KEAMANAN JARINGAN DENGAN PACKET FILTERING FIREWALL (STUDI KASUS: PT. SUKSES BERKAT MANDIRI JAKARTA)

Siti Nur Khasanah
STMIK Nusa Mandiri Jakarta
Email : Siti.skx@nusamandiri.ac.id

ABSTRACT

Network security is currently a very important issue and continues to grow. Development of computer technology, besides causing many benefits also have many bad side. One of them is an attack on computer systems connected to the Internet. As a result of the attack, many computer systems or networks disrupted even be damaged. Given these problems, then as soon as possible we must immediately secure computer networks from attack. Untangle is a Linux distribution that is used as a regulator of tissue. Untangle is an open source first terintegerasi to deal with spam, spyware, viruses, adware, web-filtering and report. Based on Debian Linux with supporting JAVA applications. Untangle Server delivers the ease in securing, controlling and monitoring of computer networks. Ease is a technology that is needed to secure from threats such as viruses and spyware, web access and control over the availability of the report of the Untangle Server to perform a system analysis. Everything is packaged within an interface / GUI (Graphical User Interface). Untangle is very handy and has a full feature in managing and securing the network from LAN to WAN scale.

Keywords: *Network Security, Packet Filtering Firewall, Untangle*

1. PENDAHULUAN

Keamanan jaringan saat ini menjadi isu yang sangat penting dan terus berkembang. Perkembangan teknologi komputer, selain menimbulkan banyak manfaat juga memiliki banyak sisi buruk. Salah satunya adalah serangan terhadap sistem komputer yang terhubung ke *Internet*. Sebagai akibat dari serangan itu, banyak sistem komputer atau jaringan yang terganggu bahkan menjadi rusak. Untuk menanggulangi hal tersebut, diperlukan sistem keamanan yang dapat menanggulangi dan mencegah kegiatan-kegiatan yang mungkin menyerang sistem jaringan kita.

Dalam perkembangan teknologi dewasa ini, sebuah informasi menjadi sangat penting bagi sebuah organisasi. Informasi tersebut biasanya dapat diakses oleh para penggunanya. Akan tetapi, ada masalah baru yang berakibat dari keterbukaan akses tersebut. Masalah-masalah tersebut antara lain adalah sebagai berikut:

1. Pemeliharaan validitas dan integritas data atau informasi tersebut.
2. Jaminan ketersediaan informasi bagi pengguna yang berhak.
3. Pencegahan akses sistem dari yang tidak berhak.
4. Pencegahan akses informasi dari yang tidak berhak.

Dengan adanya masalah-masalah tersebut, maka secepat mungkin kita harus segera mengamankan jaringan komputer dari serangan. Dengan memanfaatkan berbagai teknik, khususnya teknik keamanan dan pemeliharaan *(maintenance)*, maka hadirlah solusi untuk pemeliharaan *(maintenance)* dengan menggunakan sistem operasi manajemen jaringan yang menyediakan berbagai fasilitas yang mendukung keamanan dan akses data jaringan. Sistem operasi ini juga menyediakan fasilitas dalam pengelolaan *system* dan *network* infrastruktur. Sistem operasi ini dinamakan *"Untangle"*.

Menurut Primartha dan Sukemi (2009:23) "*Untangle Gateway* adalah solusi jaringan berbasis *open source* yang telah terintegrasi dengan modul-modul untuk memfilter *spam* dan *virus*".

2. LANDASAN TEORI

2.1. Jaringan Komputer

Menurut Oetomo dalam Herlambang (2008:1) "mengemukakan bahwa Jaringan komputer adalah sekelompok komputer otonom yang saling menggunakan protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi data, informasi, program aplikasi, dan perangkat keras seperti *printer, scanner, CD-Drive* ataupun *harddisk*, serta memungkinkan untuk saling berkomunikasi secara elektronik". Potensi jaringan komputer antara lain:

a. Mengintegrasikan dan berbagai pakai peralatan
b. Komunikasi
   Jaringan komputer memungkinkan terjadinya komunikasi antar pemakai komputer.
c. Perlindungan Data dan Informasi
   Jaringan komputer dimanfaatkan pula untuk mendistribusikan proses dan aplikasi sehingga dapat mengurangi terjadinya *bottleneck* atau tumpukan pekerjaan pada satu bagian.
d. Keteraturan Aliran Infomasi
   Jaringan komputer mampu mengalirkan data-data komputer *client* dengan cepat untuk mengintegrasikan dalam komputer *server*.

