BAB I
PENDAHULUAN

1.1. Latar Belakang

Dalam era globalisasi dan perkembangan teknologi informasi yang pesat, interkoneksi jaringan menjadi semakin penting untuk mendukung operasional organisasi, perusahaan, dan institusi. Interkoneksi jaringan ini memungkinkan berbagai lokasi atau cabang dalam suatu organisasi untuk terhubung secara efisien dan berkomunikasi antar host untuk berbagi data dan sumber daya. Salah satu metode yang umum digunakan untuk interkoneksi jaringan adalah melalui koneksi Site to Site.

Interkoneksi Site to Site adalah koneksi jaringan yang menghubungkan dua atau lebih jaringan lokal (LAN) pada lokasi yang berbeda melalui jaringan publik atau internet. Koneksi ini memungkinkan data dan informasi untuk dikirim dan diterima antara lokasi tersebut dengan cepat dan aman. Namun, dengan semakin meningkatnya ancaman keamanan siber, seperti serangan Man-in-the-Middle (MITM), keamanan interkoneksi Site to Site menjadi semakin penting untuk melindungi integritas dan kerahasiaan data.

Serangan Man-in-the-Middle (MITM) merupakan salah satu serangan keamanan yang paling umum dan berbahaya dalam jaringan. Pada serangan ini, seorang penyerang memposisikan diri di tengah-tengah komunikasi antara dua pihak yang berkomunikasi dan dapat mencuri, memodifikasi, atau menyadap data yang dikirimkan. Penyerang ini melakukan aksi tanpa sepengetahuan kedua pihak yang berkomunikasi, sehingga mereka tidak menyadari bahwa data mereka telah disusupi atau dimanipulasi.

Dalam konteks interkoneksi Site to Site, serangan MITM dapat menyebabkan kerugian serius bagi organisasi atau perusahaan. Informasi

rahasia, seperti data pelanggan, keuangan, atau strategi bisnis, dapat dicuri dan digunakan dengan tujuan jahat. Selain itu, manipulasi data dalam koneksi Site to Site dapat mengakibatkan kerusakan pada integritas data dan dapat menyebabkan kerugian finansial, reputasi, dan kepercayaan pelanggan.

Oleh karena itu, perlindungan terhadap serangan MITM dan keamanan interkoneksi Site to Site menjadi hal yang sangat penting. Saat ini, ada berbagai metode dan protokol keamanan yang dapat digunakan untuk mengamankan koneksi Site to Site, salah satunya adalah Layer 2 Tunneling Protocol (L2TP).

Layer 2 Tunneling Protocol (L2TP) adalah protokol tunneling yang beroperasi pada lapisan 2 model referensi OSI (Open Systems Interconnection). L2TP memungkinkan data untuk dikirimkan melalui jaringan publik dengan aman dan efisien. Protokol ini bekerja dengan mengenkapsulasi protokol jaringan lainnya, seperti IP, IPX, dan NetBIOS, dalam sebuah tunel yang diamankan. Dengan menggunakan L2TP, koneksi Site to Site dapat dijamin keamanannya dan melindungi dari serangan MITM.

Namun, meskipun L2TP menawarkan berbagai keunggulan dalam mengamankan koneksi Site to Site, implementasinya juga memiliki tantangan dan kelemahan. Beberapa masalah yang mungkin timbul meliputi konfigurasi yang rumit, pengaturan yang kompleks, dan kinerja jaringan yang terpengaruh. Oleh karena itu, diperlukan penelitian dan eksperimen lebih lanjut untuk memahami secara menyeluruh tentang implementasi L2TP dalam konteks interkoneksi Site to Site.

Dalam penelitian ini, bertujuan untuk menyelidiki dan menganalisis implementasi L2TP dalam interkoneksi Site to Site sebagai langkah untuk berkomunikasi antar host dan mengamankan koneksi dari serangan MITM. Penelitian ini bertujuan untuk mengidentifikasi perbedaan hasil dari traffic analyzer dari sisi penyerang MITM ketika host berkomunikasi menggunakan

protokol L2TP dan ketika host berkomunikasi tanpa menggunakan protokol L2TP. Selain itu, Penelitian ini juga akan mengidentifikasi perbedaan hasil traffic analyzer dari sisi penyerang MITM ketika koneksi L2TP dienkripsi menggunakan algoritma enkripsi AES-192 CBC pada fitur IPSec (Internet Protocol Security) Mikrotik dan ketika koneksi L2TP dienkripsi menggunakan algoritma enkripsi AES-256 CBC pada fitur IPSec Mikrotik.

