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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall dan NAT

Bintang Narindra Putra Pratama - 5024231038

2025

1 Pendahuluan

1.1 Latar Belakang

Jaringan komputer sudah menjadi bagian kehidupan kita sehari-hari di era modern ini. Contoh paling utamanya adalah internet yang dapat diakses hampir oleh semua orang di berbagai belahan dunia. Dengan adanya internet kita dapat mencari, bertukar, dan mengakses informasi dari negara lain dengan mudah. Namun, karena jaringan dari internet ini sangat luas, bukan tidak mungkin terdapat orang-orang yang memiliki niat jahat untuk menggunakan internet dengan tujuan mencuri data pribadi kita, melakukan penipuan, dan sebagainya. Hal ini menjadi sesuatu yang perlu kita perhatikan, utamanya ketika mengirimkan sebuah data yang penting ke internet. Pada praktikum ini akan dibahas beberapa metode pengamanan data yang ada yaitu Tunneling dan IPSec. Serta dibahas juga tentang Queue agar praktikan memahami tentang pemberian layanan internet.

1.2 Dasar Teori

VPN merupakan sebuah mekanisme jaringan yang memungkinkan pengguna atau organisasi untuk membangun koneksi pribadi yang aman melalui jaringan publik, seperti internet. Tujuan utama dari VPN adalah untuk menjaga kerahasiaan, integritas, dan autentikasi data yang ditransmisikan, sehingga mencegah pihak ketiga atau penyusup dari mengakses atau memanipulasi informasi. VPN bekerja dengan menciptakan sebuah jalur atau "terowongan" terenkripsi antara perangkat pengguna dan server tujuan. Jalur ini disebut sebagai tunneling, yang memungkinkan paket data melintasi jaringan publik tanpa dapat diakses oleh pihak luar. Teknologi tunneling ini melakukan pembungkusan data asli dalam protokol lain, sehingga dapat dilewatkan secara tersembunyi dan aman. Pembungkusan ini disebut sebagai encapsulating. Data yang tadi dibungkus akan dibuka oleh penerima. Tunneling sendiri memiliki beberapa jenis protokol. Yang pertama adalah GRE(Generic Routing Encapsulation) yaitu tunneling yang membukus IP packet dengan header tambahan, namun hanya beberapa router tertentu yang dapat membuka isi dari protokol ini. Selanjutnya adalah IPSex (Internet Protocol Security) yang paling sering digunakan. IPSec melakukan enkripsi isi data ketika dikirim, kemudian ketika akan dibuka maka akan dilakukan pengecekan apakah paket ini bersumber dari pengirim langsung atau sudah dimanipulasi oleh pihak ketiga. Kemudian ada protokol IP-in-IP, dimana IP dimasukan kedalam IP. Kemudian adalah SSH(Secure Shell). Metode lain adalah PPTP(Point-to-Point Tunneling protocol) yaitu tunneling yang dilakukan pada point-to-point. Selanjutnya adalah SSTP(Secure Socket Tunneling Protocol) yaitu Tunneling milik Microsoft yang hanya dapat digunakan oleh Windows. Lalu ada L2TP(Layer 2 Tunneling Protocol) yaitu protokol yang menggabungkan PPTP dan L2F. Terakhir adalah VXLAN(Virtual Exetensible LAN) yang merupakan metode virtualisasi jaringan.
Namun, meskipun VPN dapat meningkatkan keamanan, keberadaannya juga menimbulkan tantangan dalam hal Quality of Service (QoS). QoS adalah sekumpulan mekanisme yang digunakan dalam jaringan untuk mengelola dan memprioritaskan lalu lintas data berdasarkan jenis layanan, kebutuhan bandwidth, toleransi terhadap delay, jitter, dan kehilangan paket (packet loss). QoS menjadi sangat penting dalam aplikasi-aplikasi real-time seperti VoIP (Voice over IP), video conferencing, dan streaming, yang sangat peka terhadap gangguan jaringan. Dalam konteks VPN, karena data telah dienkripsi dan dibungkus, perangkat jaringan sering kali kesulitan untuk mengidentifikasi jenis lalu lintas tersebut, sehingga penerapan QoS menjadi lebih kompleks. Dalam implementasinya, terdapat dua metode antrian utama yang digunakan dalam konfigurasi QoS, yaitu Simple Queue dan Queue Tree.