Berdasarkan letak geografis jaringan komputer dapat dibagi menjadi tiga jenis yaitu:

a. *Local Area Network* (LAN)
b. *Metropolitan Area Network* (MAN)
c. *Wide Area Network* (WAN)

2.2. Keamanan Jaringan Komputer

Menurut Aziz dan Purnama (2012:1) "Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi adalah sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak dimana usaha tersebut bisa dilakukan baik dari dalam maupun dari luar sistem".

2.3. *Firewall*

Menurut Aziz dan Purnama (2012:1) "*Firewall* merupakan suatu cara atau mekanisme yang diterapkan baik terhadap *hardware, software* ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan atau kegiatan suatu segmen pada jaringan lokal dengan jaringan luar yang bukan merupakan ruang lingkupnya".

Sedangkan menurut riadi (2011:73) "*Firewall* adalah sebuah sistem atau kelompok sistem yang menerapkan sebuah *access control policy* terhadap lalu lintas jaringan yang melewati titik-titik akses dalam jaringan. Tugas *firewall* adalah untuk memastikan bahwa tidak ada tambahan diluar ruang lingkup yang diizinkan. *Firewall* bertanggung jawab untuk memastikan bahwa *access control policy* yang diikuti oleh semua pengguna di dalam jaringan tersebut. *Firewall* sama seperti alat-alat jaringan lain dalam hal untuk mengontrol aliran lalu lintas jaringan. Namun, tidak seperti alat-alat jaringan lain, sebuah *firewall* harus mengontrol lalu lintas *network* dengan memasukkan faktor pertimbangan bahwa tidak semua paket-paket data yang dilihatnya adalah apa yang seperti terlihat. *Firewall* digunakan untuk mengontrol akses antara *network internal* sebuah organisasi *Internet*."

Berdasarkan tinjauan jurnal maka penulis memutuskan untuk merancang sistem keamanan jaringan yang handal yang pengaturannya terpusat pada *firewall* tetapi mudah dalam penyettingannya, dan *software* yang digunakan penulis adalah *untangle.*

2.4. Topologi Jaringan

Menurut Herlambang (2008:10) "Topologi atau arsitektur jaringan

merupakan pola hubungan antar terminal dalam suatu sistem jaringan komputer". Topologi jaringan adalah istilah yang digunakan untuk menguraikan cara bagaimana komputer terhubung dalam suatu jaringan. Topologi-topologi jaringan diantaranya sebagai berikut:

1. Topologi *Bus*

Menurut Sofana (2011:11) "Topologi *Bus* menggunakan sebuah kabel *backbone* dan semua *host* terhubung secara langung pada kabel tersebut". Topologi ini paling banyak dipergunakan pada masa penggunaan kabel *coaxial* menjamur. Topologi *bus* atau *linear* mempunyai karakteristik sebagai berikut:

a. Merupakan satu kabel yang kedua ujungnya ditutup dimana sepanjang kabel terdapat *node.*
b. Paling sederhana dalam instalasi.
c. Signal melewati kabel 2 arah sehingga memungkinkan terjadinya *collision.*
d. Masalah terbesar jika salah satu segmen kabel terputus, maka seluruh jaringan akan terhenti.
e. Topologi *bus* adalah jalur transmisi dimana sinyal diterima dan dikirimkan pada setiap alat/*device* yang tersambung pada satu garis lurus (kabel), sinyal hanya akan ditangkap oleh alat yang dituju, sedangkan alat lainnya yang bukan tujuan akan mengabaikan sinyal tersebut.

2. Topologi *Ring*

Menurut Sofana (2011:12) "Topologi *Ring* menghubungkan *host* dengan *host* lainnya membentuk lingkaran tertutup atau *loop*". Jaringan topologi *ring* ini mirip topologi *bus*, hanya saja pada ujung-ujungnya saling berhubungan membentuk suatu lingkaran dengan menggunakan segmen kabel. Pada lingkaran tertutup ini, sejumlah komputer dihubungkan ke lingkaran tersebut. Kinerja topologi *ring* ini diperkenalkan oleh perusahaan IBM untuk mendukung protokol, *Token Ring* yang juga diciptakan oleh IBM.

