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

Laporan Sementara
Praktikum Jaringan Komputer

VPN & QoS

Rafli J.S.P.T. - 5024231061

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital saat ini, kebutuhan akan komunikasi data yang aman dan berkualitas tinggi menjadi semakin penting, terutama dengan meningkatnya penggunaan jaringan publik seperti internet untuk keperluan bisnis, pendidikan, maupun komunikasi pribadi. Virtual Private Network (VPN) muncul sebagai solusi untuk mengatasi masalah keamanan dalam transmisi data dengan menyediakan koneksi terenkripsi yang memungkinkan pengguna mengakses jaringan secara aman dari lokasi mana pun. Teknologi ini sangat berguna untuk melindungi informasi sensitif dari ancaman siber, seperti penyadapan atau pencurian data, terutama saat bekerja dari jarak jauh. Namun, keamanan saja tidak cukup apabila kualitas koneksi jaringan tidak mendukung, terutama untuk layanan yang sensitif terhadap keterlambatan seperti video conference, panggilan suara, dan streaming. Di sinilah peran Quality of Service (QoS) menjadi sangat vital. QoS adalah mekanisme yang digunakan untuk mengatur dan memprioritaskan lalu lintas jaringan agar layanan penting mendapatkan alokasi bandwidth yang memadai dan dapat beroperasi dengan lancar. Dengan QoS, jaringan dapat meminimalkan delay, jitter, dan packet loss, sehingga performa aplikasi tetap terjaga meskipun terjadi kepadatan lalu lintas. Oleh karena itu, integrasi antara VPN dan QoS menjadi strategi penting dalam membangun sistem komunikasi jaringan yang tidak hanya aman, tetapi juga andal dan efisien dalam menangani berbagai jenis layanan secara bersamaan.

1.2 Dasar Teori

VPN bekerja dengan membuat "terowongan" terenkripsi antara perangkat pengguna dan server VPN. Teknologi ini menggunakan protokol seperti PPTP, L2TP, IPSec, atau OpenVPN untuk memastikan kerahasiaan dan integritas data. Dengan mengenkripsi data yang dikirim dan diterima, VPN menyembunyikan aktivitas pengguna dari pengintaian dan memalsukan lokasi geografis dengan menggunakan alamat IP dari server VPN, memungkinkan akses yang aman dan privat ke jaringan. Sementara itu,QoS adalah mekanisme dalam manajemen jaringan yang digunakan untuk mengalokasikan sumber daya dan mengatur lalu lintas berdasarkan prioritas. Dengan menggunakan teknik seperti traffic shaping, policing, dan prioritization, QoS dapat mengatur delay, jitter, dan packet loss agar tetap dalam batas yang dapat diterima. Parameter-parameter ini sangat penting untuk layanan real-time seperti suara dan video yang sensitif terhadap keterlambatan transmisi.

2 Tugas Pendahuluan

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)
    - Parameter keamanan yang harus disepakati (algoritma enkripsi, metode autentikasi, lifetime key)
    - Konfigurasi sederhana pada sisi router untuk memulai koneksi IPSec site-to-site
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
3. Buatlah skema Queue Tree yang lengkap:
    - Parent dan child queue
    - Penjelasan marking
    - Prioritas dan limit rate pada masing-masing queue

    Dari tiap jawaban yang kalian berikan wajib memberikan referensi

Jawaban :

1 Dalam konfigurasi VPN IPSec pada MikroTik, proses negosiasi terdiri dari dua fase utama menggunakan protokol IKE (Internet Key Exchange). Pada Phase 1, dua perangkat (peer) membentuk saluran komunikasi yang aman dan terautentikasi, dikenal sebagai ISAKMP SA (Security Association). Fase ini bertujuan untuk melindungi pertukaran pesan negosiasi IKE dan dapat dilakukan dalam mode Main atau Aggressive. Setelah Phase 1 berhasil, Phase 2 dimulai untuk membentuk IPsec SA yang akan mengatur parameter enkripsi dan autentikasi untuk lalu lintas data yang sebenarnya. Proses ini disebut Quick Mode dan menggunakan parameter yang disepakati pada Phase 1 untuk melindungi data yang ditransmisikan melalui VPN tunnel

