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

Laporan Sementara
Praktikum Jaringan Komputer

Crimping dan Routing IPv4

Moh. Wildan Risqi Maulidi - 5024231056

2025

1 Pendahuluan

1.1 Latar Belakang

praktikumini dilakukan untuk mengetahui cara Tunneling pada jaringan komputer, dengan tujuan untuk memahami konsep dasar tunneling, cara kerja, serta penerapannya dalam jaringan. Tunneling adalah teknik yang digunakan untuk mengirimkan data melalui jaringan yang tidak mendukung protokol tertentu dengan cara membungkus data tersebut dalam paket yang sesuai dengan protokol yang didukung oleh jaringan tersebut. Dengan memahami tunneling, diharapkan mahasiswa dapat mengimplementasikan teknik ini dalam berbagai skenario jaringan, seperti VPN (Virtual Private Network) dan komunikasi antar jaringan yang berbeda protokol.

1.2 Dasar Teori

1.2.1 Tunneling

Tunneling adalah metode dalam jaringan komputer yang memungkinkan pengiriman data dari satu protokol jaringan melalui jaringan lain dengan cara membungkus (encapsulating) data asli ke dalam format paket dari protokol perantara. Teknik ini umum digunakan dalam Virtual Private Network (VPN) untuk memungkinkan koneksi aman antar jaringan yang terpisah secara fisik maupun logis. Proses encapsulation membuat paket data seperti "boneka matryoshka," di mana satu paket dibungkus dalam paket lain untuk dapat melewati jaringan berbeda.
Tunneling mendukung berbagai protokol seperti:

- **GRE (Generic Routing Encapsulation)** : protokol sederhana untuk membungkus paket.
- **IP-in-IP** : membungkus IP dalam IP untuk koneksi antar jaringan IP.
- **IPSec** : menyediakan keamanan pada data yang ditransmisikan.
- **SSH dan SSL** : menyediakan tunneling terenkripsi untuk keamanan ekstra.
- **PPTP, L2TP, SSTP** : protokol tunneling untuk VPN.

1.2.2 IPSec (Internet Protocol Security)

IPSec adalah rangkaian protokol yang dirancang untuk mengamankan komunikasi data pada jaringan IP dengan menyediakan autentikasi, integritas, dan enkripsi data. IPSec bekerja pada lapisan jaringan (network layer) dan sangat umum digunakan dalam VPN untuk menciptakan "terowongan" komunikasi yang aman.
Fitur utama IPSec meliputi:

- Autentikasi: Memastikan pengirim adalah pihak yang sah.
- Enkripsi: Mengacak isi data agar tidak bisa dibaca oleh pihak tak berwenang.
- Integritas: Menjamin data tidak diubah selama pengiriman.
- Key Management: Pengelolaan kunci enkripsi melalui protokol seperti IKE.

- Mode Operasi: Terdapat dua mode, yaitu Transport Mode (hanya payload yang dienkripsi) dan Tunnel Mode (seluruh paket termasuk header dienkripsi).

Protokol-protokol penting dalam IPSec antara lain:

- **AH (Authentication Header)**: Menyediakan autentikasi dan integritas data tanpa enkripsi.
- **ESP (Encapsulating Security Payload)**: Menyediakan enkripsi, autentikasi, dan integritas data.
- **IKE (Internet Key Exchange)**: Protokol untuk negosiasi kunci dan parameter keamanan.

1.2.3 Manajemen Bandwidth

- **Simple Queue** adalah metode pengaturan bandwidth yang sederhana dan langsung, cocok digunakan pada jaringan kecil atau ketika hanya ingin mengatur kecepatan berdasarkan IP tertentu. Pengguna hanya perlu menentukan parameter dasar seperti IP dan kecepatan maksimal.
- **Queue Tree** merupakan metode pengaturan yang lebih kompleks dan fleksibel. Diperlukan konfigurasi tambahan seperti mangle rule untuk menandai trafik. Cocok untuk implementasi bandwidth sharing berbasis protokol, interface, VLAN, maupun jenis trafik lainnya, serta mendukung struktur bertingkat (parent_child queue).

1.2.4 Prioritas Trafik Bandwidth

Manajemen prioritas trafik dalam jaringan bertujuan untuk memastikan bahwa jenis trafik yang dianggap penting mendapatkan jalur komunikasi terlebih dahulu dibanding trafik yang tidak penting, terutama saat bandwidth terbatas. Penerapan prioritas penting dalam menjaga kualitas layanan (QoS/Quality of Service), misalnya untuk VoIP, video conference, atau akses ke server internal yang kritikal.
Faktor-faktor yang menjadi pertimbangan dalam pemberian prioritas antara lain:

- Tingkat kepentingan trafik (misalnya, trafik real time seperti video call lebih penting daripada download biasa).
- Keadaan darurat atau kondisi jaringan terbatas.
- Penggunaan sumber daya secara adil antar pengguna.