Kelemahan:

a. Penambahan atau pengurangan terminal sangat sulit.
b. Kerusakan pada media pengirim dapat menghentikan kerja seluruh jaringan.
c. Harus ada kemampuan untuk mendeteksi kesalahan dan metode pengisolasian kesalahan.
d. Kerusakan pada salah satu terminal dapat mengakibatkan kelumpuhan jaringan.
e. Tidak kondusif untuk pengiriman suara, gambar dan data.

Kelebihan:

a. Laju data *(transfer rate)* tinggi.
b. Dapat melayani lalu lintas data yang padat.
c. Tidak diperlukan *Host*, relatif lebih murah.
d. Dapat melayani berbagai media pengirim.
e. Komunikasi antar terminal mudah.
f. Waktu yang diperlukan untuk mengakses data optimal.

3. Topologi Star

Menurut Sofana (2011:12) "Topologi *Star* menghubungkan semua komputer pada sentral atau kosentrator. Biasanya kosentrator berupa perangkat *hub* atau *switch*". Kabel yang sering digunakan pada topologi ini adalah UTP kategori 5.

Kelemahan:

a. Lalu lintas data yang padat dapat menyebabkan jaringan lambat.
b. Jaringan tergantung pada terminal pusat.

Kelebihan:

a. Keterandalan terbesar diantara topologi yang lain.
b. Mudah dikembangkan.
c. Keamanan data tinggi.
d. Kemudahan akses ke jaringan LAN lain.

4. Topologi *Star-Bus*

Menurut Sofana (2011:15) "Topologi *Star-Bus* adalah menggabungkan beberapa topologi *Star* menjadi satu kesatuan. Alat

yang digunakan untuk menghubungkan masing-masing toplogi *Star* adalah *hub* atau *switch*". Topologi ini merupakan topologi yang paling sering digunakan. Komputer-komputer dihubungkan ke *hub*, sedangkan *hub* satu dengan *hub* lainnya dihubungkan sebagai jalur tulang punggung (*Backbone*) yang menyerupai Topologi *Bus*.

5. Topologi Mesh

Menurut Sofana (2011:13) "Topologi *Mesh* menghubungkan setiap komputer secara *point-to-point*. Artinya semua komputer akan saling terhubung satu-satu sehingga tidak dijumpai ada *link* yang terputus". Topologi *Mesh* merupakan jenis topologi yang digunakan *internet*, setiap *link* menghubungkan suatu *router* dengan *router* yang lain.

Dalam membangun jaringan beberapa jenis alat yng berfungsi untuk membangun topologi-topologi tersebut diatas. Dibawah ini adalah beberapa alat tersebut:

1. *Network Interface Card* (NIC)

Menurut Sofana (2011:75) "NIC merupakan perangkat keras utama yang harus ada di setiap komputer. NIC bertugas melakukan menyesuaikan tegangan dan arus listrik yang keluar/masuk komputer. Informasi yang melalui media penghantar dapat dikirim/diterima oleh komputer berkat keberadaan NIC ". Selain itu NIC juga mengontrol *dataflow* antara sistem komputer dengan sistem kabel yang terpasang dan menerima data yang dikirim dari komputer lain lewat media kabel dan menterjemahkanya ke dalam BIT yang dimengerti oleh komputer.

2. Repeater

Menurut Herlambang (2008:9) "*Repeater* berfungsi untuk memperkuat sinyal dengan cara menerima sinyal dari suatu segmen kabel lalu memancarkan kembali sinyal tersebut dengan kekuatan yang sama dengan sinyal asli pada segmen kabel lain". Dengan demikian jarak antara kabel dapat diperpanjang.

2.5. IP Address

Menurut Safrizal (2005:110) "*IP Address* merupakan pengenal yang digunakan untuk memberi alamat pada tiap-tiap komputer dalam jaringan". Sedangkan "Format *IP address* adalah bilangan 32 bit yang tiap 8 bit-nya dipisahkan oleh tanda titik" menurut Safrizal (2005:110). *IP Address* sebenarnya terdiri dari dua bagian, yaitu : *Network ID* dan *Host ID*. *Network ID* menentukan alamat dari suatu jaringan komputer dan *Host Id* menentukan alamat dari suatu komputer *(host)* dalam suatu jaringan komputer. *IP Address* memberikan alamat lengkap dari suatu komputer *(host)* yang merupakan gabungan dari nama *Network Id* dan Nama *Host ID*. Hal ini mirip dengan pemberian nama jalan dan nomor rumah pada sistem pemberian alamat rumah.

