Implementasi dan analisis mitigasi serangan DDOS untuk proteksi DNS penapisan konten negatif berbasis BGP FlowSpec = Implementation and analysis on mitigation of DDOS attacks to protect DNS negative content filtering with BGP FlowSpec based

Stella Gabriella Apriliani, author

Abstrak

Pemerintah sedang fokus menangani konten negatif pada internet yang memiliki pengaruh buruk dengan membuat regulasi yang mengikat ISP untuk melakukan filtering konten negatif. Awalnya, para pihak ISP melakukan filtering konten negatif dengan pendekatan teknologi DNS yang database situsnya dikirimkan melalui email oleh Kominfo kepada masing-masing ISP dan hal tersebut dirasa kurang efektif, sehingga pemerintah mengeluarkan metode baru dengan menggunakan fitur DNS-RPZ dimana semua data terpusatkan pada database Kominfo yang diupdate melalui aduan konten negatif TRUST dan disebarluaskan ke masing-masing ISP melalui protokol DNS - RPZ tersebut. Akan tetapi DNS rentan oleh serangan, seperti Distributed Denial of Service DDoS. Oleh karena itu, pada penelitian ini akan ditinjau lebih lanjut tentang cara yang dapat dilakukan untuk menangani adanya serangan pada DNS. Serangan DDoS tersebut dapat dideteksi secara otomatis oleh FastNetMon dan juga dimitigasi oleh ExaBGP dengan melakukan injeksi informasi routing BGP FlowSpec pada router mitigasi.
<hr>The government lately has been focusing on handling negative contents on the internet those have bad impacts by establishing regulation that binds ISPs to filter negative contents. Earlier, the ISPs do the filtering with a DNS approach whose database of the site is sent by email by the ministry of communication and information to each ISP, and such method is considered less efficient. Thus, the government has established a new method using the feature of DNS RPZ where all data is centralized to the database of the ministry of communication and information which is updated through TRUST negative content reports and widely spread to each ISP through the DNS RPZ protocol. However, DNS is fragile to attacks, such as Distributed Denial of Service DDoS. Therefore, this research will observe through ways that can be done to handle attacks to DNS. DDoS attacks can be detected automatically by FastNetMon and also mitigated by ExaBGP which injected routing information BGP FlowSpec on the mitigation router.