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

Laporan Sementara
Praktikum Jaringan Komputer

VPN QoS

Muhammad Fawaaz Dhawi - 5024231052

2025

1 Pendahuluan

1.1 Latar Belakang

Perkembangan pesat era digital menjadikan jaringan komputer sebagai elemen krusial dalam mendukung aktivitas bisnis dan komunikasi modern. Organisasi, institusi pendidikan, dan perusahaan sangat bergantung pada infrastruktur jaringan untuk berbagi informasi, mengakses sumber daya, serta menjalankan operasional sehari-hari. Ketergantungan ini menimbulkan risiko meningkatnya ancaman keamanan siber yang semakin kompleks dan canggih, mulai dari malware, akses ilegal, pencurian data, hingga serangan siber lainnya yang dapat merugikan secara finansial maupun reputasi. Seiring dengan kemajuan teknologi, metode serangan pun berkembang, mengeksploitasi kelemahan dalam sistem jaringan. Oleh karena itu, sistem keamanan jaringan yang tangguh dan efektif menjadi kebutuhan mutlak. Firewall merupakan salah satu komponen utama dalam arsitektur keamanan jaringan yang berfungsi sebagai garis pertahanan pertama terhadap ancaman eksternal. Dengan penyaringan lalu lintas jaringan, firewall mampu mengizinkan akses yang aman dan menolak koneksi berbahaya, sehingga dapat mengurangi risiko serta memberikan kontrol yang lebih baik terhadap data yang keluar dan masuk jaringan.

Dalam dunia pendidikan, khususnya pada pembelajaran jaringan komputer, pemahaman teori saja tidak cukup untuk mempersiapkan mahasiswa menghadapi tantangan nyata di dunia kerja. Diperlukan pendekatan praktis yang memberikan pengalaman langsung dalam mengelola dan mengamankan jaringan secara real-time. Modul praktikum ini dirancang untuk menjembatani kesenjangan antara teori dan praktik melalui penerapan firewall dan routing secara langsung. Keterampilan dalam konfigurasi sistem keamanan jaringan, khususnya firewall dan routing, merupakan kompetensi penting yang sangat dibutuhkan oleh industri IT saat ini. Profesi seperti network administrator, system administrator, dan cybersecurity specialist menuntut penguasaan teknis dalam mengimplementasikan sistem keamanan dengan berbagai tingkat kompleksitas. Modul ini memberikan dasar yang kokoh dalam membangun keterampilan tersebut, sekaligus membekali mahasiswa untuk siap menghadapi tantangan keamanan jaringan yang terus berkembang di masa depan.

1.2 Dasar Teori

1.2.1 Virtual Private Network (VPN)

VPN (Virtual Private Network) adalah suatu teknologi yang memungkinkan terciptanya koneksi jaringan yang aman dan terenkripsi melalui jaringan publik seperti internet. Tujuan utama VPN adalah untuk menjaga kerahasiaan, integritas, dan autentikasi data yang dikirimkan antara dua titik atau lebih dalam jaringan. VPN memungkinkan pengguna untuk mengakses jaringan internal secara remote seolah-olah mereka berada di dalam jaringan tersebut secara fisik. VPN bekerja dengan cara membentuk sebuah "terowongan" (tunnel) virtual antara perangkat pengguna dan server VPN menggunakan protokol-protokol tertentu seperti PPTP, L2TP, IPsec, atau OpenVPN. Data yang dikirimkan melalui tunnel ini dienkripsi sehingga tidak dapat dengan mudah diakses oleh pihak ketiga. Teknologi ini banyak digunakan oleh perusahaan untuk menghubungkan cabang-cabang kantor ke jaringan pusat, atau oleh individu untuk melindungi privasi dan melewati pembatasan geografis di internet.

1.3 Quality Of Service (QoS)

QoS (Quality of Service) adalah mekanisme dalam jaringan komputer yang digunakan untuk mengatur prioritas lalu lintas data agar dapat menjamin kinerja layanan tertentu, seperti suara (VoIP), video streaming, atau aplikasi real-time lainnya. Tujuan utama QoS adalah untuk mengoptimalkan penggunaan bandwidth dan meminimalkan masalah jaringan seperti latency (keterlambatan), jitter (fluktuasi delay), dan packet loss (kehilangan paket data). Dalam implementasinya, QoS mengklasifikasikan dan memberi prioritas pada jenis-jenis trafik jaringan berdasarkan tingkat kepentingannya. Misalnya, lalu lintas suara dan video biasanya diberikan prioritas lebih tinggi dibandingkan dengan transfer file atau browsing web biasa. Teknik-teknik yang digunakan dalam QoS antara lain traffic shaping, bandwidth reservation, dan packet scheduling. QoS sangat penting dalam jaringan modern, terutama pada jaringan yang padat trafiknya, untuk menjamin performa layanan yang konsisten dan dapat diandalkan.