Apabila suatu organisasi memiliki *IP Address* dengan *Network Id* 222.124.14.0 memerlukan lebih dari satu *netwok Id,* maka organisasi tersebut harus mengajukan permohonan ke IANA (*Internet Assigned Number Authority)* untuk mendapatkan *IP Address* baru. Permasalahan saat ini adalah persediaan *IP Address* sangat terbatas, karena banyaknya perusahan dotcom yang membuat situs-situs di Internet. Untuk mengatasi permasalahan yang ada dan menghindari mengajukan *IP Address* yang baru ke *IANA,* dibuatlah suatu metode untuk memperbanyak *Network ID* dari suatu *Network ID* yang telah dimiliki sebelumnya. Metode ini sering disebut dengan istilah *Subnetting*, yaitu mengorbankan sebagian *Host ID* untuk digunakan dalam membuat *Network ID* tambahan.

3. METODE PENELITIAN

Metode penelitian yang digunakan oleh penulis adalah :

a. Analisa Kebutuhan

Pada tahap ini penulis melakukan analisa terhadap sistem jaringan komputer yang sedang berjalan di PT. Sukses Berkat Mandiri. Analisa yang dilakukan meliputi topologi jaringan yang digunakan, spesifikasi perangkat jaringan dan permasalahan yang terjadi. Hasil analisa yang didapat merumuskan terhadap kebutuhan teknologi untuk bisa memberikan solusi terhadap permasalahan yang terjadi.

b. Desain
Pada tahap ini penulis merancang sistem jaringan komputer berdasarkan hasil analisa kebutuhan yang telah dilakukan terhadap teknologi jaringan komputer yang akan digunakan. Rancangan meliputi topologi jaringan komputer, protokol jaringan serta perangkat yang dibutuhkan.

c. Testing
Pada tahap ini penulis melakukan percobaan terhadap sistem jaringan komputer yang baru disesuaikan dengan rancangan yang telah dibuat dan melakukan analisa apabila terjadi permasalahan yang terjadi pada saat percobaan sebelum diimplementasikan. Penulis menggunakan *Oracle VM VirtualBox* dan *Packet Tracer* untuk melakukan percobaan.

d. Implementasi
Pada tahap ini sistem jaringan komputer diterapkan dilingkungan perusahaan dan digunakan langsung oleh *user* yang berwenang.

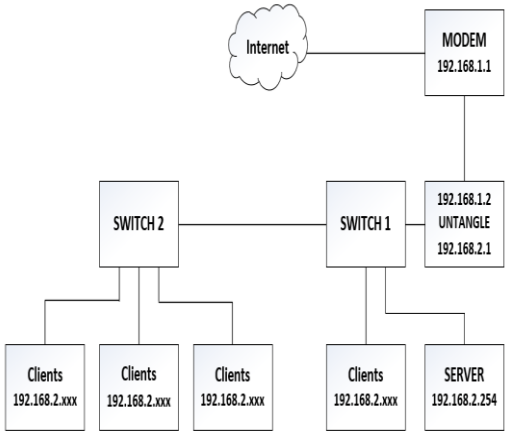
4. PEMBAHASAN

Manajemen Jaringan Usulan

Berikut ini penulis mencoba menggambarkan dan merancang sistem jaringan usulan terhadap jaringan komputer yang ada di kantor PT. Sukses Berkat Mandiri. Adapun rancangan sistem jaringan usulannya sebagai berikut.

