ANALISIS DAN DESAIN KEAMANAN JARINGAN KOMPUTER DENGAN METODE *NETWORK DEVELOPMENT LIFE CYCLE* (STUDI KASUS: UNIVERSITAS TELKOM)

[1] Ramadhan Triyanto Prabowo, [2]Mochamad Teguh Kurniawan
[1, 2] Program Studi Sistem Informasi, Fakultas Rekayasa Industri, Telkom University
[1] ramadhantriyantoprabowo@gmail.com , [2] ujangtegoeh@gmail.com

Abstrak—Keamanan jaringan komputer merupakan hal yang tidak terpisahkan dalam jaringan komputer. Keamanan jaringan komputer yang tidak dirancang dengan baik dapat menyebabkan kebocoran data, pelanggaran privasi, hingga kerugian finansial. Oleh karena itu, dibutuhkan rancangan keamanan jaringan komputer yang dapat memenuhi kebutuhan dari pengguna layanan jaringan komputer. Penelitian ini bertujuan untuk mendesain keamanan jaringan komputer dengan obyek penelitian adalah Universitas Telkom dengan menggunakan NDLC. Hasil desain keamanan jaringan komputer menjadi usulan untuk pengembangan keamanan jaringan komputer pada universitas tersebut. Hasil dan desain kemanan jaringan komputer di Universitas Telkom diperlukan adanya IDPS untuk mendeteksi adanya serangan karena pada kondisi *existing* tidak dapat terdeteksi.

Kata kunci: Universitas Telkom, Keamanan, NDLC

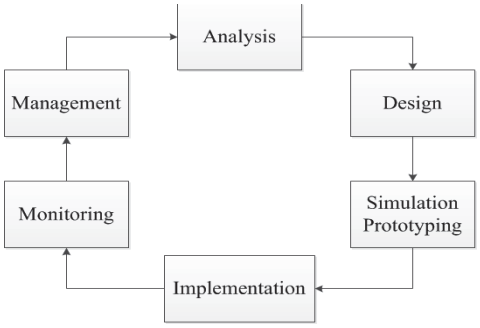
I. PENDAHULUAN

Pada era globalisasi sekarang, keamanan teknologi informasi memiliki peran yang penting bagi perusahaan baik yang bergerak di bidang barang maupun jasa. Keamanan teknologi informasi dianggap penting karena dapat mencegah perusahaan mengalami kerugian baik finansial maupun hukum. Salah satu fungsi keamanan teknologi informasi adalah menjaga data yang bersifat rahasia. Jika data yang bersifat rahasia ini didapatkan dan diubah oleh pihak yang tidak berhak, maka akan menimbulkan kerugian dalam hal materi maupun kebocoran informasi pribadi.

Universitas adalah perguruan tinggi yang terdiri dari sejumlah fakultas yang menyelenggarakan pendidikan ilmiah atau profesional dalam sejumlah disiplin ilmu tertentu [1]. Dalam menyelenggarakan proses bisnisnya, universitas membutuhkan teknologi informasi untuk menyimpan berbagai data seperti data pribadi mahasiswa, nilai-nilai mahasiswa, bahkan data-data rahasia seperti nomor identitas penduduk dan nomor rekening. Jika data-data pribadi dan rahasia tersebut berhasil didapatkan dan diubah oleh yang tidak berhak, maka akan menimbulkan kerugian baik dari pihak universitas maupun pihak-pihak yang terkait dengan universitas seperti mahasiswa. Hal ini pernah terjadi pada tanggal 23 Mei 2012 di University of Nebraska, di mana NeSIS, yaitu database yang berisi *social security numbers*, alamat, transkrip nilai, asrama, dan bantuan keuangan milik mahasiswa mengalami peretasan sehingga data-data tersebut dapat diakses oleh yang tidak berhak [2]. Apabila data-data tersebut disalahgunakan, maka akan menimbulkan kerugian bagi mahasiswa University of Nebraska. Berdasarkan contoh tersebut, keamanan teknologi informasi untuk sebuah universitas harus mulai diperhatikan.

