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

Laporan Sementara
Praktikum Jaringan Komputer

Tunneling dan IP security

Bintang Arya Mahendra - 5024231058

2025

1 Pendahuluan

1.1 Latar Belakang

Seiring dengan perkembangan teknologi informasi dan komunikasi, kebutuhan akan konektivitas jaringan yang aman dan efisien semakin meningkat. Tunneling sebagai salah satu teknologi fundamental dalam jaringan komputer memungkinkan pengiriman data melintasi berbagai jenis jaringan yang berbeda dengan cara membungkus data dalam format yang kompatibel dengan jaringan perantara. Konsep ini mirip dengan memasukkan satu paket ke dalam paket lainnya, sehingga data dapat dikirim melalui jalur yang tidak langsung kompatibel dengan format aslinya.

Virtual Private Network (VPN) merupakan implementasi praktis dari teknologi tunneling yang memberikan koneksi aman melalui internet publik. IPSec sebagai salah satu protokol VPN yang paling robust, menyediakan otentikasi, enkripsi, dan integritas data melalui mekanisme yang kompleks namun reliable. Selain aspek keamanan, manajemen bandwidth melalui Quality of Service (QoS) juga menjadi komponen penting dalam memastikan performa jaringan yang optimal.

1.2 Dasar Teori

Tunneling adalah teknik enkapsulasi yang memungkinkan protokol jaringan untuk mentransmisikan data melalui jaringan yang menggunakan protokol berbeda. Proses ini melibatkan pembungkusan (encapsulation) paket data asli ke dalam header protokol yang sesuai dengan jaringan pembawa, kemudian dilakukan dekapsulasi di titik akhir untuk mengembalikan data ke format aslinya. Beberapa protokol tunneling yang umum digunakan meliputi GRE (Generic Routing Encapsulation), IP-in-IP, L2TP (Layer 2 Tunneling Protocol), dan IPSec.

IPSec (Internet Protocol Security) merupakan suite protokol yang menyediakan keamanan pada layer network dari model OSI. Protokol ini mengimplementasikan tiga komponen utama: otentikasi untuk memverifikasi identitas pengirim, enkripsi untuk melindungi kerahasiaan data, dan integritas untuk memastikan data tidak dimodifikasi selama transmisi. IPSec beroperasi dalam dua mode: Transport Mode yang hanya mengenkripsi payload, dan Tunnel Mode yang mengenkripsi seluruh paket IP termasuk header aslinya.

Quality of Service (QoS) dalam konteks manajemen bandwidth merujuk pada kemampuan jaringan untuk memberikan prioritas berbeda kepada aplikasi, user, atau aliran data tertentu. Implementasi QoS dalam MikroTik dapat dilakukan melalui Simple Queue untuk pengaturan sederhana per IP/user, atau Queue Tree untuk konfigurasi yang lebih kompleks dengan struktur hierarkis parent-child yang memungkinkan pembagian bandwidth berdasarkan berbagai kriteria.

2 Tugas Pendahuluan

2.1 Soal 1: Konfigurasi VPN IPSec

Diberikan studi kasus untuk konfigurasi VPN IPSec. Suatu perusahaan ingin membuat koneksi aman antara kantor pusat dan cabang. Jelaskan secara detail:

2.1.1 Fase Negosiasi IPSec (IKE Phase 1 dan Phase 2)

IKE Phase 1 (Main Mode)

Phase 1 bertujuan untuk membangun secure tunnel ISAKMP SA (Security Association) antara dua gateway VPN. Tahapan yang dilakukan meliputi:

1. Inisiasi koneksi dan proposal algoritma keamanan
2. Otentikasi menggunakan pre-shared key atau digital certificate
3. Diffie-Hellman key exchange untuk menghasilkan master key
4. Pembentukan encrypted tunnel untuk fase selanjutnya

IKE Phase 2 (Quick Mode)

Phase 2 membangun IPSec SA untuk enkripsi data aktual dengan langkah:

1. Negosiasi parameter enkripsi untuk data traffic
2. Penentuan protokol IPSec (ESP atau AH)
3. Konfigurasi Perfect Forward Secrecy (PFS)
4. Penetapan lifetime untuk session key

