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

Laporan Sementara
Praktikum Jaringan Komputer

VPN & QoS

Natania Christin Agustina - 5024231014

2025

1 Pendahuluan

1.1 Latar Belakang

Di era digital yang semakin berkembang pesat, jaringan komputer menjadi fondasi utama dalam mendukung komunikasi, kolaborasi, dan pertukaran data secara global. Kebutuhan akan akses informasi yang cepat, aman, dan stabil mendorong pengembangan berbagai teknologi jaringan yang mampu memenuhi tuntutan tersebut. Namun, seiring meningkatnya mobilitas pengguna dan kompleksitas lalu lintas data, tantangan dalam menjaga privasi, keamanan, serta kualitas layanan jaringan pun semakin besar. Dua teknologi penting yang muncul sebagai solusi dalam menjawab tantangan ini adalah Virtual Private Network (VPN) dan Quality of Service (QoS). VPN merupakan teknologi yang memungkinkan pengguna untuk membuat koneksi aman melalui jaringan publik seperti internet. Dengan VPN, data yang dikirimkan akan dienkripsi dan dialihkan melalui "terowongan" virtual, sehingga aktivitas komunikasi menjadi lebih aman dan tidak mudah disadap. VPN sangat penting terutama bagi perusahaan atau individu yang membutuhkan akses jarak jauh ke jaringan internal secara privat. Selain memberikan perlindungan terhadap penyadapan dan pengintaian, VPN juga membantu pengguna menghindari pembatasan geografis serta meningkatkan fleksibilitas dalam bekerja secara remote. Di sisi lain, QoS merupakan mekanisme pengelolaan lalu lintas jaringan yang bertujuan untuk memastikan bahwa layanan penting seperti video konferensi, streaming, dan VoIP mendapatkan prioritas yang sesuai dalam pengiriman data. Dalam jaringan yang padat atau mengalami kemacetan, QoS akan menentukan skala prioritas paket data, mengurangi latensi, jitter, dan kehilangan data, sehingga pengalaman pengguna tetap optimal. Tanpa QoS, layanan sensitif terhadap waktu dapat mengalami gangguan yang signifikan, mengganggu produktivitas dan kualitas layanan. Dengan penerapan VPN dan QoS yang tepat, sebuah jaringan tidak hanya menjadi lebih aman tetapi juga lebih andal dalam menyediakan layanan yang konsisten dan berkualitas tinggi. Oleh karena itu, pemahaman tentang VPN dan QoS menjadi sangat penting dalam studi jaringan komputer, terutama dalam konteks keamanan dan manajemen performa di era digital saat ini.

1.2 Dasar Teori

- Tunneling
  Tunneling merupakan metode untuk mengirim data dari satu jaringan ke jaringan lain yang berbeda jenis dengan cara membungkus data dalam protokol lain agar bisa melewati perantara, layaknya melewati sebuah "terowongan digital". Misalnya, dua komputer yang menggunakan jaringan Ethernet ingin berkomunikasi, tetapi harus melewati jaringan WAN terlebih dahulu. Data dari komputer A akan dibungkus (proses ini disebut encapsulation) agar bisa melewati jaringan WAN dan kemudian dibuka kembali saat sampai di komputer B. Proses ini bisa dianalogikan seperti boneka matryoshka, di mana satu paket data dimasukkan ke dalam paket lain. Tunneling bekerja melalui beberapa tahapan. Pertama, komputer A membuat paket data yang ditujukan ke komputer B. Paket tersebut dikirim dalam bingkai Ethernet ke router M1. Di router M1, data dibungkus ulang menggunakan format protokol WAN dan dikirim ke router M2. Setelah sampai di router M2, data dibuka dari bungkus WAN-nya dan dikirim ke komputer B dalam bentuk aslinya. Proses membungkus dan membuka ini disebut encapsulation. Ada berbagai jenis protokol tunneling yang digunakan dalam dunia jaringan. GRE (Generic Routing Encapsulation) digunakan untuk membungkus paket IP dengan header tambahan agar dapat dikirim melalui

