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

Laporan Sementara
Praktikum Jaringan Komputer

VPN dan QoS

Muhammad Jaysyurrahman - 5024231057

2025

1 Pendahuluan

1.1 Latar Belakang

VPN (Virtual Private Network) IPSec adalah salah satu solusi keamanan yang digunakan untuk melindungi komunikasi data di jaringan yang terbuka, seperti internet. Dalam konteks perusahaan atau organisasi yang memiliki lebih dari satu lokasi, pengaturan VPN IPSec Site-to-Site menjadi sangat penting untuk menjaga kerahasiaan, integritas, dan autentikasi data antar kantor pusat dan cabang. Melalui penerapan teknologi tunneling dan enkripsi yang disediakan oleh IPSec, koneksi antar kantor dapat dilakukan secara aman, sehingga data yang dipertukarkan tidak mudah diakses oleh pihak yang tidak berwenang. Praktikum ini bertujuan untuk memberikan pemahaman mengenai konfigurasi IPSec yang tepat, serta mengelola manajemen bandwidth menggunakan Queue Tree, sehingga dapat memenuhi kebutuhan jaringan dengan lebih efisien dan aman.

1.2 Dasar Teori

IPSec adalah protokol yang digunakan untuk memberikan keamanan tingkat tinggi pada komunikasi data di jaringan IP, baik untuk komunikasi antar perangkat lokal maupun melalui internet. Protokol ini menyediakan tiga fitur utama: enkripsi, autentikasi, dan integritas data. Enkripsi digunakan untuk menyamarkan isi paket data agar tidak dapat dibaca oleh pihak yang tidak berwenang, sementara autentikasi memastikan bahwa data yang diterima berasal dari sumber yang sah. Integritas memastikan bahwa data yang dikirimkan tidak berubah atau rusak selama proses transmisi. IPSec bekerja dalam dua mode, yaitu Transport Mode dan Tunnel Mode. Pada Transport Mode, hanya isi data yang dienkripsi, sementara pada Tunnel Mode, seluruh paket, termasuk header IP, akan dienkripsi. Tunnel Mode sering digunakan untuk implementasi VPN site-to-site, di mana komunikasi antar kantor atau cabang perusahaan dilindungi dengan enkripsi end-to-end

Internet Key Exchange (IKE) adalah protokol yang digunakan dalam fase negosiasi IPSec untuk pertukaran kunci dan pengaturan keamanan. IKE memastikan bahwa kedua perangkat yang berkomunikasi memiliki kunci yang sesuai dan aman untuk melanjutkan komunikasi. IKE terbagi menjadi dua fase: Phase 1 dan Phase 2. Pada Phase 1, kedua perangkat melakukan autentikasi satu sama lain dan menciptakan kanal komunikasi aman menggunakan algoritma Diffie-Hellman untuk pertukaran kunci. Fase ini membentuk dasar dari komunikasi yang aman. Setelah itu, Phase 2 digunakan untuk negosiasi lebih lanjut mengenai parameter komunikasi, seperti pemilihan algoritma enkripsi dan autentikasi untuk data yang akan ditransmisikan. Fase ini menggunakan ESP (Encapsulation Security Payload) untuk enkripsi dan autentikasi data. Proses pertukaran kunci yang dilakukan oleh IKE memastikan bahwa koneksi tetap aman sepanjang waktu koneksi IPSec berlangsung

Queue Tree adalah fitur pada perangkat MikroTik yang memungkinkan pengelolaan bandwidth secara lebih kompleks dan terstruktur. Dengan Queue Tree, bandwidth dapat dibagi menjadi beberapa level prioritas, dengan struktur parent-child. Parent queue berfungsi untuk mengelola alokasi bandwidth total, sementara child queue membagi bandwidth tersebut ke dalam kategori-kategori trafik tertentu. Setiap jenis trafik seperti e-learning, akses staf, atau CCTV dapat diberi prioritas dan alokasi bandwidth yang berbeda. Dalam konteks pengaturan jaringan sekolah, misalnya, e-learning dapat diberikan prioritas tertinggi dengan alokasi bandwidth yang lebih besar, sedangkan trafik untuk browsing dapat diberikan prioritas rendah. Hal ini penting agar aplikasi yang membutuhkan koneksi stabil, seperti video conference atau aplikasi pembelajaran daring, tidak terganggu oleh trafik yang

kurang penting.

