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

Laporan Sementara
Praktikum Jaringan Komputer

Tunelling dan IPsec

Salman Al Ghifary - 5024221003

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital saat ini, keamanan dan efisiensi jaringan menjadi kebutuhan utama. Praktikum ini membahas tunneling sebagai metode pengiriman data antar jaringan berbeda, serta IPSec untuk menjamin keamanan data melalui enkripsi. Selain itu, dipelajari juga pengelolaan bandwidth menggunakan Simple Queue dan Queue Tree, serta pengaturan prioritas trafik agar layanan penting tetap berjalan lancar. Praktikum ini penting untuk memahami cara kerja jaringan modern yang aman dan efisien.

1.2 Dasar Teori

Tunneling dalam jaringan komputer adalah sebuah metode untuk mengirimkan data dari satu jaringan ke jaringan lain dengan melewati jalur atau protokol yang berbeda. Ibaratnya seperti membuat terowongan digital yang memungkinkan data bergerak melewati media yang tidak secara langsung kompatibel dengan format aslinya. Dalam proses ini, data dari satu komputer dibungkus ke dalam format tertentu (disebut encapsulation) agar bisa melewati jaringan perantara, lalu dibuka kembali setelah mencapai tujuan. Contohnya adalah ketika dua komputer yang menggunakan jaringan Ethernet ingin berkomunikasi namun harus melewati jaringan WAN; data dari komputer pengirim akan dibungkus terlebih dahulu dengan format yang dimengerti oleh WAN, kemudian dibuka lagi di jaringan penerima. Teknologi tunneling ini didukung oleh berbagai protokol, masing-masing memiliki fungsi dan keunggulan yang berbeda. GRE (Generic Routing Encapsulation) adalah protokol yang membungkus paket IP dengan header tambahan. IPSec (Internet Protocol Security) merupakan protokol yang lebih aman karena menggunakan enkripsi dan autentikasi untuk menjaga keamanan data. Ada juga protokol lain seperti IP-in-IP yang membungkus paket IP ke dalam IP lainnya secara sederhana, SSH untuk akses aman jarak jauh, serta PPTP, SSTP, dan L2TP yang banyak digunakan dalam implementasi VPN. Di lingkungan virtualisasi dan data center, protokol seperti VXLAN memungkinkan terbentuknya jaringan virtual yang seolah-olah menyatu, meskipun secara fisik berjauhan. SSL Tunneling merupakan pendekatan lain dalam pengiriman data secara aman melalui internet. Dalam hal ini, data yang terenkripsi menggunakan SSL dikirim melalui perantara (seperti proxy) yang hanya meneruskan data tanpa bisa mengakses isinya. Metode ini menjaga privasi dan keamanan komunikasi antara client dan server. Salah satu protokol penting dalam keamanan jaringan adalah IPSec. Protokol ini berfungsi sebagai pengaman data yang dikirim melalui jaringan publik seperti internet, dengan cara mengenkripsi data agar tidak dapat dibaca atau dimanipulasi oleh pihak tidak berwenang. IPSec tidak hanya mengenkripsi data, tetapi juga memverifikasi integritas dan keasliannya melalui proses autentikasi. Teknologi ini umum digunakan dalam VPN (Virtual Private Network), yang memungkinkan pengguna mengakses jaringan perusahaan dari lokasi lain secara aman. Dalam penerapannya, IPSec memiliki fitur-fitur utama seperti autentikasi pengirim data, enkripsi untuk menjaga kerahasiaan informasi, serta integritas untuk memastikan data tidak berubah selama proses transmisi. IPSec juga mendukung manajemen kunci, yaitu proses untuk mengatur dan menyepakati kunci rahasia yang digunakan selama koneksi berlangsung. Dua mode operasi yang tersedia adalah tunnel mode dan transport mode, di mana keduanya memiliki pendekatan berbeda dalam membungkus paket data. Tunnel mode umumnya digunakan untuk koneksi antar jaringan, sedangkan transport mode lebih cocok untuk komunikasi antar perangkat. Meskipun menawarkan tingkat keamanan yang tinggi, IPSec

juga memiliki kekurangan, seperti kebutuhan konfigurasi yang rumit dan penggunaan sumber daya yang cukup besar karena proses enkripsi dan dekripsi. Namun, fleksibilitas dan kompatibilitasnya dengan banyak perangkat dan sistem membuat IPSec menjadi solusi ideal untuk skala jaringan yang luas.