2 Untuk Authentication Method Biasanya menggunakan pre-shared key (PSK) yang harus sama di kedua perangkat. PSK digunakan untuk saling mengenali sebelum pertukaran kunci dilakukan.Lalu Encryption Algorithm MikroTik mendukung berbagai algoritma seperti aes-128, aes-256, dan 3des. Pemilihan AES-256 umum dilakukan untuk tingkat keamanan tinggi.Hash Algorithm Untuk menjamin integritas data, digunakan algoritma seperti sha1 atau sha256.Diffie-Hellman Group Digunakan dalam pertukaran kunci untuk Phase 1 dan Phase 2. Misalnya, modp1024, modp2048, atau ecp256.Untuk Lifetime Parameter ini menentukan berapa lama satu sesi IPSec berlangsung sebelum dilakukan renegosiasi. Lifetime default untuk Phase 1 biasanya 1 jam (3600 detik), dan Phase 2 sekitar 30 menit hingga 1 jam.

3 untuk menambahkan peer: /ip ipsec peer add address=203.0.113.2/32 auth-method=pre-shared-key secret="vpnsharedkey" exchange-mode=main send-initial-contact=yes

Proposal vpn: /ip ipsec proposal add name="vpn-proposal" auth-algorithms=sha256 enc-algorithms=aes-256-cbc pfs-group=modp2048

Untuk policy: /ip ipsec policy add src-address=192.168.1.0/24 dst-address=192.168.2.0/24 sa-src-address=203.0.113.1 sa-dst-address=203.0.113.2 tunnel=yes proposal=vpn-proposal

Refrensi:https://help.mikrotik.com/docs/spaces/ROS/pages/11993097/IPsec#IPsec-InternetKeyExchangeProtocol(IKE)

4 Untuk mengelola bandwidth total 100 Mbps di lingkungan sekolah, Queue Tree digunakan untuk membagi bandwidth sesuai kebutuhan: Untuk mengelola bandwidth total 100 Mbps di lingkungan sekolah, Queue Tree digunakan untuk membagi bandwidth sesuai kebutuhan:

4.1 Parent Queue: "total-bandwidth" dengan max-limit=100M.help.mikrotik.com

4.2 Child Queues:

- e-learning: max-limit=40M, priority=1
- guru-staf: max-limit=30M, priority=2
- siswa: max-limit=20M, priority=3
- cctv-update: max-limit=10M, priority=4

Queue Tree memungkinkan pengalokasian bandwidth yang efisien dan prioritas layanan yang sesuai kebutuhan.

5 Untuk marking sendiri dibutuhkan fitur mangle contoh

5.1 /ip firewall mangle add chain=forward src-address=192.168.10.0/24 action=mark-packet new-packet-mark=e-learning passthrough=yes add chain=forward src-address=192.168.20.0/24 action=mark-packet new-packet-mark=guru-staf passthrough=yesadd 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-update passthrough=yes .marking ini dilakukan untuk bisa membatasi akses internet berdasarkan siapa penggunanya

6 Dalam Queue Tree, prioritas ditentukan dengan nilai 1 (tertinggi) hingga 8 (terendah). Dengan menetapkan prioritas yang lebih tinggi untuk layanan kritis seperti e-learning, sistem akan memastikan bahwa layanan tersebut mendapatkan bandwidth yang memadai meskipun terjadi kepadatan lalu lintas. Pengaturan max-limit pada setiap child queue memastikan bahwa tidak ada kategori pengguna yang melebihi alokasi bandwidth yang ditentukan.

- Refrensi: https://help.mikrotik.com/docs/spaces/ROS/pages/328088/Queues