II. METODE PENELITIAN

Network Development Life Cycle (NDLC) merupakan suatu metode yang digunakan dalam mengembangkan atau merancang jaringan infrastruktur yang memungkinkan terjadinya pemantauan jaringan untuk mengetahui statistik dan kinerja jaringan [3]. Metode ini bersifat *continuous improvement* dimana hasil dari analisis akan terus dijadikan sebagai bahan pertimbangan untuk melakukan perbaikan terus menerus.



Gambar 1 Urutan metode NDLC

Dari Gambar 1 dapat dilihat adanya perbaikan yang dilakukan terus menerus dari perancangan, simulasi, implementasi, *monitoring* sampai ke analisis dan seterusnya.

III. HASIL DAN PEMBAHASAN

Perancangan keamanan *data center* mengacu pada kondisi *existing* dan identifikasi kebutuhan. Dari hasil analisis kondisi *existing* dan kebutuhan dari pengguna *data center* maka dapat dirancang suatu desain keamanan *data center*.

Berdasarkan metode yang digunakan, simulasi dibutuhkan dalam pengujian untuk memastikan bahwa desain usulan dapat memenuhi kebutuhan dari pengguna. Jika hasil simulasi mampu untuk memenuhi kebutuhan dari pengguna, maka rancangan usulan keamanan *data center* dapat dikatakan berhasil.

A. Keadaan *Existing*

Keadaan *existing* adalah data yang dibutuhkan untuk merancang keamanan data center pada Universitas Telkom. Data keadaan *existing* didapatkan dengan cara melakukan wawancara di Direktorat Sistem Informasi pusat dan pada masing-masing fakultas. Adapun fakultas yang dimaksud adalah Fakultas Teknik Elektro (FTE), Fakultas Rekayasa Industri (FRI), Fakultas Informatika (FIF), Fakultas Komunikasi Bisnis (FKB), Fakultas Ekonomi Bisnis (FEB), Fakultas Ilmu Terapan (FIT), Fakultas Industri Kreatif (FIK), dan terdapat juga Direktorat Bandung Techno Park (BTP).

1. Insiden Keamanan Jaringan pada Universitas

Pada tahun 2012, salah satu fakultas pada Universitas yang diteliti menerima serangan DoS dari internet. Serangan tersebut menggunakan protokol UDP dengan *port* tujuan di atas 1024. Hal itu mengakibatkan beberapa server tidak dapat diakses. Penyebabnya adalah tidak adanya perlindungan server pada serangan DoS/DDoS.

Pada tahun yang sama, fakultas lain pada Universitas yang sama menerima serangan *deface* pada salah satu servernya.

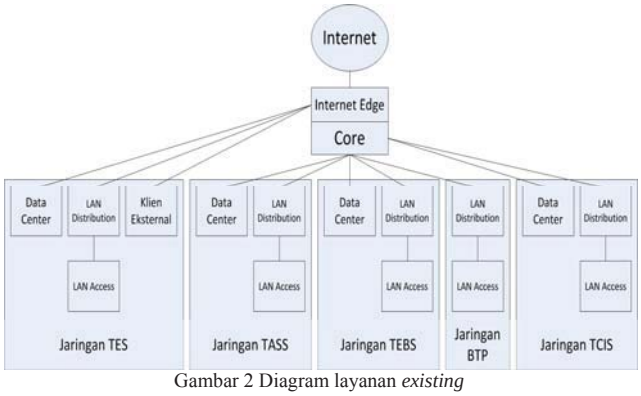
2. Topologi Jaringan *Existing*

Topologi jaringan *existing* adalah sebagai berikut:

Pada Gambar 4 Universitas memiliki lima buah *router* dengan merek Juniper yang dimiliki oleh masing-masing fakultas. Pada *router* yang terhubung ke Internet, *router* tersebut juga memiliki fitur *firewall*.

3. Diagram Layanan *Existing*

Pada Gambar 2 layanan yang disediakan pada *layer Internet edge* adalah *firewall*, WAN *routing*, sekaligus menjalankan fungsi *high-speed routing* pada *layer core*. Layanan yang diberikan oleh Internet *edge layer* tumpang tindih dengan layanan yang diberikan oleh *core layer*. Satu-satunya perlindungan pada data center adalah *firewall*.