jaringan yang berbeda jenis. IPSec (Internet Protocol Security) menawarkan tunneling yang sangat aman karena menggunakan enkripsi, sangat cocok untuk koneksi yang membutuhkan privasi tinggi. IP-in-IP merupakan metode sederhana namun efektif untuk membungkus IP ke dalam IP. Protokol lain seperti SSH (Secure Shell) digunakan untuk akses jarak jauh yang aman, sedangkan PPTP (Point-to-Point Tunneling Protocol) adalah salah satu protokol VPN tertua yang kompatibel dengan berbagai sistem operasi. SSTP (Secure Socket Tunneling Protocol) milik Microsoft menggunakan SSL untuk menjamin koneksi yang aman. L2TP (Layer 2 Tunneling Protocol) adalah hasil kombinasi dari PPTP dan L2F milik Cisco, dan cocok untuk VPN lintas platform. Sementara itu, VXLAN (Virtual Extensible LAN) digunakan dalam virtualisasi jaringan skala besar seperti di lingkungan cloud dan data center, memungkinkan jaringan virtual terhubung meskipun lokasi fisiknya berjauhan. Salah satu bentuk khusus dari tunneling adalah SSL Tunneling. Ini adalah metode mengirim data terenkripsi menggunakan SSL melalui perantara (seperti proxy). Meskipun data melewati perantara, isinya tetap aman dan hanya bisa dibaca oleh server dan klien yang berkomunikasi langsung.

- IPSec (Internet Protocol Security)
  IPSec adalah protokol keamanan jaringan yang berfungsi layaknya pengawal pribadi untuk data yang dikirim melalui internet. Ketika data dikirim dari satu perangkat ke perangkat lain, IPSec akan mengenkripsi data tersebut agar tidak bisa dibaca atau diubah oleh pihak ketiga di tengah jalan. Selain itu, IPSec juga memastikan bahwa data memang berasal dari sumber yang sah, dan tidak dimanipulasi selama perjalanan. Karena kemampuannya ini, IPSec banyak digunakan dalam VPN (Virtual Private Network) untuk memberikan akses aman ke jaringan perusahaan dari jarak jauh, serta mencegah berbagai serangan siber. Beberapa fitur utama dari IPSec mencakup autentikasi, enkripsi, integritas data, manajemen kunci, dan kemampuan membuat tunneling aman. Autentikasi memastikan data berasal dari pengirim yang sah. Enkripsi digunakan untuk mengacak data agar tidak bisa dibaca oleh pihak yang tidak berwenang. Integritas menjamin bahwa data tidak mengalami perubahan selama dikirim. Manajemen kunci memungkinkan kedua pihak membuat dan menggunakan kunci rahasia untuk komunikasi. Selain itu, IPSec cukup fleksibel karena bisa digunakan di berbagai perangkat dan sistem operasi, serta pada jaringan kecil maupun besar. Cara kerja IPSec dimulai dari kedua perangkat yang hendak berkomunikasi menginisiasi koneksi dan saling bertukar informasi untuk membentuk jalur aman. Mereka akan bertukar kunci rahasia melalui proses yang disebut IKE (Internet Key Exchange). Setelah disepakati, terbentuklah “terowongan” aman untuk mengirim data yang sudah terenkripsi dan dijamin keasliannya. Setelah komunikasi selesai, koneksi akan ditutup. IPSec memiliki dua mode utama, yaitu Tunnel Mode dan Transport Mode. Tunnel Mode digunakan untuk mengamankan seluruh paket IP termasuk header-nya, dan cocok untuk komunikasi antar jaringan seperti antar cabang kantor. Transport Mode biasanya digunakan dalam koneksi antar perangkat di jaringan yang sama dan hanya mengenkripsi isi data, bukan header-nya. Protokol-protokol penting dalam IPSec antara lain ESP (Encapsulation Security Payload) yang bertugas mengenkripsi data dan memberi autentikasi, AH (Authentication Header) yang hanya menyediakan autentikasi dan integritas tanpa enkripsi, serta IKE yang digunakan untuk negosiasi dan pertukaran kunci keamanan. Meskipun IPSec menawarkan banyak keunggulan seperti tingkat keamanan tinggi, fleksibilitas penggunaan, dan dukungan lintas perangkat, ada pula beberapa kekurangan. Konfigurasi IPSec bisa rumit dan memerlukan pemahaman teknis yang mendalam. Tidak semua perangkat atau aplikasi kompatibel dengan IPSec, dan proses enkri-

psi memerlukan sumber daya yang besar sehingga bisa menurunkan performa jaringan. Selain itu, jika kunci enkripsi bocor, maka data juga berisiko terbuka. IPSec juga hanya melindungi lalu lintas IP, sehingga protokol lain tetap rentan jika tidak diamankan secara terpisah.

