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

Laporan Sementara Praktikum Jaringan Komputer

VPN dan QoS

Nur Rahman Fauzan - 5024231069

Kamis, 5 Juni 2025

1 Dasar Teori

1.1 VPN (Virtual Private Network)

1.1 Konsep Tunneling Tunneling adalah teknik mengemas satu paket data ke dalam paket lain agar dapat melintasi jaringan yang berbeda jenis atau menembus firewall/firewallsesuai kebijakan. Proses inti tunneling meliputi:

1. **Encapsulation:** Paket IP asli (payload) dibungkus di dalam paket baru dengan header protokol tunneling (misalnya GRE atau IPSec).
2. **Transmisi:** Paket tunneling melintasi internet publik atau WAN, melindungi data asli dari inspeksi langsung.
3. **Decapsulation:** Di ujung terowongan (tunnel endpoint), paket baru dibuka, sehingga paket IP asli bisa diteruskan ke jaringan internal tanpa perubahan.

Contoh ilustrasi:

- Komputer A (di kantor cabang) $\rightarrow$ kirim paket ke Router M1.
- Router M1 = encapsulation ke IPSec (mode tunnel), datanya terenkripsi $\rightarrow$ kirim ke Router M2 lewat internet.
- Router M2 = decapsulation, paket asli kembali utuh $\rightarrow$ kirim ke Komputer B (kantor pusat).

1.2 JenisJenis Protokol Tunneling Beberapa protokol tunneling yang sering digunakan dalam VPN, antara lain:

- **GRE (Generic Routing Encapsulation)**: Membungkus paket IP (atau nonIP) dengan header GRE. Router kedua harus mendukung GRE untuk membuka bungkusan.
- **IPSec (Internet Protocol Security)**: Menyediakan keamanan (enkripsi + autentikasi) bagi paket IP. Biasanya digunakan dalam mode *tunnel* untuk VPN *sitetosite* atau mode *transport* untuk komunikasi hosttohost.
- **PPTP (PointtoPoint Tunneling Protocol)**: Protokol VPN lawas yang banyak digunakan di Windows. Saat ini relatif kurang aman dibanding IPSec.
- **SSTP (Secure Socket Tunneling Protocol)**: Memanfaatkan SSL/TLS (port 443) untuk membuat terowongan VPN. Umumnya hanya tersedia pada platform Windows/Router yang mendukung SSTP.
- **L2TP (Layer 2 Tunneling Protocol)**: Digabung dengan IPSec untuk keamanan ganda (L2TP + IPSec). L2TP hanya menangani tunneling; IPSec menangani enkripsi.

- **SSH Tunnel**: Mem-forward port TCP tertentu melalui saluran SSH yang sudah terenkripsi. Sering dipakai untuk akses jarak jauh ke server.
- **VXLAN (Virtual Extensible LAN)**: Bukan VPN tradisional, tetapi membuat *overlay network* di atas infrastruktur Layer 3 (misalnya data center). Packet Ethernet dibungkus di atas UDP/Multicast.

1.3 IPSec (IP Security) IPSec adalah kumpulan protokol yang berjalan pada layer 3 untuk mengamankan trafik IP. Fitur utamanya meliputi enkripsi, autentikasi, dan integritas data. Komponen IPSec yang penting:

- **IKE (Internet Key Exchange)**: Proses negosiasi parameter keamanan dan pertukaran kunci (phase 1 dan phase 2).
- **ESP (Encapsulating Security Payload)**: Menyediakan enkripsi payload dan dukungan autentikasi untuk integritas.
- **AH (Authentication Header)**: Hanya menyediakan autentikasi dan integritas (HMAC) tanpa enkripsi isi paket.
- **Mode Tunnel vs Transport:**
  - *Tunnel Mode:* Seluruh paket IP (header + payload) dibungkus dalam paket IP baru. Umum dipakai untuk koneksi *sitetosite*.
  - *Transport Mode:* Hanya payload yang dienkripsi/diautentikasi, header IP asli tetap terbuka. Cocok untuk komunikasi hosttohost.

