BAB I
Pendahuluan

1.1. Latar Belakang

Serangan DoS (*Denial-of-Service*) merupakan suatu ancaman di era digital dikarenakan mengganggu ketersediaan layanan pada sistem dan kehidupan sehari-hari [1]. Serangan DoS biasanya dilakukan dengan membanjiri *host* atau infrastruktur yang ditargetkan dengan permintaan berlebih untuk membebani sistem dan mencegah permintaan yang asli untuk di proses. Sementara itu serangan DDoS (*Distributed Denial-of-Service*) adalah beberapa serangan DoS yang terpusat untuk menyerang satu target yang sama, hal ini bertujuan untuk meningkatkan tingkat efektifitas serangan karena penyerang lebih sulit dilacak dan sumber serangan sulit untuk dimatikan. Teknik mitigasi serangan DDoS yang efektif sangat diperlukan untuk menangani serangan DDoS dikarenakan beberapa teknik mitigasi tidak efektif untuk menahan serangan [2].

Terdapat 3 tipe Serangan DDoS yang bebeda, diantaranya adalah serangan berbasis volume, serangan protokol, dan serangan layer aplikasi. Pada serangan berbasis volume, terdapat UDP *flood*, ICMP *flood*, dan beberapa paket *flood* lainnya. Pada serangan protocol terdapat SYN *flood*, serangan paket yang terfragmentasi, *Ping of Death*, dan sebagainya. Pada serangan layer aplikasi, terdapat GET/POST *flood*, serangan yang menargetkan celah Apache, Windows, OpenBSD, dan sebagainya [3].

Terdapat beberapa teknik mitigasi serangan DDoS diantaranya IPS/IDS (*Intrusion Prevention/Detection System*), *Firewall*, *Router* Cisco, Pemfilteran Upstream. IDS memiliki kelebihan daripada *firewall* tradisional karena IDS dapat mendeteksi dan merespon apabila terdapat penyusupan dalam trafik menggunakan beberapa macam metode seperti *signature-based detection* dan anomaly-based detection yang membutuhkan *machine learning* [4]. IPS merupakan bagian dari IDS, namun memiliki fitur tambahan untuk mencegah trafik mencurigakan yang telah ditandai oleh IDS agar tidak masuk. *Firewall* tradisional hanya membatasi akses didalam jaringan untuk mencegah penyusupan apabila set *rule* sudah dikonfigurasi dengan baik dan tidak memberikan peringatan dari dalam jaringan. Beberapa *Router* Cisco telah dilengkapi dengan IOS (*Internetworking Operating System*) yang didalamnya terdapat beberapa fungsi seperti VPN (*Virtual Private Network*), *Firewall*, IP SLA (*Internet Protocol*

Service Level Agreement), dan NAC (*Network Access Control*) sebagai fitur keamanan untuk meminimalisir serangan. Pemfilteran Upstream berupa beberapa metode seperti proxy, terowongan, koneksi silang digital, dan sirkuit langsung yang bertujuan memisahkan trafik buruk seperti serangan DDoS dan yang lain agar lalu lintas yang asli bisa berkomunikasi dengan *host*.

IDS dapat dikustomisasi untuk tujuan yang spesifik seperti mendeteksi trafik mencurigakan dan mencegah penyusupan terjadi, namun kekurangan dari hal ini adalah perlunya model training untuk mengenali apakah trafik yang dideteksi adalah trafik yang benar-benar asli atau tidak. Berbeda dengan *firewall* tradisional, beberapa set aturan dibutuhkan untuk mencegah penyusupan namun hal ini jauh lebih mudah untuk diterapkan karena tidak memerlukan *machine learning* seperti IDS. Mikrotik *router* memiliki beberapa fitur layaknya *router* pada umumnya, namun memiliki kelebihan pada konfigurasinya yang lebih mudah dan beberapa fitur lain seperti IDS apabila dikonfigurasi dengan benar.

Pada penelitian yang dilakukan oleh Agustini et al, telah dilakukan penelitian tentang Analisa IDS berbasis mikrotik terhadap beberapa 6 serangan DoS. Namun penelitian yang dilakukan hanya terbatas pada deteksi serangan dan tidak ada teknik mitigasi sama sekali.

Pada penelitian yang dilakukan oleh RANA et al, telah dilakukan penelitian tentang peningkatan dari algoritma klasifikasi SVM yang tertanam pada SNORT IPS untuk mendeteksi dan mitigasi serangan DDoS. Namun dari segi implementasi hal ini menghabiskan banyak biaya, terlebih pada SNORT IPS. Tentunya ini sangat tidak cocok untuk di implementasikan pada skala jaringan yang memiliki keterbatasan *resource*.

Pada penelitian yang dilakukan oleh Nuroji, telah dilakukan penelitian tentang pencegahan serangan *port-scanning* seperti nmap. Namun hal tersebut tidak cukup untuk melakukan mitigasi serangan DDoS.

Pada penelitian lanjutan ini, peneliti melakukan pengujian *firewall* mikrotik untuk mitigasi serangan DDoS, mikrotik dipilih karena harganya yang terjangkau dan konfigurasi yang mudah, hal ini sangat cocok digunakan untuk jaringan LAN seperti café, warnet, atau jaringan rumah karena jarang sekali terdapat solusi ketika terjadi serangan. Serangan yang digunakan juga serangan yang umum terjadi, seperti SYN

flood, UDP *flood*, HTTP *flood*, DNS *flood*, dan *Smurf attack*. Dengan beberapa kombinasi dari *firewall* setting, *firewall* mikrotik dapat melakukan mitigasi serangan DDoS tanpa bantuan pihak ketiga. Namun *Smurf attack* tidak dapat ditangani oleh *firewall* mikrotik sendirian dikarenakan kurangnya fitur dari mikrotik untuk memblokir alamat IP broadcast.

1.2. Rumusan Masalah

1. Seberapa Efektif kustom *firewall* mikrotik untuk mitigasi serangan DDoS pada jaringan LAN tanpa bantuan IDS/IPS pihak ketiga?
2. Apakah kustom *firewall* mikrotik memiliki pengaruh pada penggunaan *resource server* dan *router*?

1.3. Tujuan Penelitian

Penelitian ini dilakukan dengan tujuan untuk membuktikan seberapa efektif kustom *firewall* dari mikrotik untuk melakukan mitigasi serangan DDoS yang umum terjadi.

1.4. Batasan Masalah

Penelitian dilakukan hanya pada jaringan LAN karena jaringan LAN dengan *resource* yang sangat terbatas jarang sekali terdapat solusi apabila terjadi serangan DDoS. Teknik mitigasi juga hanya terfokus pada mikrotik *router* tanpa bantuan IDS/IPS pihak ketiga. Serangan yang digunakan adalah SYN *flood*, UDP *flood*, HTTP *flood*, DNS *flood*, dan *Smurf attack*. *Monitoring* dilakukan dengan batas waktu 60 detik untuk meminimalisir *error* berlebih.