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

Laporan Sementara
Praktikum Jaringan Komputer

VPN QoS

Syela Akhul Khalimi - 5024231015

2025

1 Pendahuluan

1.1 Latar Belakang

Di tengah transformasi digital yang pesat, tuntutan terhadap infrastruktur jaringan yang secure, reliable, dan optimal menjadi kebutuhan fundamental, khususnya untuk memfasilitasi komunikasi serta transfer data lintas geografis. Solusi teknologi networking seperti tunneling protocols, Virtual Private Network (VPN), dan bandwidth management telah menjadi pendekatan utama dalam mengatasi challenges tersebut di berbagai sektor termasuk korporasi, institusi pendidikan, dan organisasi pemerintah. Implementasi praktikum ini dirancang untuk mengembangkan pemahaman komprehensif serta kemampuan aplikatif dalam konfigurasi network infrastructure menggunakan platform Mikrotik, dengan fokus khusus pada pengelolaan bandwidth melalui Queue Tree mechanism dan proteksi komunikasi data via protokol IPSec. Berbagai problematika jaringan yang kerap dijumpai seperti distribusi akses internet yang tidak proporsional, vulnerabilitas terhadap data interception, serta suboptimal bandwidth allocation, menjadi dasar fundamental pentingnya penguasaan materi ini. Melalui eksplorasi konfigurasi VPN IPSec, participants akan memperoleh insight mendalam tentang establishment encrypted connection antara multiple network locations (contohnya headquarters dan branch office), yang sangat applicable dalam konteks professional contemporary dimana remote connectivity dan data security menjadi concern utama. Sementara itu, implementasi Queue Tree memungkinkan participants untuk memahami traffic prioritization management sesuai requirement spesifik, seperti segregasi bandwidth untuk online learning platform, staff activities, student access, dan surveillance systems. Materi-materi tersebut tidak hanya memiliki significance dari perspektif technical implementation, namun juga menawarkan practical application dalam designing dan managing modern network infrastructure yang secure, well-structured, dan efficient. Konsekuensinya, praktikum ini memiliki importance tinggi dalam mempersiapkan mahasiswa dengan competencies baik teoritis maupun praktis yang directly applicable.

1.2 Dasar Teori

Virtual Private Network (VPN) merupakan teknologi yang memungkinkan terbentuknya koneksi aman dan terenkripsi melalui jaringan publik, seperti internet, sehingga perangkat dapat terhubung ke jaringan privat secara aman. VPN banyak digunakan oleh organisasi yang memiliki beberapa cabang untuk mengintegrasikan jaringan mereka tanpa khawatir terhadap ancaman penyadapan data. Pada dasarnya, VPN bekerja dengan membuat sebuah tunnel atau jalur logis yang melindungi data menggunakan protokol-protokol seperti IPSec atau SSTP. Selain itu, VPN juga menerapkan enkripsi dengan algoritma tertentu, misalnya AES atau 3DES, untuk menjaga kerahasiaan data selama transmisi. Proses otentikasi juga menjadi bagian penting dalam VPN untuk memastikan hanya pengguna yang berhak yang dapat mengakses jaringan. Di sisi lain, Quality of Service (QoS) adalah mekanisme dalam jaringan yang berfungsi untuk mengatur dan mengelola penggunaan sumber daya jaringan agar kebutuhan layanan tertentu dapat terpenuhi secara optimal. QoS sangat penting untuk menjamin kualitas layanan, khususnya pada aplikasi yang sensitif terhadap delay, jitter, dan packet loss, seperti video conference atau VoIP. Parameter utama dalam QoS meliputi bandwidth (kapasitas transmisi data), delay (waktu tempuh paket dari sumber ke tujuan), jitter (variasi delay antar paket), serta packet loss (persentase paket yang hilang selama transmisi). Implementasi QoS biasanya melibatkan klasifikasi trafik berdasarkan prioritas, manajemen antrian (queue management) dengan algoritma

seperti Queue Tree pada perangkat Mikrotik, serta traffic shaping untuk mengatur alokasi bandwidth pada aplikasi tertentu. Integrasi antara VPN dan QoS sangat penting untuk memastikan performa jaringan tetap optimal meskipun data dienkripsi dan dialirkan melalui tunnel VPN. Dengan penerapan QoS pada jaringan VPN, trafik yang bersifat real-time seperti VoIP atau video conference dapat diprioritaskan, sehingga tetap mendapatkan bandwidth dan kualitas layanan yang memadai. Selain itu, manajemen bandwidth secara dinamis juga dapat dilakukan untuk membagi sumber daya antara trafik VPN dan non-VPN sesuai kebutuhan. Pemantauan parameter QoS seperti delay, throughput, dan packet loss juga penting untuk memastikan stabilitas dan efisiensi jaringan. Studi menunjukkan bahwa penerapan QoS pada VPN, misalnya pada VPN Site-to-Site menggunakan protokol SSTP, dapat meningkatkan keandalan jaringan secara signifikan, dengan tingkat packet loss yang rendah dan latency yang tetap terjaga. Dengan demikian, kombinasi antara VPN dan QoS sangat relevan dalam perancangan jaringan modern yang aman, stabil, dan efisien, baik di lingkungan bisnis, pendidikan, maupun pemerintahan.