1.4 Cara Kerja IPSec (Singkat)

1. Kedua pihak (mis. dua router atau host) melakukan negosiasi IKE phase 1 untuk membuat ISAKMP SA (Security Association), tukarmenukar kunci DiffieHellman, dan menyepakati algoritma enkripsi (AES, 3DES), autentikasi (SHA256), serta metode pertukaran kunci.
2. Setelah phase 1 sukses, dibentuk IPSec SA (phase 2) untuk mengamankan data: memilih ESP atau AH, mengonfigurasi lifetimes, dan menentukan parameter enkripsi/autentikasi.
3. Saat data dikirim:
   - Jika *Tunnel Mode*: Paket IP asli terenkripsi/diautentikasi, dibungkus ke dalam header IP baru, lalu dikirim ke endpoint VPN.
   - Jika *Transport Mode*: Payload paket IP terenkripsi/diautentikasi, tetapi header IP asli tetap utuh.

4. Di sisi penerima, paket didecaps (ESP/AH didekoding), kemudian paket IP asli diteruskan ke aplikasi tujuan.

5. Setelah masa SA berakhir, IKE phase 2 dapat berjalan ulang (rekeying) untuk memperbarui kunci.

1.2 QoS (Quality of Service)

2.1 Konsep Dasar QoS Quality of Service (QoS) adalah mekanisme untuk mengatur, memprioritaskan, dan menjamin kualitas layanan tertentu pada jaringan yang padat. Tanpa QoS, saat trafik banyak, paket data berebut bandwidth sehingga layanan sensitif seperti VoIP atau video conferencing bisa terputus atau mengalami jitter tinggi. QoS memastikan bahwa trafik kritikal mendapat jalur istimewa agar latency dan jitter tetap rendah.

2.2 Simple Queue vs Queue Tree (MikroTik)

- **Simple Queue:**
  - Cara termudah untuk membatasi kecepatan (upload/download) per IP, per user, atau per interface.
  - Konfigurasi hanya menentukan target (IP/host/interface) dan batas (limitat, maxlimit).
  - Struktur satu tingkat: satu Simple Queue = satu IP atau satu interface.
  - Kekurangan: Kurang fleksibel untuk lalu lintas kompleks karena tidak dapat mengelompokkan trafik berdasarkan kategori (port, protokol, VLAN).
- **Queue Tree:**
  - Lebih fleksibel dan kompleks. Memerlukan *mangle* untuk menandai paket/koneksi (mark packet atau mark connection).
  - Membentuk struktur parentchild, sehingga bisa membagi total bandwidth ke beberapa *child queue* sesuai kategori trafik.
  - Sangat cocok untuk ISP kecil atau jaringan besar yang perlu membagi bandwidth ke beberapa layanan (video streaming, game, HTTP, dsb.).
  - Kekurangan: Konfigurasi lebih rumit, harus memahami cara melakukan marking paket dan menempatkan queue pada parent yang tepat.

Fitur	Simple Queue	Queue Tree
Tingkat Kesulitan	Mudah (GUI/Winbox)	MenengahSulit (butuh *mangle*/mark)
Memerlukan Mangle/Mark?	Tidak	Ya
Struktur	Satu tingkat (per IP/interface)	Bertingkat (parentchild)
Cocok untuk	Jaringan kecil, batas per IP	Jaringan besar, trafik kompleks
Keuntungan	Cepat disetup, langsung jalan	Sangat fleksibel, granularitas tinggi
Kekurangan	Terbatas untuk satu IP/interface saja	Konfigurasi rumit, butuh logika pemetaan trafik

