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

Laporan Sementara
Praktikum Jaringan Komputer

Tunelling

Muhammad Zidane Faiq Sidqi - 5024231040

2025

1 Pendahuluan

1.1 Latar Belakang

Seiring meningkatnya ketergantungan terhadap jaringan internet dalam berbagai sektor, mulai dari pendidikan, bisnis, hingga pemerintahan kebutuhan akan keamanan data dan efisiensi penggunaan bandwidth menjadi sangat krusial. Ancaman terhadap keamanan jaringan, seperti penyadapan data atau manipulasi informasi, dapat mengganggu operasional dan menimbulkan kerugian besar. Oleh karena itu, penguasaan teknologi Virtual Private Network (VPN), khususnya IPSec (Internet Protocol Security), menjadi penting untuk menjamin keamanan komunikasi data melalui jaringan publik seperti internet.

Selain aspek keamanan, tantangan lain yang dihadapi dalam pengelolaan jaringan modern adalah bagaimana membagi dan memprioritaskan pemakaian bandwidth secara efisien. Dalam lingkungan dengan banyak pengguna dan layanan seperti sekolah, kantor, atau instansi pemerintahan dibutuhkan sistem manajemen bandwidth yang mampu memberikan prioritas kepada trafik penting seperti e-learning atau video conference, tanpa mengabaikan layanan lainnya. Di sinilah konsep Queue Tree pada perangkat jaringan seperti MikroTik berperan besar dalam pembagian dan pengendalian lalu lintas data. Praktikum ini dirancang untuk memperkenalkan dan melatih pemahaman serta kemampuan teknis dalam: Mengimplementasikan VPN IPSec secara aman antara dua lokasi (site-to-site), mendesain dan mengatur manajemen bandwidth menggunakan Queue Tree secara efisien.

Permasalahan yang ingin diselesaikan mencakup bagaimana menjamin keamanan komunikasi data antar kantor serta bagaimana membagi bandwidth agar layanan prioritas tetap berjalan lancar di tengah keterbatasan jaringan.

1.2 Dasar Teori

VPN merupakan teknologi yang memungkinkan koneksi jaringan yang aman dan terenkripsi melalui jaringan publik seperti internet. VPN menciptakan "terowongan" komunikasi privat, sehingga data yang dikirim tidak dapat diakses atau dimanipulasi oleh pihak ketiga. Salah satu bentuk implementasi VPN yang banyak digunakan adalah IPSec VPN.

IPSec adalah seperangkat protokol keamanan jaringan yang digunakan untuk mengamankan komunikasi di lapisan IP. IPSec menyediakan layanan seperti: Enkripsi (Encryption): Menyandikan data agar tidak bisa dibaca oleh pihak yang tidak berwenang, autentikasi (Authentication): Memastikan bahwa data berasal dari sumber yang sah, integritas (Integrity): Menjamin data tidak mengalami perubahan selama transmisi, manajemen Kunci (Key Management): Mengatur pertukaran kunci rahasia antara dua pihak melalui protokol IKE (Internet Key Exchange). IPSec bekerja dalam dua mode: Tunnel Mode: Mengamankan seluruh paket IP, umum digunakan dalam koneksi antar jaringan (site-to-site). Dan transport Mode: Mengamankan hanya data di dalam paket IP, digunakan untuk komunikasi end-to-end antar perangkat.

Tunneling adalah proses mengenkapsulasi data dalam protokol lain untuk memungkinkan pengiriman melalui jalur jaringan yang tidak mendukung protokol asli. Teknik ini digunakan oleh VPN untuk mengangkut data antar jaringan dengan aman. Manajemen bandwidth adalah teknik pengaturan lalu lintas data untuk memastikan setiap layanan atau pengguna mendapatkan porsi kecepatan jaringan sesuai kebutuhannya. Dalam jaringan kompleks, tidak semua trafik memiliki tingkat kepentingan yang sama, sehingga pengaturan prioritas diperlukan untuk menjaga kualitas layanan utama. Queue Tree

adalah fitur manajemen bandwidth pada perangkat MikroTik yang memungkinkan pengaturan trafik secara hierarkis (parent-child). Fitur ini bekerja bersama dengan Mangle (fitur untuk menandai paket berdasarkan kriteria tertentu), sehingga trafik dapat dikategorikan dan dialokasikan bandwidth secara efisien.

