BAB II
TINJAUAN PUSTAKA DAN DASAR TEORI

2.1. Tinjauan Pustaka

Dalam rangka memperoleh pemahaman yang komprehensif tentang implementasi Layer 2 Tunneling Protocol (L2TP) dalam interkoneksi Site to Site untuk mengamankan koneksi dari serangan Man-in-the-Middle (MITM), beberapa sumber pustaka yang relevan telah ditinjau. Berikut adalah tinjauan pustaka terhadap tiga sumber yang menjadi acuan dalam penelitian ini.

Hedy Pratama, Nila Feby Puspitasari. (2020) Analisis dan Penerapan Layer 2 Tunneling Protocol (L2TP) pada Jaringan VPN (Virtual Private Network)"
[https://citec.amikom.ac.id/main/index.php/citec/article/view/253/171]

Artikel jurnal ini membahas tentang analisis dan penerapan Layer 2 Tunneling Protocol (L2TP) pada jaringan Virtual Private Network (VPN). Dalam penelitian ini, penulis melakukan analisis terhadap kinerja dan keamanan L2TP sebagai protokol tunneling dalam menghubungkan jaringan VPN. Hasil analisis menunjukkan bahwa L2TP memiliki kinerja yang baik dalam memfasilitasi komunikasi antar host dan memungkinkan penggunaan VPN secara aman. Referensi ini relevan dengan skripsi yang sedang dibahas karena membahas tentang penggunaan L2TP dalam koneksi VPN, meskipun dalam konteks yang berbeda.

Ikhsan, D., Mulyanto, H., & Hidayat, R. (2016). Penerapan L2TP/IPsec VPN Site to Site pada Jaringan E-Learning STMIK AMIKOM Purwokerto. Oktal Jurnal Informatika, 4(1), 21-28.
[https://journal.mediapublikasi.id/index.php/oktal/article/view/893/584]

Artikel dari Oktal Jurnal Informatika 2016, membahas tentang penerapan L2TP/IPsec VPN Site to Site pada jaringan e-learning. Artikel ini menjelaskan tentang penerapan L2TP/IPsec dalam konteks jaringan Site to Site secara praktis. Artikel ini digunakan sebagai referensi untuk memperoleh wawasan mengenai pengalaman praktis dalam mengimplementasikan L2TP/IPSec dalam konteks Site to Site VPN.

Rahmayuni, A. D., Syaefullah, M., & Firdaus, R. (2020). Implementasi L2TP/IPSec (Layer 2 Tunneling Protocol/Internet Protocol Security) pada Interkoneksi Jaringan Site to Site untuk Meningkatkan Keamanan Jaringan. Jurnal Komunikasi dan Teknologi Informasi (J-Komtekinfo), 5(1), 30-38. [https://jkomtekinfo.org/ojs/index.php/komtekinfo/article/view/128/124]

Artikel dari Jurnal Komunikasi dan Teknologi Informasi (J-Komtekinfo) 2020, membahas implementasi L2TP/IPSec dalam interkoneksi jaringan Site to Site untuk meningkatkan keamanan jaringan. Artikel ini memberikan penjelasan tentang konfigurasi dan pengaturan L2TP/IPSec dalam konteks Site to Site VPN. Artikel ini digunakan sebagai referensi untuk memperoleh pemahaman lebih lanjut tentang langkah-langkah implementasi L2TP/IPSec dan manfaatnya dalam meningkatkan keamanan koneksi Site to Site.

Wijaya, I. G., Saputra, I. A., & Jayadi, K. (2017). Rancang Bangun Site To Site VPN Menggunakan L2TP/IPSec Pada Jaringan Statis. Prosiding Seminar Nasional Teknologi Informasi dan Multimedia (SNASTIA) 2017. [http://repository.unsri.ac.id/23265/1/senoprosiding.pdf]

Artikel dari Prosiding Seminar Nasional Teknologi Informasi dan Multimedia (SNASTIA) 2017, membahas tentang rancang bangun jaringan Site to Site VPN menggunakan L2TP/IPSec dalam konteks jaringan statis. Artikel ini memberikan gambaran tentang implementasi L2TP/IPSec sebagai

solusi keamanan dalam interkoneksi Site to Site. Dalam penelitian ini, artikel ini digunakan sebagai referensi untuk memperoleh pemahaman awal tentang konsep implementasi L2TP dalam konteks interkoneksi Site to Site.

Dengan tinjauan pustaka terhadap sumber-sumber tersebut, penelitian ini dapat memperoleh landasan teoritis yang solid untuk melaksanakan implementasi L2TP dalam interkoneksi Site to Site sebagai langkah untuk mengamankan koneksi dari serangan MITM.

2.2. Dasar Teori

Dalam penelitian ini, terdapat beberapa dasar teori yang relevan untuk memahami implementasi Layer 2 Tunneling Protocol (L2TP) dalam interkoneksi Site to Site dalam konteks mengamankan koneksi dari serangan Man-in-the-Middle (MITM).