2.4 Prioritas Trafik

- **Mengapa Dibutuhkan?** Saat link sedang penuh, paket data yang kurang penting (mis. download besar, streaming nonkritikal) harus ditunda sementara agar paket penting (VoIP, video conference, VPN kantor) bisa lewat lebih dulu.
- **Kategori Umum Prioritas:**
  - **Tinggi:** VPN perusahaan, VoIP, Video Conference, Remote Desktop.
  - **Sedang:** Browsing (HTTP/HTTPS), Email, Akses Aplikasi Bisnis.
  - **Rendah:** Download file besar, streaming video nonkritikal (YouTube, Netflix).
  - **Sangat Rendah:** Peertopeer (Torrent), update OS otomatis, sinkronisasi backup.
- **Langkah Implementasi di MikroTik:**
  1. Tandai paket/koneksi (mark packet/mark connection) berdasarkan port, protokol, atau IP tujuan menggunakan menu */ip firewall mangle*.
  2. Buat *Queue Tree* untuk struktur parentchild:
     - Parent Queue: menampung total bandwidth (misalnya 20 Mbps).
     - Child Queue: alokasikan porsi (misalnya 5 Mbps untuk VoIP, 10 Mbps untuk HTTP, 5 Mbps untuk download besar).
  3. Atur `priority` (1=tertinggi 8=terendah) dan `limitat` maupun `maxlimit` untuk tiap child queue.
  4. Uji coba dengan menjalankan aplikasi realtime (VoIP/video conference) sambil trafik lain padat, lalu cek apakah prioritas berjalan sesuai konfigurasi.

2 Tugas Pendahuluan

Berikut jawaban untuk tugas pendahuluan Modul 5 (VPN dan QoS) dalam format LaTeX. Setiap jawaban menyertakan referensi yang relevan.

1. **Studi Kasus Konfigurasi VPN IPSec Site-to-Site** Sebuah perusahaan ingin membuat koneksi aman antara kantor pusat (Subnet A: `10.1.202.0/24`) dan kantor cabang (Subnet B: `10.1.101.0/24`). Jelaskan:

   a. **Fase Negosiasi IPSec (IKE Phase 1 dan Phase 2)**

   IKE Phase 1:

   - Tujuan: Mendirikan kanal IKE SA (ISAKMP SA) untuk melindungi negosiasi selanjutnya.
   - Mode:
     - *Main Mode*: 6 paket, identitas peer tersembunyi.
     - *Aggressive Mode*: 3 paket, lebih cepat tapi identitas peer terekspos.
   - Pertukaran:
     i. Negosiasi algoritma enkripsi, hash, DH group, dan metode autentikasi.
     ii. Pertukaran kunci Diffie-Hellman (DH) untuk membuat kunci bersama.
     iii. Autentikasi peer (misal: pre-shared key).
   - Hasil: Terbentuknya IKE SA yang mengenkripsi semua pesan IKE selanjutnya.

   IKE Phase 2:

   - Tujuan: Mendirikan IPSec SA untuk mengenkripsi *data plane*.
   - Proses:
     i. Negosiasi parameter IPSec (protokol ESP/AH, algoritma enkripsi + integritas, PFS).
     ii. Pertukaran kunci baru (jika PFS diaktifkan, dilakukan DH tambahan).
   - Hasil: Pasangan IPSec SA (satu untuk setiap arah) siap mengenkripsi dan mengecek integritas paket data antar subnet.

   Referensi:

   - D. Harkins, D. Carrel, The Internet Key Exchange (IKE), RFC 2409, IETF, Nov 1998. **rfc2409**

   b. **Parameter Keamanan yang Harus Disepakati** Berikut parameter utama yang harus identik di kedua router (pusat dan cabang):

   - **Algoritma Enkripsi:** AES-128 atau AES-256.
   - **Algoritma Hash/Integritas:** SHA-256 (SHA-1 jika perangkat lama, namun tidak direkomendasikan).

- **Metode Autentikasi:** Pre-Shared Key (PSK) atau sertifikat digital (PKI). Pada contoh ini digunakan PSK.
- **Grup Diffie-Hellman:** modp2048 (Group 14) untuk keamanan kunci awal (PFS).
- **Lifetime (Masa Berlaku Kunci):**
  - IKE SA (Phase 1): 86400 detik (24 jam).
  - IPSec SA (Phase 2): 3600 detik (1 jam).