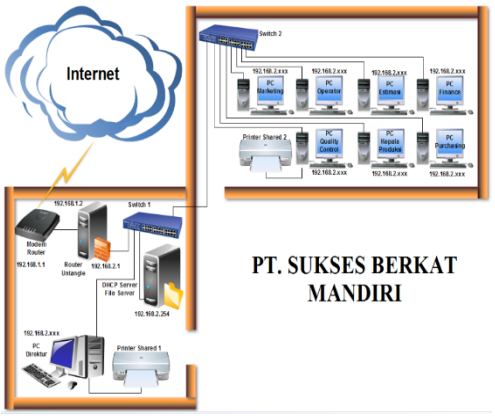
1. Topologi Jaringan

Topologi jaringan merupakan sebuah pola rancang bangun untuk membentuk sebuah *arsitektur* jaringan. Dalam rancangan jaringan usulan yang penulis rancang untuk PT. Sukses Berkat Mandiri masih menggunakan *topologi* jaringan yang berjalan di PT. Sukses Berkat Mandiri, yaitu: *topologi bus-star.* Perbedaannya, penulis menambah 1 unit komputer yang nantinya digunakan sebagai *router* tambahan, yang nantinya akan di instal *software Untangle*. *Router* itu nantinya akan berfungsi sebagai *firewall*(dinding pemisah) yang akan melindungi jaringan internal(*private*/LAN) dari ancaman bahaya jaringan eksternal(*public*/WAN/*Internet*). Berdasarkan rancangan jaringan usulan ini maka *IP Address* pada jaringan internal(*private*/ LAN) harus diubah dan tidak lagi menggunakan 192.168.1.xxx. IP Address yang penulis sarankan disini masih menggunakan *IP Address* kelas C, karena jumlah banyaknya *user* pada jaringan internal(*private*/LAN) masih bisa dibilang sedikit dan untuk *IP Address* jaringan internal (*private*/LAN) yang baru adalah 192.168.2.xxx. Jadi *IP Address* yang digunakan adalah 192.168.1.xxx untuk jaringan eksternal(*public*/WAN/*Internet*) dan 192.168.2.xxx untuk jaringan internal(*private*/ LAN).



Gambar 1 *Topologi* Rancangan Jaringan Usulan PT. Sukses Berkat Mandiri

2. Skema Jaringan



Gambar 2 Skema Jaringan Usulan PT. Sukses Berkat Mandiri

Gambar diatas adalah skema jaringan usulan yang telah penulis rancang untuk mengamankan jaringan komputer yang terdapat di PT. Sukses Berkat Mandiri. Pada skema jaringan usulan penulis menambahkan *Untangle* sebagai *Router* tambahan dan sekaligus penulis gunakan sebagai *firewall* yang nantinya berguna untuk mengamankan jaringan internal (*private*/LAN) dari jaringan eksternal (*public*/WAN/*Internet*).

Perbedaan antara skema jaringan berjalan dengan rancangan skema jaringan usulan:

a. Pada jaringan usulan kita dapat menjadikan *router untangle* sebagai *firewall* sehingga proses lalu-lintas data dari *internet* ke LAN atau sebaliknya menjadi lebih aman dan cepat.
b. Dengan *untangle* penyetingan *firewall* menjadi lebih berlapis baik di-*filter* dari segi *port, url* ataupun *ip address.*
c. Dapat melakukan penyetingan *untangle* dari komputer *server* atau *client* dengan menggunakan aplikasi *web browser IE*, *Mozilla Firefox*, dll.
d. Dapat memblok/mem-*filter* situs-situs yang dapat menurunkan kinerja karyawan, dengan mengaktifkan *web blocker* dan dapat mengamankan jaringan internal dari virus atau ancaman lainnya dengan mengaktifkan *virus blocker, spyware blocker, phish blocker.*

Keamanan Jaringan

Dalam keamanan jaringan disini penulis merancang sebuah keamanan jaringan dengan metode *packet filtering firewall* yang nantinya berguna untuk mengamankan jaringan internal(*private*/LAN) di PT. Sukses Berkat Mandiri.

Berikut ini adalah langkah-langkah dalam proses membangun dan menyetting *software Untangle* :

1. Instalasi Untangle

Berikut ini adalah langkah-langkahnya :

a. Siapkan 1 unit komputer dengan 2 buah LAN *Card*
b. Siapkan CD insalasi *Untangle* dengan cara :
   1) *Download file* ISO dari *server Untangle* di alamat *www.Untangle.com*. ISO adalah sebuah *file* yang berisi sebuah *image* yang siap di bakar (di-*burn*) menjadi sebuah CD instalasi *Untangle* yang *bootable*.
c. Masukan CD instalasi *Untangle* pada CD *drive,* kemudian *restart* komputer kita dengan CD tersebut. Pastikan bahwa komputer melakukan *booting* lewat CD.
d. Jika komputer kita *booting* dengan CD instalasi *Untangle*, *program wizard* akan memandu kita dalam melakukan tahapan instalasinya.
e. Dalam proses instalasi *Untangle*, *Hard disk* komputer akan diformat. Jadi, jika kita melakukan proses coba-coba dengan komputer bekas yang berisi data penting, pastikan data tersebut sudah di *back up* sebelumnya.
f. Berikut ini adalah proses instalasinya:
   1) Kita akan diminta untuk memilih bahasa pengantar proses instalasi.
   2) Kemudian kita akan diminta untuk memilih wilayah.

