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

Laporan Sementara
Praktikum Jaringan Komputer

VPN dan QoS

Muhammad Risang Radityatama - 5024231028

2025

1 Pendahuluan

1.1 Latar Belakang

Seiring dengan berkembangnya jumlah popularitas internet, semakin banyak pula entitas yang menggunakan internet, baik perorangan maupun organisasi atau perusahaan. Namun, tidak semua orang yang menggunakan internet memiliki niatan baik, karena ada individu bahkan organisasi yang memiliki niat buruk dalam pemanfaatan internet, contohnya seperti hacker yang mencuri data pengguna internet lain untuk dijual atau menyebarkan ransomware untuk menginfeksi perangkat orang lain dan meminta uang sebagai tebusan untuk menghapus ransomware tersebut. Oleh karena itu, diperlukan suatu sistem keamanan untuk melindungi data-data dan privasi pengguna. VPN atau virtual private network dapat menjawab kebutuhan ini. VPN memungkinkan pengguna untuk menyembunyikan alamatnya dan memberi enkripsi pada data yang dikirimkan sehingga tidak dapat dibaca dan dilacak oleh pihak-pihak yang tidak bertanggung jawab, sehingga bisa menjaga privasi dan keamanan data pengguna.

Selain keamanan, popularitas internet juga menuntut peningkatan kualitas layanan atau QoS (quality of service). Salah satu hal yang diperhatikan dalam QoS adalah pengaturan bandwidth. Pengaturan bandwidth diperlukan agar penggunaan internet dapat dimaksimalkan tanpa mengganggu proses-proses yang sedang berlangsung. Misalnya ada dua proses yang membutuhkan koneksi internet yaitu online meeting dan download file, QoS dan pengaturan bandwidth yang baik akan memprioritaskan trafik bandwidth untuk online meeting terlebih dahulu dibanding download file karena meeting membutuhkan kecepatan tinggi dan latensi rendah. Karena VPN dan QoS merupakan hal penting dalam sistem jaringan modern, maka dilaksanakan prakitkum jaringan komputer modul VPN dan QoS untuk memperdalam pemahaman mengenai kedua hal tersebut.

1.2 Dasar Teori

VPN atau virtual private network merupakan koneksi privat yang diterapkan dengan membuat koneksi terenkripsi antara perangkat dengan internet. Pada dasarnya, saat menggunakan VPN paket data yang dikirimkan beserta alamat IP seluruhnya disamarkan dari pihak selain penerima sehingga tidak bisa dibaca oleh pihak lain seperti hacker, ISP, atau bahkan pemerintah, sekalipun bisa dibaca maka diperlukan usaha lebih dari biasanya. Prinsip kerja VPN mencakup 2 proses, yaitu tunneling dan enkripsi. Tunneling merupakan proses dimana data dikirimkan melalui sebuah server proxy milik penyedia layanan VPN yang bertindak sebagai "terowongan" yang menghubungkan antara perangkat pengirim dengan perangkat penerima sehingga lalu lintas paket data tidak bisa dilihat oleh pihak luar. Beberapa contoh protokol tunneling adalah GRE, IPSec, IP-in-IP, SSH, PPTP, SSTP, L2TP, dan VXLAN. Enkripsi merupakan protokol untuk mengamankan isi dari paket data yang masuk melewati terowongan yang dibuat dari tunneling. Enkripsi akan mengacak isi data dari pengirim yang hanya akan bisa diterjemahkan dan dibacca oleh penerima, sehingga isi dari data yang dikirimkan tidak dapat dibaca oleh pihak luar yang tidak memiliki kunci enkripsi. Salah satu protokol enkripsi yang sering digunakan adalah IPSec. IPSec menawarkan tunneling dan enkripsi dalam satu protokol, sehingga sering digunakan karena kelengkapan dan keamanannya.

QoS atau quality of service merupakan mekanisme atau metode yang digunakan dalam sebuah jaringan untuk mengatur trafik dan menjamin aplikasi yang dijalankan tetap dalam performa yang baik dengan kapasitas jaringan yang terbatas. QoS membuat organisasi atau perusahaan untuk meng-

atur trafik network mereka secara keseluruhan dengan memprioritaskan aplikasi yang membuthkan koneksi dengan performa tinggi. Salah satu hal yang diperhatikan dalam QoS adalah bandwidth. Bandwidth merupakan kecepatan download dan upload dari sebuah jaringan saat melakukan komunikasi. Sebuah sistem QoS dapat memberikan aturan kepada router tentang bagaiana cara menggunakan dan mengatur bandwidth, seperti prioritas dan batas kecepatan yang diberikan untuk aplikasi-aplikasi tertentu. Ada dua metode yang dapat digunakan untuk mengatur bandwidth, yaitu simple queue dan queue tree. Simple queue merupakan sistem pengaturan bandwidth yang dapat mengatur bandwidth secara satu per satu untuk pengguna dan alamat IP, dengan masing-masing pengguna atau alamat IP memiliki pengaturan bandwidth masing-masing. Queue tree merupakan metode pengaturan bandwidth yang dapat digunakan untuk mengatur aturan bandwidth bagi banyak pengguna dan alamat IP secara fleksibel dan terstruktur, dengan masing-masing queue dapat terdiri atas parent dan child sehingga pembagian dapat dilakukan dengan lebih mudah, fleksibel, dan merata.

