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

Laporan Sementara
Praktikum Jaringan Komputer

NAT dan Firewall

Sultan Syafiq Rakan - 5024231009

2025

1 Pendahuluan

Dalam dunia jaringan komputer, keamanan dan pengelolaan lalu lintas data menjadi aspek krusial untuk memastikan performa, efisiensi, dan perlindungan terhadap ancaman siber. Teknologi seperti *tunneling*, *IPSec*, serta metode pengelolaan antrian seperti *Simple Queue* dan *Queue Tree* digunakan untuk mengatasi tantangan tersebut. *Tunneling* memungkinkan pengiriman data melalui jaringan yang tidak langsung terhubung dengan aman, *IPSec* memberikan lapisan keamanan tambahan untuk melindungi data, sedangkan *Simple Queue* dan *Queue Tree* digunakan untuk mengatur bandwidth dan prioritas lalu lintas jaringan. Makalah ini akan membahas konsep dasar, fungsi, dan perbandingan teknologi-teknologi tersebut untuk memberikan pemahaman yang komprehensif tentang penerapannya dalam jaringan.

2 Dasar Teori

1. Tunneling

Tunneling adalah teknik yang digunakan untuk mengenkapsulasi satu protokol jaringan di dalam protokol jaringan lain, sehingga data dapat dikirim melalui jaringan yang mungkin tidak mendukung protokol asli. *Tunneling* menciptakan "terowongan virtual" yang memungkinkan komunikasi aman antar dua titik, meskipun melalui jaringan publik seperti internet. Contoh teknologi *tunneling* meliputi:

- **PPTP** (*Point-to-Point Tunneling Protocol*): Protokol sederhana untuk VPN, namun kurang aman dibandingkan teknologi modern.
- **L2TP** (*Layer 2 Tunneling Protocol*): Sering dikombinasikan dengan *IPSec* untuk keamanan tambahan.
- **GRE** (*Generic Routing Encapsulation*): Protokol serbaguna yang mendukung berbagai jenis lalu lintas jaringan.

Tunneling umumnya digunakan untuk keperluan VPN (*Virtual Private Network*), menghubungkan jaringan privat melalui internet, atau mengamankan komunikasi antar lokasi geografis yang berbeda.

2. IPSec

IPSec (*Internet Protocol Security*) adalah rangkaian protokol yang digunakan untuk mengamankan komunikasi jaringan pada lapisan IP. *IPSec* menyediakan autentikasi, integritas data, dan kerahasiaan melalui mekanisme seperti:

- **AH** (*Authentication Header*): Menyediakan autentikasi dan integritas data tanpa enkripsi.

- **ESP** (*Encapsulating Security Payload*): Menyediakan autentikasi, integritas, dan enkripsi data.
- **IKE** (*Internet Key Exchange*): Mengelola kunci enkripsi untuk komunikasi aman.

IPSec dapat beroperasi dalam dua mode:

- **Transport Mode**: Hanya *payload* data yang dienkripsi, digunakan untuk komunikasi antar host.
- **Tunnel Mode**: Seluruh paket IP dienkripsi dan dikapsulasi dalam paket IP baru, umum digunakan untuk VPN situs-ke-situs.

IPSec sering digunakan bersama teknologi *tunneling* seperti *L2TP* untuk meningkatkan keamanan komunikasi.

3. Simple Queue

Simple Queue adalah metode pengelolaan antrian sederhana yang digunakan dalam perangkat seperti MikroTik untuk mengatur lalu lintas jaringan berdasarkan aturan tertentu. *Simple Queue* memungkinkan pembatasan *bandwidth*, pengaturan prioritas, dan pengelolaan lalu lintas berdasarkan alamat IP, *subnet*, atau antarmuka jaringan. Ciri utama *Simple Queue* meliputi:

- **Kemudahan Konfigurasi**: Mudah diatur untuk skenario sederhana seperti pembagian *bandwidth* per pengguna.
- **Penggunaan Dasar**: Cocok untuk jaringan kecil atau kebutuhan manajemen lalu lintas yang tidak kompleks.
- **Batasan**: Kurang fleksibel untuk skenario kompleks karena hanya mendukung aturan linier.