2 Tugas Pendahuluan

- dibawah terdapat jawaban studi kasus ketiganya.

  Fase negosiasi IPSec (IKE Phase 1 dan Phase 2).

  * IKE Phase 1

    bertujuan untuk Membuat saluran komunikasi yang aman dan terenkripsi antara dua perangkat. langkah langkahnya sebagai berikut:

    1. Negosiasi parameter keamanan (algoritma enkripsi, autentikasi, dll).
    2. Pertukaran kunci Diffie-Hellman (DH).
    3. Otentikasi identitas masing-masing pihak.

4. Membentuk ISAKMP Security Association (SA).

* IKE Phase 2 bertujuan untuk Menyepakati parameter untuk melindungi data aktual (data yang lewat terowongan).langkah langkahnya sebagai berikut:
  1. Negosiasi parameter seperti enkripsi ESP dan protokol AH.
  2. Membuat IPSec SA untuk masing-masing arah komunikasi.
  3. Proses ini lebih cepat karena berjalan dalam tunnel yang sudah aman.

  Referensi:
  Cisco Systems, Inc., "Configure a Site-to-Site IPSec IKEv1 Tunnel Using a Pre-shared Key on Cisco IOS Routers," Cisco Support Community. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios/218432-configure-a-site-t html. [Accessed: Jun. 4, 2025].
  WatchGuard Technologies, Inc., "About IPSec VPN Negotiations," WatchGuard Help Center. [Online]. Available: https://www.watchguard.com/help/docs/help-center/en-us/Content/en-US/Fireware/mvpn/general/ipsec_vpn_negotiations_c.html. [Accessed: Jun. 4, 2025].

– Parameter Keamanan dalam Konfigurasi IPSec.
  Dalam konfigurasi VPN IPSec, beberapa parameter keamanan penting yang harus disepakati antara kedua perangkat adalah:

  1. Algoritma Enkripsi: Digunakan untuk menjaga kerahasiaan data. Contoh: AES (Advanced Encryption Standard).
  2. Metode Autentikasi: Digunakan untuk memastikan keaslian data. Contoh: HMAC-SHA1 atau HMAC-SHA2.
  3. Grup Diffie-Hellman: Digunakan untuk pertukaran kunci secara aman.
  4. Masa Berlaku Kunci (Lifetime): Menentukan durasi waktu sebelum kunci enkripsi harus diperbarui.

  Referensi:
  Kontributor Wikipedia, "IPsec," Wikipedia, Ensiklopedia Bebas. [Online]. Available: https://en.wikipedia.org/wiki/IPsec. [Accessed: Jun. 4, 2025].

– Konfigurasi Sederhana IPSec Site-to-Site pada Router:
  Berikut adalah langkah-langkah umum untuk mengkonfigurasi koneksi VPN IPSec site-to-site antara dua router:

  * Konfigurasi Fase 1 (IKE Phase 1)
    · Menentukan parameter seperti metode autentikasi, algoritma enkripsi, dan grup Diffie-Hellman.
    · Membentuk IKE SA antara kedua perangkat.
  * Konfigurasi Fase 2 (IKE Phase 2)
    · Menentukan parameter seperti protokol enkripsi (ESP), algoritma enkripsi dan autentikasi, serta masa berlaku kunci.
    · Membentuk IPSec SA untuk mengenkripsi data yang dikirim.

* Parameter Keamanan yang Harus Disepakati Dalam konfigurasi VPN IPSec, beberapa parameter keamanan penting yang harus disepakati antara kedua perangkat adalah:

  - Algoritma Enkripsi: Digunakan untuk menjaga kerahasiaan data. Contohnya termasuk AES (Advanced Encryption Standard) dan 3DES (Triple Data Encryption Standard).
  - Metode Autentikasi: Digunakan untuk memverifikasi identitas perangkat. Metode umum meliputi Pre-Shared Key (PSK) dan sertifikat digital.
  - Lifetime Key: Menentukan durasi waktu atau jumlah data yang dapat ditransmisikan sebelum kunci enkripsi harus diperbarui.