- Simple Queue vs Queue Tree
  Dalam manajemen jaringan MikroTik, pengaturan bandwidth bisa dilakukan menggunakan dua fitur utama: Simple Queue dan Queue Tree. Keduanya digunakan untuk mengatur seberapa besar kecepatan upload dan download yang dialokasikan untuk pengguna atau jenis trafik tertentu, namun memiliki cara kerja dan kompleksitas yang berbeda. Simple Queue adalah metode paling mudah untuk mengatur bandwidth per IP atau user tertentu. Pengguna hanya perlu menentukan IP target dan menetapkan batasan kecepatan upload dan download. Metode ini cocok untuk pemula atau jaringan kecil karena setting-nya cepat dan sederhana. Meskipun bisa mengatur prioritas, kemampuannya terbatas pada skenario yang sederhana. Sebaliknya, Queue Tree digunakan untuk pengaturan bandwidth yang lebih kompleks. Untuk menggunakannya, administrator perlu membuat aturan mangle untuk menandai koneksi atau paket terlebih dahulu. Queue Tree memungkinkan pembuatan struktur bertingkat (parent-child) dan cocok untuk membagi bandwidth berdasarkan jenis trafik, protokol, port, atau interface. Misalnya, total bandwidth 20 Mbps bisa dibagi menjadi 10 Mbps untuk video streaming, 5 Mbps untuk game, dan 5 Mbps untuk download. Queue Tree memberikan fleksibilitas tinggi namun memerlukan pemahaman mendalam tentang routing dan trafik jaringan.

- Prioritas Trafik Bandwidth
  Dalam situasi jaringan yang padat, pengaturan prioritas trafik menjadi sangat penting agar layanan penting tetap berjalan lancar. Konsep ini memungkinkan sistem untuk menentukan mana jenis trafik yang harus didahulukan ketika kapasitas jaringan terbatas. Misalnya, rapat online melalui video conference atau sambungan VPN ke kantor harus diprioritaskan dibandingkan dengan aktivitas seperti streaming video atau download file besar. Ada tiga alasan utama mengapa prioritas trafik diperlukan. Pertama, untuk memastikan komunikasi penting seperti rapat kerja atau sambungan remote tetap lancar meski jaringan penuh. Kedua, untuk menjaga layanan penting tetap aktif saat terjadi gangguan jaringan, seperti pemutusan link atau kesalahan server. Ketiga, untuk menghemat bandwidth, terutama di jaringan dengan kapasitas terbatas, dengan memprioritaskan aplikasi penting dibandingkan aktivitas yang bersifat hiburan atau konsumsi bandwidth tinggi. Contoh pengaturan prioritas dapat dilakukan dengan memberi tingkat tinggi untuk trafik VPN dan video conference, sedang untuk aktivitas browsing biasa, dan rendah untuk aktivitas seperti download game atau streaming. Pengaturan ini bisa dilakukan melalui fitur Simple Queue atau Queue Tree di MikroTik, dengan tambahan teknik seperti marking untuk membedakan jenis trafik berdasarkan port, IP, atau protokol. Beberapa perangkat bahkan mendukung fitur QoS (Quality of Service) otomatis yang bisa mengenali dan mengatur trafik berdasarkan jenisnya tanpa perlu konfigurasi manual yang rumit.

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:

   - Fase negosiasi IPSec (IKE Phase 1 dan Phase 2)
   - Parameter keamanan yang harus disepakati (algoritma enkripsi, metode autentikasi, lifetime key)
   - Konfigurasi sederhana pada sisi router untuk memulai koneksi IPSec site-to-site

   Jawaban :

   - Fase negosiasi IPSec (IKE Phase 1 dan Phase 2)
     - Phase 1 : Membangun saluran komunikasi yang aman (ISAKMP SA) dengan proses autentikasi dan pertukaran kunci menggunakan metode Diffie-Hellman. Tahapan ini bisa dijalankan dalam Mode Utama (Main Mode) atau Mode Agresif (Aggressive Mode).
     - Phase 2 : Membentuk IPSec Security Association (IPSec SA) untuk keperluan pertukaran data, dengan melakukan negosiasi terhadap parameter enkripsi dan verifikasi integritas (menggunakan ESP atau AH) melalui Quick Mode.
   - Parameter keamanan yang harus disepakati (algoritma enkripsi, metode autentikasi, lifetime key) :
     IKE Phase 1 Parameters:
     - Algoritma Enkripsi: AES-256
     - Hash Algorithm: SHA-256
     - Metode Autentikasi: Pre-shared key
     - Diffie-Hellman Group: Group 14
     - Lifetime: 28800 detik (8 jam)