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

   Jawab:

   - KE Phase 1 – Pembuatan IKE SA Tujuan dari fase ini adalah untuk membentuk kanal komunikasi aman (ISAKMP Security Association) antara dua peer VPN. Proses yang terjadi pada fase ini antara lain Negosiasi parameter keamanan seperti algoritma enkripsi dan autentikasi, pertukaran kunci menggunakan metode Diffie-Hellman, autentikasi peer menggunakan Pre-Shared Key (PSK) atau sertifikat digital.

     Terdapat dua mode dalam IKE Phase 1: Main Mode yang dimana Lebih aman, melalui 6 langkah pertukaran pesan dan Aggressive Mode yang lebih cepat, hanya 3 langkah, tetapi keamanan lebih rendah.
   - IKE Phase 2 – Pembuatan IPSec SA Fase ini digunakan untuk membentuk Security Association (SA) untuk enkripsi data. Langkah-langkah utamanya Negosiasi protokol IPSec (ESP atau AH), Menentukan parameter seperti SPI, lifetime, PFS, dll, Menentukan traffic selector, seperti subnet mana yang akan dienkripsi, Rekey otomatis saat lifetime habis.
   - Parameter Keamanan yang Harus Disepakati adalah
     - Algoritma Enkripsi, Contoh: AES-256, 3DES. AES lebih cepat dan aman.
     - Algoritma Hashing, Contoh: SHA-256, SHA-1. SHA-256 lebih kuat.
     - Metode Otentikasi Menggunakan PSK atau sertifikat digital.
     - Group DH (modp) Gunakan minimal Group 14 (2048-bit).
     - Lifetime Key pada Phase 1: 3600 detik, Phase 2: 1800 detik.

- konfigurasi

```
    /ip ipsec peer
add address=198.51.100.1/32 exchange-mode=main secret="vpn12345" enc-
    algorithm=aes-256 hash-algorithm=sha256 dh-group=modp2048

/ip ipsec proposal
add name="vpnProposal" auth-algorithms=sha256 enc-algorithms=aes-256-cbc
    lifetime=1h pfs-group=modp2048

/ip ipsec policy
add src-address=192.168.1.0/24 dst-address=192.168.2.0/24 sa-dst-address
    =198.51.100.1 sa-src-address=203.0.113.1 tunnel=yes proposal=vpnProposal

/ip ipsec identity
add peer=198.51.100.1 secret="vpn12345"
```

2. Sebuah sekolah memiliki bandwidth internet 100 Mbps yang dibagi menjadi:

   - 40 Mbps untuk e-learning
   - 30 Mbps untuk guru dan staf (akses email, cloud storage)
   - 20 Mbps untuk siswa (browsing umum)
   - 10 Mbps untuk CCTV dan update sistem

   Jawaban:

   - E-learning: 40 Mbps (40)
   - Guru Staf: 30 Mbps (30)
   - Siswa: 20 Mbps (20)
   - CCTV Update Sistem: 10 Mbps (10)

3. Buatlah skema Queue Tree yang lengkap:

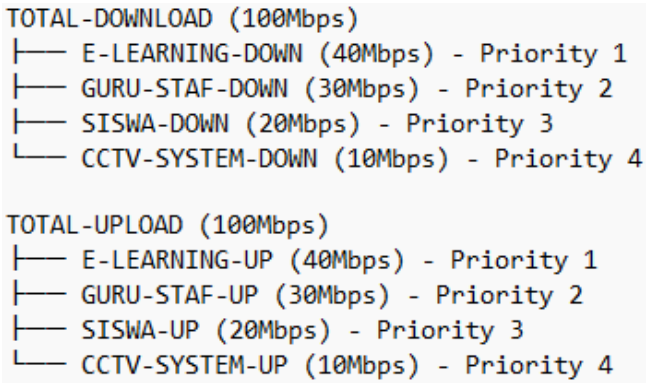
   - Parent dan child queue
   - Penjelasan marking
   - Prioritas dan limit rate pada masing-masing queue

   Jawaban

   - Parent dan child queue
   - Penjelasan marking

```
            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=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 passthrough=yes


```



Gambar 1: Caption

- Prioritas dan limit rate pada masing-masing queue

  Jawaban: learning(prioritas 1 40 Mbps), guru dan staf(prioritas 2 30 Mbps), siswa Prioritas 3 20 Mbps), cctv dan update (Prioritas 4 10 Mbps)

2.1 referensi

- MikroTik Wiki: Queue Tree
- MikroTik MUM: Bandwidth Control Design Wiki: IPSec Site-to-Site
- MikroTik Documentation: IPSec Configuration
- NIST SP 800-77 Rev.1 – Guide to IPsec VPNs item StrongSwan Wiki: IKEv2 Cipher Suites