

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Jaringan komputer pada perusahaan harus menyediakan kehandalan dan kenyamanan yang tinggi. Hal ini bertujuan untuk mendukung proses tercapainya tujuan bersama perusahaan secara cepat dan efektif. Namun kedua hal tersebut harus diimbangi dengan keamanan yang tinggi, supaya aset perusahaan seperti data atau informasi dapat terjaga kerahasiaan dan keamanannya sehingga tidak disalahgunakan oleh pihak yang tidak bertanggungjawab.

Berdasarkan hasil wawancara dengan administrator jaringan komputer PT Reka Patria Ekaguna (PT. RPE), didapatkan informasi bahwa jaringan komputer PT. RPE sering terjadi penyerangan dan masih memiliki celah keamanan yang harus segera diperbaiki atau ditingkatkan. Diantaranya jaringan komputer sering mengalami *overload bandwidth* yang besar sehingga menimbulkan perangkat dan server dalam jaringan menjadi terganggu dan kurang optimal.

Bandwidth internet yang semula di fungsikan untuk mendukung kegiatan kantor secara tidak langsung disalahgunakan oleh karyawan untuk kepentingan pribadi. Sehingga untuk mengoptimalkan kembali penggunaan *bandwidth* haruslah ada *filtering* paket dalam *firewall* PT. RPE. *Filtering* paket digunakan untuk mengidentifikasi paket besar maupun kecil, dari dalam maupun luar jaringan, berbahaya atau aman untuk di akses sehingga selanjutnya di tentukan apakah paket

dapat diteruskan untuk dikirim atau diterima. Tujuannya adalah untuk menghemat atau mengoptimalkan *bandwidth* dan mengamankan jaringan PT RPE.

Masalah lain adalah apabila server atau perangkat jaringan mengalami masalah (*trouble*), dan administrator sedang berada di luar kantor dikarenakan PT RPE merupakan perusahaan yang bergerak pada sektor migas yang mengharuskan terdapat jaringan komputer di lapangan atau saat admin sedang di luar kantor dengan alasan lain, maka ketika masalah terjadi administrator akan menanganinya dengan melakukan *remote* jaringan untuk menhandel server dan perangkat yang terkena masalah tersebut untuk memperbaikinya. Proses *remote* menggunakan aplikasi *remote desktop connection* yang merupakan fitur bawaan Windows Server.

Menurut hasil wawancara, hal tersebut dirasa kurang aman karena rentan dilakukan penyadapan atau penyerangan ke jaringan. Tidak ada enkripsi atau kamufase yang digunakan untuk mengamankan integritas data saat melakukan koneksi *remote desktop connection*. Oleh karena itu untuk meningkatkan keamanan pada *firewall* dan VPN di jaringan komputer PT. RPE, peneliti akan melakukan perbaikan dengan menerapkan "Implementasi Firewall Filter dan VPN Ipsec pada PT RPE".

1.2 Rumusan Masalah

Dari permasalahan yang telah dijelaskan, maka didapat sebuah rumusan masalah yaitu bagaimana untuk meningkatkan seluruh keamanan jaringan PT

Reka Patria Ekaguna khususnya pada *firewall filtering* supaya *bandwidth* dapat digunakan dengan tepat dan pada *remote* jaringan jika dilakukan administrator dari luar agar koneksi VPN terjaga keamanannya.

1.3 Batasan Masalah

Batasan masalah yang digunakan adalah sebagai berikut :

1. Area penelitian hanya dalam satu jaringan komputer milik PT Reka Patria Ekaguna.
2. Perangkat yang akan digunakan yaitu perangkat yang sudah tersedia dalam jaringan tersebut.
3. Jika memungkinkan pengadaan perangkat untuk meningkatkan keamanan jaringan komputer PT RPE, maka akan diajukan ke bagian terkait.
4. Sumber utama layanan internet PT RPE menggunakan salah satu provider swasta.
5. Sistem operasi pada server dan client berbasis Windows.

1.4 Maksud dan Tujuan Penelitian

1.4.1 Maksud Penelitian

Maksud dilakukannya penelitian ini yaitu :

1. Sebagai syarat bagi peneliti dalam menyelesaikan program studi sarjana.
2. Sebagai bahan dan acuan dalam pengembangan studi selanjutnya.

