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

Laporan Sementara
Praktikum Jaringan Komputer

VPN & QoS

Joycelyn Emmanuella Passandaran - 5024231001

2025

1 Pendahuluan

1.1 Latar Belakang

Seiring dengan berkembangnya kebutuhan akan koneksi jaringan yang aman dan bisa diakses dari lokasi yang berbeda, penggunaan teknologi seperti Virtual Private Network (VPN) menjadi semakin penting. VPN memungkinkan perangkat terhubung ke jaringan pribadi melalui internet secara aman, dengan bantuan proses tunneling dan enkripsi yang menjaga data tetap terlindungi. Dalam penerapannya, beberapa protokol seperti PPTP dan L2TP sering digunakan untuk membangun koneksi antar perangkat atau antar kantor yang berjauhan. Untuk menjaga kestabilan jaringan saat banyak perangkat mengakses secara bersamaan, diperlukan juga pengaturan bandwidth agar layanan penting tetap berjalan lancar.Di saat itu peran Quality of Service (QoS) diperlukan, yang membantu mengatur prioritas lalu lintas data sesuai kebutuhan. Praktikum ini bertujuan agar praktikan dapat memahami cara kerja VPN, proses tunneling, serta penerapan QoS menggunakan fitur Simple Queue dan Queue Tree.

1.2 Dasar Teori

Virtual Private Network (VPN) merupakan teknologi yang memungkinkan suatu perangkat terhubung ke jaringan pribadi melalui jaringan publik (seperti internet) secara aman. VPN bekerja dengan cara mengenkripsi data sehingga informasi yang dikirim tidak dapat diakses oleh pihak yang tidak berwenang. Salah satu teknik utama yang digunakan dalam VPN adalah tunneling, yaitu proses pengiriman data dengan membungkus paket data asli dalam protokol lain untuk melintasi jaringan yang berbeda. Dengan tunneling, dua jaringan yang berbeda jenis dapat saling terhubung seolah-olah berada dalam satu jaringan lokal.

Tunneling memungkinkan data dari satu perangkat dibungkus menggunakan protokol tertentu untuk melewati jaringan publik dan dibuka kembali di sisi penerima. Terdapat beberapa protokol tunneling seperti PPTP (Point-to-Point Tunneling Protocol) yang merupakan protokol lama namun masih digunakan untuk koneksi dasar, L2TP (Layer 2 Tunneling Protocol) yang menggabungkan fitur dari PPTP dan L2F untuk keamanan dan fleksibilitas yang lebih tinggi, serta EOIP (Ethernet over IP) yang merupakan protokol khusus dari MikroTik untuk membuat tunnel antar perangkat MikroTik. Proses tunneling mendukung kemampuan jaringan yang berbeda untuk saling terhubung dan menjadi komponen penting dalam pengembangan jaringan yang aman dan fleksibel, terutama dalam implementasi VPN antar kantor atau akses jarak jauh.

IPSec (Internet Protocol Security) adalah seperangkat protokol keamanan jaringan yang dirancang untuk melindungi komunikasi data melalui jaringan IP. IPSec menggunakan teknik enkripsi dan autentikasi untuk menjaga kerahasiaan dan keaslian data. Terdapat dua mode dalam IPSec yaitu tunnel mode yang mengenkripsi seluruh paket termasuk header IP, dan transport mode yang hanya mengenkripsi isi data. IPSec umum digunakan dalam VPN untuk memastikan koneksi antar situs atau perangkat berjalan dengan aman, terutama pada jaringan yang memerlukan perlindungan tinggi dari ancaman pihak ketiga.

Quality of Service (QoS) adalah mekanisme manajemen jaringan yang digunakan untuk mengatur prioritas dan alokasi bandwidth terhadap berbagai jenis lalu lintas data. QoS bertujuan untuk memastikan layanan penting seperti video conference, VoIP, dan akses sistem kerja tetap mendapatkan jalur transmisi yang stabil dan cepat meskipun jaringan dalam kondisi padat. Salah satu metode yang di-

gunakan untuk mengimplementasikan QoS adalah dengan mengatur antrian data menggunakan fitur Simple Queue dan Queue Tree.

Simple Queue merupakan metode manajemen bandwidth yang paling sederhana, digunakan untuk mengatur kecepatan akses internet berdasarkan IP, interface, atau pengguna tertentu. Simple Queue mudah dikonfigurasi dan cocok untuk jaringan kecil karena hanya memerlukan parameter dasar seperti alamat IP dan batas bandwidth. Satu antrian dibuat untuk satu entitas, dengan pengaturan kecepatan upload dan download secara langsung.

Queue Tree merupakan kontrol yang lebih kompleks dan fleksibel dalam pengaturan bandwidth. Berbeda dengan Simple Queue, Queue Tree memungkinkan pembentukan struktur hierarki (parent-child) dan dapat membagi bandwidth berdasarkan jenis trafik, port, atau protokol. Penggunaan Queue Tree membutuhkan konfigurasi mangle terlebih dahulu untuk menandai trafik yang akan dikelola. Queue Tree umum digunakan dalam jaringan besar atau ISP karena kemampuannya dalam mengelompokkan dan mengalokasikan bandwidth berdasarkan kategori lalu lintas yang lebih spesifik.

Prioritas trafik merupakan bagian penting dari QoS yang menentukan urutan pemrosesan data berdasarkan tingkat kepentingannya. Pengaturan prioritas ini dapat dilakukan dengan memberi nilai prioritas lebih tinggi pada layanan penting, sehingga walaupun kondisi jaringan padat, layanan utama tetap dapat berjalan lancar. Mikrotik dan perangkat jaringan lainnya biasanya menyediakan fitur prioritas melalui konfigurasi queue dan mangle.

