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

Laporan Sementara
Praktikum Jaringan Komputer

Tunneling & IPSec

Muhammad Navis Azka Atqiya - 5024231035

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital yang semakin berkembang, kebutuhan akan koneksi jaringan yang aman dan efisien menjadi sangat penting, terutama bagi organisasi atau perusahaan yang memiliki banyak cabang. Salah satu solusi yang umum digunakan adalah implementasi VPN (Virtual Private Network) berbasis IPSec, yang memungkinkan pertukaran data secara aman melalui jaringan publik seperti internet. IPSec menawarkan proteksi data melalui proses enkripsi dan autentikasi, memastikan informasi penting tidak mudah diakses atau dimanipulasi oleh pihak tak berwenang. Untuk membangun koneksi VPN yang efektif, proses negosiasi keamanan (IKE Phase 1 dan 2), pemilihan algoritma enkripsi, serta konfigurasi perangkat jaringan seperti router harus dilakukan dengan cermat.

Di sisi lain, manajemen bandwidth juga menjadi aspek krusial untuk menjaga performa jaringan, terutama di lingkungan dengan banyak pengguna dan layanan, seperti di sekolah. Tanpa pengaturan yang tepat, layanan penting seperti e-learning atau CCTV dapat terganggu oleh trafik yang kurang prioritas. Dengan memanfaatkan fitur Queue Tree pada MikroTik, administrator dapat membagi bandwidth secara adil dan memberikan prioritas berdasarkan kebutuhan, seperti mendahulukan akses untuk guru dan e-learning dibandingkan trafik siswa atau pembaruan sistem. Oleh karena itu, pemahaman mengenai konfigurasi IPSec dan manajemen bandwidth sangat penting dalam membangun jaringan yang aman, stabil, dan efisien.

1.2 Dasar Teori

Tunneling adalah teknik dalam jaringan komputer yang memungkinkan data dari satu jaringan dikirim ke jaringan lain melalui "terowongan virtual". Data yang dikirim melalui tunneling akan dienkapsulasi ke dalam protokol lain agar bisa melewati jalur komunikasi yang berbeda, seperti dari jaringan lokal ke internet. Proses ini memungkinkan dua titik jaringan yang berjauhan untuk berkomunikasi seolah-olah berada dalam satu jaringan yang sama. Contoh penggunaan tunneling adalah pada VPN (Virtual Private Network), yang memberikan koneksi aman dan terenkripsi melalui jaringan publik.

Salah satu protokol tunneling yang paling umum digunakan untuk keamanan adalah IPSec (Internet Protocol Security). IPSec menyediakan autentikasi, integritas, dan enkripsi data pada level jaringan. IPSec beroperasi dalam dua mode: transport mode yang hanya mengenkripsi isi paket data, dan tunnel mode yang mengenkripsi seluruh paket IP. Protokol ini sering digunakan dalam skenario VPN site-to-site untuk menghubungkan kantor pusat dan cabang dengan aman melalui internet. Proses pertukaran kunci dan parameter keamanan dalam IPSec dilakukan melalui protokol IKE (Internet Key Exchange), yang terdiri dari dua fase negosiasi.

Untuk mendukung manajemen bandwidth di jaringan yang padat, MikroTik menyediakan fitur Queue Tree, yang memungkinkan pembagian dan pengaturan prioritas lalu lintas jaringan berdasarkan jenis layanan atau pengguna. Queue Tree bekerja dengan sistem parent-child dan memerlukan penandaan (marking) paket menggunakan fitur mangle. Fitur ini sangat berguna dalam mengalokasikan bandwidth secara proporsional, seperti pembagian bandwidth di sekolah antara e-learning, akses guru dan staf, siswa, serta layanan CCTV. Dengan konfigurasi yang tepat, administrator jaringan dapat memastikan layanan prioritas tetap berjalan lancar meskipun terjadi kepadatan trafik.

2 Tugas Pendahuluan

2.1 Konfigurasi VPN IPSec Site-to-Site

Fase Negosiasi IPSec

1. **IKE Phase 1**: Membangun kanal aman antara dua perangkat. Dua mode negosiasi:
   - **Main Mode**: Lebih aman (6 pesan).
   - **Aggressive Mode**: Lebih cepat (3 pesan).

