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

Laporan Sementara
Praktikum Jaringan Komputer

Tunneling

Aminah Nur'aini Muchayati - 5024231034

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam dunia yang semakin terkoneksi secara digital, pertukaran data melalui jaringan komputer telah menjadi bagian penting dalam berbagai aktivitas manusia, mulai dari komunikasi pribadi hingga operasional bisnis dan pemerintahan. Namun, kemudahan akses jaringan tersebut juga membawa tantangan besar terkait keamanan dan kualitas layanan. Data yang dikirim melalui jaringan publik seperti internet sangat rentan terhadap berbagai ancaman, seperti penyadapan, manipulasi, hingga peretasan oleh pihak-pihak tidak bertanggung jawab. Untuk menjawab tantangan ini, teknologi Virtual Private Network (VPN) dikembangkan sebagai solusi untuk menciptakan koneksi yang aman dan terenkripsi antara pengguna dan jaringan tujuan. VPN memungkinkan pengguna untuk mengakses jaringan secara privat melalui jalur publik dengan membentuk terowongan virtual yang menjaga kerahasiaan dan integritas data. Meski demikian, penggunaan VPN tidak lepas dari isu teknis seperti peningkatan latensi, penurunan throughput, serta gangguan performa layanan tertentu, terutama aplikasi real-time seperti video conference, VoIP, dan layanan cloud. Di sinilah peran Quality of Service (QoS) menjadi sangat relevan, yaitu sebagai mekanisme manajemen trafik jaringan yang mampu menjamin performa layanan dengan cara mengatur prioritas, bandwidth, delay, jitter, dan packet loss. Dengan mengimplementasikan QoS bersamaan dengan VPN, diharapkan jaringan tidak hanya mampu memberikan perlindungan terhadap data pengguna, tetapi juga tetap mempertahankan kualitas layanan yang stabil, efisien, dan responsif terhadap kebutuhan pengguna. Oleh karena itu, topik mengenai integrasi antara VPN dan QoS menjadi sangat penting untuk dikaji lebih dalam dalam konteks jaringan komputer modern, terutama dalam mendesain sistem jaringan yang tidak hanya aman tetapi juga optimal dalam hal kinerja.

1.2 Dasar Teori

1. Tunneling Tunneling merupakan sebuah mekanisme fundamental dalam jaringan komputer yang memfasilitasi pengiriman paket data dari satu protokol atau bisa disebut protokol inner dengan membungkusnya di dalam paket data protokol lain(Kurose & Ross, 2017). Proses ini sering diibaratkan seperti memasukkan sebuah surat ke dalam amplop yang lebih besar agar dapat dikirimkan melalui layanan pos yang berbeda. Tujuan utama dari tunneling sangat beragam, meliputi peningkatan keamanan melalui enkripsi data, melewati pembatasan jaringan seperti firewall atau NAT dengan memungkinkan protokol yang diblokir untuk "menumpang" di dalam protokol yang diizinkan, serta menghubungkan jaringan heterogen yang menggunakan protokol berbeda. Mekanisme dasarnya melibatkan enkapsulasi, di mana paket data asli dibungkus dengan header protokol tunneling dan header protokol transport di titik awal terowongan, dan de-enkapsulasi di titik akhir, di mana header pembungkus dilepaskan untuk mendapatkan kembali paket data asli. Protokol tunneling populer yang relevan termasuk GRE (Generic Routing Encapsulation) yang fleksibel namun non-enkripsi dan sering dikombinasikan dengan IPsec untuk keamanan (Cisco Systems, 2005), serta berbagai protokol VPN (Virtual Private Network) seperti PPTP, L2TP/IPsec, OpenVPN, dan WireGuard, yang dirancang khusus untuk menciptakan koneksi aman dan terenkripsi melalui jaringan publik.