2 Tugas Pendahuluan

2.1. 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)
  - IKE Phase 1 (Main Mode atau Aggressive Mode): Tujuan utama IKE Phase 1 adalah membangun saluran komunikasi yang aman (secure tunnel) antara dua peer IPSec untuk pertukaran informasi sensitif yang akan datang. Ini menghasilkan satu bidirectional SA yang disebut IKE SA atau ISAKMP SA.
    1. Negosiasi Kebijakan IKE: Kedua peer setuju pada metode enkripsi (misalnya, AES-256), algoritma hashing (misalnya, SHA-256), metode autentikasi (misalnya, pre-shared key atau sertifikat), dan grup Diffie-Hellman (DH) untuk pertukaran kunci.
    2. Pertukaran Diffie-Hellman: Menggunakan grup DH yang disepakati, kedua peer menghasilkan kunci rahasia bersama tanpa pernah mengirimkannya melalui jaringan. Ini menciptakan shared secret key yang akan digunakan untuk mengamankan komunikasi IKE Phase 1.
    3. Autentikasi: Peer mengautentikasi satu sama lain menggunakan metode yang disepakati (pre-shared key atau sertifikat digital) untuk memastikan bahwa mereka berkomunikasi dengan pihak yang sah.

    Output: Sebuah ISAKMP SA yang telah diautentikasi dan terenkripsi, yang akan digunakan untuk melindungi pesan-pesan IKE Phase 2.
  - IKE Phase 2 (Quick Mode):

    Tujuan utama IKE Phase 2 adalah membangun SAs untuk data IPSec itu sendiri. Ini menghasilkan satu atau dua unidirectional IPSec SA (satu untuk setiap arah komunikasi).
    1. Negosiasi Kebijakan IPSec: Dalam saluran aman yang dibangun di IKE Phase 1, kedua peer menegosiasikan parameter untuk IPSec SA, termasuk protokol IPSec (AH atau ESP), algoritma enkripsi (jika menggunakan ESP), algoritma hashing, dan lifetime SA.
    2. Pertukaran Nonce: Nonce adalah angka acak yang digunakan untuk memastikan replay protection dan liveliness dari pertukaran kunci.
    3. Pertukaran Identitas (opsional): Peer dapat bertukar informasi identitas (misalnya, subnet yang diizinkan untuk melewati VPN).
    4. Generasi Kunci Anak: Kunci IPSec untuk enkripsi dan autentikasi lalu lintas data dihasilkan dari shared secret key yang dibuat di Phase 1 dan Nonce yang ditukarkan.

    Output: Satu atau lebih IPSec SA yang digunakan untuk melindungi lalu lintas data aktual (enkripsi dan/atau autentikasi). Jika menggunakan Perfect Forward Secrecy (PFS), IKE

Phase 2 akan melakukan pertukaran DH baru untuk setiap SA yang baru, memastikan bahwa kompromi satu kunci tidak akan membahayakan kunci-kunci sebelumnya atau yang akan datang.

- Parameter keamanan yang harus disepakati (algoritma enkripsi, metode autentikasi, lifetime key)

  1. Algoritma Enkripsi: Digunakan untuk menjaga kerahasiaan data. Contoh:
     - DES (Data Encryption Standard): Usang, tidak direkomendasikan.
     - 3DES (Triple DES): Lebih aman dari DES, namun relatif lambat.
     - AES (Advanced Encryption Standard): Saat ini merupakan standar emas, tersedia dalam ukuran kunci 128, 192, atau 256 bit (AES-128, AES-192, AES-256). Direkomendasikan.
  2. Metode Autentikasi: Digunakan untuk memastikan integritas data dan autentikasi pengirim. Contoh:
     - MD5 (Message Digest 5): Usang, tidak direkomendasikan karena rentan terhadap serangan kolisi.
     - SHA-1 (Secure Hash Algorithm 1): Juga memiliki kerentanan, meskipun lebih baik dari MD5. Tidak direkomendasikan untuk aplikasi baru.
     - SHA-2 (Secure Hash Algorithm 2): Keluarga SHA-2 mencakup SHA-256, SHA-384, dan SHA-512. Saat ini direkomendasikan untuk integritas data.
  3. Lifetime Key : Durasi waktu atau jumlah data yang boleh melewati Security Association (SA) sebelum perlu dinegosiasikan ulang. Ini adalah mekanisme keamanan untuk membatasi jumlah data yang dapat diakses jika kunci terkompromi.
     - Lifetime Time: Biasanya dalam detik
     - Lifetime Volume: Dalam Kilobyte atau Megabyte
     - Ketika lifetime hampir habis, proses rekeying otomatis akan terjadi untuk membuat SA baru.