   Hasilnya adalah pembentukan **IKE Security Association (SA)**.
2. **IKE Phase 2 (Quick Mode)**: Menyepakati parameter pertukaran data (ESP/AH, PFS, proxy ID). Menghasilkan **IPSec SA** untuk transfer data.

Parameter Keamanan Umum

- **Enkripsi**: AES-256 atau 3DES
- **Autentikasi**: SHA-256
- **Diffie-Hellman Group**: Group 14 (2048-bit)
- **Key Lifetime**: 86400 detik (24 jam)
- **Tipe Autentikasi**: Pre-shared key (PSK)
- **PFS**: Disarankan untuk keamanan tambahan

Contoh Konfigurasi Router Cisco

Listing 1: Konfigurasi IPSec Site-to-Site

```
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
 group 14
 lifetime 86400

crypto isakmp key mysecretkey address 192.168.2.1

crypto ipsec transform-set TS esp-aes 256 esp-sha-hmac
 mode tunnel

crypto map VPN-MAP 10 ipsec-isakmp
 set peer 192.168.2.1
 set transform-set TS
 match address VPN-TRAFFIC

access-list VPN-TRAFFIC permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

interface GigabitEthernet0/0
```

```
21 ip address 192.168.1.1 255.255.255.0
22 crypto map VPN-MAP
```

Referensi

1. *Guide to IPsec VPNs*, https://csrc.nist.gov/publications/detail/sp/800-77/rev-1/final
2. *Site-To-Site VPN using IPSEC Tunnelx*, https://robertalvianus.wordpress.com/2014/05/09/site-to-site-vpn-using-ipsec-tunnel/

2.2 Manajemen Bandwidth dengan Queue Tree (MikroTik)

Kebutuhan Bandwidth

- E-learning: 40 Mbps
- Guru dan staf: 30 Mbps
- Siswa: 20 Mbps
- CCTV dan sistem: 10 Mbps

Struktur Queue Tree

Parent: `Total-BW` (interface: `ether1`, max-limit: 100M)

- **E-Learning** – limit-at: 40M, priority: 1
- **Guru-Staf** – limit-at: 30M, priority: 2
- **Siswa** – limit-at: 20M, priority: 3
- **CCTV-System** – limit-at: 10M, priority: 4

Penandaan Paket (Mangle Rules)

Listing 2: MikroTik Mangle Rule

```
1 /ip firewall mangle
2 add chain=forward protocol=tcp dst-port=443,80 src-address=192.168.10.0/24 action=
    mark-packet new-packet-mark=e-learning
3 add chain=forward src-address=192.168.20.0/24 action=mark-packet new-packet-mark=guru
4 add chain=forward src-address=192.168.30.0/24 action=mark-packet new-packet-mark=
    siswa
5 add chain=forward src-address=192.168.40.0/24 action=mark-packet new-packet-mark=cctv
```

Konfigurasi Queue Tree

Listing 3: Queue Tree Configuration

```
/queue tree
add name="Total-BW" parent=ether1 max-limit=100M
add name="E-Learning" parent=Total-BW packet-mark=e-learning limit-at=40M max-limit
    =40M priority=1
add name="Guru-Staf" parent=Total-BW packet-mark=guru limit-at=30M max-limit=30M
    priority=2
add name="Siswa" parent=Total-BW packet-mark=siswa limit-at=20M max-limit=20M
    priority=3
add name="CCTV-System" parent=Total-BW packet-mark=cctv limit-at=10M max-limit=10M
    priority=4
```

Ringkasan Prioritas

Queue	Limit-at	Max-limit	Priority
E-Learning	40 Mbps	40 Mbps	1
Guru-Staf	30 Mbps	30 Mbps	2
Siswa	20 Mbps	20 Mbps	3
CCTV-System	10 Mbps	10 Mbps	4

Referensi

1. Citraweb, *Manajemen Bandwidth Menggunakan Simple Queue*, https://citraweb.com/artikel_lihat.php?id=53
2. Mikrotik Manual, *Manual:IP/Firewall/Mangle*, https://wiki.mikrotik.com/Manual:IP/Firewall/Mangle
3. Mikrotik Documentation, *Queues - Queue Tree*, https://help.mikrotik.com/docs/spaces/ROS/pages/328088/Queues