2 Tugas Pendahuluan

Bagian ini berisi jawaban dari tugas pendahuluan yang telah anda kerjakan, beserta penjelasan dari jawaban tersebut

1 Studi Kasus Konfigurasi VPN IPSec

1.1 Fase Negosiasi IPSec (IKE Phase 1 dan Phase 2)

- Implementasi VPN IPSec site-to-site untuk menghubungkan kantor pusat dengan kantor cabang pada perangkat Cisco IOS/IOS-XE memerlukan konfigurasi dua tahap negosiasi utama beserta parameter keamanan yang tepat. Tahap pertama melibatkan pengaturan policy ISAKMP yang menentukan spesifikasi keamanan seperti enkripsi AES-256, fungsi hash SHA-256, kelompok Diffie-Hellman 14, autentikasi berbasis pre-shared key, dan durasi sesi 86400 detik untuk membangun kanal kontrol yang terenkripsi. Kedua router harus dikonfigurasi dengan kunci yang identik dan saling mengenali alamat IP publik masing-masing. Tahap kedua fokus pada pembentukan IPSec Security Association untuk enkripsi data aktual melalui konfigurasi transform set (seperti esp-aes 256 esp-sha-hmac), pengaktifan Perfect Forward Secrecy menggunakan Grup 14, dan penetapan lifetime SA selama 3600 detik. Traffic yang akan dienkripsi didefinisikan melalui Access Control List yang mengidentifikasi komunikasi antar subnet internal, contohnya antara jaringan kantor pusat 10.10.0.0/16 dan cabang 10.20.0.0/16. ACL tersebut kemudian diacu dalam crypto map yang diaplikasikan pada interface WAN seperti GigabitEthernet0/0/0. Alternatif modern menggunakan Virtual Tunnel Interface dengan IPSec profile yang memberikan fleksibilitas lebih tinggi untuk dynamic routing dan per-tunnel QoS marking, dimana interface tunnel dikonfigurasi dengan alamat private /30 dan diamankan menggunakan IPSec profile yang telah ditentukan.

Referensi:

- `https://learningnetwork.cisco.com/s/question/0D53i00000KsP6qCAF/relations-of-ike-phase-1-ar`

2 Manajemen Bandwidth dengan Queue Tree

2.1 Penguraian Desain QoS (QoS Berbasis Kelas dan Berbasis Kebijakan)

- Implementasi Quality of Service (QoS) pada sekolah dengan bandwidth 100 Mbps memerlukan strategi alokasi yang terstruktur untuk mendistribusikan kapasitas secara optimal. Pembagian bandwidth dirancang dengan mengalokasikan 40 Mbps untuk aplikasi e-learning seperti Zoom dan Google Meet, 30 Mbps untuk aktivitas staf termasuk email dan layanan cloud, 20 Mbps untuk aktivitas browsing siswa secara umum, serta 10 Mbps untuk sistem CCTV dan update perangkat. Klasifikasi traffic dilakukan melalui class-map yang memanfaatkan NBAR protocol recognition atau Access Control List untuk mengelompokkan traffic berdasarkan VLAN atau segmen IP subnet. Implementasi DSCP marking dilakukan pada tahap awal jaringan, idealnya di access layer switch atau core router, dengan pemberian marking AF41 untuk traffic e-learning guna memastikan low-latency delivery, AF31 untuk traffic staf, AF21 untuk aktivitas siswa, dan CS3 untuk traffic CCTV serta system update. Pada interface WAN, policy-map mengimplementasikan klasifikasi tersebut dengan menempatkan traffic e-learning dalam Low Latency Queue (LLQ) menggunakan strict priority yang dibatasi maksimal setengah dari total link capacity. Traffic kategori lainnya memperoleh alokasi bandwidth sesuai persentase yang ditetapkan dan dikelola melalui Class-Based Weighted Fair Queuing (CBWFQ). Penerapan Weighted Random Early Detection (WRED) atau fair queuing mechanism membantu mencegah buffer overflow saat terjadi kongesti, khususnya pada kelas traffic staf dan siswa. Seluruh policy dikonfigurasi dengan traffic shaping 100 Mbps untuk menyesuaikan dengan kapasitas circuit fisik dan mencegah packet drop di sisi ISP.