Melalui pengujian dan eksperimen ini, Diharapkan dapat memberikan pemahaman yang lebih mendalam tentang efektivitas dan kekuatan enkripsi dalam melindungi koneksi Site to Site dari serangan MITM. Hasil penelitian ini diharapkan dapat memberikan panduan yang berguna bagi para praktisi jaringan dalam memilih solusi keamanan yang tepat untuk melindungi koneksi Site to Site mereka.

Dengan pemahaman yang lebih baik tentang implementasi L2TP dalam konteks interkoneksi Site to Site, diharapkan keamanan dan integritas data dalam koneksi tersebut dapat dijaga dengan lebih baik. Dengan demikian, organisasi dan perusahaan dapat melaksanakan operasional mereka dengan lebih tenang dan fokus tanpa terganggu oleh potensi serangan keamanan.

1.2.Rumusan Masalah

Dalam konteks implementasi L2TP dalam interkoneksi site-to-site, terdapat sejumlah permasalahan yang perlu diidentifikasi dan dijawab. Dalam penelitian ini, rumusan masalah yang diajukan adalah sebagai berikut:

1. Bagaimana keamanan komunikasi antara Branch yang terhubung dapat ditingkatkan melalui implementasi L2TP Mikrotik dalam interkoneksi site-to-site ketika terdapat serangan MITM

2. Bagaimana Implementasi L2TP Mikrotik dalam Interkoneksi site to site dapat mempengaruhi transmisi data antar branch / device

3. Bagaimana konfigurasi dan manajemen infrastruktur jaringan dapat mempengaruhi keberhasilan implementasi L2TP dalam interkoneksi site-to-site

Dengan merumuskan masalah-masalah diatas, penelitian ini bertujuan untuk menyelidiki implementasi L2TP dalam konteks interkoneksi site-to-site dengan fokus pada melindungi koneksi dari serangan MITM. Diharapkan bahwa hasil penelitian ini akan memberikan pemahaman yang lebih baik tentang keefektifan dan keefisienan implementasi L2TP dalam melindungi koneksi dari serangan MITM, serta memberikan rekomendasi yang berguna bagi organisasi dan perusahaan dalam mengoptimalkan penggunaan L2TP untuk tujuan keamanan dalam interkoneksi site-to-site mereka.

1.3.Ruang lingkup

Ruang lingkup penelitian ini mencakup beberapa aspek terkait implementasi L2TP dalam interkoneksi Site to Site dalam konteks untuk mengamankan koneksi dari serangan Man-in-the-Middle (MITM). Adapun batasan-batasan yang akan diterapkan dalam penelitian ini adalah sebagai berikut:

1. Fokus penelitian akan difokuskan pada penggunaan protokol Layer 2 Tunneling Protocol (L2TP) Mikrotik dalam interkoneksi Site to Site. Penelitian ini tidak akan membahas protokol lainnya yang dapat digunakan untuk tujuan yang serupa.

2. Penjelasan terkait konfigurasi hanya berfokus pada parameter yang dibutuhkan dalam penelitian ini, Konfigurasi yang tidak dibutuhkan dalam penelitian ini atau sifatnya opsional tidak akan menjadi fokus dalam pembahasan.

3. Penelitian akan berfokus pada implementasi L2TP dengan menggunakan algoritma enkripsi aes-192 cbc dan aes-256 cbc dari IPSec (Internet Protocol Security) yang sudah terdapat pada fitur Mikrotik untuk mengamankan koneksi dari serangan MITM. Implementasi L2TP tanpa penggunaan IPSec dan selain menggunakan algoritma enkripsi aes-192 cbc dan aes-256 cbc tidak akan menjadi fokus penelitian ini.

4. Pengujian pada aspek keamanan penelitian ini hanya berfokus pada hasil dari traffic analyzer wireshark ketika koneksi tanpa protokol L2TP dan koneksi menggunakan protokol L2TP yang dilengkapi dengan algoritma enkripsi aes-192 cbc dari IPSec (Internet Protocol Security) yang sudah terdapat pada fitur Mikrotik dan aes-256 cbc dari IPSec (Internet Protocol Security) yang sudah terdapat pada fitur Mikrotik. Pengujian selain menggunakan traffic analyzer wireshark dan selain menggunakan algoritma enkripsi aes-192 cbc dan aes-256 cbc tidak akan menjadi fokus pada penelitian ini.

