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

Laporan Sementara
Praktikum Jaringan Komputer

VPN dan Qos

Aaron Smeraldo Olivier Manik - 5024231070

2025

1 Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi informasi yang pesat menuntut sistem jaringan komputer untuk memiliki tingkat keamanan dan performa yang tinggi. Dalam lingkungan yang terhubung secara global, kebutuhan untuk mengakses jaringan secara aman dari lokasi yang berbeda serta menjamin kualitas komunikasi data menjadi hal yang sangat penting. Oleh karena itu, dibutuhkan pemahaman dan keterampilan dalam mengelola aspek keamanan dan efisiensi jaringan.

Praktikum ini dirancang untuk memberikan pengalaman langsung dalam mengimplementasikan dua komponen penting dalam manajemen jaringan, yaitu Virtual Private Network (VPN) dan Quality of Service (QoS). Keduanya memainkan peran kunci dalam membangun jaringan yang dapat diandalkan, baik dari segi perlindungan data maupun pengaturan lalu lintas jaringan.

Melalui praktikum ini, mahasiswa diharapkan mampu memahami permasalahan nyata dalam pengelolaan jaringan serta mampu menerapkan solusi teknis untuk meningkatkan keamanan dan kualitas layanan jaringan. Hal ini penting sebagai bekal menghadapi tantangan di dunia kerja yang menuntut efisiensi dan keamanan dalam sistem jaringan modern.

1.2 Dasar Teori

1.3 Virtual Private Network (VPN)

Virtual Private Network (VPN) adalah teknologi jaringan yang memungkinkan terciptanya koneksi aman melalui jaringan publik seperti internet. VPN bekerja dengan membentuk *tunnel* atau jalur terenkripsi antara dua titik jaringan, sehingga data yang ditransmisikan tidak dapat diakses oleh pihak yang tidak berwenang. Teknologi ini banyak digunakan untuk menghubungkan jaringan antar lokasi secara aman dan juga untuk mengakses jaringan internal perusahaan dari jarak jauh.

Protokol umum yang digunakan dalam VPN antara lain:

- **PPTP (Point-to-Point Tunneling Protocol)**: Salah satu protokol VPN tertua yang mudah dikonfigurasi tetapi memiliki keamanan yang lebih rendah.
- **L2TP/IPSec (Layer 2 Tunneling Protocol)**: Menggabungkan kelebihan L2TP dan keamanan IPSec untuk koneksi yang lebih aman.
- **OpenVPN**: Protokol open-source yang fleksibel dan aman, mendukung enkripsi yang kuat dan berbagai platform.
- **IPSec (Internet Protocol Security)**: Protokol tingkat jaringan yang digunakan untuk mengamankan lalu lintas IP melalui enkripsi dan otentikasi.

1.4 Quality of Service (QoS)

Quality of Service (QoS) adalah sekumpulan teknik dan mekanisme dalam jaringan komputer yang digunakan untuk mengatur dan mengontrol lalu lintas data guna meningkatkan kualitas layanan. QoS bertujuan untuk memastikan bahwa aplikasi jaringan tertentu seperti *VoIP*, video streaming, dan layanan real-time lainnya mendapatkan prioritas dan sumber daya jaringan yang memadai.

Parameter-parameter penting dalam QoS meliputi:

- **Bandwidth**: Kapasitas maksimal jalur komunikasi yang tersedia untuk transmisi data.
- **Latency (Delay)**: Waktu yang dibutuhkan paket data untuk mencapai tujuan.
- **Jitter**: Variasi waktu kedatangan antar paket data yang dapat mengganggu komunikasi real-time.
- **Packet Loss**: Persentase paket data yang hilang selama transmisi.

Beberapa teknik yang digunakan dalam implementasi QoS antara lain:

- **Traffic Shaping**: Mengatur aliran lalu lintas jaringan agar sesuai dengan kapasitas.
- **Priority Queuing**: Memberikan prioritas tinggi untuk jenis lalu lintas tertentu.
- **Bandwidth Allocation**: Pembagian lebar pita untuk memastikan layanan penting tetap stabil.

2 Tugas Pendahuluan

1. Diberikan studi kasus untuk konfigurasi VPN IPSec. Suatu erusahaan ingin membuat koneksi aman antara kantor pusat dan cabang. Jelaskan secara detail:

   UNegosiasi IPSec dilakukan dalam dua tahap utama:

   - **IKE Phase 1:** Tahapan awal ini bertujuan membentuk koneksi yang aman antara dua perangkat melalui proses autentikasi dan pembuatan kanal terenkripsi, yang dikenal sebagai ISAKMP SA (Security Association). Parameter keamanan seperti algoritma enkripsi (misalnya AES), autentikasi (seperti SHA-256), dan metode pertukaran kunci (Diffie-Hellman) dinegosiasikan pada tahap ini.
   - **IKE Phase 2 (Quick Mode):** Tahap ini menghasilkan IPSec SA, yang digunakan untuk mengenkripsi data aktual. Parameter yang disepakati mencakup jenis protokol keamanan (ESP/AH), algoritma enkripsi dan autentikasi yang digunakan, serta masa berlaku kunci (key lifetime).