Referensi:

- Cisco Systems, *Configuring and Verifying IPsec Site-to-Site VPNs on Cisco Routers*, Cisco IOS XE 17.x Release Configuration Guide, 2020. **cisco-ios-ipsec-guide**

c. **Konfigurasi Sederhana pada Router MikroTik dan Cisco**

a. MikroTik (RouterOS):

i. Phase 1 Profile & Phase 2 Proposal:

Listing 1: MicroTik: Phase 1 Profile dan Phase 2 Proposal

```
1 /ip ipsec profile add name=ike1-site2 dh-group=modp2048 enc-
    algorithm=aes-128
2 /ip ipsec proposal add name=ike1-site2 enc-algorithms=aes-128-
    cbc pfs-group=modp2048
3
```

ii. Peer dan PSK:

Listing 2: MicroTik: Peer dan PSK

```
1 /ip ipsec peer add name=ike1-site2 address=<IP_Public_Cabang>
    profile=ike1-site2
2 /ip ipsec identity add peer=ike1-site2 secret=mySharedSecret123
3
```

Gantilah `<IP_Public_Cabang>` dengan IP publik router kantor cabang.

iii. IPSec Policy:

Listing 3: MicroTik: IPSec Policy

```
1 /ip ipsec policy add src-address=10.1.202.0/24 dst-address
    =10.1.101.0/24 \
2     peer=ike1-site2 proposal=ike1-site2 tunnel=yes action=
    encrypt
3
```

Buat policy di kedua sisi dengan subnet dibalik untuk meng-enkripsi trafik antar subnet.

Referensi:

- MikroTik, IPSec Configuration Examples, MikroTik Wiki, 2025. **mikrotik-ipsec-wiki**

b. Cisco IOS:

i. ISAKMP Policy (Phase 1):

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

ii. Pre-Shared Key:

```
crypto isakmp key mySharedSecret123 address 192.0.2.2
```

Gantilah `192.0.2.2` dengan IP publik router kantor cabang.

iii. Transform Set (Phase 2):

```
crypto ipsec transform-set mySET esp-aes esp-sha256-hmac
```

iv. Access List (Interesting Traffic):

```
access-list 100 permit ip 10.1.1.0 0.0.0.255 172.16.2.0 0.0.0.255
```

v. Crypto Map dan Penerapan pada Interface:

```
crypto map myMAP 10 ipsec-isakmp
 set peer 192.0.2.2
 set transform-set mySET
 match address 100

interface GigabitEthernet0/0
 description WAN Interface
 ip address 198.51.100.1 255.255.255.0
 crypto map myMAP
```

Referensi:

- Cisco Systems, *Configuring and Verifying IPsec Site-to-Site VPNs on Cisco Routers*, Cisco IOS XE 17.x Release Guide, 2020. **cisco-ios-ipsec-guide**

2. **Pembagian Bandwidth 100 Mbps di Sekolah (Queue Tree)** Sebuah sekolah memiliki koneksi internet 100 Mbps yang harus dibagi sebagai berikut:

   - 40 Mbps untuk **e-learning**
   - 30 Mbps untuk **guru & staf**
   - 20 Mbps untuk **siswa (browsing umum)**

- 10 Mbps untuk **CCTV & update sistem**

a. **Skema Penandaan Trafik (Mangle)** Kita asumsikan subnet:

   - `10.0.1.0/24` = e-learning
   - `10.0.2.0/24` = guru & staf
   - `10.0.3.0/24` = siswa browsing
   - `10.0.4.0/24` = CCTV & update

   Lakukan marking koneksi dan paket dengan baris berikut:

Listing 4: Mangle: Penandaan Trafik

```
/ip firewall mangle
  # E-learning
  add chain=forward src-address=10.0.1.0/24 action=mark-connection
     \
      new-connection-mark=conn_elearning passthrough=yes
  add chain=forward connection-mark=conn_elearning action=mark-
    packet \
      new-packet-mark=pkt_elearning passthrough=yes

  # Guru & Staf
  add chain=forward src-address=10.0.2.0/24 action=mark-connection
     \
      new-connection-mark=conn_guru passthrough=yes
  add chain=forward connection-mark=conn_guru action=mark-packet \
      new-packet-mark=pkt_guru passthrough=yes

  # Siswa Browsing
  add chain=forward src-address=10.0.3.0/24 action=mark-connection
     \
      new-connection-mark=conn_siswa passthrough=yes
  add chain=forward connection-mark=conn_siswa action=mark-packet
    \
      new-packet-mark=pkt_siswa passthrough=yes

  # CCTV & Update
  add chain=forward src-address=10.0.4.0/24 action=mark-connection
     \
      new-connection-mark=conn_cctv passthrough=yes
  add chain=forward connection-mark=conn_cctv action=mark-packet \
      new-packet-mark=pkt_cctv passthrough=yes
```