1.4.2 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk meningkatkan keamanan, membatasi penggunaan *bandwidth* yang tidak perlu, serta memaksimalkan sumber daya yang

ada dengan menerapkan *firewall filtering* dan VPN *Ipssec* pada jaringan PT RPE sehingga nantinya jaringan komputer PT RPE memiliki kemampuan :

1. Memprioritaskan paket yang penting.
2. Mengidentifikasi paket yang penting dan tidak penting bagi perusahaan.
3. Membatasi paket atau menghilangkan paket yang tidak penting.
4. Mengatur penggunaan *bandwidth* pada karyawan sesuai otorisasi yang ditentukan perusahaan.
5. Memudahkan administrator saat melakukan VPN dari luar jaringan.
6. Meningkatkan keamanan saat melakukan koneksi VPN, yaitu menggunakan *Ipssec*.

1.5 Metode Penelitian

1.5.1 Metode Pengumpulan Data

1. Wawancara

Penulis melakukan wawancara langsung kepada administrator PT. RPE yaitu Bapak Titik Sefur. Didapat informasi bahwa terdapat masalah seperti dijelaskan pada bagian latar belakang masalah.

2. Observasi

Observasi dilakukan di PT. Reka Patria Ekaguna, Jakarta pada tanggal 5 Mei 2017. Penulis menganalisa permasalahan jaringan, otorisasi karyawan, dan semua sistem dan perangkat yang bekerja dalam jaringan komputer PT RPE.

3. Studi Pustaka

Studi pustaka dilakukan dengan membaca berbagai karya ilmiah dan mencari informasi di internet yang membantu penulis memahami tentang *firewall filtering* dan VPN menggunakan *Ipssec*.

1.5.2 Metode Pengembangan Jaringan

Dalam pengembangan jaringan, peneliti menggunakan metode *Network Development Life Cycle* (NDLC). Metode NDLC bersifat *continous improvement* dimana hasil dari analisis akan dijadikan sebagai bahan pertimbangan untuk melakukan perbaikan terus menerus. Berikut merupakan uraian dari tahapan NDLC, yaitu :

a. *Analysis*

Tahap ini yaitu menganalisa kebutuhan, permasalahan, keinginan user, dan topologi jaringan yang sudah ada. Metode yang dilakukan adalah wawancara dan survey langsung ke PT RPE.

b. *Design*

Dari data yang telah didapat, maka akan membuat *design* topologi jaringan yang akan dibangun. Berupa *design* struktur topologi, akses data, tata layout pengkabelan.

c. *Simulation Prototype*

Yaitu membuat bentuk simulasi awal untuk melihat bagaimana nantinya jaringan dibangun.

d. *Implementation*

Tahap menerapkan semua yang telah direncanakan dan di *design* sebelumnya.

e. Monitoring

Tahap untuk memastikan bahwa jaringan yang dibangun sesuai dengan analisis yang semula menjadi masalah atau keinginan user. Dimaksudkan untuk mengetahui kelemahan dan kekurangan sehingga dapat diperbaiki secepatnya.

f. Management

Yaitu tahap mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur *reability* terjaga. Pembuatan *policy* akan tergantung dari kebijakan *level management* dan strategi bisnis perusahaan.

1.6 Sistematika Penulisan

Untuk memahami lebih jelas laporan ini, maka materi-materi yang tertera pada Laporan Skripsi ini dikelompokkan menjadi beberapa sub bab dengan sistematika penyampaian sebagai berikut :

1.6.1 BAB I PENDAHULUAN

Berisi tentang latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, metode penelitian, dan sistematika penulisan.

1.6.2 BAB II LANDASAN TEORI

Bab ini berisikan teori yang berupa pengertian dan definisi yang diambil dari kutipan buku yang berkaitan dengan penyusunan laporan skripsi serta beberapa literature *review* yang berhubungan dengan penelitian.

1.6.3 BAB III ANALISIS DAN PERANCANGAN

Bab ini berisikan gambaran umum dan sejarah singkat PT Reka Patria Ekaguna, analisa sistem jaringan yang sudah berjalan, permasalahan yang dihadapi, penyelesaian masalah, dan konfigurasi jaringan komputer yang baru.

1.6.4 BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini merupakan proses selanjutnya setelah desain yaitu pembuatan simulasi *prototype* dan kemudian di buatlah jaringan komputer yang baru sesuai desain yang diusulkan. Selain itu terdapat proses *monitoring* dan *management* jaringan yang bertujuan untuk mengetahui apakah jaringan yang di bangun telah berjalan baik atau tidak.

1.6.5 BAB V PENUTUP

Bab ini berisi kesimpulan dan saran yang berkaitan dengan optimalisasi serta peningkatan keamanan jaringan komputer berdasarkan yang telah diuraikan pada bab-bab sebelumnya.

1.6.7 DAFTAR PUSTAKA

Bab ini berisi pustaka yang dijadikan sebagai bahan dan acuan dalam pembuatan skripsi.

1.6.8 LAMPIRAN

Berisi tentang keseluruhan konfigurasi dan desain jaringan yang yang diterapkan.