     IKE Phase 2 Parameters:
     - Protokol Keamanan: ESP
     - Algoritma Enkripsi: AES-256
     - Algoritma Autentikasi: SHA-256-HMAC
     - PFS (Perfect Forward Secrecy): Ya (menggunakan Group 14)
     - Lifetime: 3600 detik (default IPSec SA lifetime di banyak perangkat)
   - Konfigurasi sederhana pada sisi router untuk memulai koneksi IPSec site-to-site : **Langkah-langkah Konfigurasi di Kantor Pusat:**

```
1         ! IKE Phase 1
2 crypto isakmp policy 10
3  encr aes 256
4  hash sha256
5  authentication pre-share
6  group 14
```

```
 lifetime 28800

! Pre-shared Key
crypto isakmp key vpnkey123 address 198.51.100.1

! IKE Phase 2 - Transform Set
crypto ipsec transform-set TRANS-SET esp-aes 256 esp-sha-hmac
 mode tunnel

! Aktifkan PFS
crypto map VPN-MAP 10 ipsec-isakmp
 set peer 198.51.100.1
 set transform-set TRANS-SET
 set pfs group14
 match address 110

! Access List untuk trafik yang dienkripsi
access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

! Terapkan ke interface WAN
interface GigabitEthernet0/0
 ip address 203.0.113.1 255.255.255.0
 crypto map VPN-MAP

```

Langkah-langkah Konfigurasi di Kantor Cabang:

```
            ! IKE Phase 1
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
 group 14
 lifetime 28800

! Pre-shared Key
crypto isakmp key vpnkey123 address 203.0.113.1

! IKE Phase 2 - Transform Set
crypto ipsec transform-set TRANS-SET esp-aes 256 esp-sha-hmac
 mode tunnel

! Aktifkan PFS
crypto map VPN-MAP 10 ipsec-isakmp
 set peer 203.0.113.1
 set transform-set TRANS-SET
 set pfs group14
 match address 110

! Access List untuk trafik yang dienkripsi
access-list 110 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

! Terapkan ke interface WAN
interface GigabitEthernet0/0
 ip address 198.51.100.1 255.255.255.0
```

```
29 crypto map VPN-MAP
30
31
```

Referensi :

- www.watchguard.com/help/docs/help-center/en-us/Content/en-US/Fireware/mvpn/general/ipsec_vpn_negotiations_c.html
- www.firewall.cx/cisco/cisco-routers/cisco-router-site-to-site-ipsec-vpn.html
- networklessons.com/security/ipsec-internet-protocol-security
- www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/217432-understand-ipsec-ikev1-protocol.html

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:

   - Parent dan child queue
   - Penjelasan marking
   - Prioritas dan limit rate pada masing-masing queue

   Jawaban :

   - Parent dan child queue :

```
1         Parent Queue:
2 name="TOTAL" parent=global limit-at=100M max-limit=100M
3
4 Child Queues:
5 name="E-LEARNING" parent=TOTAL limit-at=40M max-limit=40M priority=1 packet-
      mark=e-learning
6 name="GURU-STAF"  parent=TOTAL limit-at=30M max-limit=30M priority=2 packet-
      mark=guru-staf
7 name="SISWA"      parent=TOTAL limit-at=20M max-limit=20M priority=3 packet-
      mark=siswa
8 name="CCTV-UPDATE" parent=TOTAL limit-at=10M max-limit=10M priority=4 packet
      -mark=cctv-update
9
```

   - Penjelasan marking :

```
1             /ip firewall mangle
2 add chain=forward src-address=192.168.10.0/24 dst-port=80,443 protocol=tcp
    action=mark-packet new-packet-mark=e-learning
3 add chain=forward src-address=192.168.20.0/24 action=mark-packet new-packet-
    mark=guru-staf
4 add chain=forward src-address=192.168.30.0/24 action=mark-packet new-packet-
    mark=siswa
5 add chain=forward src-address=192.168.40.0/24 action=mark-packet new-packet-
    mark=cctv-update
6
7
```

- Prioritas dan limit rate pada masing-masing queue :
  E-LEARNING, Limit = 40Mbps, Priority = 1
  GURU-STAFF, Limit = 20Mbps, Priority = 2
  SISWA, Limit = 20Mbps, Priority = 3
  CCTV-UPDATE, Limit = 10Mbps, Priority = 4

Referensi :

- wiki.mikrotik.com/Manual:IP/Firewall/Mangle
- help.mikrotik.com/docs/spaces/ROS/pages/328088/Queues