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

Laporan Sementara
Praktikum Jaringan Komputer

Tunneling dengan IPsec

Athariq Qurani Fajri - 5024231031

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital saat ini, kebutuhan akan komunikasi data yang aman dan efisien menjadi sangat penting, terutama bagi organisasi atau institusi yang memiliki banyak cabang atau unit terdistribusi. Salah satu solusi untuk menjaga kerahasiaan dan integritas data saat melintasi jaringan publik adalah dengan menggunakan teknologi Virtual Private Network (VPN), khususnya protokol IPSec. Dengan memanfaatkan IPSec tunneling, dua lokasi dapat dihubungkan secara aman melalui internet, seolah-olah mereka berada dalam satu jaringan lokal. Praktikum ini memberikan pemahaman praktis mengenai bagaimana konfigurasi dan negosiasi IPSec dilakukan serta bagaimana jaringan dapat diamankan dalam skenario nyata.

Selain aspek keamanan, manajemen lalu lintas jaringan juga menjadi komponen penting dalam menjaga kualitas layanan (Quality of Service). Dalam sebuah lingkungan jaringan yang memiliki beragam jenis trafik—seperti e-learning, video streaming, browsing, hingga CCTV—dibutuhkan metode untuk membagi dan memprioritaskan bandwidth sesuai kebutuhan. Melalui praktikum ini, mahasiswa mempelajari perbedaan implementasi Simple Queue dan Queue Tree, serta bagaimana konfigurasi dan penandaan trafik (packet marking) dilakukan untuk mengelola sumber daya jaringan secara optimal.

1.2 Dasar Teori

IPSec (Internet Protocol Security) adalah seperangkat protokol yang dirancang untuk mengamankan komunikasi IP melalui otentikasi dan enkripsi. IPSec bekerja dalam dua fase negosiasi: IKE Phase 1 dan IKE Phase 2. Pada fase pertama, dibentuk jalur komunikasi yang aman antara dua perangkat melalui pertukaran kunci dan autentikasi. Fase kedua melanjutkan dengan membentuk Security Association (SA) untuk mengenkripsi lalu lintas data. IPSec mendukung dua mode utama, yaitu transport mode dan tunnel mode, di mana tunnel mode umum digunakan untuk menghubungkan dua jaringan berbeda melalui internet secara aman.

Dalam konteks manajemen bandwidth, Simple Queue dan Queue Tree adalah dua metode berbeda yang digunakan pada perangkat MikroTik. Simple Queue lebih mudah dikonfigurasi dan cocok untuk pembatasan bandwidth individu, namun tidak ideal untuk pengaturan prioritas trafik yang kompleks. Queue Tree memungkinkan pengelompokan dan pembagian bandwidth berdasarkan kategori trafik dengan prioritas berbeda, serta membutuhkan marking pada paket melalui fitur Mangle. Dengan pendekatan ini, administrator jaringan dapat menjamin bandwidth minimum untuk layanan penting dan menurunkan prioritas untuk layanan yang kurang krusial, sehingga kualitas layanan tetap terjaga.

Tugas Pendahuluan

1. Studi Kasus VPN IPSec

Fase Negosiasi IPSec (IKE Phase 1 dan Phase 2)

IPSec bekerja dalam dua fase utama menggunakan protokol IKE (Internet Key Exchange):

- **IKE Phase 1:** Digunakan untuk membangun jalur komunikasi aman antar dua perangkat (peer) dan membentuk ISAKMP SA. Tahapan ini menggunakan Main Mode atau Aggressive Mode untuk negosiasi parameter awal seperti algoritma enkripsi dan metode autentikasi. Setelah berhasil, terbentuk secure channel untuk Phase 2.
- **IKE Phase 2:** Dilakukan dalam Quick Mode. Tujuannya adalah untuk membentuk IPSec SA yang akan digunakan untuk mengenkripsi lalu lintas data antar site. Pada tahap ini, parameter seperti enkripsi dan hash untuk data, serta protokol tunneling seperti ESP dinegosiasikan.

Parameter Keamanan yang Disepakati

Beberapa parameter keamanan yang umum disepakati antara kedua endpoint:

- **Algoritma Enkripsi:** AES-256, AES-128, atau 3DES.
- **Metode Autentikasi:** Pre-shared key (PSK) atau sertifikat digital (X.509).
- **Algoritma Hashing:** SHA-256, SHA-1.
- **Diffie-Hellman Group:** Group 14 atau yang lebih tinggi untuk keamanan yang lebih kuat.
- **Lifetime Key:** Umumnya 3600 detik untuk Phase 1, dan 28800 detik untuk Phase 2.

Contoh Konfigurasi Router (MikroTik)

Berikut contoh konfigurasi site-to-site IPSec menggunakan MikroTik RouterOS:

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

/ip ipsec peer
add address=203.0.113.2/32 exchange-mode=main secret="sharedkey123" dh-group=modp2048 \
    enc-algorithm=aes-256 hash-algorithm=sha256

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

Referensi:

- https://www.cbtnuggets.com/blog/technology/networking/how-ipsec-site-to-site-vpn-tunnels-w
- https://docs.opnsense.org/manual/how-tos/ipsec-s2s.html

2. Pembagian Bandwidth Sekolah

Sebuah sekolah memiliki koneksi internet sebesar 100 Mbps yang dibagi sebagai berikut:

- 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

3. Skema Queue Tree Lengkap

Parent dan Child Queue

Skema Queue Tree dengan pembagian 100 Mbps:

```
/queue tree
add name="total-bandwidth" parent=global limit-at=100M max-limit=100M

add name="e-learning" parent=total-bandwidth packet-mark=elearning limit-at=40M max-limit=40M pr
add name="guru-staf" parent=total-bandwidth packet-mark=guru limit-at=30M max-limit=30M priority
add name="siswa" parent=total-bandwidth packet-mark=siswa limit-at=20M max-limit=20M priority=3
add name="cctv" parent=total-bandwidth packet-mark=cctv limit-at=10M max-limit=10M priority=4
```

Penjelasan Marking

Marking dilakukan melalui fitur Mangle:

```
/ip firewall mangle
add chain=forward src-address=192.168.10.0/24 action=mark-packet new-packet-mark=elearning passt
add chain=forward src-address=192.168.20.0/24 action=mark-packet new-packet-mark=guru
add chain=forward src-address=192.168.30.0/24 action=mark-packet new-packet-mark=siswa
add chain=forward src-address=192.168.40.0/24 action=mark-packet new-packet-mark=cctv
```

Prioritas dan Limit Rate

- Prioritas 1 (tertinggi) diberikan pada e-learning.
- Guru dan staf mendapatkan prioritas 2.
- Siswa diberikan prioritas 3.
- CCTV dan sistem update mendapatkan prioritas terendah (4).
- `limit-at` menjamin bandwidth minimum.
- `max-limit` menetapkan batas maksimum yang dapat digunakan.

Referensi:

- MikroTik Queue Tree Documentation: `https://help.mikrotik.com/docs/spaces/ROS/pages/328088/Queues`
- `https://superuser.com/questions/1722877/bandwidth-control-with-queue-in-mikrotik`