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

Laporan Sementara
Praktikum Jaringan Komputer

VPN & QoS

Devlin Jeychovhinn Saputra - 5024231019

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam zaman modern ini yang semakin mengandalkan konektivitas jarak jauh, kebutuhan akan akses jaringan yang aman dan efisien menjadi sangat penting. Salah satu tantangan utama dalam jaringan modern adalah menyediakan koneksi yang terenkripsi bagi pengguna yang bekerja secara remote tanpa mengorbankan performa jaringan lokal. Virtual Private Network (VPN) menjadi solusi yang banyak digunakan untuk menjawab kebutuhan tersebut, khususnya protokol Point to Point Tunneling Protocol (PPTP) yang masih populer karena kemudahannya dalam implementasi. Di sisi lain, pengelolaan lalu lintas jaringan lokal seperti pengaturan kecepatan internet dan pengalihan paket data juga menjadi aspek penting. Penggunaan Proxy ARP memungkinkan bridging antar segmen jaringan berbeda tanpa konfigurasi tambahan pada perangkat klien, sedangkan Quality of Service (QoS) melalui Simple Queue berfungsi untuk mengatur bandwidth agar pengguna mendapatkan layanan yang adil dan sesuai dengan kebutuhan. Modul ini membahas konfigurasi PPTP VPN, aktivasi Proxy ARP, serta manajemen QoS pada perangkat MikroTik, sebagai bentuk integrasi antara keamanan akses jarak jauh dan efisiensi pengelolaan lalu lintas jaringan lokal.

1.2 Dasar Teori

PPTP (Point to Point Tunneling Protocol) adalah salah satu protokol VPN yang digunakan untuk membuat koneksi terenkripsi antara klien dan server melalui jaringan publik, seperti internet. PPTP bekerja dengan membuat saluran (tunnel) dan mengenkripsi data yang dikirimkan melalui tunnel tersebut. Meskipun protokol ini tergolong lama dan memiliki kelemahan dalam aspek keamanan dibandingkan protokol modern seperti L2TP atau OpenVPN, PPTP tetap banyak digunakan karena dukungan luas dari sistem operasi dan kemudahan konfigurasi.
Proxy ARP adalah metode di mana sebuah router menjawab permintaan ARP untuk alamat IP yang bukan miliknya, dengan mengirimkan alamat MAC-nya sendiri. Dengan fitur ini, perangkat yang berada di jaringan berbeda dapat berkomunikasi seolah-olah berada dalam jaringan yang sama. Proxy ARP sangat berguna dalam implementasi bridging dan VPN, karena menghilangkan kebutuhan pengaturan gateway tambahan di sisi klien.
QoS (Quality of Service) merupakan mekanisme untuk mengelola lalu lintas jaringan dengan cara mengatur prioritas, bandwidth, dan penanganan paket berdasarkan jenis layanan atau pengguna. Salah satu metode sederhana dalam QoS adalah *Simple Queue* yang tersedia di MikroTik, yang memungkinkan admin jaringan untuk membatasi kecepatan upload dan download berdasarkan IP address atau network tertentu. Dengan pengaturan ini, trafik dapat dibagi secara adil dan mencegah pengguna tertentu menghabiskan seluruh bandwidth yang tersedia.

2 Tugas Pendahuluan

1. **D**iberikan 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)

  - IKE Phase 1: Tahap ini digunakan untuk membangun secure tunnel antara dua peer. Tujuannya adalah untuk membentuk IKE SA (Security Association) menggunakan metode autentikasi dan pertukaran kunci. Fase ini memiliki dua mode yang adalah Main mode lebih aman karena menyembunyikan identitas dan Aggressive Mode lebih cepat, namun kurang aman.
  - IKE Phase 2: Setelah secure channel terbentuk, fase ini bertujuan untuk membentuk IPSec SA yang digunakan untuk pertukaran data, biasanya menggunakan Quick Mode.
- Parameter keamanan yang harus disepakati (algoritma enkripsi, metode autentikasi, lifetime key)

  Agar koneksi VPN aman, parameter berikut harus disepakati oleh kedua belah pihak:
  - Algoritma Enkripsi: AES-256, 3DES, atau ChaCha20.
  - Metode Autentikasi: Pre-shared Key (PSK), RSA digital signature, atau X.509 certificate.
  - Integrity Algorithm: SHA-256 atau SHA-1.
  - Diffie-Hellman Group: Misal Group 14 (2048-bit).
  - Lifetime Key: Biasanya 3600 detik (1 jam) untuk Phase 1, dan 1800 detik untuk Phase 2.
- Konfigurasi sederhana pada sisi router untuk memulai koneksi IPSec site-to-site

Listing 1: Konfigurasi IPSec Router Cisco

```
! Phase 1 - ISAKMP Policy
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
 group 14
 lifetime 3600

crypto isakmp key MYSECRETKEY address 192.168.2.1

! Phase 2 - IPSec Transform Set
crypto ipsec transform-set MYSET esp-aes 256 esp-sha-hmac

! Crypto Map
crypto map VPNMAP 10 ipsec-isakmp
 set peer 192.168.2.1
 set transform-set MYSET
 match address 110

! Access List untuk traffic yang dienkripsi
access-list 110 permit ip 10.0.0.0 0.0.0.255 10.1.0.0 0.0.0.255

interface GigabitEthernet0/1
 crypto map VPNMAP
```

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
- Parent dan child queue

Listing 2: Konfigurasi IPSec Router Cisco

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

add name="e-learning" parent=total-bandwidth packet-mark=e-learning-mark \
    limit-at=40M max-limit=40M priority=1 queue=default

add name="guru-staf" parent=total-bandwidth packet-mark=guru-staf-mark \
    limit-at=30M max-limit=30M priority=2 queue=default

add name="siswa" parent=total-bandwidth packet-mark=siswa-mark \
    limit-at=20M max-limit=20M priority=3 queue=default

add name="cctv-update" parent=total-bandwidth packet-mark=cctv-update-mark \
    limit-at=10M max-limit=10M priority=4 queue=default
```

3. Penjelasan marking

   Dilakukan dengan firewall mangle:

Listing 3: Konfigurasi IPSec Router Cisco

```
/ip firewall mangle
add chain=forward protocol=tcp dst-port=443 src-address=192.168.1.0/24 \
    action=mark-packet new-packet-mark=e-learning-mark passthrough=yes

add chain=forward src-address=192.168.2.0/24 \
    action=mark-packet new-packet-mark=guru-staf-mark passthrough=yes

add chain=forward src-address=192.168.3.0/24 \
    action=mark-packet new-packet-mark=siswa-mark passthrough=yes

add chain=forward src-address=192.168.4.0/24 \
    action=mark-packet new-packet-mark=cctv-update-mark passthrough=yes
```

4. Prioritas dan limit rate pada masing-masing queue
   - E-Learning = priority pertama
   - Guru & Staf = priority kedua
   - Siswa = priority ketiga
   - CCTV/Update = priority keempat

- Limit Rate: Ditentukan dengan limit-at (minimum bandwidth yang dijamin) dan max-limit (maksimum yang bisa digunakan jika tersedia).

Referensi:

- Cisco. (2020). *IPSec VPN Configuration Guide*. https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14149-ike-debug-14149.html
- MikroTik. (2021). *IPSec Manual*. https://help.mikrotik.com/docs/display/ROS/IPsec
- MikroTik. (2023). *Queue Trees*. https://help.mikrotik.com/docs/display/ROS/Queue+Tree
- MikroTik Academy Training Manual. (2022). *Traffic Control with Queues*.