2.1.2 Parameter Keamanan yang Harus Disepakati

Parameter keamanan yang perlu disepakati kedua endpoint:

- **Encryption Algorithm**: AES-256, AES-128, atau 3DES
- **Hash Algorithm**: SHA-256, SHA-1, atau MD5
- **Authentication Method**: Pre-Shared Key atau Digital Certificate
- **Diffie-Hellman Group**: Group 14 (2048-bit) atau Group 5 (1536-bit)
- **SA Lifetime**: Durasi session (umumnya 3600 detik)
- **Mode Operation**: Tunnel Mode untuk site-to-site VPN

2.1.3 Konfigurasi Router untuk IPSec Site-to-Site

Asumsi topologi:

- Kantor Pusat: LAN 10.10.1.0/24, Gateway 203.0.113.1
- Kantor Cabang: LAN 10.10.2.0/24, Gateway 203.0.113.2

Konfigurasi MikroTik (Kantor Pusat):

```
# IPSec Proposal
/ip ipsec proposal add name="site-proposal" \
    auth-algorithms=sha256 enc-algorithms=aes-256-cbc \
    pfs-group=modp2048

# IPSec Peer
/ip ipsec peer add address=203.0.113.2 \
    exchange-mode=main secret="sharedkey123"

# IPSec Identity
/ip ipsec identity add peer=203.0.113.2 \
    secret="sharedkey123"

# IPSec Policy
/ip ipsec policy add src-address=10.10.1.0/24 \
    dst-address=10.10.2.0/24 \
    sa-src-address=203.0.113.1 \
    sa-dst-address=203.0.113.2 \
    tunnel=yes proposal=site-proposal
```

2.2 Soal 2: Skema Queue Tree untuk Sekolah

Sebuah sekolah memiliki bandwidth internet 100 Mbps dengan pembagian:

- 40 Mbps untuk e-learning
- 30 Mbps untuk guru & staf
- 20 Mbps untuk siswa
- 10 Mbps untuk CCTV & sistem

2.2.1 Parent dan Child Queue

Struktur Queue Tree:

```
Parent Queue: "Total-Bandwidth"
 Max Limit: 100 Mbps
 Interface: ether1-gateway
```

```
Child Queues:
    e-learning-queue (40 Mbps, Priority 1)
    guru-staf-queue (30 Mbps, Priority 2)
    siswa-queue (20 Mbps, Priority 3)
    cctv-sistem-queue (10 Mbps, Priority 4)
```

2.2.2 Penjelasan Marking

Traffic marking dilakukan melalui Mangle rules berdasarkan:

- **Source IP**: Range IP untuk setiap kategori user
- **Destination**: Server/layanan spesifik (e-learning platform)
- **Port**: Port aplikasi tertentu (CCTV port, email port)

Contoh marking:

```
# Mark e-learning traffic
/ip firewall mangle add chain=prerouting \
    src-address=192.168.10.0/24 \
    action=mark-packet new-packet-mark=e-learning

# Mark guru-staf traffic
/ip firewall mangle add chain=prerouting \
    src-address=192.168.20.0/24 \
    action=mark-packet new-packet-mark=guru-staf
```

2.2.3 Prioritas dan Limit Rate

Kategori	Limit Rate	Max Limit	Prioritas
E-learning	30 Mbps	40 Mbps	1
Guru & Staf	20 Mbps	30 Mbps	2
Siswa	15 Mbps	20 Mbps	3
CCTV & Sistem	8 Mbps	10 Mbps	4

Tabel 1: Alokasi Bandwidth dan Prioritas

Stallings, W. (2017). *Network Security Essentials: Applications and Standards*. 6th Edition. Pearson. Doraswamy, N., & Harkins, D. (2003). *IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*. 2nd Edition. Prentice Hall. MikroTik Wiki. (2024). *Manual:Queue*. Retrieved from https://wiki.mikrotik.com/wiki/Manual:Queue Cisco Systems. (2023). *IPSec VPN Configuration Guide*. Retrieved from https://www.cisco.com/c/en/us/support/docs/security-vpn/ Ferguson, P., & Huston, G. (2012). *Quality of Service: Delivering QoS on the Internet and in Corporate Networks*. John Wiley & Sons.