BAB I PENDAHULUAN

I.1 Latar Belakang

Peningkatan penggunaan teknologi dalam kalangan perusahaan telah menjadi suatu tren yang semakin menonjol. Konsep komputasi awan (*cloud computing*) memberikan perusahaan akses ke sumber daya TI dengan fleksibilitas dan efisiensi yang tinggi, tanpa perlu membeli, mengelola, atau merawat infrastruktur perangkat lunak secara mandiri. Namun, walaupun memberikan berbagai keuntungan tersebut, penggunaan teknologi *cloud* juga membawa potensi risiko yang serius terkait dengan aspek keamanan.

Salah satu risiko keamanan yang sangat krusial dalam lingkungan *cloud* adalah isu keamanan jaringan. Lingkungan komputasi awan cenderung lebih terdistribusi dan kompleks bila dibandingkan dengan lingkungan IT tradisional, yang mengakibatkan kesulitan dalam mengidentifikasi dan melindungi setiap titik akhir jaringan. Tambahan lagi, penggunaan aplikasi dan layanan *cloud* juga berkontribusi pada peningkatan risiko terhadap serangan siber. Hal ini terjadi karena data dan aplikasi disimpan di luar kendali langsung perusahaan, yang pada gilirannya menciptakan tantangan baru dalam manajemen serta perlindungan informasi yang bersifat sensitif.

Untuk mengatasi risiko keamanan jaringan di lingkungan *cloud*, *Cloud -based microsegmentation firewall* menjadi solusi yang efektif. *Microsegmentation firewall* memungkinkan *administrator* jaringan untuk memisahkan jaringan menjadi beberapa segmen yang lebih kecil, sehingga setiap segmen dapat diatur kebijakan keamanannya secara *independen*. Hal ini memungkinkan *administrator* untuk membatasi akses pengguna dan aplikasi hanya pada segmen yang diperlukan, sehingga memperkecil risiko penyebaran serangan siber ke seluruh jaringan.

Penggunaan *cloud microsegmentation firewall* juga memungkinkan *administrator* untuk memantau dan mengelola keamanan jaringan secara lebih efektif. *Firewall* dapat diatur untuk mengambil tindakan otomatis terhadap serangan atau ancaman keamanan tertentu, seperti memblokir lalu lintas atau mengirimkan notifikasi ke

administrator. Hal Ini memungkinkan *administrator* untuk mengambil tindakan yang tepat dan cepat untuk mengurangi dampak serangan siber pada jaringan.

Dengan meningkatnya penggunaan teknologi *cloud* dan risiko keamanan yang semakin kompleks, *cloud microsegmentation firewall* menjadi solusi keamanan yang penting dan efektif untuk melindungi jaringan *cloud* perusahaan.

I.2 Rumusan Masalah

Rumusan masalah untuk dokumen penelitian ini adalah sebagai berikut:

1. Bagaimana kinerja *microsegmentation firewall* dalam *Quality of Service*?
2. Bagaimana kinerja *microsegmentation firewall* terhadap *Resource Utilization?*

I.3 Tujuan Penelitian

Berdasarkan rumusan masalah, tujuan penelitian penelitian ini adalah sebagai berikut:

1. Menganalisa *firewall microsegmentation* dalam mempengaruhi *qualilty of service*.
2. Menganalisa *firewall microsegmentation* dalam mempengaruhi *resource utilization.*

I.4 Batasan Penelitian

Batasan penelitan yang akan di gunakan dalam penelitian ini sebagai berikut:

1. Pelenlitian ini berfukus pada membangun *network microsegmentation* di dalam GNS3 Sebagai *network simulautor*.
2. Penelitian ini membangun dan membandingkan kedua topologi antara topologi *Segmentation firewall* dengan topologi *segmentation non firewall.*
3. Analisa serangan dari *external zone* berupa ICMP *flood attack* dan SYN *flood attack* yang bertujuan untuk membandingkan kinerja *cloud.*
4. Analisa *Quality of Service* dalam segi throughput, Packet loss, Jitter.
5. Analisa Resource dengan mengtahui penggunaan sumber daya dari FortiGate dan *cloud* dalam segi CPU *utilization* dan *memory utilization*.

6. Penelitian ini menggunakan metode PPDIO *life cycle*, yang berarti proses penelitian ini akan di lakukan berdasarkan tahapan pada PPDIO life cycle di tiga tahapan yaitu, *Plan, Pripare, Design.*

I.5 Manfaat Penelitian

Secara akademis, penelitian diharapkan dapat menjelaskan secara tepat mengenai *firewall* untuk menjadi referensi ataupun rekomendasi bagi peneliti lain yang bergerak dalam bidang yang sama, terutama *Network Segmentation*.

Secara Non akademis Penelitian ini dapat di gunakan untuk merancang *firewall microsegmentation* dapat membantu meningkatkan keamanan *server* dan jaringan dalam lingkungan. Dengan membatasi aliran lalu lintas antara segmen jaringan, solusi ini dapat mengurangi risiko serangan dan memperkuat perlindungan keamanan.

I.6 Sistematikan Penulisan

Penelitian ini diuraikan dengan sistematika penulisan sebagai berikut:

Bab I Pendahuluan

Bab ini membahas latar belakang penelitian, rumusan dan batasan masalah yang ada, tujuan penelitian, metodologi pengerjaan penelitian, dan sistematika penulisan laporan penelitian.

Bab II Tinjauan Pustaka

Pada bab ini berisi beberapa teori yang digunakan dalam pengerjaan Proyek Akhir sehingga penelitian menjadi jelas.

Bab III Sistematika Penelitian

Bab ini membahas perancangan sistem yang akan diuji beserta spesifikasi alat-alat penunjang penelitian.

Bab IV Perancangan Sistem

Bab ini membahas pengujian yang dilakukan terhadap sistem dan analisis terhadap hasil pengujian.

Bab V Skenario Pengujian

Bab ini membahas kesimpulan dari pengujian yang telah dilakukan dan saran sebagai acuan untuk penelitian selanjutnya.

Bab VI Kesimpulan dan Saran

Bab ini membahas kesimpulan dari penelitian yang telah dilakukan dan terdapat saran dari penulis untuk penelitian selanjutnya yang berhubungan dengan topik yang sama.