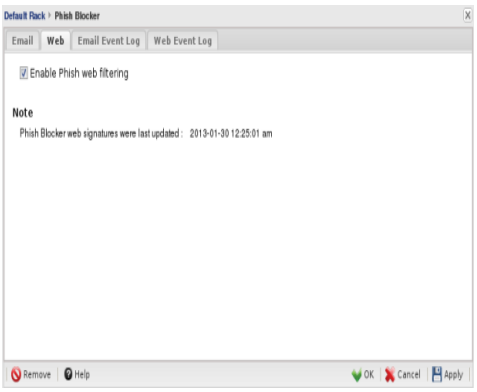
3) Kemudian kita akan diminta untuk Proses Instalasi, Memilih Zona Waktu
4) Kemudian kita akan diminta untuk memformat *Harddisk*
5) Kemudian *Untangle* meng-*copy file* ke *Harddisk*
6) Proses Instalasi selesai, dan komputer akan melakukan *reboot*

2. Setting Awal *(Setting Router)*

Setelah proses instalasi selesai dan komputer melakukan proses *reboot*, maka kita akan masuk ke pengaturan awal, yaitu pengaturan untuk membuat *untangle* menjadi *router* OS, berikut adalah langkah-langkahnya :

a. Saat pertama kali *server untangle* dinyalakan, sebuah *web browser* akan terbuka, dan melalui *web browser* ini lah kita akan melakukan penyettingan awal yang terdiri dari : bahasa, *network* dan sebagainya.
(Perhatikan bagian URL. Alamatnya adalah http://localhost/setup/language.do?console=1.)

b. Setelah mengklik *Next*, kita akan



diminta memasukkan *password admin*

Gambar 3 Penyettingan *Password Admin*

c. Setelah mengklik *Next*, *Untangle* secara otomatis akan melakukan identifikasi kartu jaringan (NIC).
d. Setelah mengklik *Next*, kita harus melakukan konfigurasi koneksi *internet*, dan *IP Address* yang di isikan adalah *IP Address* Eksternal (*public*/WAN/*Internet*)
e. Jika isian yang kita masukkan benar kemudian coba klik *Test Connectivity*, tunggu sampai ada pesan *"Success!"* lalu klik *Next* dan pilih *"Setting* sebagai *Router"*, lalu kita melakukan pengaturan *IP Address* Internal (*private*/LAN), pengaturannya dilakukan secara *static* dan *IP Address* yang dipakai adalah 192.168.2.1 dengan *subnet mask* 255.255.255.0
f. Klik *Next*, untuk melanjutkan ke pengaturan *Automatic Upgrades*, disini kita bisa mengatur *Untangle* bisa meng-*upgrade* secara *automatis* atau tidak
g. Klik *Next* dan penyettingan awal pun selesai

3. Setting aplikasi *Untangle*

a. Pengaturan *Bandwidth*

Setelah proses penyettingan awal selesai maka *Untangle* akan men-*download* beberapa aplikasi *open source* bawaan *untangle* itu sendiri. Selanjutnya adalah penyettingan *bandwidth* dengan *Bandwidth Control*, fungsinya adalah untuk membagi akses *internet* secara merata sehingga semua karyawan dapat mengakses *internet* dengan kapasitas *bandwidth* yang sama.

