BAB I

PENDAHULUAN

1.1 Latar Belakang

Serangan *Distributed Denial-of-Service (DDoS)* adalah serangan yang menyebabkan crash pada server dan sistem di jaringan dengan membanjiri paket atau permintaan di jaringan. Karena makin berkembangnya sistem jaringan, jumlah pengguna didalamnya pun semakin banyak. Oleh karena itu, sangat sulit untuk mengidentifikasi siapa pengguna legal dan siapa peretas *(hacker)*. Dan juga seiring berkembangnya teknologi, teknik untuk membuat serangan Ddos juga semakin meningkat. Mengidentifikasi serangan *DDos* menjadi masalah yang lebih kompleks karenaada berbagai jenis strategi serangan DDoS.Beberapa jenis serangan *DDoS* yaitu *ICMP flood, SYN flood,* IP packet flood, dan lain-lain.

Teknik *DDoS flooding* terus berevolusi, mulai dari serangan lapisan jaringan (Layer 3/4) seperti *UDP/ICMP flood* hingga eksploitasi protokol aplikasi (Layer 7) seperti *HTTP flood*. Serangan volumetrik, seperti DNS amplification, mampu menghasilkan lalu lintas hingga ratusan Gbps dengan memanfaatkan kerentanan protokol yang tidak diamankan.

Dalam arsitektur jaringan modern yang menghadapi ancaman serangan DDoS semakin masif dan kompleks, implementasi *Routing Trigger Blackhole* melalui protokol *BGP (Border Gateway Protocol)* telah menjadi suatu kebutuhan strategis. Teknik ini memungkinkan jaringan untuk secara selektif membuang (drop) lalu lintas yang menuju ke prefix tertentu yang sedang diserang. Keunggulan utama dari teknik ini adalah kecepatan respons dan skalabilitas. Karena BGP merupakan protokol yang sudah digunakan secara global dalam pertukaran rute internet, blackhole routing dapat diimplementasikan dalam hitungan detik setelah serangan terdeteksi. Hal ini sangat krusial mengingat serangan DDoS sering kali terjadi secara tiba-tiba dengan volume lalu lintas yang sangat besar.

karakteristik serangan DDoS modern yang bersifat volumetrik dan multi-vektor membutuhkan respons yang hampir instan. Teknik tradisional seperti ACL (Access Control List) atau rate-limiting seringkali tidak cukup efektif ketika menghadapi serangan dengan volume ratusan Gbps. Dengan memanfaatkan BGP blackhole, jaringan dapat mengisolasi lalu lintas serangan di tepian (edge) jaringan dalam hitungan detik setelah deteksi, mencegah overload pada infrastruktur inti. Mekanisme ini menjadi pertahanan terakhir (last line of defense) yang vital ketika serangan melebihi kapasitas mitigasi lainnya.

Skalabilitas BGP merupakan faktor kunci dalam keberhasilan protokol ini sebagai tulang punggung routing di Internet global. Dengan kemampuannya menangani ribuan hingga ratusan ribu entri rute, BGP telah menunjukkan efisiensi tinggi dalam mengelola routing antar domain otonom (AS). Namun, kompleksitas pengelolaan tabel routing yang terus berkembang menjadi tantangan tersendiri, terutama dalam hal penggunaan memori, waktu konvergensi, serta stabilitas jaringan. Oleh karena itu, peningkatan efisiensi dalam mekanisme route filtering, policy control, dan path selection menjadi sangat penting untuk mempertahankan skalabilitas BGP di masa depan

Route tagging menggunakan *atribut BGP Community* telah menjadi praktik umum dalam pengelolaan kebijakan routing antar domain. Dengan menandai rute menggunakan nilai komunitas, operator jaringan dapat menyampaikan informasi kebijakan routing secara efisien kepada mitra BGP mereka (Robert Raszuk, Jeff Haas, Alexander Lange, Bruno Decraene, Shane Amante, Paul Jakma, 2023). Dengan penggunaan attribute ini nantinya akan terbentuk rute dengan tag terntentu yang akan dikenali oleh router upstream, terbacanya tag rute yang dikirimkan tadi secara otomatis router upstream akan mengetahui apa maksud dari tag tersebut dan melakukan aksi sesuai yang diperintahkan.

Implementasi BGP (Border Gateway Protocol) community sebagai salah satu strategi mitigasi serangan *DDoS (Distributed Denial of Service)* memiliki potensi yang signifikan dalam meningkatkan keamanan jaringan. Salah satu cara BGP digunakan untuk melindungi dari serangan DDoS adalah melalui

mekanisme blackholing. Menurut Farasat dan Khan, blackholing dalam BGP memungkinkan pengelolaan lalu lintas yang mencurigakan dengan menandai dan memblokir paket yang berasal dari sumber yang teridentifikasi sebagai penyerang sebelum mencapai tujuan mereka (Farasat & Khan, 2020). Dengan mengandalkan atribut komunitas BGP, administrator jaringan dapat memberikan instruksi kepada router tentang bagaimana menangani lalu lintas tertentu, terutama dalam situasi serangan *DDoS* (Farasat & Khan, 2020).

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, rumusan masalah yang akan dipecahkan dalam penelitian ini adalah sebagai berikut:

1. Bagaimana cara mengimplementasikan BGP Community dalam infrastruktur jaringan Dinas Komunikasi dan Informatika Provinsi Jawa Timur?
2. Sejauh mana implementasikan BGP Community dalam mitigasi serangan DDOS Flooding trafik?

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Untuk mengendalikan ddos trafic flooding, yang diperlukan untuk percepatan mitigasi ketika mendapatkan serangan

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat yang signifikan bagi berbagai pihak, antara lain:

1. Penelitian ini dapat memperkaya kajian ilmu komputer dan teknologi informasi di Universitas Narotama, khususnya di bidang administrasi dan keamanan jaringan. Penelitian ini juga diharapkan dapat memperkuat reputasi universitas dalam pengembangan teknologi informasi.

2. Penelitian ini dapat memberikan kontribusi ilmiah bagi mitra lembaga riset atau perguruan tinggi dalam melakukan mitigasi terkait insiden siber khususnya DDOS Trafic Flooding.
3. Bagi mahasiswa, penelitian ini memberikan pemahaman yang lebih dalam mengenai penerapan BGP Community dalam admistrasi Routing BGP.