Universitas Indonesia Library >> UI - Tesis Membership

Evaluasi Performa Jaringan Pusat Data Berbasis Software Defined Networking dengan Model Keamanan Zero Trust Berbasis Micro-segmentation = Performance Evaluation of Data Center Network based on Software Defined Networking using Zero Trust Security Model with Micro-segmentation.

Muhammad Mujib, author

Deskripsi Lengkap: https://lib.ui.ac.id/detail?id=20504875&lokasi=lokal

---

Abstrak

Pusat data merupakan pusat dari berbagai layanan sistem informasi yang saling terhubung satu dengan lainnya yang merupakan interkoneksi antar server ke server, selanjutnya disebut lalu lintas timur-barat, yang memiliki dominasi dari total lalu lintas sebesar 85 persen. Pada umumnya sistem keamanan jaringan pusat data hanya memperhatikan sisi perimeter untuk mencegah serangan eksternal yang datang melalui lalu lintas jaringan yang keluar masuk pusat data yaitu lalu lintas utara-selatan, sedangkan serangan internal yang datang melalui lalu lintas timur-barat terjadi 60 sampai dengan 80 persen dari insiden keamanan pada pusat data. Salah satu cara untuk mengatasi permasalahan tersebut dengan menerapkan model keamanan zero trust berbasis micro-segmentation pada lalu lintas timur-barat. Model keamanan zero trust berpedoman pada prinsip "never trust, always verify", sehingga tidak ada lagi konsep yang terpercaya dan tidak terpercaya pada lalu lintas jaringan. Zero trust menerapkan keamanan dengan konsep tidak tepercaya pada lalu lintas jaringan. Micro-segmentation merupakan salah satu cara untuk menerapkan zero trust dengan membagi jaringan menjadi segmen logical yang lebih kecil untuk membatasi akses lalu lintas jaringan. Pada penelitian ini, performa jaringan pusat data berbasis software defined networking dengan model keamanan zero trust berbasis micro-segmentation dievaluasi menggunakan simulasi testbed Cisco Application Centric Infrastructure dengan melakukan pengukuran terhadap round trip time, jitter, packet loss, port scanning, dan serangan distributed denial of services. Berdasarkan hasil simulasi testbed menunjukkan bahwa micro-segmentation menambah rata-rata round trip time sebesar 4 µs dan jitter sebesar 11 µs tanpa packet loss. Di sisi lain, micro-segmentation berhasil mencegah serangan port scanning dan distributed denial of services, sehingga dengan penerapan model keamanan zero trust berbasis micro-segmentation dapat meningkatkan keamanan tanpa mempengaruhi performa jaringan pusat data secara signifikan.
.....The data center is a resource center that is interconnected with one another, in which intra-data of server-to-server traffic, or so-called east-west traffic, makes a dominant of approximately 85 % of the total traffic. The security of the data center network is carried out on the perimeter side to prevent the external attacks come from the traffic that enters and exits the data center, known as north-south traffic. In contrast, the internal attacks come from the east-west traffic occur of approximately 60 to 80 percent of the incidents-one way to surmount this by implementing the zero trust security model based on micro-segmentation in east-west traffic. Zero trust is a security idea based on the principle of "never trust, always verify" that there are no concepts of trust and untrust in network traffic. The zero trust security model implemented network traffic in the form of untrust. Microsegmentation is a way to achieve zero trust by dividing a network into smaller logical segments to restrict the traffic. In this study, the performance of a data center network based on software defined networking with a zero trust security model based on micro-segmentation was evaluated using a Cisco Application Centric Infrastructure testbed simulation by measuring round trip time, jitter,

packet loss, port scanning, and distributed denial of services attack. Performance evaluation results show that micro-segmentation adds an average round trip time of 4 µs and jitter of 11 µs without packet loss. On the other hand, micro-segmentation has succeeded in preventing port scanning and distributed denial of service attacks so that the security can be improved without significantly affecting network performance on the data center.