Simple Queue ideal untuk lingkungan dengan kebutuhan manajemen *bandwidth* dasar, seperti jaringan rumah atau kantor kecil.

4. Queue Tree

Queue Tree adalah metode pengelolaan antrian yang lebih canggih dibandingkan *Simple Queue*, juga digunakan pada perangkat seperti MikroTik. *Queue Tree* memungkinkan pengaturan lalu lintas jaringan dengan struktur hierarkis, memberikan fleksibilitas lebih besar dalam mengelola *bandwidth* dan prioritas. Ciri utama *Queue Tree* meliputi:

- **Struktur Hierarkis**: Memungkinkan pembuatan aturan bertingkat untuk mengelola lalu lintas berdasarkan jenis data, protokol, atau tujuan.
- **Kontrol Lanjutan**: Mendukung pengaturan kompleks seperti pengelompokan lalu lintas (misalnya, VoIP, *streaming*, atau *browsing*).

- **Kombinasi dengan Mangle**: Sering digunakan bersama fitur *mangle* untuk menandai paket dan menerapkan aturan khusus.

Queue Tree lebih cocok untuk jaringan besar atau skenario yang membutuhkan pengelolaan lalu lintas yang sangat spesifik, seperti ISP atau perusahaan dengan banyak pengguna.

3 Tugas Pendahuluan

Tugas Pendahuluan

Nomor 1

Diberikan studi kasus untuk konfigurasi VPN IPSec. Suatu perusahaan ingin membuat koneksi aman antar 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:

- **Fase negosiasi IPSec (IKE Phase 1 dan Phase 2)**: Fase negosiasi IPSec dimulai dengan IKE Phase 1 yang bertujuan membentuk saluran aman untuk pertukaran kunci melalui autentikasi dan negosiasi parameter keamanan. Phase 2 melanjutkan dengan negosiasi parameter spesifik untuk melindungi data, termasuk algoritma enkripsi dan autentikasi.
- **Parameter keamanan yang harus disepakati (algoritma enkripsi, metode autentikasi, lifetime key)**: Parameter keamanan meliputi algoritma enkripsi seperti AES-256, metode autentikasi seperti pre-shared key (PSK) atau sertifikat digital, serta lifetime key yang menentukan durasi keabsahan kunci sebelum diperbarui (misalnya, 8 jam).
- **Konfigurasi sederhana pada sisi router untuk memulai koneksi IPSec site-to-site**: Konfigurasi dasar meliputi pengaturan kebijakan IPSec, pembuatan tunnel interface, penentuan jaringan lokal dan remote, serta pengaturan kunci prabagi dan parameter keamanan yang seragam di kedua sisi router.

Referensi: Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks*. Pearson.

Nomor 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:

- **Parent dan child queue**: Parent queue dikonfigurasi dengan total bandwidth 100 Mbps, di mana child queue dibuat untuk masing-masing kategori (e-learning, guru-/staf, siswa, CCTV) dengan alokasi sesuai kebutuhan.
- **Penjelasan marking**: Marking dilakukan menggunakan fitur Mangle untuk menandai paket berdasarkan alamat IP, port, atau jenis lalu lintas (misalnya, port 80 untuk browsing, port 443 untuk email).
- **Prioritas dan limit rate pada masing-masing queue**: Prioritas diberikan kepada e-learning (prioritas 1) dan guru/staf (prioritas 2), dengan limit rate masing-masing 40 Mbps dan 30 Mbps. Siswa dan CCTV diberi prioritas 3 dan 4 dengan limit rate 20 Mbps dan 10 Mbps.

Referensi: MikroTik Documentation. (2023). *Queue Tree Configuration Guide*. MikroTik.