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

Laporan Sementara
Praktikum Jaringan Komputer

Tunneling & IPSec

Kenny Joe Neville - 5024231079

2025

1 Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi telah mendorong kebutuhan akan infrastruktur jaringan yang aman, efisien, dan mampu mengelola lalu lintas data secara optimal. Dalam lingkungan jaringan modern, tantangan seperti keamanan data, pengelolaan bandwidth, dan konektivitas antar-lokasi menjadi isu utama yang harus diatasi. Teknologi seperti tunneling dan IPSec hadir sebagai solusi untuk menjamin keamanan dan integritas data selama transmisi melalui jaringan yang tidak aman, seperti internet. Selain itu, pengelolaan bandwidth melalui metode seperti Simple Queue dan Queue Tree memungkinkan administrator jaringan untuk mengatur distribusi sumber daya jaringan secara efisien, memastikan prioritas trafik tertentu dapat terpenuhi sesuai kebutuhan.

Laporan ini disusun untuk membahas konsep-konsep tersebut, yang menjadi dasar penting dalam pengelolaan jaringan komputer. Dengan memahami teknologi tunneling, IPSec, serta teknik pengelolaan bandwidth, diharapkan dapat diterapkan solusi jaringan yang lebih aman, andal, dan efisien. Pembahasan ini relevan dalam konteks organisasi atau institusi yang mengandalkan jaringan untuk operasional sehari-hari, seperti perusahaan, institusi pendidikan, atau penyedia layanan internet.

1.2 Dasar Teori

Tunneling adalah proses pembuatan lorong bawah tanah melalui penggalian material batuan atau tanah untuk berbagai keperluan, seperti transportasi, drainase, atau utilitas. Secara teknis, tunneling melibatkan analisis geoteknik untuk memahami sifat batuan, tekanan tanah, dan kondisi air tanah di lokasi proyek. Metode tunneling yang umum digunakan meliputi metode konvensional (drill and blast), Tunnel Boring Machine (TBM), dan New Austrian Tunneling Method (NATM). Setiap metode memiliki keunggulan dan tantangan tergantung pada kondisi geologi, panjang terowongan, dan tujuan penggunaan. Selain itu, stabilitas struktur terowongan bergantung pada desain lining (pelapisan) dan sistem penyangga untuk mencegah keruntuhan. Faktor keselamatan, seperti ventilasi dan pengendalian risiko kebakaran, juga menjadi pertimbangan utama dalam perencanaan tunneling. Pemahaman teoritis ini menjadi dasar untuk merancang terowongan yang aman, ekonomis, dan berkelanjutan.

Internet Protocol Security (IPSec) adalah rangkaian protokol yang digunakan untuk mengamankan komunikasi jaringan pada lapisan IP. IPSec menyediakan autentikasi, integritas, dan kerahasiaan data melalui mekanisme seperti enkripsi dan tanda tangan digital. IPSec dapat beroperasi dalam dua mode, yaitu Transport Mode (hanya payload data yang dienkripsi) dan Tunnel Mode (seluruh paket dienkripsi dan dienkapsulasi). Penggunaan IPSec sering dikombinasikan dengan tunneling untuk membangun VPN yang aman.

Simple Queue dan Queue Tree adalah fitur pengelolaan bandwidth yang umum digunakan pada perangkat jaringan, seperti MikroTik. Simple Queue memungkinkan konfigurasi sederhana untuk membatasi kecepatan internet per pengguna atau per alamat IP, cocok untuk skenario jaringan kecil hingga menengah. Sementara itu, Queue Tree menawarkan pengelolaan yang lebih kompleks dengan struktur hierarkis, memungkinkan pengaturan prioritas dan pembag

Prioritas trafik bandwidth adalah strategi pengelolaan jaringan yang bertujuan untuk menga-

tur alokasi bandwidth berdasarkan tingkat kepentingan jenis data atau aplikasi tertentu. Strategi ini merupakan bagian dari Quality of Service (QoS), yang memungkinkan administrator jaringan untuk menetapkan prioritas pada trafik tertentu agar mendapatkan kecepatan dan keandalan yang lebih tinggi. Misalnya, dalam sebuah jaringan, trafik untuk aplikasi real-time seperti video conference dapat diprioritaskan di atas trafik unduhan file untuk mencegah latensi atau gangguan.

2 Tugas Pendahuluan

Bagian ini berisi jawaban dari tugas pendahuluan yang telah anda kerjakan, beserta penjelasan dari jawaban tersebut.

1. Diberikan studi kasus untuk konfigurasi VPN IPSec. Suatu erusahaan ingin membuat koneksi aman antara kantor pusat dan cabang.