5. Pengujian pada aspek kemampuan L2TP Mikrotik hanya berfokus pada pengujian menggunakan tool Ping digunakan menguji komunikasi menggunakan besaran packet tertentu, Traceroute untuk memvalidasi bahwasanya komunikasi sudah menggunakan Layer 2 dari koneksi L2TP, Telnet untuk melakukan pengujian komunikasi TCP/IP. pengujian selain menggunakan tool Ping, Traceroute, dan Telnet tidak akan menjadi fokus dalam penelitian ini.

6. Evaluasi kinerja, pengujian, dan efektivitas solusi implementasi L2TP dalam interkoneksi Site to Site akan dilakukan melalui pengujian dan eksperimen di lingkungan laboratorium. Namun, penelitian ini tidak akan membahas implementasi secara langsung di lingkungan produksi yang kompleks.

Dengan batasan-batasan diatas, penelitian ini diharapkan dapat memberikan pemahaman yang jelas dan terfokus tentang implementasi L2TP dalam interkoneksi Site to Site sebagai langkah untuk mengamankan koneksi dari serangan MITM. Penelitian ini juga akan memberikan evaluasi kinerja dan efektivitas solusi yang diusulkan serta memberikan wawasan tentang praktik keamanan tambahan yang dapat diterapkan untuk meningkatkan keamanan jaringan secara menyeluruh dalam konteks khusus implementasi L2TP.

1.4. Tujuan Penelitian

Penelitian ini mempunyai beberapa tujuan mulai untuk kebutuhan identifikasi pengujian dan analisa. Beberapa Tujuan dari penelitian ini sebagai berikut:

1. Mengidentifikasi perbedaan hasil traffic analyzer dari sisi Penyerang MITM ketika host berkomunikasi menggunakan protokol L2TP dan hasil traffic analyzer ketika host berkomunikasi tidak menggunakan protokol L2TP.

2. Mengidentifikasi perbedaan traffic analyzer dari sisi penyerang MITM ketika koneksi L2TP di enkripsi menggunakan algoritma enkripsi aes-192 cbc pada fitur IPSec (Internet Protocol Security) Mikrotik dan ketika koneksi L2TP di enkripsi menggunakan algoritma enkripsi aes-256 cbc pada fitur IPSec (Internet Protocol Security) Mikrotik

3. Menguji kapasitas L2TP ketika digunakan untuk komunikasi antar host menggunakan besaran packet tertentu dan menggunakan protokol tertentu sehingga dapat digunakan untuk bahan analisa.

Melalui pencapaian tujuan-tujuan ini, penelitian ini diharapkan dapat memberikan kontribusi terhadap pemahaman tentang penggunaan L2TP dalam konteks interkoneksi Site to Site dan memberikan panduan yang berguna bagi para praktisi jaringan dalam mengamankan koneksi dari serangan MITM.

1.5. Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat yang signifikan dalam beberapa aspek.

1. Memberikan pemahaman yang lebih jelas tentang pengaruh penggunaan L2TP terhadap keamanan koneksi dan kemungkinan serangan MITM. Hal ini berkorelasi dengan tujuan penelitian pada point Identifikasi Perbedaan Hasil Traffic Analyzer dari Sisi Penyerang MITM.

2. Memberikan informasi tentang performa dan efisiensi L2TP dalam kondisi khusus, sehingga dapat menjadi bahan analisis yang relevan bagi para praktisi jaringan. Hal ini berkorelasi dengan tujuan penelitian pada point pengujian Kapasitas L2TP untuk Koneksi Antara Host dengan Besaran Packet dan Protokol Tertentu.

Dengan manfaat-manfaat tersebut, diharapkan penelitian ini dapat memberikan kontribusi dalam pengembangan dan implementasi solusi keamanan yang efektif dalam interkoneksi Site to Site. Manfaat ini akan membantu dalam memastikan integritas, kerahasiaan, dan ketersediaan data yang dikirim melalui koneksi tersebut, serta melindungi organisasi dari potensi serangan MITM dan kerugian yang mungkin terkait dengan serangan tersebut.