Referensi:

- MikroTik, Queue Tree Examples and Tutorials, MikroTik Wiki, 2025. **mikrotik-qos-wiki**

b. **Skema Queue Tree Lengkap** Buat satu parent queue (100 Mbps) dan empat child queue sesuai marking:

Listing 5: Queue Tree: Parent dan Child

```
# Parent queue: Total bandwidth 100 Mbps pada interface ether1
/queue tree add name="TotalBandwidth" parent=ether1 max-limit=100M

# Child queue: E-learning (40 Mbps, priority 1)
 /queue tree add name="Q_eLearning" parent=TotalBandwidth \
     packet-mark=pkt_elearning max-limit=40M priority=1

# Child queue: Guru & Staf (30 Mbps, priority 2)
 /queue tree add name="Q_GuruStaf" parent=TotalBandwidth \
     packet-mark=pkt_guru max-limit=30M priority=2

# Child queue: Siswa (20 Mbps, priority 3)
 /queue tree add name="Q_Siswa" parent=TotalBandwidth \
     packet-mark=pkt_siswa max-limit=20M priority=3

# Child queue: CCTV & Update (10 Mbps, priority 4)
 /queue tree add name="Q_CCTV_Update" parent=TotalBandwidth \
     packet-mark=pkt_cctv max-limit=10M priority=4
```

Penjelasan:

- **Parent Queue** Ditetapkan pada interface WAN (`ether1`) dengan `max-limit=100M` untuk mencerminkan total kapasitas link **mikrotik-qos-wiki**.
- **Child Queue** Tiap child queue memakai `packet-mark` sesuai kategori, `max-limit` sesuai alokasi bandwidth (40M, 30M, 20M, 10M), dan `priority` untuk menentukan urutan pemenuhan saat trafik bersaing.
- **Borrowing Mechanism** Jika suatu queue anak (misal CCTV) tidak menghabiskan jatah 10 Mbps-nya, sisa dapat dipinjam oleh queue lain hingga batas maksimum masing-masing **mikrotik-qos-wiki**.

c. **Prioritas dan Limit Rate pada Masing-masing Queue**

- **E-learning (Priority 1, max-limit = 40M)** Paling tinggi, memastikan platform pembelajaran online tetap responsif saat link padat.
- **Guru & Staf (Priority 2, max-limit = 30M)** Prioritas di bawah e-learning, namun tetap di atas siswa/public browsing.
- **Siswa Browsing (Priority 3, max-limit = 20M)** Didahulukan setelah e-learning dan guru/staf; jika ada sisa bandwidth dapat memperbesar alokasi hingga 20 Mbps maksimum.
- **CCTV & Update (Priority 4, max-limit = 10M)** Prioritas terendah; hanya mendapat akses jika queue yang lebih tinggi belum memanfaatkan jatahnya sepenuhnya.

Referensi:

- MikroTik, Queue Tree Examples and Tutorials, MikroTik Wiki, 2025. **mikrotik-qos-wiki**

Pustaka

[1] D. Harkins and D. Carrel, “The Internet Key Exchange (IKE),” RFC 2409, IETF, Nov 1998. https://tools.ietf.org/html/rfc2409

[2] Cisco Systems, *Configuring and Verifying IPsec Site-to-Site VPNs on Cisco Routers*, Cisco IOS XE 17.x Release Configuration Guide, 2020. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsec/configuration/xe-17/ipsec-xe-17-book.pdf

[3] MikroTik, “IPSec Configuration Examples,” MikroTik Wiki, 2025. https://wiki.mikrotik.com/wiki/IPsec

[4] MikroTik, “Queue Tree Examples and Tutorials,” MikroTik Wiki, 2025. https://wiki.mikrotik.com/wiki/Manual:Queue_tree