Gambar 2 Diagram layanan *existing*

4. Kondisi DMZ

Ditinjau dari topologi yang ada, *firewall* yang diletakkan pada jaringan DMZ yang menghadap ke jaringan publik (Internet) menggunakan perangkat Juniper tipe SRX 650. Konfigurasi *firewall* ini memungkinkan pengguna dari Internet untuk mengakses beberapa server penting menggunakan protokol HTTP dan SSH. Namun, khusus untuk koneksi SSH hanya dibatasi sebanyak 6 koneksi selama satu menit untuk setiap IP *address*.

Firewall yang digunakan pada jaringan ini tidak diterapkan mekanisme *monitoring*. Hal ini mengakibatkan kondisi *real-time firewall* tersebut sulit diawasi dengan baik sehingga terdapat beberapa akibat yang ditimbulkan seperti *load* CPU, ketersediaan *memory*, dan kondisi lalu lintas data menjadi sulit diketahui.

B. Perancangan Keamanan *Data Center* Usulan

Berdasarkan hasil analisis yang telah dilakukan, maka akan dilakukan perancangan keamanan jaringan komputer di Universitas.

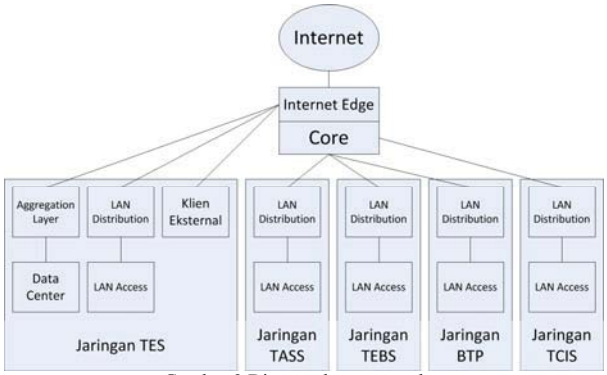
1. Topologi Jaringan Usulan

Topologi jaringan komputer yang diusulkan dapat dilihat pada Gambar 5.

Pada jaringan usulan, dilakukan penambahan perangkat *intrusion detection/prevention system* yang terletak antara *firewall* dengan DMZ. Selain itu, beberapa *data center* yang terdistribusi pada masing-masing fakultas ditempatkan terpusat pada *server farm* yang terletak di belakang IDS untuk memudahkan pengelolaan.

2. Diagram Layanan Usulan

Rancangan diagram layanan usulan adalah sebagai berikut.