Simple Queue adalah metode yang paling dasar dalam manajemen bandwidth dan QoS. Metode ini memungkinkan administrator jaringan untuk menetapkan batas kecepatan unggah dan unduh secara individual untuk setiap IP address atau layanan. Konfigurasi Simple Queue relatif mudah dan cepat diterapkan, namun memiliki keterbatasan dalam hal fleksibilitas dan skalabilitas, terutama jika digunakan pada jaringan yang kompleks atau besar. Queue Tree menawarkan fleksibilitas dan kontrol yang lebih tinggi. Queue Tree memungkinkan pembuatan struktur antrian yang hierarkis, di mana bandwidth total dapat dibagi menjadi beberapa kelas atau kategori lalu lintas. Setiap kelas dapat diberi prioritas tertentu dan batasan bandwidth sendiri. Misalnya, lalu lintas VoIP bisa diberi prioritas tertinggi, sementara lalu lintas download atau browsing diberi prioritas yang lebih rendah. Hal ini memungkinkan optimasi performa jaringan yang jauh lebih baik, khususnya dalam kondisi jaringan yang padat atau ketika menggunakan VPN yang menyembunyikan detail lalu lintas.

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: • IKE fase 1 adalah fase membangun secure tunnel untuk pertukaran parameter keamanan. Fase ini memiliki dua mode yaitu Main Mode dan Aggresive Mode yang lebih cepat namun kurang aman.Kemudian IKE fase 2 adakah fase membangun Tunnel IPSec untuk lalu lintas data
   • Parameter keamanan tang harus disepakati adalah Algoritma Enkripsi, Metode Autentikasi, Lifetime Key, dan Key Exchange
   • a) Konfigurasi Fase 1
   crypto isakmp policy 10 encryption aes 256
   hash sha256
   authentication pre-share
   group 15
   lifetime 28800
   exit

   crypto isakmp key SECRET_KEY address 192.168.200.10
   b) Konfigurasi Fase 2
   crypto ipsec transform-set TRANS_SET esp-aes 256 esp-sha-hmac mode tunnel

   crypto map VPN-MAP 10 ipsec-isakmp
   set peer 192.168.2.1
   set transform-set TRANS_SET
   match address VPN-ACL
   sumber: Kaufman, C. (2014). Internet Key Exchange (IKEv2) Protocol (RFC 7296). Internet

Engineering Task Force (IETF). https://datatracker.ietf.org/doc/html/rfc7296

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 Queue
   name="TOTAL" parent=global limit-at=100M max-limit=100M
   Child Queue
   name="E-LEARNING" parent=TOTAL limit-at=40M max-limit=40M priority=1 packet-mark=e-learning
   name="GURU-STAF" parent=TOTAL limit-at=30M max-limit=30M priority=2 packet-mark=guru-staf
   name="SISWA" parent=TOTAL limit-at=20M max-limit=20M priority=3 packet-mark=siswa
   name="CCTV-UPDATE" parent=TOTAL limit-at=10M max-limit=10M priority=4 packet-mark=cctv-update
   Penjelasan Marking:
   dst-port=443,80 src-address=192.168.10.0/24 action=mark-packet new-packet-mark=e-learning -> E-Learning di tandai berdasarkan Source Address dan Destination Port untuk web E-Learning
   src-address=192.168.20.0/24 action=mark-packet new-packet-mark=guru-staf -> Guru-staff di tandai berdasarkan Source Address (192.168.20.0)
   src-address=192.168.30.0/24 action=mark-packet new-packet-mark=siswa -> Siswa di tandai berdasarkan Source Address (192.168.30.0)
   src-address=192.168.40.0/24 action=mark-packet new-packet-mark=cctv-update -> CCTV di tandai berdasarkan Source Address (192.168.40.0)

   Penjelasan Priotitas dan limit rate queue
   E-LEARNING, Limit = 40Mbps, Priority = 1
   GURU-STAFF, Limit = 20Mbps, Priority =2
   SISWA, Limit = 20Mbps, Priority = 3
   CCTV-UPDATE, Limit = 10Mbps, Priority = 4
   Sumber: MikroTik. (n.d.). Queues. MikroTik Documentation. https://help.mikrotik.com/docs/spaces/ROS/pages/328088/Queues