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:
   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

   Pada fase negosiasi IKE Phase 1, dinegosiasikan mengenai hashing, autentikasi, DH group, lifetime, dan algoritma enkripsi yang digunakan untuk membuat tunnel. Setelah itu, dilakukan DH key sharing agar kedua pihak memiliki kunci protokol yang sama. Terakhir, akan dilakukan autentikasi antara kedua pihak menggunakan metode autentikasi yang telah disepakati di tahap negosiasi, langkah ini mengakhiri phase 1. Pada IKE Phase 2 dinegosiasikan mengenai protokol IPSec yang akan digunakan, mode enkapsulasi, enkripsi, metode autentikasi, dan lifetime yang akan digunakan untuk melindungi data. Semua proses dalam phase 2 dilakukan di dalam tunnel yang dibuat di phase 1 sehingga tidak bisa dilacak pihak luar.

   Parameter keamanan yang harus disepakati meliputi enkripsi, hash, metode autentikasi, DH group, dan lifetime key. Sebagai contoh, pada kasus ini disepakati untuk algoritma enkripsi yang digunakan adalah AES-256, algoritma hash SHA-256, metode autentikasi pre-shared key dengan kunci autentikasi "authkey098", DH group 14, dan lifetime selama 3600 detik (1 jam).

   Berikut merupakan konfiguasi sederhana pada sisi router kantor pusat, dengan IP kantor pusat adalah 203.0.113.1:

```
1    ##IKE Phase 1##
2    crypto isakmp policy 10
3    encr aes 256
4    hash sha256
5    authentication pre-share
6    group 14
7    lifetime 3600
8
9    crypto isakmp key authkey098 address 192.168.2.1
```

```
10
11      ##IKE Phase 2##
12      crypto ipsec transform-set MYSET esp-aes 256 esp-sha-hmac
13
14      ##Crypto map##
15      crypto map VPN-MAP 10 ipsec-isakmp
16      set peer 192.168.2.1
17      set transform-set MYSET
18      match address 101
19
20      ##Konfigurasi ACL##
21      access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
22
23      ##Implementasi ke interface##
24      interface GigabitEthernet0/0
25      ip address 203.0.113.1 255.255.255.0
26      crypto map VPN-MAP
27
```

Berikut merupakan konfigurasi pada router kantor cabang dengan IP address 192.168.2.1:

```
1       ##IKE Phase 1##
2       crypto isakmp policy 10
3       encr aes 256
4       hash sha256
5       authentication pre-share
6       group 14
7       lifetime 3600
8
9       crypto isakmp key authkey098 address 203.0.113.1
10
11      ##IKE Phase 2##
12      crypto ipsec transform-set MYSET esp-aes 256 esp-sha-hmac
13
14      ##Crypto Map##
15      crypto map VPN-MAP 10 ipsec-isakmp
16      set peer 203.0.113.1
17      set transform-set MYSET
18      match address 102
19
20      ##Konfigurasi ACL##
21      access-list 102 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
22
23      ##Implementasi ke interface##
24      interface GigabitEthernet0/0
25      ip address 192.0.2.1 255.255.255.0
26      crypto map VPN-MAP
27
```

Referensi:

https://www.cisco.com/en/US/docs/routers/access/800/850/software/configuration/guide/vpngre.html

https://networklessons.com/security/ipsec-internet-protocol-security

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

   Parent queue:
   Parent queue dibagi menjadi 2 queue, yaitu untuk download dan upload. Download diprioritaskan daripada upload. Pembagian bandwidth adalah 60% untuk download dan 40% untuk upload.

   (a) Parent download
       Nama: down_sekolah
       Max limit: 60 Mbps
       Priority: 1

   (b) Parent upload
       Nama: up_sekolah
       Max limit: 40 Mbps
       Priority: 2

   Child queue:

   (a) Child queue untuk parent queue down_sekolah:

       - Nama: e-learning
         Parent: down_sekolah
         Marking: down_user
         Limit at: 24 Mbps
         Max limit: 60 Mbps
         Priority: 1
       - Nama: guru
         Parent: down_sekolah
         Marking: down_user
         Limit at: 18 Mbps
         Max limit: 60 Mbps
         Priority: 2
       - Nama: siswa
         Parent: down_sekolah
         Marking: down_user
         Limit at: 12 Mbps
         Max limit: 60 Mbps
         Priority: 3

- Nama: CCTV
  Parent: down_sekolah
  Marking: down_user
  Limit at: 6 Mbps
  Max limit: 60 Mbps
  Priority: 4

(b) Child queue untuk parent queue up_sekolah:

- Nama: e-learning
  Parent: up_sekolah
  Marking: upl_user
  Limit at: 16 Mbps
  Max limit: 40 Mbps
  Priority: 1
- Nama: guru
  Parent: up_sekolah
  Marking: upl_user
  Limit at: 12 Mbps
  Max limit: 40 Mbps
  Priority: 2
- Nama: siswa
  Parent: up_sekolah
  Marking: upl_user
  Limit at: 8 Mbps
  Max limit: 40 Mbps
  Priority: 3
- Nama: CCTV
  Parent: up_sekolah
  Marking: upl_user
  Limit at: 4 Mbps
  Max limit: 40 Mbps
  Priority: 4

Referensi:
https://blog.dnetprovider.id/2018/12/04/tutorial-mikrotik-pembagian-bandwidth-dengan-queue