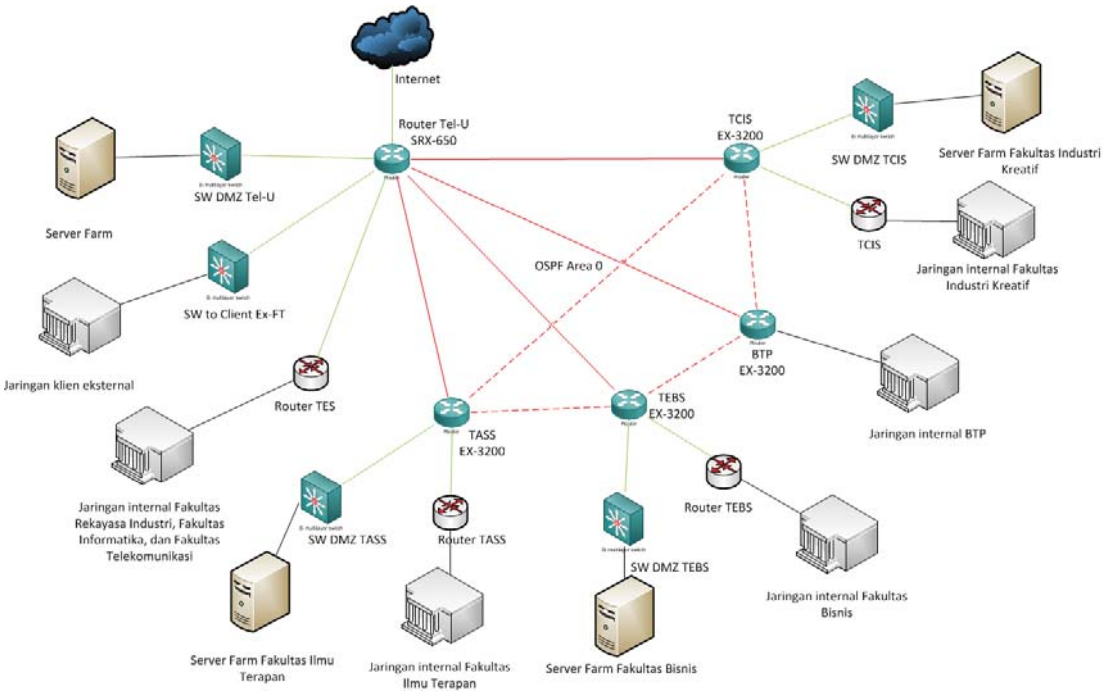
Gambar 3 Diagram layanan usulan

Pada Gambar 3 *data center* tidak lagi menjadi tanggung jawab masing-masing fakultas, tetapi terpusat dan menjadi tanggung jawab Direktorat Sistem Informasi Universitas.

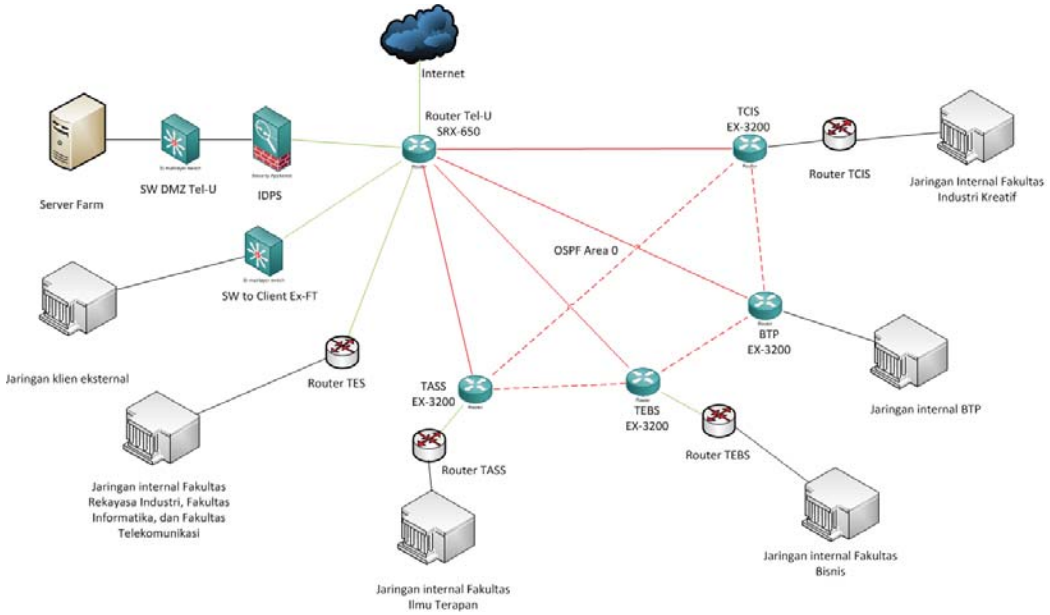
Selain itu, lokasi *data center* berada di belakang *aggregation layer* yang memberikan layanan keamanan seperti *intrusion detection/prevention system* dan *firewall* sehingga data center menjadi lebih terlindung.

C. Simulasi Perbandingan Keadaan *Existing* dengan Usulan

Untuk mengetahui efektivitas dari keadaan usulan dibandingkan dengan keadaan *existing* maka dilakukan simulasi pada lingkungan yang terkontrol.