1. L2TP adalah protokol tunneling yang digunakan untuk mengirimkan data melalui jaringan IP. Protokol ini bekerja pada lapisan 2 dalam model referensi OSI (Open Systems Interconnection) dan dapat digunakan untuk menghubungkan jaringan remote atau cabang dengan jaringan pusat. L2TP memiliki kemampuan untuk mengenkapsulasi protokol jaringan lainnya, seperti IP, IPX, atau NetBIOS, dalam sebuah tunnel yang diamankan.

2. Man in the Middle Attack atau yang disingkat MitM adalah salah satu jenis cyber attack yang menyusup ke dalam jaringan dan menyadap komunikasi yang sedang berlangsung antara pengguna jaringan dan web server tujuan. Serangan Man-in-the-Middle (MITM) terjadi ketika seorang penyerang mengintersepsi komunikasi antara dua entitas yang

berkomunikasi, dan dapat memodifikasi atau mencuri informasi yang dikirimkan. Penyerang ini memposisikan dirinya di tengah-tengah komunikasi dan sering kali menggunakan teknik seperti perekaman lalu lintas jaringan, pemalsuan identitas, atau serangan sniffing untuk mencapai tujuan mereka. Serangan MITM mengancam keamanan dan kerahasiaan data yang dikirimkan melalui koneksi Site to Site.

3. IPSec adalah seperangkat aturan atau protokol komunikasi untuk mengatur koneksi aman melalui jaringan. Protokol Internet (IP) adalah standar umum yang menentukan bagaimana data berjalan melalui internet. IPSec digunakan untuk mengamankan koneksi Site to Site dari serangan MITM, penggunaan IPSec (Internet Protocol Security) sering kali diterapkan bersama dengan L2TP. IPSec adalah sebuah protokol keamanan yang menyediakan mekanisme enkripsi, autentikasi, dan integritas data dalam lalu lintas IP. Dengan menggabungkan L2TP dan IPSec, koneksi Site to Site dapat diamankan melalui enkripsi data yang dikirimkan antara kedua ujung koneksi.

4. IP public adalah alamat IP yang digunakan umum dalam jaringan yang tanpa batas. IP public digunakan oleh semua perangkat keras agar dapat mengakses sumber dari internet. Pada implementasi L2TP IP Public digunakan untuk parameter akses L2TP client ke L2TP Server apabila konteksnya berbeda provider maka IP Public ini menjadi penting, Namun apabila L2TP di gunakan pada provider yang sama IP Public tidak lagi menjadi hal yang penting , IP Public bisa digantikan dengan IP Private Asalkan kedua host (L2TP client dan L2TP server) dapat saling berkomunikasi secara TCP/IP.

5. AES-192 CBC:

   AES (Advanced Encryption Standard): AES adalah algoritma enkripsi

simetris yang menggunakan blok cipher dengan panjang 192-bit kunci. Algoritma ini bekerja dengan membagi data menjadi blok-blok 128-bit dan mengenkripsi setiap blok secara terpisah. CBC (Cipher Block Chaining): Mode operasi CBC menggabungkan setiap blok teks terbuka dengan blok teks terenkripsi sebelumnya sebelum melakukan enkripsi. Hal ini memungkinkan untuk menciptakan dependensi antar blok, sehingga mempersulit analisis statistik.

6. AES-256 CBC:

   AES (Advanced Encryption Standard): AES-256 menggunakan kunci 256-bit dan merupakan varian AES yang paling kuat. Kunci yang lebih panjang meningkatkan tingkat keamanan enkripsi. CBC (Cipher Block Chaining): Mode operasi CBC digunakan bersama dengan AES-256 untuk mengenkripsi data dalam blok-blok. Seperti pada AES-192 CBC, setiap blok teks terbuka digabungkan dengan blok teks terenkripsi sebelumnya sebelum dienkripsi.

Dengan pemahaman dasar teori ini, akan memungkinkan pemahaman yang lebih mendalam tentang konsep, mekanisme, dan metode yang terlibat dalam implementasi L2TP dalam interkoneksi Site to Site sebagai upaya untuk mengamankan koneksi dari serangan MITM.

Tabel 2.1 Daftar Jurnal yang di Review

Jurnal	Protokol	Metode Pengujian
http://repository.unsri.ac.id/23265/1/senoprosiding.pdf	L2TP, PPTP	Komparasi performa jaringan menggunakan L2TP dan PPTP
https://jkomtekinfo.org/ojs/index.php/komtekinfo/article/view/128/124	L2TP	Packet Loss Test dan DoS Test
https://journal.mediapublikasi.id/index.php/oktal/article/view/893/584	L2TP	Packet Sniffing Test

https://citec.amikom.ac.id/main/index.php/citec/article/view/253	L2TP	Port Forwarding