BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian terapan yang telah dilakukan dengan konfigurasi Winbox Mikrotik untuk megatur aktivitas jaringan guna melakukana proteksi jaringan untuk melindungi dari masuknya virus dan malware dari website, router mikrotik sebagai akses lalu lintas jaringan harus benar-benar dimaksimalkan dalam pemanfaatan *firewall* dalam keamanan jaringan. Sehingga pengamanan jaringan dengan konfigurasi Winbox Mikrotik dapat disimpulkan dalam poin sebagai berikut :

1. Dengan memahami mikrotik dan penggunaanya dalam system keamanan jaringan bisa mengontrol aktivitas pengguna jaringan dengan maksimal dengan melakukan menejemen via winbox;
2. Dengan memanfaatkan winsox dalam mengelola router mikrotik maka bisa melihat *traffic* data yang dipakai *user* serta *statistic;*
3. Dengan bantuan fitur *firewall* yang didalamnya ada beberapa fitur pembantu seperti *filter rule, NAT, mangle, conection, service port, layer 7 protocol,* menjadi kunci dalam mengatur keamanan jaringan;
4. Dari fitur diatas bisa melakukan pemblokiran terhadap suatu *website* yang tidak aman untuk diakses, baik blok melalui *content*, *IP address* dengan batuan fitur dalam *firewall*;

5. Dengan memahami penggunaan dan konfigurasi yang tepat pada fitur yang ada pada Mikrotik, maka akan menghasilkan sistem keamanan jaringan yang maksimal dan sangat bermanfaat bagi keamanan jaringan itu sendiri;

Sedangkan dalam melakukan tindakan dalam rangka meminimmalisir serangan *malware* dari luar adalah dengan mengaktifkan *filtering* dan proteksi terhadap jaringan dengan dukungan fitur Mikrotik dalam *firewall*. Dengan melihat dan mengetahui lalulintas jaringan secara teliti maka pemegang keamanan bisa medeteksi hal yang masuk melalui jaringan yang bisa mngakibatkan masuknya virus ke perangkat jaringan dan menginfeksi sistem jaringan sehingga mengganggu keamanan jaringan, langkah langkah dalam meminimalisir serangan dari luar diantaranya :

1. Melakukan pemantauan secara *remote* pada jaringan oleh teknisi penanggung jawab keamanan;
2. Melakukan pemeriksaan aktivitas jaringan pada winbox secara rutin;
3. Memberikan *alert* pada *address* yang teridentifikasi sebagai *malware*;
4. Memahami kode dan lisensi dalam *install* sebuah software;
5. Melakukan pemeriksaan pada performa yang dilakukan oleh mikrotik *router* sehingga bisa selalu mengikuti update fitur dan hal lain yang dianggap penting;

5.2 Saran

Dari kesimpulan diatas penulis memberikan beberapa hal terkait dengan tambahan sebagai saran sebagai berikut :

1. Penggunaan dari fitur mikrotik belum-lah aman secara maksimal pada jaringan ini. Disarankan untuk membeli *firewall* dengan system *up-date* karena *malware* dan virus juga selalu *up-date* supaya jaringan dan data perusahaan menjadi aman;
2. Menambah *bandwidth ISP* agar bisa mampu meng-cover semua jaringan ketika *ISP* fastnet terputus koneksinya.
3. Membeli *router* atau *accesspoint* yang kapasitasnya lebih dari 300 Mbps per lantainya untuk dapat meng-cover lebih dari 50 *user* dalam satu *router* ataupun *access point*.
4. Melakukan pemeriksaan terhadap performa *Router* dan melakukan *restart* secara rutin dan terjadwal;
5. Selalu teliti dalam melakukan blok via *address* karena ada beberapa *website* yang mempunyai *address* lebih dari satu jadi harus diblok semuanya agar tidak lolos akses;