    - 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 Jelaskan secara detail:

    Jawab:

    - Pada IKE Phase 1, kedua perangkat (router atau firewall) membentuk terowongan manajemen aman untuk pertukaran kunci menggunakan protokol Internet Key Exchange (IKE). Fase ini menetapkan Security Association (SA) melalui Main Mode (enam pesan untuk autentikasi dan pertukaran kunci yang lebih aman) atau Aggressive Mode (tiga pesan, lebih cepat namun kurang aman). Tujuannya adalah menciptakan saluran aman untuk negosiasi lebih lanjut dengan menyepakati parameter seperti algoritma enkripsi, fungsi hash, dan grup Diffie-Hellman (DH).

      IKE Phase 2 memanfaatkan terowongan Phase 1 untuk menegosiasikan SA guna melindungi data aktual yang dikirim melalui VPN, dengan parameter seperti protokol (ESP atau AH), mode (Tunnel atau Transport), dan kunci enkripsi. Phase 2 lebih cepat karena menggunakan saluran aman dari Phase 1.
    - Algoritma metode autentikasi seperti SHA-1 atau SHA-256 untuk memverifikasi integritas data, metode autentikasi seperti Pre-Shared Key (PSK) atau sertifikat digital, grup Diffie-Hellman (misalnya, Group 2 atau Group 5 untuk keseimbangan keamanan dan performa), dan lifetime key (misalnya, 86400 detik untuk Phase 1) untuk pembaruan kunci. Parameter ini harus sama di kedua sisi agar negosiasi berhasil.
    - Konfigurasi sederhana pada router untuk IPsec site-to-site dimulai dengan IKE Phase 1, misalnya pada router Cisco: crypto isakmp policy 10, diikuti encryption aes 256, hash sha, authentication pre-share, group 2, dan lifetime 86400. Kunci bersama diatur dengan crypto isakmp key <kunci> address <IP-peer>. Untuk Phase 2, buat access-list untuk lalu lintas yang dienkripsi, misalnya access-list 100 permit ip

192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255, lalu konfigurasikan transform-set dengan crypto ipsec transform-set TS esp-aes 256 esp-sha-hmac. Terakhir, buat peta kripto dengan crypto map CMAP 10 ipsec-isakmp, tetapkan access-list, peer, dan transform-set, lalu terapkan ke antarmuka dengan interface GigabitEthernet0/0 dan crypto map CMAP. Konfigurasi ini harus dicerminkan di router peer dengan alamat IP dan subnet yang sesuai.

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

   Jawab:

   - Parent Queue dinamakan "Total_Bandwidth" dengan max-limit 100 Mbps untuk mengatur seluruh lalu lintas jaringan, diterapkan pada interface WAN untuk upload dan LAN untuk download. Empat **child queue** dibuat: "E-Learning" (max-limit 40 Mbps), "Guru_Staf" (30 Mbps), "Siswa" (20 Mbps), dan "CCTV_Update" (10 Mbps)
   - Packet marking dilakukan melalui firewall mangle untuk mengidentifikasi jenis lalu lintas. Misalnya, untuk e-learning, gunakan IP server aplikasi pembelajaran atau port 80/443 (HTTP/HTTPS) dengan perintah seperti ‘/ip firewall mangle add chain=prerouting src-address=<IP-elearning> action=mark-packet new-packet-mark=elearning passthrough=no‘. Guru & staf ditandai berdasarkan subnet IP staf atau port email (25, 110, 143, 993, 995) dan cloud storage (443), misalnya ‘/ip firewall mangle add chain=prerouting src-address=<subnet-staf> action=mark-packet new-packet-mark=guru_staf passthrough=no‘. Siswa ditandai dengan subnet IP perangkat siswa untuk browsing umum (port 80/443), dan CCTV & update sistem ditandai dengan IP perangkat CCTV atau port spesifik seperti 123 (NTP) untuk update.
   - Prioritas diatur sebagai berikut: E-Learning prioritas 1 (tertinggi) untuk menjamin kelancaran pembelajaran, Guru_Staf prioritas 2 untuk administrasi, Siswa prioritas 3 untuk browsing umum, dan CCTV_Update prioritas 4 (terendah) karena bersifat non-kritis. Limit rate untuk masing-masing queue adalah: E-Learning 40 Mbps, Guru_Staf 30 Mbps, Siswa 20 Mbps, dan CCTV_Update 10 Mbps, dengan queue type PCQ untuk distribusi adil antar pengguna dalam setiap kategori. Contoh konfigurasi: ‘/queue tree add name=E-Learning parent=Total_Bandwidth packet-mark=elearning max-limit=40M queue=pcq-upload priority=1‘. Burst-rate dapat ditambahkan (misalnya, 48 Mbps untuk E-Learning) untuk menangani lonjakan sementara. Skema ini memastikan bandwidth terbagi sesuai kebutuhan dan prioritas, mencegah kemacetan jaringan.

2.1 Referensi

- Cisco Systems. (2020). IPsec VPN Configuration Guide. Cisco Press.
- Cisco Configuration Guide. (2023). Site-to-Site VPN Configuration Examples. Cisco Documentation.
- https://help.mikrotik.com/docs/spaces/ROS/pages/328088/Queues
- https://help.mikrotik.com/docs/spaces/ROS/pages/48660587/Mangle