2 Tugas Pendahuluan

1. IPSec menggunakan protokol IKE (Internet Key Exchange) untuk membentuk koneksi yang aman. Proses negosiasi dilakukan dalam dua fase:
   - IKE Phase 1 : Membangun secure channel untuk melindungi komunikasi IKE Phase 2. Autentikasi dilakukan menggunakan metode seperti Pre-Shared Key (PSK) atau sertifikat digital, Negosiasi parameter keamanan seperti enkripsi dan algoritma hash, Membangun ISAKMP SA (Security Association).
   - IKE Phase 2 : Membangun IPSec SA yang digunakan untuk enkripsi lalu lintas data. Menentukan protokol keamanan (ESP/AH), algoritma enkripsi, dan integritas, proses ini lebih cepat karena dilakukan melalui channel yang sudah aman.
   Dalam koneksi IPSec, kedua perangkat harus sepakat terhadap: Algoritma enkripsi (AES-128, AES-256, 3DES), Metode Autentikasi (Pre-Shared Key (PSK), Sertifikat), Algoritma Hash (SHA-1, SHA-256), Lifetime Key (3600 detik (1 jam), 86400 detik (1 hari)).

   Contoh konfigurasi IPsec site to site di mikrotik :
   Misal:
   Kantor pusat: 192.168.1.0/24
   Kantor cabang: 192.168.2.0/24
   IP Publik kantor pusat: 1.1.1.1
   IP Publik kantor cabang: 2.2.2.2

   # Di Kantor Pusat
   /ip ipsec peer
   add address=2.2.2.2/32 auth-method=pre-shared-key secret="vpnkey123"
   /ip ipsec proposal
   set default enc-algorithms=aes-256-cbc pfs-group=modp2048
   /ip ipsec policy
   add src-address=192.168.1.0/24 dst-address=192.168.2.0/24 sa-dst-address=2.2.2.2 sa-src-address=1.1.1.1 tunnel=yes action=encrypt
   # Di Kantor Cabang
   /ip ipsec peer
   add address=1.1.1.1/32 auth-method=pre-shared-key secret="vpnkey123"
   /ip ipsec policy
   add src-address=192.168.2.0/24 dst-address=192.168.1.0/24 sa-dst-address=1.1.1.1 sa-src-address=2.2.2.2 tunnel=yes action=encrypt.

   Referensi : https://help.mikrotik.com/docs/spaces/ROS/pages/11993097/IPsec

2. # Parent Queue : 100 Mbps total bandwidth.

   # Child Queues :
   E-Learning (priority=1): 40 Mbps
   Guru dan Staf (priority=2): 30 Mbps
   Siswa (priority=3): 20 Mbps
   CCTV dan Update (priority=4): 10 Mbps

   # Skema Mangle :
   /ip firewall mangle
   add chain=forward protocol=tcp dst-port=80,443 src-address=192.168.10.0/24 action=mark-packet new-packet-mark=elearning passthrough=yes
   add chain=forward src-address=192.168.20.0/24 action=mark-packet new-packet-mark=guru-staf passthrough=yes
   add chain=forward src-address=192.168.30.0/24 action=mark-packet new-packet-mark=siswa passthrough=yes
   add chain=forward src-address=192.168.40.0/24 action=mark-packet new-packet-mark=cctv pass-through=yes

   # Queue tree configuration :
   /queue tree
   add name="ParentQueue" parent=global max-limit=100M
   add name="E-Learning" parent=ParentQueue packet-mark=elearning max-limit=40M priority=1
   add name="Guru-Staf" parent=ParentQueue packet-mark=guru-staf max-limit=30M priority=2
   add name="Siswa" parent=ParentQueue packet-mark=siswa max-limit=20M priority=3
   add name="CCTV-System" parent=ParentQueue packet-mark=cctv max-limit=10M priority=4

   Referensi : https://wiki.mikrotik.com/Manual:Queue