- Konfigurasi sederhana pada sisi router untuk memulai koneksi IPSec site-to-site

  1. Topologi
     - Site A : LAN: 192.168.1.0/24, WAN: 203.0.113.1
     - Site B : LAN: 192.168.2.0/24, WAN: 203.0.113.2
  2. site A

     /ip ipsec peer add address=203.0.113.2/32
     exchange-mode=main
     secret="vpn123"
     dh-group=modp2048
     enc-algorithm=aes-256
     hash-algorithm=sha256
     generate-policy=no
     /ip ipsec proposal set [find default=yes]

enc-algorithms=aes-256-cbc
auth-algorithms=sha256
lifetime=1h
pfs-group=modp2048
/ip ipsec policy add
src-address=192.168.1.0/24
dst-address=192.168.2.0/24
sa-src-address=203.0.113.1
sa-dst-address=203.0.113.2
tunnel=yes
action=encrypt
proposal=default
/ip firewall filter add
chain=input
protocol=udp
dst-port=500,4500
action=accept
/ip firewall filter add
chain=input
protocol=ipsec-esp
action=accept
/ip firewall nat add
chain=srcnat
action=masquerade
out-interface=ether1
src-address=192.168.1.0/24
dst-address=!192.168.2.0/24

3. site B

/ip ipsec peer add
address=203.0.113.1/32
exchange-mode=main
secret="vpn123"
dh-group=modp2048
enc-algorithm=aes-256
hash-algorithm=sha256
generate-policy=no
/ip ipsec proposal set [find default=yes]
enc-algorithms=aes-256-cbc
auth-algorithms=sha256
lifetime=1h

pfs-group=modp2048
/ip ipsec policy add
src-address=192.168.2.0/24
dst-address=192.168.1.0/24
sa-src-address=203.0.113.2
sa-dst-address=203.0.113.1
tunnel=yes
action=encrypt
proposal=default
/ip firewall filter add
chain=input
protocol=udp
dst-port=500,4500
action=accept
/ip firewall filter add
chain=input
protocol=ipsec-esp
action=accept
/ip firewall nat add
chain=srcnat
action=masquerade
out-interface=ether1
src-address=192.168.2.0/24 dst-address=!192.168.1.0/24

Tanenbaum, Andrew S., Wetherall, David J. Jaringan Komputer. Edisi Bahasa Indonesia.
https://www.cloudaja.id/artikel/tutorial-vpn-mikrotik-site-to-site/
https://citraweb.com/artikel/372/

2.2. Skema Queue Tree.

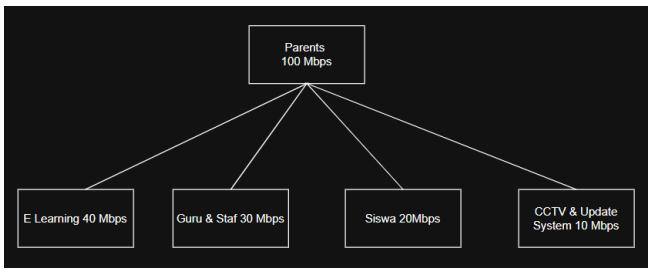
Sebuah sekolah memiliki bandwidth internet 100 Mbps yang dibagi menjadi:

- 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

2.2.1 Gambar Queue Tree

2.2.2 Marking

1. E-Learninh



Gambar 1: Skema Queue Tree

- Chain: forward
- Address: IP server LMS / domain LMS
- Action: mark-connection → conn-elearning

2. Guru dan Staff
   - Chain: forward
   - Address: IP pool guru dan staf
   - Action: mark-connection → conn-guru
3. Siswa
   - Chain: forward
   - Address: IP pool siswa
   - Action: mark-connection → conn-siswa
4. CCTV dan Update System
   - Chain: forward
   - Address: IP DVR, NTP server, Windows update domain
   - Action: mark-connection → conn-cctv

2.2.3 Konfigurasi Queue Tree

/queue tree

add name="e-learning" parent=global packet-mark=pkt-elearning max-limit=40M priority=1

add name="guru-staf" parent=global packet-mark=pkt-guru max-limit=30M priority=2

add name="siswa" parent=global packet-mark=pkt-siswa max-limit=20M priority=3

add name="cctv-update" parent=global packet-mark=pkt-cctv max-limit=10M priority=4

Referensi

https://www.youtube.com/watch?v=L-LWTQWOBa8

https://wiki.mikrotik.com/Manual:Queue