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

Laporan Sementara
Praktikum Jaringan Komputer

VPN & QoS

Muhammad Zia Alhambra - 5024231059

2025

1 Pendahuluan

1.1 Latar Belakang

Jaringan Pribadi Virtual (VPN) adalah teknologi yang memungkinkan komunikasi aman melalui jaringan publik dengan menciptakan terowongan terenkripsi antara perangkat. Teknologi ini banyak digunakan oleh organisasi untuk menghubungkan kantor cabang atau karyawan ke jaringan pusat secara aman, memastikan bahwa data sensitif tetap terlindungi dari akses yang tidak sah. VPN beroperasi menggunakan berbagai protokol seperti IPSec, SSL/TLS, dan L2TP, masing-masing menawarkan tingkat enkripsi dan otentikasi yang berbeda. Dalam konteks bisnis, VPN sangat penting untuk menjaga kerahasiaan dan integritas transmisi data, terutama saat mengakses sumber daya melalui internet atau menghubungkan beberapa lokasi dalam jaringan area luas (WAN).

Quality of Service (QoS), di sisi lain, merujuk pada sekelompok teknologi yang digunakan untuk mengelola lalu lintas jaringan dengan memprioritaskan jenis data tertentu. Hal ini memastikan bahwa layanan kritis seperti suara, video, dan aplikasi real-time mendapatkan bandwidth yang diperlukan dan latensi rendah untuk kinerja optimal. Mekanisme QoS dapat mengalokasikan bandwidth, mengurangi kehilangan paket, dan mengelola kemacetan, yang sangat penting dalam lingkungan di mana aplikasi dan pengguna yang berbeda berbagi koneksi internet yang sama. Misalnya, di lembaga pendidikan atau perusahaan, QoS dapat memprioritaskan platform e-learning atau aplikasi bisnis kritis di atas lalu lintas yang kurang penting, seperti unduhan file atau akses media sosial.

Bersama-sama, VPN dan QoS memainkan peran krusial dalam manajemen jaringan modern—VPN menyediakan konektivitas aman, sementara QoS memastikan kinerja jaringan yang efisien dan andal. Implementasi kedua teknologi ini memungkinkan organisasi untuk mendukung akses jarak jauh, melindungi data sensitif, dan mempertahankan pengiriman layanan berkualitas tinggi di lingkungan jaringan terdistribusi.

1.2 Dasar Teori

Konsep Jaringan Pribadi Virtual (VPN) secara teoritis berakar pada disiplin ilmu keamanan jaringan, kriptografi, dan komunikasi data yang aman. VPN dirancang untuk meniru keamanan dan privasi jaringan pribadi melalui infrastruktur publik seperti internet. Pada dasarnya, VPN menggunakan protokol tunneling seperti IPSec (Internet Protocol Security), SSL/TLS (Secure Sockets Layer/Transport Layer Security), dan L2TP (Layer 2 Tunneling Protocol) untuk mengenkapsulasi paket data, sehingga menyembunyikan isi dan asal-usulnya. Enkapsulasi ini biasanya disertai dengan algoritma enkripsi yang kuat seperti AES (Advanced Encryption Standard) atau 3DES (Triple Data Encryption Standard) untuk memastikan kerahasiaan, serta fungsi hashing seperti SHA (Secure Hash Algorithm) untuk memastikan integritas data. Metode autentikasi seperti kunci pra-bagi (PSK) atau sertifikat digital digunakan untuk memverifikasi identitas pihak yang berkomunikasi, melindungi dari akses tidak sah dan serangan man-in-the-middle. VPN sangat bergantung pada prinsip-prinsip CIA triad—Kerahasiaan, Integritas, dan Ketersediaan—sebagai landasan teoretis. Dalam hal lapisan jaringan, VPN umumnya beroperasi di lapisan jaringan (Layer 3) atau lapisan transportasi (Layer 4) model OSI, memungkinkan pengiriman paket yang aman melalui jaringan yang beragam dan potensial tidak tepercaya.

Di sisi lain, kerangka kerja Quality of Service (QoS) didasarkan pada teori prioritas lalu lintas jaringan, manajemen bandwidth, dan komunikasi yang sensitif terhadap penundaan. Dalam jaringan, tidak semua paket data memiliki tingkat penting yang sama; misalnya, paket suara atau video real-

time jauh lebih sensitif terhadap penundaan dan jitter daripada email atau unduhan file. QoS secara teoritis mengatasi hal ini dengan menggunakan klasifikasi dan penandaan lalu lintas untuk mengidentifikasi jenis-jenis lalu lintas jaringan yang berbeda, yang kemudian dikenakan tingkat layanan yang berbeda. Proses ini diimplementasikan melalui model seperti Integrated Services (IntServ), yang menggunakan sinyal eksplisit dan reservasi sumber daya untuk aliran individu, dan Differentiated Services (DiffServ), yang menerapkan penandaan lalu lintas (misalnya DSCP) dan perilaku per-hop tanpa memerlukan status per-aliran. Setelah lalu lintas diklasifikasikan, disiplin antrian seperti Priority Queuing, Weighted Fair Queuing (WFQ), dan Hierarchical Token Bucket (HTB) digunakan untuk menentukan urutan dan laju transmisi paket. Selain itu, mekanisme seperti pengendalian kemacetan, pembentukan lalu lintas, dan pembatasan laju diterapkan untuk memastikan sumber daya jaringan dialokasikan sesuai kebijakan dan permintaan.

