada Masing-Masing Queue**
  - `Limit At`**:** Jaminan bandwidth minimal yang akan diterima antrian.
  - `Max Limit`**:** Batas kecepatan maksimum absolut untuk antrian.
  - `Priority` **(1-8, 1 tertinggi):** Menentukan urutan layanan saat terjadi perebutan bandwidth. Antrian dengan prioritas lebih tinggi akan didahulukan.

  Dalam skema ini, E-learning (prioritas 1) menjadi yang utama, diikuti Guru/Staf dan CCTV/Sistem (prioritas 2), kemudian Siswa (prioritas 3). Total `limit-at` sesuai kapasitas total.

Referensi

Penjelasan dalam tugas pendahuluan ini disusun berdasarkan prinsip-prinsip umum dalam keamanan jaringan dan manajemen lalu lintas data, serta mengacu pada dokumentasi standar dan praktik industri berikut:

Untuk IPSec dan IKE

- Internet Engineering Task Force (IETF). (2005). *RFC 4301: Security Architecture for the Internet Protocol*.
- Internet Engineering Task Force (IETF). (2014). *RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2)*.
- Internet Engineering Task Force (IETF). (2005). *RFC 4302: IP Authentication Header (AH)*.
- Internet Engineering Task Force (IETF). (2005). *RFC 4303: IP Encapsulating Security Payload (ESP)*.
- Cisco Systems. Dokumentasi Dukungan dan Konfigurasi untuk Protokol IPSec Negotiation/IKE. Tersedia dari: Dokumentasi online resmi Cisco.
- Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson Education.

Untuk Queue Tree dan Mangle MikroTik

- MikroTik. (Tanpa Tahun). *Manual:Queue Tree*. MikroTik Wiki.
- MikroTik. (Tanpa Tahun). *Manual:IP/Firewall/Mangle*. MikroTik Wiki.
- Materi pelatihan resmi MikroTik (misalnya, MTCNA, MTCRE, MTCINE).
- Berbagai sumber daring dan forum diskusi komunitas MikroTik mengenai implementasi Quality of Service (QoS).

Penggunaan sumber-sumber ini bertujuan untuk memastikan akurasi teknis dan kesesuaian dengan standar industri yang berlaku.