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

Laporan Sementara
Praktikum Jaringan Komputer

Tunneling, IPSec, Query Tree & Pembagian Bandwidth

Nur Anisa Hidayatul Masruroh - 5024231025

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital saat ini, jaringan komputer telah menjadi tulang punggung komunikasi dan pertukaran data antar individu, organisasi, bahkan negara. Seiring dengan meningkatnya ketergantungan terhadap jaringan, berbagai tantangan teknis mulai bermunculan, seperti kebutuhan akan keamanan komunikasi, efisiensi pertukaran data, serta pengelolaan lalu lintas jaringan yang adil dan stabil. Oleh karena itu, diperlukan pemahaman dan keterampilan teknis yang mendalam mengenai berbagai solusi jaringan yang telah dikembangkan untuk mengatasi tantangan tersebut.

Salah satu masalah yang sering dihadapi dalam jaringan modern adalah kebutuhan untuk melewati batasan atau filter jaringan tanpa mengorbankan keamanan data. Di sinilah konsep tunneling menjadi sangat relevan. Tunneling memungkinkan data yang dikirim melalui jaringan publik seperti internet dapat disalurkan seolah-olah berada dalam jaringan privat, yang sangat berguna untuk remote access dan koneksi antar cabang perusahaan. Namun, penggunaan tunneling tanpa perlindungan tambahan tetap menyisakan celah keamanan.

Untuk menjawab kebutuhan akan keamanan tersebut, teknologi IPSec hadir sebagai solusi yang mampu mengamankan pertukaran data pada lapisan IP. Banyak organisasi saat ini harus menghadapi ancaman seperti penyadapan (eavesdropping), pemalsuan data, hingga serangan man-in-the-middle. IPSec memungkinkan data yang ditransmisikan dienkripsi dan diverifikasi sehingga hanya dapat diakses oleh pihak yang berwenang. Tanpa teknologi ini, komunikasi yang berjalan melalui jaringan terbuka akan sangat rentan terhadap serangan.

Di sisi lain, dalam sistem yang melibatkan banyak perangkat seperti RFID, sensor nirkabel, atau jaringan IoT, muncul tantangan dalam mengatur komunikasi agar tidak terjadi tabrakan (collision) antar perangkat. Hal ini melahirkan kebutuhan akan algoritma yang efisien dalam mengidentifikasi perangkat secara individual, yang kemudian dijawab oleh algoritma Query Tree. Dengan menggunakan pendekatan pohon pencarian, metode ini memungkinkan pengenalan ID perangkat secara sistematis tanpa gangguan sinyal antar perangkat yang aktif secara bersamaan.

Terakhir, masalah umum dalam jaringan yang digunakan secara bersama-sama adalah ketimpangan dalam penggunaan bandwidth. Beberapa pengguna atau aplikasi mungkin menyerap sebagian besar kapasitas jaringan, menyebabkan layanan lain terganggu. Oleh karena itu, pembagian bandwidth menjadi krusial untuk menjaga performa dan keadilan dalam penggunaan sumber daya jaringan. Praktik ini juga penting dalam skenario dunia nyata seperti laboratorium komputer, perusahaan, dan sekolah yang memiliki jaringan padat.

Berdasarkan berbagai permasalahan tersebut, praktikum ini menjadi penting untuk dilakukan agar mahasiswa tidak hanya memahami konsep secara teori, tetapi juga mampu mengimplementasikan solusi nyata dalam mengatasi tantangan jaringan. Dengan memahami tunneling, IPSec, query tree, dan pembagian bandwidth, mahasiswa diharapkan memiliki kompetensi teknis yang relevan dan siap menghadapi kompleksitas dunia jaringan komputer di lapangan.

1.2 Dasar Teori

Tunneling adalah teknik dalam jaringan komputer yang digunakan untuk mengirimkan data dari satu protokol melalui jaringan yang menggunakan protokol berbeda. Teknik ini bekerja dengan cara membungkus (encapsulate) paket data dalam format baru agar bisa melewati jaringan tertentu, seperti

jaringan publik yang tidak mengenal protokol aslinya. Salah satu contoh paling umum dari tunneling adalah penggunaan VPN (Virtual Private Network), yang memungkinkan pengguna mengakses jaringan privat melalui internet dengan aman. Beberapa jenis tunneling yang populer antara lain GRE (Generic Routing Encapsulation), L2TP (Layer 2 Tunneling Protocol), dan PPTP (Point-to-Point Tunneling Protocol). Kelebihan tunneling adalah kemampuannya untuk menyediakan jalur komunikasi yang aman dan melewati firewall atau NAT, namun kekurangannya termasuk penambahan beban data (overhead) dan potensi penurunan performa koneksi.