Cara penyettingan adalah:

1) Klik *Bandwidth Control*, lalu klik *Run bandwidth control setup wizard*
2) Klik *Next*, lalu isi kolom *bandwidth download* dan *bandwidth upload*, disini penulis menyetting 300Kbit untuk *bandwidth download* dan 200Kbit untuk *bandwidth upload*
3) Selanjutnya mengisi kolom *IP Address* yang berhak mendapatkan *Bandwidth Control*
4) Setelah selasai klik *Apply* dan OK

b. Packet Filtering Firewall

Pengaturan selanjutnya adalah mem-*filter* akses *internet* jaringan itu sendiri, karena banyak hal-hal yang

sangat berbahaya yang beredar luas di *internet*, khususnya : Virus. banyak aplikasi *untangle* yang dapat digunakan dalam mem-*filter* jaringan, semua itu tergantung kebutuhan pada jaringan tersebut. Adapun pengaturan yang penulis *setting* disini adalah *Firewall, Web Blocker, Virus Blocker, Spyware Blocker, Phish Blocker, Attack Blocker.*

Berikut adalah proses penyettingannya :

1) *Firewall*
   a) Klik *Firewall*, lalu karena *default*nya semua *port* terbuka/*open*, maka klik *block* semua aplikasi yang tersedia. Karena hanya beberapa aplikasi yang di butuhkan maka tambahkan pengaturan *firewall* dengan klik *Add*, disini yang ditambahkan adalah aplikasi *browsing* yaitu: HTTP(port 80), DNS(port 53), dan FTP(port 21) dan *setting* dalam keadaan terbuka/*open* lalu klik *Apply* dan OK
   b) Klik *Event Log* untuk memantau lalu lintas jaringan yang melewati *firewall*

2) *Web Blocker*
   a) Klik *Web Blocker*, lalu klik *Categories*, disini kita tinggal men-*ceklist block* pada bagian katagori *website*. *Default*nya katagori *pornography* dan *proxy sites* di blok, disini penulis menambahkan katagori *social networking* untuk di blok sehingga karyawan tidak dapat membuka situs-situs jejaring sosial. Lalu klik *Apply* dan OK

3) *Virus Blocker*
   a) Klik *Virus Blocker* lalu *ceklist Scan* HTTP dan *Scan* FTP, lalu klik *Apply* dan OK

4) *Spyware Blocker*
   Klik *Spyware Blocker*, lalu *ceklist* pada kolom *Block Malware Urls, Block Tracking & Ad Cookies, Monitor Suspicious Traffic,* lalu klik *Apply* dan OK.

5) *Phish Blocker*
   Klik *Phish Blocker* dan *ceklist Enable phish web filtering*, lalu klik *Apply* dan OK.

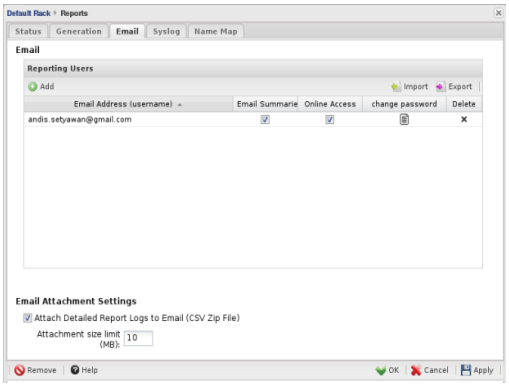
6) *Attack Blocker*
   Klik tombol ON pada *Attack blocker* untuk mengaktifkan.

c. *Report*

Report adalah bentuk sebuah laporan yang berisi hal-hal yang terjadi pada jaringan komputer. Pada *untangle*, *report* akan melaporkan tentang aktifitas aplikasi yang telah di instal, seperti *anti-virus,firewall*, dll. *Format* laporan berbentuk PDF dan dapat di akses via *Email*.

Berikut cara penyettingannya :

1) Klik *Report*, lalu *setting* apakah *report* akan dikirimkan secara harian, mingguan, atau bulanan, lalu klik *Apply.*
2) Klik bagian *email* dan *Add*/tambahkan alamat *email* penerima laporan, lalu klik *Apply* dan OK.