2. Queue
   Dalam dunia jaringan komputer, queue atau antrean berfungsi layaknya sebuah area tunggu vir-

tual yang penting untuk paket data (Tanenbaum & Wetherall, 2011). Saat perangkat jaringan, katakanlah sebuah router, menerima lonjakan paket data yang melebihi kapasitas pengirimannya, alih-alih membuang paket-paket tersebut, ia menempatkannya dalam antrean. Konsep antrean ini sangat vital dalam beberapa aspek manajemen jaringan. Pertama, ia esensial untuk manajemen lalu lintas (traffic management), membantu mengatur aliran data agar tidak terjadi congestion atau kemacetan, sehingga memastikan setiap paket tiba di tujuan dengan efisien. Kedua, antrean menjadi dasar implementasi Quality of Service (QoS), di mana administrator dapat memberikan jalur prioritas bagi jenis lalu lintas tertentu, memastikan data penting terkirim lebih cepat daripada yang kurang krusial. Ketiga, ia mendukung pembentukan lalu lintas (traffic shaping), memungkinkan kita untuk membatasi rate pengiriman data dari jenis lalu lintas tertentu, mencegah satu aplikasi atau pengguna memonopoli seluruh bandwidth yang tersedia. Namun, penting untuk diingat bahwa setiap antrean memiliki batas kapasitas. Jika antrean terisi penuh, paket data yang baru datang terpaksa akan drop atau dibuang, yang secara langsung berdampak pada packet loss dan penurunan kualitas koneksi yang kita rasakan.

3. Queue Tree
   Queue Tree adalah sebuah inovasi yang memperkaya konsep antrean, memungkinkan kita membangun struktur antrean yang lebih cerdas dan terhierarki, seperti sebuah pohon keluarga dalam manajemen bandwidth. Berbeda dengan antrean sederhana yang bekerja secara terpisah, Queue Tree memberikan fleksibilitas yang luar biasa dalam mengelola bandwidth, memungkinkan kita untuk mendefinisikan hubungan parent-child antar antrean. Konsep utamanya berpusat pada Parent Queue, yang bertindak sebagai "induk" yang memegang kendali atas total bandwidth yang akan didistribusikan kepada child queue. Bandwidth yang tidak terpakai oleh satu child queue dapat secara otomatis dibagikan kepada child queue lain yang membutuhkan, selama tidak melebihi batas maksimumnya. Child Queue mewarisi max-limit dari parent mereka, tetapi kita bisa memberikan batasan limit-at (jaminan minimum) dan max-limit (batas maksimum) yang lebih spesifik untuk setiap jenis traffic. Agar setiap child queue dapat mengenali traffic-nya, paket data perlu diberi tanda khusus terlebih dahulu menggunakan fitur Mangle.Selain itu, Priority menentukan urutan paket diproses saat terjadi congestion, di mana prioritas yang lebih rendah (misalnya angka 1) menunjukkan prioritas yang lebih tinggi. Dengan kapabilitas ini, Queue Tree memungkinkan administrator untuk membuat kebijakan manajemen bandwidth yang kompleks, seperti menjamin bandwidth minimum untuk e-learning, memberikan prioritas tinggi untuk guru dan staf, sambil secara efektif membatasi bandwidth untuk Browse siswa agar tidak mengganggu layanan yang lebih kritikal.

2 Tugas Pendahuluan

1. Diberikan studi kasus untuk konfigurasi VPN IPSec. Suatu perusahaan ingin membuat koneksi aman antara kantor pusat dan cabang. Jelaskan secara detail:
   a Fase negosiasi IPSec (IKE Phase 1 dan Phase 2)
   b Parameter keamanan yang harus disepakati (algoritma enkripsi, metode autentikasi, lifetime key)
   c Konfigurasi sederhana pada sisi router untuk memulai koneksi IPSec site-to-site

Jawab :

a Fase negosiasi IPSec (IKE Phase 1 dan Phase 2)

IKE Phase 1 (Internet Key Exchange)

- Tujuan: Membangun secure channel untuk pertukaran kunci menggunakan protokol ISAKMP.
- Hasil: Dibentuknya SA (Security Association) untuk management trafik (ISAKMP SA).
- Pertukaran informasi dilakukan melalui mode: Main Mode: Lebih aman, lebih lambat. Aggressive Mode: Lebih cepat, sedikit lebih terbuka.