IPSec (Internet Protocol Security) adalah sekumpulan protokol yang digunakan untuk mengamankan komunikasi data pada lapisan jaringan. IPSec menyediakan layanan keamanan seperti otentikasi, integritas, dan enkripsi data pada tingkat IP, sehingga sangat cocok digunakan dalam koneksi antar situs melalui jaringan publik. IPSec memiliki dua mode utama: Transport Mode, yang hanya mengenkripsi data di dalam paket IP, dan Tunnel Mode, yang mengenkripsi seluruh paket IP termasuk header-nya. Biasanya IPSec digunakan bersamaan dengan VPN untuk meningkatkan keamanan transmisi data. Keunggulan IPSec adalah memberikan tingkat keamanan tinggi dan perlindungan terhadap ancaman seperti sniffing dan spoofing. Namun, konfigurasi IPSec cukup kompleks dan membutuhkan sumber daya komputasi yang besar, yang bisa menjadi tantangan tersendiri dalam implementasi praktis.

Query Tree adalah metode yang digunakan dalam sistem identifikasi seperti RFID untuk menghindari konflik saat banyak perangkat mencoba merespon secara bersamaan. Metode ini menggunakan pendekatan struktur pohon biner untuk melakukan pencarian ID secara bertahap dan sistematis. Ketika ada banyak perangkat, query tree membantu mengatur komunikasi agar tidak terjadi tabrakan data (collision). Terdapat beberapa varian dari metode ini, termasuk Basic Query Tree dan Modified Query Tree. Basic Query Tree bekerja dengan meminta respon berdasarkan awalan ID, sedangkan versi modifikasinya dapat mengurangi waktu pencarian dengan logika tambahan. Kelebihan dari metode ini adalah efisiensinya dalam mengatur komunikasi perangkat masif, terutama dalam sistem RFID atau sensor nirkabel. Kekurangannya terletak pada waktu pencarian yang bisa lama jika jumlah perangkat sangat besar atau jika tidak ada optimasi tambahan.

Pembagian Bandwidth adalah proses pengaturan kapasitas jaringan agar setiap pengguna atau aplikasi mendapatkan alokasi bandwidth yang sesuai. Dalam jaringan yang memiliki banyak pengguna, pembagian bandwidth menjadi sangat penting agar tidak ada satu pengguna yang menghabiskan seluruh kapasitas jaringan. Pembagian ini dapat dilakukan secara statis (fixed allocation) atau dinamis (dynamic allocation), serta dapat didukung oleh teknologi seperti QoS (Quality of Service) dan traffic shaping. Misalnya, administrator jaringan dapat memberikan prioritas lebih pada layanan video conference dibandingkan dengan browsing biasa. Kelebihan dari pembagian bandwidth adalah kemampuannya menjaga performa jaringan tetap stabil dan adil antar pengguna. Namun, jika tidak dilakukan dengan benar, pembagian ini bisa menimbulkan ketimpangan dan membuat aplikasi tertentu tidak berjalan optimal.

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

Negosiasi IPSec terdiri dari 2 fase, yaitu IKE phase 1 dan phase 2. IKE phase 1 merupakan fase dimana perangkat saling mengenali dan mengautentikasi sebelum membetuk saluran aman bagi pertukaran data selanjutnya (Phase 2). Pada fase 1 ini, akan terbentuk ISAKMP SA yang berisi parameter-parameter yang telah saling disepakati. Bisa dikatakan, phase 1 merupakan tunnel awal yang mengakomodir keamanan pertukaran parameter keamanan. Parameter yang ditentukan dalam fase ini adalah cara autentikasi, algoritma enkripsi, algoritma hash, lifetime, dan DH group. DH group merupakan penentuan group atau jenis DH (mekanisme pertukaran secret key tanpa mengirimkan secret key nya) yang akan digunakan. Phase kedua merupakan fase di mana perangkat akan menyepakati IPSec policy dan terbentuknya IPSec SA. Hasil dari fase ini adalah tunnel yang akan digunakan untuk mengirimkan data via VPN. Isi dari IPSec yang disepakati dalam fase ini diantaranya, protokol IPSec, algoritma untuk enkripsi, algoritma hash, mode, lifetime dan traffice selector. Traffic selector merupakan parameter yang menetukan jaringan aman yang akan dipasangin VPN.

Link Referensi : `https://networklessons.com/security/ipsec-internet-protocol-security`

Koneksi IPSec site to site merupakan konfigurasi yang memungkinakan router dari 2 tempat berbeda terhubung langsung selayaknya 1 jaringan internal. Konfigurasi untuk kedua router sebagaimana berikut:

Konfigurasi Jaringan Cabang (Client):

- Public IP: 203.0.113.2
- LAN: 192.168.2.0/24

Pusat (Server):