  Parameter-parameter ini harus disepakati selama proses negosiasi IKE untuk memastikan keamanan dan kompatibilitas antara kedua perangkat VPN.
* Konfigurasi Sederhana pada Sisi Router untuk Memulai Koneksi IPSec Site-to-Site

```
        ! Konfigurasi Phase 1
        crypto isakmp policy 10
        encr aes 256
        hash sha256
        authentication pre-share
        group 14
        lifetime 86400

        crypto isakmp key YOUR_PRESHARED_KEY address REMOTE_PEER_IP

        ! Konfigurasi Phase 2
        crypto ipsec transform-set TRANSFORM_SET_NAME esp-aes 256 esp-
    sha-hmac

        ! Konfigurasi Crypto Map
        crypto map CRYPTO_MAP_NAME 10 ipsec-isakmp
        set peer REMOTE_PEER_IP
        set transform-set TRANSFORM_SET_NAME
        match address ACL_NAME

        interface GigabitEthernet0/0
        crypto map CRYPTO_MAP_NAME

        ! Access List untuk menentukan lalu lintas yang akan dienkripsi
        access-list ACL_NAME permit ip LOCAL_SUBNET LOCAL_WILDCARD
    REMOTE_SUBNET REMOTE_WILDCARD

```

  Pastikan untuk mengganti YOUR_PRESHARED_KEY, REMOTE_PEER_IP, TRANSFORM_SET_
  CRYPTO_MAP_NAME, ACL_NAME, LOCAL_SUBNET, LOCAL_WILDCARD, REMOTE_SUBNET
  dan REMOTE_WILDCARD sesuai dengan kebutuhan jaringan Anda. Referensi:
  Cisco Systems, Inc., “Configure ASA to Router IPSec VPN Tunnel (Main Mode and Aggressive Mode),” Cisco Support Community. [Online]. Available: `https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/117337-config-asa-router-00.html`. [Accessed: Jun. 4, 2025].

- Skema Queue Tree untuk Pembagian Bandwidth di Sekolah

– Parent dan Child Queue

  Untuk membagi bandwidth internet 100 Mbps sesuai kebutuhan, kita dapat menggunakan Queue Tree pada MikroTik dengan struktur sebagai berikut:

  * Parent Queue: Membatasi total bandwidth hingga 100 Mbps.
  * Child Queues:
    · E learning: 40 Mbps
    · Guru & Staf: 30 Mbps
    · Siswa: 20 Mbps
    · CCTV & Update Sistem: 10 Mbps

  Referensi:

  Cisco Systems, Inc., “Understand the IPSec and IKEv1 Protocols,” Cisco Support Community. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/217432-understand-ipsec-ikev1-protoco
  html. [Accessed: Jun. 4, 2025].

– Penjelasan Marking

  Sebelum menerapkan Queue Tree, kita perlu menandai (mark) paket berdasarkan jenis lalu lintas menggunakan fitur mangle pada MikroTik. Ini memungkinkan kita untuk mengidentifikasi dan mengelompokkan lalu lintas sesuai dengan kategori yang telah ditentukan.

  Contoh konfigurasi mangle:

```
1       /ip firewall mangle
2       add chain=forward protocol=tcp dst-port=80,443 content=e-learning
    action=mark-packet new-packet-mark=e-learning passthrough=yes
3       add chain=forward src-address=192.168.1.0/24 action=mark-packet new-
    packet-mark=guru-staf passthrough=yes
4       add chain=forward src-address=192.168.2.0/24 action=mark-packet new-
    packet-mark=siswa passthrough=yes
5       add chain=forward src-address=192.168.3.0/24 action=mark-packet new-
    packet-mark=cctv-update passthrough=yes
6
```

– Prioritas dan Limit Rate pada Masing-masing Queue

  Setelah menandai paket, kita dapat membuat Queue Tree dengan prioritas dan batas kecepatan sebagai berikut:

```
1       /queue tree
2       add name=parent-queue parent=global max-limit=100M
3
4       add name=e-learning parent=parent-queue packet-mark=e-learning limit-
    at=40M max-limit=40M priority=1
5       add name=guru-staf parent=parent-queue packet-mark=guru-staf limit-at
    =30M max-limit=30M priority=2
6       add name=siswa parent=parent-queue packet-mark=siswa limit-at=20M max-
    limit=20M priority=3
7       add name=cctv-update parent=parent-queue packet-mark=cctv-update limit
    -at=10M max-limit=10M priority=4
8
```

  Referensi:

  ISPBill’s, “Traffic base priority via Queue Tree in Mikrotik,” ISPBill’s Help Center. [Online].

Available: https://help.ispbills.com/hc/en-us/articles/360018285880-Traffic-base-priorit
[Accessed: Jun. 4, 2025].