IKE Phase 2

- Tujuan: Membangun SA untuk data (IPSec SA) untuk komunikasi yang terenkripsi.
- Hasil: Negotiation parameter untuk ESP/AH.
- Mode: Quick Mode (selalu 3 pesan)

b Parameter keamanan yang harus disepakati (algoritma enkripsi, metode autentikasi, lifetime key)

IKE Phase 1 Parameters:

- Algoritma Enkripsi: AES-256, 3DES, atau DES
- Hash Algorithm: SHA-256, SHA-1, atau MD5
- Metode Autentikasi: Pre-shared key, RSA signature, atau digital certificate
- Diffie-Hellman Group: Group 14 (2048-bit), Group 5 (1536-bit), atau Group 2 (1024-bit)
- Lifetime: 28800 detik (8 jam) sebagai default

IKE Phase 2 Parameters:

- Protokol Keamanan: ESP (Encapsulating Security Payload) atau AH (Authentication Header)
- Algoritma Enkripsi: AES-256, AES-128, 3DES
- Algoritma Autentikasi: SHA-256-HMAC, SHA-1-HMAC, MD5-HMAC
- PFS (Perfect Forward Secrecy): Ya/Tidak dengan DH group
- Lifetime: 3600 detik (1 jam) atau berdasarkan volume data

c Konfigurasi sederhana pada sisi router untuk memulai koneksi IPSec slite-to-site

```
        ! Phase 1: ISAKMP
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
 group 14
 lifetime 86400

crypto isakmp key mysecurekey address 192.168.2.1

! Phase 2: IPSec
crypto ipsec transform-set TS esp-aes 256 esp-sha-hmac
 mode tunnel
```

```
14
15 crypto map VPN-MAP 10 ipsec-isakmp
16  set peer 192.168.2.1
17  set transform-set TS
18  match address VPN-TRAFFIC
19
20 interface GigabitEthernet0/0
21  ip address 192.168.1.1 255.255.255.0
22  crypto map VPN-MAP
23
24 ! ACL untuk menentukan lalu lintas yang akan dienkripsi
25 access-list 100 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
26
```

referensi: https://www.cloudflare.com/learning/network-layer/what-is-ipsec/

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
     Buatlah skema Queue Tree yang lengkap:

   a Parent dan child queue

   b Penjelasan marking

   c Prioritas dan limit rate pada masing-masing queue

   Jawab :

   a Parent dan child queue
   Queue Tree menggunakan struktur parent-child, dengan ether1 sebagai parent (interface yang mengarah ke internet) dengan nama TOTAL-BANDWIDTH

Nama Queue	Parent	Packet Mark
ELEARNING	TOTAL-BANDWIDTH	elearning
GURU-STAF	TOTAL-BANDWIDTH	guru-staf
SISWA	TOTAL-BANDWIDTH	siswa
CCTV-UPDATE	TOTAL-BANDWIDTH	cctv-update

Tabel 1: Tabel Child Queue Pembagian Bandwidth Sekolah

b Penjelasan marking
Marking dilakukan agar router dapat mengidentifikasi lalu lintas dari masing-masing kelompok pengguna berdasarkan subnet IP.
IP Address :

- E-learning: 10.10.10.0/24
- Guru & Staf: 10.20.20.0/24

- Siswa: 10.30.30.0/24
- CCTV & Update: 10.40.40.0/24

Peinrtah Marking :

```
1         /ip firewall mangle
2 add chain=forward src-address=10.10.10.0/24 action=mark-packet new-packet-mark=
    elearning passthrough=no
3 add chain=forward src-address=10.20.20.0/24 action=mark-packet new-packet-mark=
    guru-staf passthrough=no
4 add chain=forward src-address=10.30.30.0/24 action=mark-packet new-packet-mark=
    siswa passthrough=no
5 add chain=forward src-address=10.40.40.0/24 action=mark-packet new-packet-mark=
    cctv-update passthrough=no
6
```

Penjelasan :

- chain=forward digunakan untuk menandai paket yang melewati router.
- src-address disesuaikan dengan IP masing-masing jaringan.
- new-packet-mark adalah label yang akan digunakan di Queue Tree.
- passthrough=yes artinya proses firewall akan tetap dilanjutkan.

c rioritas dan limit rate pada masing-masing queue

Nama Queue	Limit At	Max Limit	Priority
ELEARNING	40 Mbps	40 Mbps	1
GURU-STAF	30 Mbps	30 Mbps	2
SISWA	20 Mbps	20 Mbps	3
CCTV-UPDATE	10 Mbps	10 Mbps	4

Referensi: https://help.mikrotik.com/docs/spaces/ROS/pages/328088/Queues