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

   I) Fase Negosiasi IPSec

   1. IKE Phase 1 (Main Mode): Phase 1 bertujuan untuk membentuk secure channel yang akan digunakan untuk negosiasi Phase 2.

   Langkah-langkah negosiasi:

   1. Policy Negotiation - Kedua peer bertukar proposal keamanan (encryption, hashing, authentication method, DH group)
   2. Diffie-Hellman Exchange - Pertukaran kunci publik untuk menghasilkan shared secret
   3. Authentication - Verifikasi identitas menggunakan pre-shared key atau sertifikat digital
   4. SA (Security Association) Establishment - Pembentukan IKE SA yang aman.

   Parameter yang dinegosiasikan:

   - Encryption algorithm (DES, 3DES, AES)
   - Hash algorithm (MD5, SHA-1, SHA-256)
   - Authentication method (Pre-shared key, RSA signatures, RSA encrypted nonces)
   - Diffie-Hellman group (Group 1, 2, 5, 14, 15, 16)
   - SA lifetime

2. IKE Phase 2 (Quick Mode): Phase 2 menggunakan secure channel dari Phase 1 untuk menegosiasikan IPSec SA yang akan melindungi data aktual.

Proses negosiasi:

1. IPSec Policy Negotiation - Pertukaran proposal untuk ESP/AH protocol
2. Key Material Generation - Pembuatan kunci enkripsi dan otentikasi untuk IPSec
3. IPSec SA Creation - Pembentukan inbound dan outbound SA

II.)Parameter keamanan yang harus disepakati (algoritma enkripsi, metode autentikasi, lifetime key)

1.Algoritma Enkripsi

Untuk IKE Phase 1:

- DES (56-bit) - tidak disarankan
- 3DES (168-bit) - masih dapat diterima
- AES-128, AES-192, AES-256 - direkomendasikan

Untuk IPSec (Phase 2):

- ESP dengan AES-128/192/256
- ESP dengan 3DES (backward compatibility)

2. Metode Autentikasi

Phase 1 Authentication:

- Pre-shared Key (PSK) - sederhana, cocok untuk site-to-site
- RSA Digital Signatures - lebih aman, menggunakan PKI
- RSA Encrypted Nonces - jarang digunakan

Phase 2 Authentication:

- HMAC-MD5 - kompatibilitas legacy
- HMAC-SHA-1 - standar minimal
- HMAC-SHA-256 - direkomendasikan

3. Lifetime Key

- IKE SA Lifetime: 86400 detik (24 jam) - default
- IPSec SA Lifetime: 3600 detik (1 jam) - default
- Data Lifetime: 4,608,000 KB - untuk memicu rekeying berdasarkan volume data

III.) Konfigurasi sederhana pada sisi router untuk memulai koneksi IPSec site-to-site Langkah pertama dalam konfigurasi IPSec adalah menambahkan peer, yaitu mengatur IP publik dari router lawan, metode pertukaran kunci (exchange mode), algoritma enkripsi dan hash, serta pre-shared key sebagai kunci bersama. Misalnya, pada sisi kantor pusat, peer ditambahkan dengan IP publik milik kantor cabang, menggunakan mode main, enkripsi AES-256, hash SHA-256, dan Diffie-Hellman Group modp1024. Setelah peer dikonfigurasi, langkah selanjutnya adalah membuat proposal IPSec yang berisi algoritma enkripsi dan autentikasi yang akan digunakan selama fase pertukaran data (Phase 2). Contohnya, menggunakan kombinasi AES-256 dan SHA-256 untuk menjaga keamanan dan integritas data. Kemudian, perlu ditambahkan policy yang menentukan jaringan mana yang akan dilewatkan melalui tunnel IPSec. Misalnya, jaringan lokal kantor pusat (10.0.0.0/24) akan dibuat dapat terhubung dengan jaringan kantor cabang (10.1.0.0/24) menggunakan IP publik masing-masing router sebagai titik akhir. Agar tunnel aktif, opsi tunnel=yes harus disetel pada bagian policy.

Refrensi:
https://www.goodaccess.com/blog/ipsec-vpn

https://citraweb.com/artikel/372/

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

   Skema Queue Tree
   Parent Queue:
   - Nama: parent-queue
   - Limit Rate: 100 Mbps
   - Prioritas: default

   Child Queues:
   1. Queue e-learning
   - Nama: queue-elearning
   - Parent: parent-queue
   - Limit Rate: 40 Mbps
   - Prioritas: 1 (prioritas tertinggi, agar e-learning lancar tanpa gangguan)
   - Penjelasan: Mengatur bandwidth khusus untuk kebutuhan e-learning supaya tetap stabil.

   2. Queue guru & staf
   - Nama: queue-guru-staf
   - Parent: parent-queue
   - Limit Rate: 30 Mbps
   - Prioritas: 2 (prioritas sedang)
   - Penjelasan: Untuk akses email dan cloud storage, membutuhkan bandwidth cukup tapi tidak sebesar e-learning.

   3. Queue siswa browsing
   - Nama: queue-siswa
   - Parent: parent-queue
   - Limit Rate: 20 Mbps
   - Prioritas: 3 (prioritas rendah)

- Penjelasan: Browsing umum siswa, diprioritaskan lebih rendah agar tidak mengganggu aktivitas penting lain.

4. Queue CCTV & update
- Nama: queue-cctv-update
- Parent: parent-queue
- Limit Rate: 10 Mbps
- Prioritas: 4 (prioritas paling rendah)
- Penjelasan: Digunakan untuk CCTV dan update sistem, dianggap non-kritis dibanding aktivitas lain.

Refrensi:
https://blog.dnetprovider.id/2018/12/04/tutorial-mikrotik-pembagian-bandwidth-dengan-queue-tree/
https://citraweb.com/artikel/251/