2.2 Klasifikasi Penandaan (NBAR + VLAN/ACL)

```
class-map match-any CM-ELEARNING
 match protocol zoom
 match protocol google meet
!
class-map match-any CM-STAFF
 match access-group name ACL-STAFF-SUBNET
!
class-map match-any CM-STUDENT
 match access-group name ACL-STUDENT-SUBNET
!
class-map CM-CCTV
 match access-group name ACL-CCTV-SUBNET
```

2.3 Konfigurasi Child Queue

```
/queue tree
add name="E-learning" parent="TOTAL-BW" packet-mark=e-learning-mark limit-at=30M max-
    limit=40M priority=1

add name="Guru-Staf" parent="TOTAL-BW" packet-mark=guru-mark limit-at=20M max-limit
    =30M priority=2

```

```
add name="Siswa" parent="TOTAL-BW" packet-mark=siswa-mark limit-at=10M max-limit=20M
    priority=3

add name="CCTV-Update" parent="TOTAL-BW" packet-mark=cctv-mark limit-at=5M max-limit
    =10M priority=4
```

2.4 WAN Egress Policy (MQC, single-level)

```
policy-map QOS-WAN-100M
 class CM-ELEARNING
  priority percent 40              ! LLQ     strict up to 40 Mbps
 class CM-STAFF
  bandwidth percent 30
  random-detect dscp-based         ! WRED, drop lowest DSCP first
 class CM-STUDENT
  bandwidth percent 20
  random-detect dscp-based
 class CM-CCTV
  bandwidth percent 10
 class class-default
  fair-queue
!
interface GigabitEthernet0/0/0   ! WAN
 service-policy output QOS-WAN-100M
 shape average 100000000         ! enforce physical link rate
```

2.5 Penguraian Queue Trees

- Setiap child queue memiliki pengaturan limit maksimum untuk menerapkan pembatasan bandwidth yang rigid, dengan hierarki mengikuti sistem prioritas queue dimana nilai numerik lebih rendah mengindikasikan prioritas lebih tinggi. Mekanisme bursting diimplementasikan melalui konfigurasi burst limit dan burst time yang memfasilitasi penggunaan bandwidth sementara melebihi alokasi normal ketika terjadi kondisi low contention. Arsitektur queue tree ini memberikan fleksibilitas skalabilitas tinggi, memungkinkan administrator untuk mengintegrasikan traffic class baru, menambahkan child queue tambahan, atau melakukan adjustment pada total bandwidth capacity melalui modifikasi pada root node. Konsep implementasi ini mengadopsi framework MQC (Modular QoS CLI) dari Cisco dan HTB (Hierarchical Token Bucket) Linux yang diadaptasi untuk environment MikroTik RouterOS.

2.6 Marking Traffic

```
/ip firewall mangle
 add chain=prerouting src-address=10.10.0.0/16       action=mark-packet new-packet-
    mark=ELEARNING
 add chain=prerouting src-address=10.11.0.0/16       action=mark-packet new-packet-
    mark=STAFF
 add chain=prerouting src-address=10.12.0.0/16       action=mark-packet new-packet-
    mark=STUDENT
```

```
5  add chain=prerouting src-address=10.13.0.0/24       action=mark-packet new-packet-
     mark=CCTV
```

2.7 Define Queue Types

```
1 /queue type
2  add name=pcq-equal kind=pcq rate=0     pcq-classifier=src-address
3  add name=pfifo-fast kind=pfifo limit=100
```

3 Queue Tree Hierarchy

```
1  /queue tree
2  ### ROOT     total Internet bandwidth ###
3  add name=TOTAL parent=global packet-mark="" max-limit=100M burst-limit=120M burst-
     threshold=90M burst-time=30s
4
5  ### Level-1 children (guaranteed rates) ###
6  add name=ELEARNING parent=TOTAL packet-mark=ELEARNING max-limit=40M priority=1 queue
     =pfifo-fast
7  add name=STAFF     parent=TOTAL packet-mark=STAFF     max-limit=30M priority=2 queue
     =pcq-equal
8  add name=STUDENT   parent=TOTAL packet-mark=STUDENT   max-limit=20M priority=3 queue
     =pcq-equal
9  add name=CCTV      parent=TOTAL packet-mark=CCTV      max-limit=10M priority=4 queue
     =pcq-equal
10
11 ### Optional Level-2 (per-host fairness for Students) ###
12 add name=STUDENT-PCQ parent=STUDENT packet-mark=STUDENT max-limit=20M queue=pcq-
     equal
```

Referensi:

- https://wiki.mikrotik.com/Manual:IP/Firewall/Mangle