Integrasi VPN dan QoS secara teoritis sangat penting dalam jaringan modern, terutama di lingkungan perusahaan dan institusi. Sementara VPN memastikan data tetap aman dan terlindungi dari penyadapan dan manipulasi, QoS memastikan data tersebut—terutama lalu lintas real-time dan kritis—dikirimkan secara efisien dengan penundaan, kehilangan, dan jitter minimal. Tanpa QoS, lalu lintas VPN yang terenkripsi mungkin mengalami kinerja buruk akibat kemacetan jaringan, sementara tanpa VPN, lalu lintas sensitif mungkin rentan terhadap penyadapan. Oleh karena itu, arsitektur jaringan yang secara teoritis kokoh menggabungkan VPN untuk jaminan keamanan dan QoS untuk jaminan kinerja, memastikan integritas dan kualitas layanan bagi pengguna di jaringan terdistribusi dan berbagi.

2 Tugas Pendahuluan

1. **Fase Negosiasi IPSec** IPSec menggunakan protokol IKE (Internet Key Exchange) dalam dua fase:

   IKE Phase 1 Tujuannya adalah membangun ISAKMP Security Association (SA), yaitu kanal aman pertama.

   - **Mode**: Main Mode (lebih aman) atau Aggressive Mode (lebih cepat, kurang aman)
   - **Proses**:
     (a) Tukar parameter keamanan (encryption, hash, DH group)
     (b) Otentikasi peer (pre-shared key, sertifikat)
     (c) Negosiasi algoritma dan membuat SA
   - **Output**: Terbentuk ISAKMP SA (Phase 1 SA) → lalu digunakan untuk melindungi Phase 2

   IKE Phase 2 Digunakan untuk membangun IPSec SA dan menyepakati parameter untuk lalu lintas data.

   - **Mode**: Quick Mode (lebih cepat, fokus pada data)
   - **Proses**:
     (a) Negosiasi protokol IPSec (ESP atau AH)
     (b) Negosiasi algoritma enkripsi dan autentikasi
     (c) Tukar keying material

(d) Membuat IPSec SA

- **Output**: Dua IPSec SA (untuk dua arah komunikasi)

Parameter Keamanan yang Harus Disepakati	
PARAMETER	KETERANGAN
Encryption Algorithm	AES-256, 3DES, AES-128
Authentication Method	Pre-Shared Key (PSK), RSA Certificates
Integrity Algorithm	SHA-256, SHA-1
DH Group	DH Group 14 (2048-bit), DH Group 5 (1536-bit)
Lifetime	Phase 1: 86400 detik (24 jam), Phase 2: 3600 detik (1 jam)

Contoh Konfigurasi Router

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

crypto isakmp key MYSECRETKEY address 203.0.113.2

crypto ipsec transform-set MYSET esp-aes 256 esp-sha-hmac

crypto map MYMAP 10 ipsec-isakmp
set peer 203.0.113.2
set transform-set MYSET
match address 101

access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

interface GigabitEthernet0/1
ip address 203.0.113.1 255.255.255.0
crypto map MYMAP

```

- 192.168.1.0/24: jaringan kantor pusat
- 192.168.2.0/24: jaringan cabang

Referensi

- Cisco Documentation: IPSec Configuration Guide
- RFC 7296 - Internet Key Exchange Protocol Version 2 (IKEv2)

2. **Skema Queue Tree**

Total bandwidth: 100 Mbps. Kita bagi menggunakan Queue Tree di MikroTik.

Parent Queue (Interface WAN):

- queue tree utama menggunakan max-limit=100M

```
/queue tree
add name="total-bandwidth" parent=ether1 max-limit=100M

```

Child Queues:

```
add name="e-learning" parent="total-bandwidth" limit-at=40M max-limit=40M priority=1 packet-mark=e-learning
add name="guru-staf" parent="total-bandwidth" limit-at=30M max-limit=30M priority=3 packet-mark=guru-staf
add name="siswa" parent="total-bandwidth" limit-at=20M max-limit=20M priority=5 packet-mark=siswa
add name="cctv-update" parent="total-bandwidth" limit-at=10M max-limit=10M priority=8 packet-mark=cctv-update

```

Penjelasan Marking (Firewall Mangle):

Digunakan untuk menandai lalu lintas sebelum diteruskan ke queue tree.

```
/ip firewall mangle
add chain=forward src-address=192.168.10.0/24 action=mark-packet new-packet-mark=e-learning passthrough=no
add chain=forward src-address=192.168.20.0/24 action=mark-packet new-packet-mark=guru-staf passthrough=no
add chain=forward src-address=192.168.30.0/24 action=mark-packet new-packet-mark=siswa passthrough=no
add chain=forward src-address=192.168.40.0/24 action=mark-packet new-packet-mark=cctv-update passthrough=no

```

Parameter Keamanan yang Harus Disepakati		
SUBNET	PENGGUNA	MARK
192.168.10.0/24	e-learning	e-learning
192.168.20.0/24	guru & staf	guru-staf
192.168.30.0/24	siswa	siswa
192.168.40.0/24	CCTV/update	cctv-update

Prioritas dan Limit Rate

- Priority (1 = tertinggi, 8 = terendah):
  - e-learning (1): akses penting
  - guru-staf (3): cukup penting
  - siswa (5): browsing umum
  - CCTV/update (8): boleh diundur saat sibuk
- Limit-at: bandwidth minimum terjamin
- Max-limit: batas maksimum

Referensi

- MikroTik Wiki - Queue Tree
- MikroTik Documentation - Mangle
- MikroTik Forum: Best Practice Bandwidth Management