Implementasi dan analisa kinerja keamanan jaringan data center berbasis VXLAN yang diintegrasikan dengan l2TPV3 dan ipsec = implementation and analysis of data center network security performance based on VXLAN integrated with l2TPV3 and ipsec

Arfan Efendi, author

Abstrak

Di era digital yang berkembang pesat, kebutuhan akan infrastruktur jaringan data center yang aman dan efisien menjadi semakin penting. Penggunaan Virtual Extensible LAN (VXLAN) dalam data center menawarkan skala dan fleksibilitas, tetapi tantangan muncul dalam menjaga keamanan data yang sensitif, terutama saat data ditransmisikan melalui jaringan yang tidak terpercaya atau terbuka. Tujuan penelitian ini adalah untuk mengembangkan dan mengevaluasi kinerja infrastruktur data center berbasis VXLAN yang diintegrasikan dengan protokol L2TPV3 dan IPsec yang bertujuan untuk meningkatkan keamanan. Metode yang diterapkan meliputi konfigurasi VXLAN yang diintegrasikan dengan L2TPV3 dan IPsec dalam lingkungan jaringan yang disimulasikan menggunakan EVE-NG. Penelitian juga memanfaatkan otomatisasi dengan Python, Ansible, dan Git untuk efisiensi
konfigurasi dan manajemen jaringan. Pengujian dilakukan pada berbagai skenario, serta evaluasi kinerja jaringan dengan menggunakan dua perbandingan MTU untuk pengetesan latensi dan rata-rata RTT. Hasil dari pengujian mengindikasikan penambahan overhead pada waktu RTT rata-rata sebesar 4 ms untuk MTU standar dan 2000 byte, serta kenaikan sebesar 3 ms untuk MTU 1500 byte. Sementara untuk MTU yang lebih besar, yaitu 3000 byte dan 4000 byte, kenaikan RTT rata-rata lebih signifikan, yakni sekitar 4 ms dan 8 ms, berturut-turut. Temuan ini menyarankan bahwa MTU 1500 byte bisa menjadi pilihan yang lebih optimal, karena mencatatkan nilai RTT yang lebih stabil dan rendah dibandingkan dengan ukuran MTU yang lebih besar. Berdasarkan hasil penelitian, MTU 2000 byte menghasilkan kinerja yang tidak berbeda dengan MTU 1500 byte sehingga membuktikan MTU 2000 byte menjadi pilihan yang aman untuk implementasi metode yang diusulkan pada jumbo frame. Data yang diperoleh menunjukkan bahwa integrasi L2TPV3 dan IPsec dapat melindungi paket menggunakan enkripsi dan berhasil di integrasikan dengan teknologi VXLAN. Hal ini terbukti dari hasil pengujian kinerja dan analisis paket, di mana data yang ditransmisikan melalui jalur yang dilindungi IPsec menunjukkan keamanan yang lebih baik dibandingkan dengan jalur tanpa IPsec. Selain itu, implementasi otomatisasi berhasil melakukan efisiensi terhadap pekerjaan konfigurasi VXLAN yang berulang. VXLAN dengan L2TPv3 dan IPSEC menyediakan solusi yang efektif dalam meningkatkan keamanan data center. Temuan ini membuka peluang untuk penerapan infrastruktur jaringan yang lebih aman dalam lingkungan data center modern.

.....In the rapidly evolving digital era, the need for secure and efficient data center network infrastructure is increasingly important. The use of Virtual Extensible LAN (VXLAN) in data centers offers scalability and flexibility, but challenges arise in maintaining the security of sensitive data, especially when transmitted over untrusted or open networks. The purpose of this study is to develop and evaluate the performance of a VXLAN-based data center infrastructure integrated with L2TPV3 and IPsec protocols aimed at enhancing security. The applied methods include the configuration of VXLAN integrated with L2TPV3 and IPsec in a network environment simulated using EVE-NG. The study also leverages automation with Python, Ansible,

and Git for efficient configuration and network management. Testing was conducted across various scenarios, along with network performance evaluation using two MTU sizes for testing latency and average RTT. The results indicate an added overhead of 4 ms for the average RTT for standard and 2000-byte MTUs, and an increase of 3 ms for the 1500-byte MTU. For larger MTUs, specifically 3000 and 4000 bytes, the increase in average RTT is more significant, approximately 4 ms and 8 ms respectively. These findings suggest that a 1500-byte MTU may be a more optimal choice, recording more stable and lower RTT values compared to larger MTU sizes. Based on the research findings, a 2000-byte MTU performs comparably to a 1500-byte MTU, proving to be a safe choice for implementing the proposed method in jumbo frames. The data obtained indicates that the integration of L2TPV3 and IPsec can protect packets using encryption and successfully integrates with VXLAN technology. This is evident from the performance testing and packet analysis results, where data transmitted through IPsec-protected paths shows better security compared to paths without IPsec. Furthermore, the implementation of automation has successfully increased efficiency for repetitive VXLAN configuration tasks. VXLAN with L2TPv3 and IPSec provides an effective solution for enhancing data center security. These findings open up opportunities for the deployment of more secure network infrastructure in modern data center environments.