Marking trafik adalah langkah pertama dalam mengelola lalu lintas data di jaringan. Dengan menggunakan fitur Mangle di MikroTik, administrator jaringan dapat memberikan label pada paket data berdasarkan berbagai kriteria, seperti IP, port, atau protokol. Setelah trafik diberi label (marking), lalu lintas data tersebut dapat diprioritaskan atau dibatasi kecepatannya menggunakan Queue Tree. Misalnya, trafik untuk e-learning dapat diberi label khusus dan dikelompokkan dalam child queue dengan prioritas lebih tinggi, sehingga mendapatkan jaminan alokasi bandwidth yang cukup. Teknik ini memungkinkan pembagian bandwidth yang lebih adil dan efisien, serta memastikan aplikasi yang membutuhkan sumber daya besar, seperti video conferencing atau VPN, mendapatkan akses yang lebih baik tanpa terganggu oleh aplikasi lain yang tidak terlalu penting, seperti streaming video atau browsing.

IPSec menawarkan fleksibilitas dalam berbagai implementasi jaringan, baik itu untuk koneksi site-to-site, remote access, atau VPN berbasis IP. Kelebihan dari IPSec adalah kemampuannya untuk bekerja pada skala yang besar, seperti menghubungkan beberapa cabang perusahaan secara aman, ataupun pada jaringan kecil, seperti menghubungkan perangkat individu dengan jaringan kantor. Meskipun demikian, IPSec membutuhkan konfigurasi yang teliti dan pemahaman yang baik mengenai cara kerjanya, karena kesalahan dalam pengaturan dapat menyebabkan kebocoran data atau kegagalan dalam koneksi. Dalam implementasinya, IPSec juga sering digunakan dalam menghubungkan berbagai perangkat yang berbeda merek, selama mereka mendukung standar yang sama, menjadikannya solusi yang sangat fleksibel dan kompatibel untuk berbagai jenis perangkat dan platform.

2 Tugas Pendahuluan

1. VPN IPSec Site-to-Site

   a. Fase Negosiasi IPSec (IKE Phase 1 dan Phase 2) IKE Phase 1:

   Tujuan: Membentuk kanal aman untuk pertukaran kunci.

   Proses: Dua perangkat menggunakan Diffie-Hellman untuk menghasilkan kunci bersama dan menyetujui parameter keamanan.

   Algoritma: AES untuk enkripsi, SHA untuk autentikasi.

   IKE Phase 2:

   Tujuan: Menentukan parameter komunikasi untuk data.

   Proses: Pertukaran kunci untuk enkripsi data.

   Algoritma: ESP (Encapsulation Security Payload) untuk enkripsi dan autentikasi.

   b. Parameter Keamanan Algoritma Enkripsi: AES, 3DES.

   Metode Autentikasi: SHA, pre-shared key (PSK) atau sertifikat digital (PKI).

   Lifetime Key: Phase 1 (8 jam), Phase 2 (1 jam).

   c. Konfigurasi Sederhana pada Router

IKE Phase 1:
crypto isakmp policy 10
encryption aes
authentication pre-share
group 2
lifetime 86400

IKE Phase 2 (ESP):
crypto ipsec transform-set TRANS1 esp-aes esp-sha-hmac

VPN Tunnel:
crypto map VPN-MAP 10 ipsec-isakmp
set peer <IP Target>
set transform-set TRANS1
match address 101

2. Skema Queue Tree
   a. Parent dan Child Queue Parent Queue: 100 Mbps

   Child Queue:
   e-learning: 40 Mbps
   guru dan staf: 30 Mbps
   siswa: 20 Mbps
   CCTV dan update sistem: 10 Mbps

   b. Penjelasan Marking
   Marking dilakukan berdasarkan kategori trafik (e-learning, siswa) dengan menggunakan mangle rules untuk membedakan trafik berdasarkan port atau IP.

   c. Prioritas dan Limit Rate
   e-learning: Prioritas tinggi, limit 40 Mbps.
   guru dan staf: Prioritas sedang, limit 30 Mbps.
   siswa: Prioritas rendah, limit 20 Mbps.
   CCTV: Prioritas sangat rendah, limit 10 Mbps.

   /queue tree
   add name="parent" parent=global packet-mark="" limit-at=100Mbps max-limit=100Mbps
   add name="e-learning" parent=parent packet-mark=e-learning limit-at=40Mbps max-limit=40Mbps priority=1
   add name="guru-staf" parent=parent packet-mark=guru-staf limit-at=30Mbps max-limit=30Mbps priority=2
   add name="siswa" parent=parent packet-mark=siswa limit-at=20Mbps max-limit=20Mbps prio-

rity=3
add name="CCTV" parent=parent packet-mark=cctv limit-at=10Mbps max-limit=10Mbps priority=4

Referensi:
- IPSec and VPN Configuration Guide by Cisco. https://www.cisco.com/c/en/us/td/docs/iosxr/
- MikroTik RouterOS Documentation by MikroTik. https://wiki.mikrotik.com/
- Networking Fundamentals by William Stallings.