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

Laporan Sementara
Praktikum Jaringan Komputer

Tunneling

Ignasius Deva - 5024231003

2025

1 Pendahuluan

1.1 Latar Belakang

Komunikasi antar perangkat dan jaringan merupakan komponen yang penting dalam teknologi informasi. Pertumbuhan penggunaan internet dan kebutuhan konektivitas yang aman, cepat, dan efisien sudah menjuadi kebutuhan primer dari semua oranng, dari personal, hingga worldwide. Permasalahan yang sering ditemui di dunia adalah bagaimana menghubungkan dua jaringan yang berbeda jenis secara efisien dan aman, serta mengolah lalu lintas data agar tetap optimal, apalagi dengan banyaknya perangkat yang terkoneksi pada koneksi yang sama. Pada praktikum ini kami dikenalkan kepada tunneling, bagaimana IPSec menjaga keamanan data, dan bagaiaman metode simple queue dan queue tree digunakan untuk manajemen bandwidth.

1.2 Dasar Teori

Tunneling adalah teknik komunikasi data yang memungkinkan suatu protokol dikirimkan melalui jaringan yang menggunakan protokol lain (beda tipe/jenis). Konsep yang digunakan untuk tunneling ini adalah encapsulation yaitu membungkus paket data dalam paket lain agar dapat melewati jaringan yang berbeda hingga sampai tujuannya. Beberapa jenis protokol tunneling : GRE (Generic Routing Encapsulation) dengan membungkus paket IP dengan header tambahan, IPSec dengan mengamankan data dengan enkripsi dan auth, L2TP (Layer 2 Tunneling Protocol) dan PPTP (Point to Point Tunneling Protocol) yang umumnya digunakan dalam VPN, SSL Tunneling dengan menggunakan secure socket layer untuk mengenkripsi data melalui proxy, SSH (Secure Shell) untuk akses jarak jauh yang aman, dan VXLAN (Virtual Extensible LAN) untuk digunakan dalam viertualisasi jaringan di cloud dan data center.

IPSec adalah protokol keamanan jaringan yang bekerja pada layer IP untuk mengamankan komunikasi antar perangkat dengan tahap auth, enksipsi, dan validasi data. IPSec memiliki dua mode operasi yaitu : Tunneling mode dengan membungkus seluruh paket IP untuk komunikasi antar jaringan, dan Transport Mode dengan menagamankan hanya bagian payload dari paket IP. Beberapa protokol lain yaitu ESP (Encapsulation Security Payload) dengan menyediakan enksipsi dan euthentikasi, AH (Authentication Header) dengan memberikan auth dan integritas data, dan IKE (Internet Key Exchange) yang bertanggung jawab atas pertukaran kunci enksipsi secara aman.

Managemen bandwidth merupakan proses mengatur dan mengoptimalisasikan traffic jaringan. Ada dua metode umum yang digunakan pada router adalah : Simple queue yang berarti peraturan bandwidth yang mudahj dan langsung berdasarkan IP atau interface teretentu (cocok untuk jaringan kecil dan penggunaan sederhana), dan Queue tree yang pengaturan bandwidth yang lebih kompleks dan fleksible dengan struktur parent-child, serta membutuhkan mangel untuk menandai traffic (cocok untuk ISP dan skala besar).

Prioritas Traffic bandwidth sangat penting untuk memastikan layanan tetap berjalan meskipun

jaringan sedang overload. Hal ini bisa diatur dengan metode seperti Qos (Quality Of Service), Simple Queue, atau Queue tree.

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**

   -. Fase Negosiasi IPSec Phase 1 dan Phase 2 :

   - Phase 1
     Phase 1 adalah fase membentuk kanal komunikasi yang aman antara dua device. Ada dua mode utama yaitu : Main Mode (lebih aman dalam menyembunyikan identitas dam cocok untuk koneksi antar kantor), Agressive Mode (Lebih cepat tapi kurang aman). Beberapa parameter yang dinegosiasikan adalah Algoritma enkripsi (AES, 3DES), Algoritma Hash (SHA-256, MD5), Metode Auth (Pre-Shared Key), Lifetime (8 jam), dan Group DH untuk pertukaran kunci.
   - Phase 2 (Quick Mode)
     Fase ini bertugas untuk membuat IPSec SA yang digunakan untuk mengamankan data aktual. Negotiation meliputi : Algoritma enkripsi dan hash, mode kerja (tunnel/transport), Lifetime key phase 2, dan selector traffic.

   Parameter Keamanan yang disepakati

   - Enkripsi = AES-256
   - Auth = SHA-256
   - Metode Pertukaran = Diffie-Hellman Group 14
   - Lifetime Key = Phase 1: 86400 detik, Phase 2: 3600 detik
   - Mode = Tunnel
   - Authentication Method = Pre-Shared Key (PSK)

   Contoh Konfigurasi IPSec Site-to-Site di Mikrotik :
   /ip ipsec peer
   add address=192.168.2.1/32 exchange-mode=main secret=12345678

   /ip ipsec policy
   add src-address=192.168.1.0/24 dst-address=192.168.2.0/24 sa-dst-address=192.168.2.1 sa-src-address=192.168.1.1 tunnel=yes

   /ip ipsec proposal

set default auth-algorithms=sha256 enc-algorithms=aes-256-cbc lifetime=1h

Pada router kantor cabang :
/ip ipsec peer
add address=192.168.1.1/32 exchange-mode=main secret=12345678

/ip ipsec policy
add src-address=192.168.2.0/24 dst-address=192.168.1.0/24 sa-dst-address=192.168.1.1 sa-src-address=192.168.2.1 tunnel=yes

/ip ipsec proposal
set default auth-algorithms=sha256 enc-algorithms=aes-256-cbc lifetime=1h

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**

-. Parent dan Child Queue :
Parent Queue = parent-upload
Fungsi: Mengelola total bandwidth keluar (100 Mbps) dari interface

Child Queue -. Penjelasan Marking (dengan Mangle)

Queue Name	Parent	Packet Mark	Max Limit	Priority
queue-elearning	parent-upload	elearning	40 Mbps	1
queue-guru	parent-upload	guru	30 Mbps	2
queue-siswa	parent-upload	siswa	20 Mbps	4
queue-cctv	parent-upload	cctv	10 Mbps	3

Tabel 1: Konfigurasi Child Queues pada Queue Tree

/ip firewall mangle
add chain=forward 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 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

-. Konfigurasi Queue Tree
/queue tree
add name=parent-upload parent=global-out max-limit=100M

add name=queue-elearning parent=parent-upload packet-mark=elearning max-limit=40M priority=1
add name=queue-guru parent=parent-upload packet-mark=guru max-limit=30M priority=2
add name=queue-siswa parent=parent-upload packet-mark=siswa max-limit=20M priority=4
add name=queue-cctv parent=parent-upload packet-mark=cctv max-limit=10M priority=3

Referensi :

MikroTik Wiki. (2021). Queue Tree Setup Examples. Retrieved from https://wiki.mikrotik.com/wiki/Manual:Queues_Queue_Tree

Juniper Networks. (2022). Understanding IKE Phase 1 and Phase 2 in IPSec VPNs. Retrieved from https://www.juniper.net

RFC 2401 – Security Architecture for the Internet Protocol. Internet Engineering Task Force (IETF). Retrieved from https://tools.ietf.org/html/rfc2401