Evaluasi perbandingan berbagai metode mitigasi interest flooding attack pada jaringan named data networking menggunakan topologi jaringan rocketfuel = Performance comparison of various interest flooding attack mitigation methods on named data networking networks using rocketfuel topology / Marion Renaldo Rotensulu

Marion Renaldo Rotensulu, author

Abstrak

ABSTRAK
Saat ini, Named Data Networking NDN telah menjadi solusi terobosan dan pilihan potensial untuk arsitektur Internet generasi berikutnya. Sebelum NDN akan merilis atau menguji ke pasar, akan lebih baik untuk meninjau aspek keamanan. Menurut arsitektur NDN dan alur kerja, NDN memiliki kemungkinan berada dalam situasi diserang melawan serangan DoS/DDoS. Serangan DoS/DDoS pada NDN selanjutnya dikenal dengan istilah Interest Flooding Attack IFA . Pending Interest Table bisa menjadi pintu masuk IFA pada kasus ini. Banyak paper yang menawarkan sejumlah metode mitigasi terhadap IFA. Tesis ini bertujuan untuk menemukenali metode yang dapat digunakan pada kondisi riil melalui simulasi pada topologi Rocketfuel dengan melakukan berbagai skenario pengujian seperti variasi nilai data payload, nilai round-trip time, dan lamanya waktu serangan. Data payload yang diujikan variative mulai dari yang berukuran 400 bytes, 700 bytes, 1100 bytes, 1500 bytes, dan 2000 bytes. Ada tiga metode mitigasi yang diujikan pada tesis ini yakni Satisfaction Pushback, Satisfaction Accept, dan Token Bucket with per Interface Fairness. Pengujian dilakukan menggunakan NDNSim versi 1.0 yang telah di custom. Hasil akhirnya Satisfaction Pushback merupakan metode mitigasi terbaik dibandingkan Satisfaction Accept dan Token Bucket with per Interface Fairness. Kemampuan metode mitigasi Satisfaction Pushback dalam memastikan Consumer mendapatkan layanan yang diinginkan dari Produser berkisar antara 63 - 85,8 . Interest Satisfaction Ratio ISR dicapai saat serangan terjadi dalam 600 detik dengan nilai round-trip time sebesar 150 ms dan data payload sebesar 2000 byte. ISR tertinggi dicapai saat serangan terjadi dalam 300 detik dengan nilai round-trip time sebesar 500 ms dan ukuran data payload sebesar 2000 byte.
<hr />
ABSTRACT
Currently, Named Data Networking NDN has become a breakthrough solution and a potential choice for next generation Internet architecture. Before NDN can be released into the market, it would be better to review its security aspect. According to the NDN architecture and workflow, NDN has the possibility of being in a situation of being attacked against a Denial of Service DoS Distributed Denial of Services DDoS . DoS DDoS attack on NDN is known as an Interest Flooding Attack IFA . Pending Interest Table could be the entrance of IFA in this case. This thesis aims to identify methods that can be used in real conditions through simulation of Rocketfuel topologies by performing various test scenarios such as variations of payload data values, round trip time values, and length of attack time. The payload data tested is varied from 400, 700, 1100, 1500, and 2000 bytes. There are three mitigation methods tested on this works namely Satisfaction Pushback, Satisfaction Accept, and Token Bucket with per Interface Fairness. Testing is done using NDNSim version 1.0 which has been customized. The end result is Satisfaction Pushback is the best

mitigation method than Satisfaction Accept and Token Bucket with per Interface Fairness. While attacks occurred, satisfaction pushback mitigation method is capable in ensuring consumer to get the desired service ranges between 63 85,8 . The lowest interest satisfaction ratio ISR achieved while attacks occurred in 600 seconds with round trip time value on 150 ms and data payload size 2000 bytes. The highest ISR achieved while attacks occurred in 300 seconds with round trip time value on 500 ms and data payload size 2000 bytes.