SARI

Voice over Internet Protocol adalah salah satu teknologi komunikasi yang memanfaatkan jaringan *Internet Protocol*, sebagai media transmisi data. Dalam implementasinya, VoIP membutuhkan sistem pengamanan serta reliabilitas jaringan internet yang baik, untuk berkomunikasi. Oleh karena itu, jika jaringan ini mengalami masalah, seperti padatnya lalu lintas *bandwidth* akibat serangan *cybercrime* (*ping flooding*) misalnya, maka kinerja VoIP pun juga akan bermasalah, sedangkan kondisi yang ada saat ini, belum ada satu pun pihak yang mampu menjamin keamanan serta reliabilitas jaringan internet, dari serangan *cybercrime* tersebut. Untuk menanggulangi masalah keamanan ini, maka Adi Kurniawan Y., seorang profesional IT, menawarkan beberapa solusi keamanan VoIP, yakni membangun jaringan dengan menggunakan metode *Virtual Private Network*, melakukan pengaturan *firewall*, atau dengan menggunakan segmentasi VLAN. Tiap-tiap metode yang ditawarkan Adi tersebut, dalam implementasi yang telah penulis lakukan, terbukti dapat melindungi jaringan dari aktivitas pencurian *Voice* VLAN ID dan peracunan jaringan dalam sistem. Hanya saja, dalam penggunaan salah satu metode yang ditawarkan, yakni segmentasi VLAN, masih terdapat celah dimana lalu lintas data dan suara yang seharusnya terpisah, masih dapat saling berkomunikasi melalui *Internet Control Message Protocol*, sehingga menyebabkan jaringan VoIP rawan terkena serangan *cybercrime* (*ping flooding*). Oleh karena itu, penulis menerapkan pengaturan *firewall* dalam tugas akhir ini, untuk memisahkan kedua lalu lintas tersebut, sehingga keduanya tidak dapat melakukan komunikasi kembali dengan menggunakan protokol ICMP (*ping*). Berdasarkan artikel keamanan VoIP yang dipublikasikannya tersebut, Adi Kurniawan menyatakan bahwa penggunaan *firewall* justru menambah waktu *delay* dalam sistem, sehingga menurunkan nilai *Quality of Service* yang dimiliki sistem. Hal ini dikarenakan, cara kerja *firewall* yang harus memproses terlebih dahulu paket VoIP yang dibebankan, sehingga untuk menanggulangi masalah tersebut, penulis menerapkan metode *Multi Protocol Label Switching* pada jaringan VPN, untuk menjaga kualitas transmisi data dan suara agar tetap stabil. Hanya saja, dalam implementasi yang telah penulis lakukan, hasil yang diperoleh dari pengujian QoS, menunjukkan perbedaan nilai yang tidak signifikan antar metode yang digunakan, baik ketika metode keamanan telah diterapkan dan belum diterapkan dalam sistem, sehingga kesimpulan terkait metode manakah yang dapat digunakan, untuk meningkatkan nilai QoS pada jaringan VoIP, belum dapat ditentukan, akibat hasil pengujian QoS yang tidak signifikan, kecuali untuk pengujian QOS dengan parameter *packet loss*, karena semua hasil pengujiannya bernilai nol.

Kata Kunci: VoIP, MPLS, VPN, segmentasi VLAN, *firewall*

TAKARIR

MPLS	= *Multi Protocol Label Switching*
VPN	= *Virtual Private Network*
VoIP	= *Voice over Internet Protocol*
Cybercrime	= Aktivitas kejahatan di dunia maya
Data network	= jaringan telekomunikasi yang memungkinkan komputer saling bertukar data
Switching	= aktivitas pembagian jalur transmisi data antar titik
Authentication	= proses identifikasi untuk memastikan valid tidaknya data yang masuk
Data Analog	= proses pengiriman sinyal menggunakan gelombang elektromagnetik, yakni gelombang yang dapat merambat walaupun tidak ada medium
Data Digital	= proses pengiriman sinyal menggunakan kode biner (sistem bilangan basis dua) 0 dan 1
Client	= pengguna yang menerima layanan
Server	= komputer yang memberikan layanan ke klien
Hacker	= sebutan bagi orang yang memiliki kemampuan mencari dan menganalisis kelemahan sistem
Interface	= antarmuka
Variable	= wadah yang digunakan untuk mendeklarasikan nilai yang memiliki banyak varian