Gambar 4 Proses Penyettingan *Report*

Pengujian Jaringan

Dalam merancang dan membangun jaringan yang lebih baik lagi maka harus

dilakukan yang namanya pengujian jaringan. Adapun pengujian jaringannya sebagai berikut:

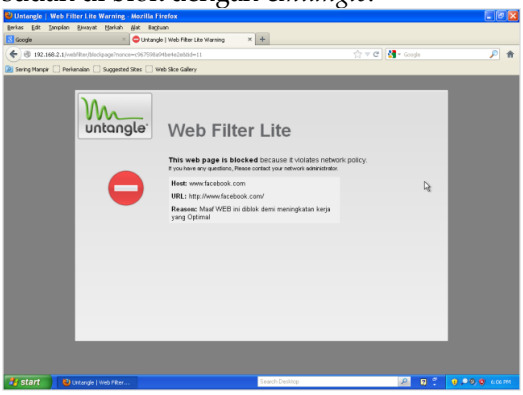
1. Pengujian Jaringan Awal

Pengujian jaringan awal adalah pengujian jaringan berdasarkan skema jaringan berjalan yang ada di PT. Sukses Berkat Mandiri. Pada pengujian jaringan awal karyawan di PT. Sukses Berkat Mandiri sering sekali melakukan sembarang *download* dalam kapasitas yang besar sehingga membuat karyawan lain kehabisan *bandwidth* untuk akses ke *internet*. Kinerja karyawan pun juga menurun karena banyak karyawan yang lebih suka bermain *Facebook* atau jejaring sosial lainnya dibandingkan mengerjakan pekerjaan mereka masing-masing.

Gambar 5 *Screenshoot Monitor* Karyawan Sebelum Menggunakan *Untangle*

2. Pengujian Jaringan Akhir

Pengujian jaringan akhir adalah pengujian jaringan berdasarkan skema jaringan usulan yang penulis rancang untuk PT. Sukses Berkat Mandiri. Pada pengujian jaringan akhir karyawan di PT. Sukses Berkat Mandiri hanya dapat melakukan *download* dengan kapasitas *bandwidth* yang sudah di tentukan *untangle* sehingga karyawan-karyawan lain juga bisa melakukan *download* dan akses *internet* dengan kapasitas yang sama untuk setiap karyawannya. Kinerja karyawan pun lebih membaik karena karyawan-karyawan yang suka bermain *Facebook* atau jejaring sosial lainnya sudah tidak lagi dapat mengakses situs tersebut karena situs-situs tersebut sudah di blok dengan *Untangle*.



Gambar 6 *Screenshoot Monitor* Karyawan Sesudah Menggunakan *Untangle*

5. PENUTUP

Dari hasil penelitian yang telah Dari semua kegiatan–kegiatan yang telah dilakukan oleh penulis maka dapat ditarik kesimpulan antara lain :

1. Penerapan teknologi *packet filtering firewall* jaringan sangat diperlukan untuk membatasi *resource* yang ada digunakan secara benar dan untuk menjadi referensi dalam menentukan pembuatan sistem keamanan jaringan.
2. *Software Untangle* memberikan tampilan simulasi yang cukup mudah dimengerti selain itu dapat mengakses langsung ke *router untangle* melalui *web browser*.
3. *Untangle* sangat berguna dan memiliki fitur yang lengkap dalam me-*manage* dan mengamankan jaringan mulai dari skala LAN hingga WAN.

DAFTAR PUSTAKA

Aziz, Saiful dan Bambang Eka Purnama. 2012. Sistem Keamanan Jaringan Komputer Dengan Firewall dan Intrusion Detection System (IDS). Jurnal Speed 13, Volume 9. No. 2, Agustus 2012: 1-6. Diambil dari: http://unsa.ac.id/ejournal/index.php/speed/article/download/64/64 (15 November 2012).

Herlambang, Moch Linto, dan Aziz Catur L. 2008. Panduan Lengkap Menguasai

Router Masa Depan Menggunakan Mikrotik OS.Jakarta: Andi Publisher.

Primartha, Rifkie dan Sukemi. 2009. Proteksi Mail Server dari Spam dan Virus Menggunakan Untangle Gateway. Jurnal Generic, Volume 4. No. 2, Juli 2009: 23-25. Diambil dari: http://uppm.ilkom.unsri.ac.id/userfiles/JurnalVol_4_No_2_Juli_2009/5-Rifkie.pdf (10 November 2012).

Riadi, Imam. 2011. Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik. JUSI Volume 1, No. 1, Februari 2011: 71-80. Diambil dari: http://is.uad.ac.id/jusi/files/08-JUSI-Vol-1-No-1-_Optimalisasi-Keamanan-Jaringan-Menggunakan-Pemfilteran-Aplikasi-Berbasis-Mikrotik.pdf (16 November 2012).

Safrizal, Melwin. 2005. Pengantar Jaringan Komputer. Yogyakarta: ANDI