Implementasi Sistem Mitigasi Keamanan Port Blocking Dan Sistem Pemantauan Dengan Lapisan Aplikasi Dalam Analisis Arsitektur Data Center Berbasis Software Defined Networking = Implementation of Port Blocking Security Mitigation System and Monitoring System with Application Layer in Analyzing Data Center Architecture Based on Software Defined Networking

Bryan Oliver, author

Abstrak

Penggunaan data center adalah hal yang perlu dilakukan demi mendukung perkembangan data dan informasi yang semakin luas dan terus bertambah. Namun dalam pembuatan dan operasionalnya, data center memiliki berbagai hal yang harus dipikirkan untuk dapat menghindari berbagai gangguan keamanan dan kesalahan yang dapat menyebabkan kerusakan dan ancaman bagi integritas data yang ada. Salah satu serangan yang sangat berbahaya dan umum menyerang data center adalah DDOS atau Distributed Denial Of Service menurut data dari Akamai, bahwa selama tahun 2020 ini DDOS memiliki peningkatan dalam volume serangan dan variasi serangan. Hal inilah yang menjadi alasan pentingnya dalam meningkatkan keamanan jaringan dengan mekanisme yang akurat dan terautomasi dalam meningkatkan efektivitas terutama pada keamanan data center dengan suatu sistem yang memantau alur/flow dalam jaringan dan memungkinkan dilakukannya pemantauan firewall, port, dan konfigurasi keamanan lainnya, untuk meningkatkan jaringan data center yang ada dengan keamanan yang lebih baik. Percobaan komunikasi dengan protocol ICMP menunjukan hasil rata-rata latensi dari tiga percobaan dengan jumlah paket yang berbeda sebesar 0.127 ms pada arsitektur Three Tier dan 0.079 ms pada arsitektur Spine Leaf. Implementasi sistematika controller untuk dapat melakukan port blocking setelah dilakukannya deteksi serangan memiliki akurasi deteksi sebesar 99.72% pada arsitektur Three Tier dan 99.45% pada arsitektur Spine Leaf. Pemanfaatan lapisan aplikasi untuk sistem pemantauan dan konfigurasi keamanan berbasis firewall secara efektif berhasil menunjang arsitektur jaringan Three Tier dan Spine Leaf, di mana penggunaan satu buah controller deteksi yang juga menjalankan fungsi API untuk lapisan aplikasi akan memiliki rata-rata delay sebesar 5.3 detik pada arsitektur Three Tier dan 5.6 detik pada arsitektur Spine Leaf, sedangkan penggunaan dua controller terpisah untuk proses deteksi dan menjalankan API akan mengurangi delay pada arsitektur Three Tier menjadi 0.8 detik dan pada arsitektur Spine Leaf menjadi 1.1 detik

.....The use of data centers is something that needs to be done to support the development of data and information that is increasingly broad and continues to grow. However, in its structure and operation, data centers have various things that must be considered to avoid various security issues and errors that can cause damage and threats to the integrity of existing data. One of the most dangerous and common attacks attacking data centers is DDOS or the Distributed Denial Of Service, according to data from Akamai, during 2020, DDOS had an increase in the volume of attacks and the variety of attacks. This is the reason why it is important to improve network security with an accurate and automated mechanism to increase effectiveness, especially in data center security with a system that monitors the flow in the network and allows monitoring of firewalls, ports, and other security configurations, to improve the existing data center network with better security. The communication experiment with the ICMP protocol shows the average latency of the three

experiments with different packet numbers with 0.127 ms on the Three Tier architecture and 0.079 ms on the Spine Leaf architecture. The implementation to applicate controller systematics to perform port blocking after attack detection has a detection accuracy of 99.72% on Three-Tier architecture and 99.45% on Spine Leaf architecture. Utilization of the application layer for monitoring systems and firewall- based security configurations has effectively succeeded in supporting the Three-Tier and Spine Leaf network architectures, where the use of one detection controller that also performs the API function for the application layer will have an average delay of 5.3 seconds on the Three Tier architecture. and 5.6 seconds on the Spine Leaf architecture, whilst the use of two separate controllers for the detection process and running the API will reduce the delay on the Three Tier architecture to 0.8 seconds and on the Spine Leaf architecture to 1.1 seconds.