Parameter Keamanan yang Digunakan

Beberapa parameter keamanan standar yang umum digunakan meliputi:

- **Algoritma Enkripsi:** AES-256 (keamanan tinggi)
- **Algoritma Autentikasi:** HMAC-SHA256 (integritas dan keaslian data)
- **Key Lifetime:** 86400 detik (setara 24 jam)
- **Diffie-Hellman Group:** Group 14 (2048-bit)
- **Mode Operasi:** Tunnel Mode (untuk komunikasi antar jaringan berbeda)

Contoh Konfigurasi Router (IPSec Site-to-Site)

```
/ip ipsec peer
add address=203.0.113.2 exchange-mode=main secret="vpnkey123" \
enc-algorithm=aes-256 hash-algorithm=sha256 dh-group=modp2048

/ip ipsec proposal
add name="vpn-proposal" auth-algorithms=sha256 \
enc-algorithms=aes-256-cbc pfs-group=none

/ip ipsec policy
add dst-address=192.168.2.0/24 sa-dst-address=203.0.113.2 \
sa-src-address=203.0.113.1 src-address=192.168.1.0/24 \
tunnel=yes proposal=vpn-proposal
```

Konfigurasi di atas memperlihatkan penerapan koneksi IPSec secara sederhana pada perangkat router, menggunakan parameter keamanan yang telah dibahas sebelumnya untuk membentuk VPN antar situs.

2. Sebuah sekolah memiliki bandwidth internet

   Tujuan Pengaturan Bandwidth

   Pengaturan bandwidth dilakukan agar alokasi sumber daya jaringan dapat diatur sesuai dengan kebutuhan dan prioritas pengguna. Dalam skema ini, bandwidth 100 Mbps dibagi untuk empat jenis layanan:

   - **40 Mbps** untuk layanan e-learning (akses utama dan prioritas tertinggi).
   - **30 Mbps** untuk guru dan staf (akses ke email dan cloud storage).
   - **20 Mbps** untuk siswa (akses internet umum seperti browsing).
   - **10 Mbps** untuk kebutuhan latar belakang seperti CCTV dan pembaruan sistem.

   Penandaan Paket (Mangle Rule)

   Penandaan digunakan untuk mengelompokkan lalu lintas berdasarkan sumber subnet IP.

```
/ip firewall mangle
add chain=forward src-address=192.168.10.0/24 action=mark-packet \
new-packet-mark=elearning passthrough=yes

add chain=forward src-address=192.168.20.0/24 action=mark-packet \
new-packet-mark=guru_staf passthrough=yes

add chain=forward src-address=192.168.30.0/24 action=mark-packet \
new-packet-mark=siswa passthrough=yes

add chain=forward src-address=192.168.40.0/24 action=mark-packet \
new-packet-mark=cctv_update passthrough=yes
```

Penjelasan: Setiap aturan menandai paket berdasarkan alamat IP sumber, dengan tujuan mengklasifikasikan trafik untuk diproses oleh antrian (queue) yang sesuai.

Konfigurasi Queue Tree

Struktur Queue Tree digunakan untuk membatasi dan mengatur bandwidth sesuai prioritas.

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

add name="queue_elearning" parent=queue_parent packet-mark=elearning \
limit-at=40M max-limit=40M priority=1

add name="queue_guru_staf" parent=queue_parent packet-mark=guru_staf \
limit-at=30M max-limit=30M priority=2

add name="queue_siswa" parent=queue_parent packet-mark=siswa \
limit-at=20M max-limit=20M priority=3

add name="queue_cctv_update" parent=queue_parent packet-mark=
    cctv_update \
limit-at=10M max-limit=10M priority=4
```

Keterangan:

- `queue_parent` adalah queue utama dengan kapasitas maksimum 100 Mbps.
- Setiap queue anak memiliki `limit-at` sebagai bandwidth minimum yang dijamin, dan `max-limit` sebagai batas maksimum.
- `priority` digunakan untuk menentukan urutan layanan ketika bandwidth sedang penuh, di mana nilai lebih kecil menandakan prioritas lebih tinggi.

Ringkasan Prioritas dan Alokasi Bandwidth

Queue	Limit-at	Max-limit	Prioritas
E-learning	40 Mbps	40 Mbps	1 (tertinggi)
Guru dan Staf	30 Mbps	30 Mbps	2
Siswa	20 Mbps	20 Mbps	3
CCTV & Update	10 Mbps	10 Mbps	4 (terendah)

Kesimpulan: Penggunaan Queue Tree dan Mangle Rule memungkinkan manajemen bandwidth yang efisien dan adil, sesuai dengan prioritas dan kebutuhan masing-masing layanan di jaringan.

REFRENSI

3. MikroTik, *RouterOS: Queue Manual*, [Online]. Tersedia: `https://wiki.mikrotik.com/wiki/Manual:Queue`
4. MikroTik, *RouterOS: Firewall Mangle*, [Online]. Tersedia: `https://wiki.mikrotik.com/wiki/Manual:Firewall/Mangle`
5. IETF, *Internet Key Exchange (IKEv2) Protocol*, RFC 7296, 2014. [Online]. Tersedia: `https://datatracker.ietf.org/doc/html/rfc7296`
6. Cisco Systems, *IPSec VPN Design Guide*, Cisco Documentation, 2020. [Online]. Tersedia: `https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation.html`
7. Oppenheimer, Priscilla, *Top-Down Network Design*, 3rd ed., Cisco Press, 2010.