- Public IP: 203.0.113.1
- LAN: 192.168.1.0/24

Pre-shared Key: mysecretkey

Konfigurasi di Router Kantor Pusat

```
# 1. Atur IP Address (sesuaikan)
ip address add address=203.0.113.1/24 interface=ether1

# 2. Buat Proposals
/ip ipsec proposal
add name="myproposal" auth-algorithms=sha256 enc-algorithms=aes-256-cbc lifetime=1h pfs-gro

# 3. Buat Peer
```

```
/ip ipsec peer
add address=203.0.113.2/32 exchange-mode=main secret="mysecretkey" enc-algorithm=aes-256 ha

# 4. Buat Policy
/ip ipsec policy
add src-address=192.168.1.0/24 dst-address=192.168.2.0/24 sa-dst-address=203.0.113.2 sa-src

# 5. (Opsional) Allow NAT Exclusion
/ip firewall nat
add chain=srcnat src-address=192.168.1.0/24 dst-address=192.168.2.0/24 action=accept
```

Konfigurasi di Router Kantor Cabang

```
# 1. Atur IP Address (sesuaikan)
ip address add address=203.0.113.2/24 interface=ether1

# 2. Buat Proposals (harus sama!)
/ip ipsec proposal
add name="myproposal" auth-algorithms=sha256 enc-algorithms=aes-256-cbc lifetime=1h pfs-gro

# 3. Buat Peer
/ip ipsec peer
add address=203.0.113.1/32 exchange-mode=main secret="mysecretkey" enc-algorithm=aes-256 ha

# 4. Buat Policy
/ip ipsec policy
add src-address=192.168.2.0/24 dst-address=192.168.1.0/24 sa-dst-address=203.0.113.1 sa-src

# 5. (Opsional) Allow NAT Exclusion
/ip firewall nat
add chain=srcnat src-address=192.168.2.0/24 dst-address=192.168.1.0/24 action=accept
```

Link Referensi : `https://cloudzy.com/blog/mikrotik-ipsec-site-to-site-vpn/`

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

Untuk kasus ini, struktur dari queue tree yang digunakan dapat dibuat dari 1 root 100Mb kemudian dibagi menjadi 4 child sesuai soal. Secara sederhana, strukturnya jadi seperti tabel di bawah ini. Prioritas yang digunakan (1 menunjukkan sangat penting dan 10 menunjukkan kurang penting) berdsarkan pada kebutuhan terkait keamanan, operasional, dan akses casual. Pada akses siswa, diberikan prioritas rendah karena asses cukup kasual pada browsing biasa. Sedangkan pada cctv, akses cukup tinggi karena berhubungan dengan keamanan.Root memiliki prioritas rendah sebagai deafult saja.

Komponen	Nama Queue	Parent Queue	Max Limit	Limit At	Priority	Marking
Total Bandwidth	total-bandwidth	(root)	100 Mbps	-	8	-
E-Learning	elearning	total-bandwidth	40 Mbps	20 Mbps	1	mark-elearning
Guru & Staf	guru-staf	total-bandwidth	30 Mbps	15 Mbps	3	mark-guru
Siswa	siswa	total-bandwidth	20 Mbps	10 Mbps	5	mark-siswa
CCTV & Sistem	cctv-sistem	total-bandwidth	10 Mbps	5 Mbps	2	mark-cctv

Pada kasus ini, marking yang digunakan adalah marking berdasrkan ip address atau alamat dari network tersebut. Secara sedrhana, pembagiannya dapat dilihat seperti pada tabel berikut.

Kategori	IP Subnet	Keterangan	Packet Marking
E-Learning	192.168.1.0/26	IP untuk perangkat e-learning	mark-elearning
Guru & Staf	192.168.1.64/26	IP untuk guru dan staf	mark-guru
Siswa	192.168.1.128/25	IP untuk siswa	mark-siswa
CCTV & Sistem	192.168.2.0/28	IP perangkat CCTV dan update sistem	mark-cctv

Konfigurasi pada router dapat dilakukan dengan perintah-perintah berikut:

```
/ip firewall mangle
# Mark paket e-learning berdasarkan sumber IP subnet 192.168.1.0/26
add chain=forward src-address=192.168.1.0/26 action=mark-packet new-packet-mark=
    mark-elearning passthrough=yes comment="Mark e-learning traffic"

# Mark paket guru & staf berdasarkan sumber IP subnet 192.168.1.64/26
add chain=forward src-address=192.168.1.64/26 action=mark-packet new-packet-mark
    =mark-guru passthrough=yes comment="Mark guru & staf traffic"

# Mark paket siswa berdasarkan sumber IP subnet 192.168.1.128/25
add chain=forward src-address=192.168.1.128/25 action=mark-packet new-packet-
    mark=mark-siswa passthrough=yes comment="Mark siswa traffic"

# Mark paket CCTV & sistem berdasarkan sumber IP subnet 192.168.2.0/28
add chain=forward src-address=192.168.2.0/28 action=mark-packet new-packet-mark=
    mark-cctv passthrough=yes comment="Mark CCTV & system traffic"
```

Link Referensi : https://help.mikrotik.com/docs/spaces/ROS/pages/328088/Queues