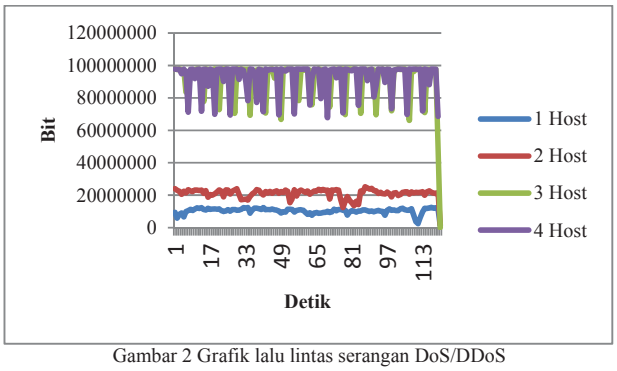
Gambar 4 Topologi jaringan dan data center *existing*



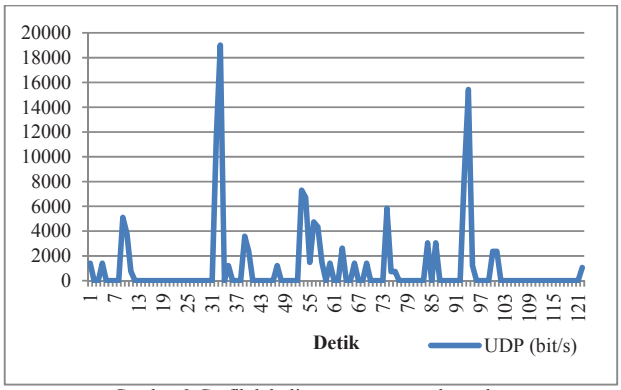
Gambar 5 Topologi jaringan dan data center usulan

1. Simulasi Serangan DoS/DDoS

Salah satu serangan yang pernah terjadi adalah UDP *flooding*. Akan dilakukan simulasi untuk mengetahui dampak dari serangan tersebut. Simulasi dilakukan dengan cara mengirimkan paket UDP secara terus-menerus oleh satu hingga empat host, lalu diukur jumlah lalu lintas paket UDP pada *server*. Pada Gambar 6 dapat disimpulkan bahwa dalam interval 120 detik rata-rata dapat dibanjiri lalu lintas paket data (berurutan) dari 10,2; 21,1; 93,1; dan 92,9 Mbps, sedangkan setelah dilakukan simulasi terhadap usulan keamanan jaringan komputer, hasilnya dapat dilihat pada Gambar 7.



Gambar 2 Grafik lalu lintas serangan DoS/DDoS



Gambar 3 Grafik lalu lintas serangan pada usulan

Pada Gambar 7 dapat disimpulkan bahwa dalam waktu 120 detik hanya ada lalu lintas paket UDP rata-rata 1 kbps. Serangan ini dilakukan oleh satu *host*. Jumlah ini cukup berbeda jika dibandingkan dengan tanpa perlindungan terhadap DoS/DdoS. Ketika dilakukan pengujian serangan oleh dua *host*, didapatkan hasil seperti Gambar 8.

Gambar 4 Serangan oleh dua *host*

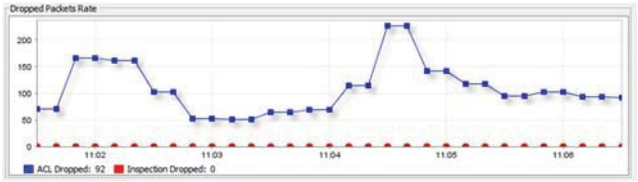
Pada Gambar 8 dapat dilihat bahwa serangan DoS/DDoS oleh dua host pada jaringan usulan menyebabkan perangkat yang menyediakan layanan perlindungan terhadap DoS/DDoS tidak mampu menangani paket data yang masuk, sehingga perangkat tersebut mematikan *interface* untuk mencegah serangan tersebut berlanjut. Hal ini mengakibatkan tidak dimungkinkan untuk melanjutkan pengujian dengan penambahan penyerang.

2. Simulasi Pengukuran Efektivitas IDPS

Salah satu usulan yang diberikan untuk meningkatkan keamanan adalah perlindungan *data center* dari ancaman peretas menggunakan perangkat *Intrusion Detection/Prevention System* (IDPS). Ada banyak jenis serangan yang dapat dideteksi oleh IDPS, beberapa diantaranya adalah serangan TCP SYN *flood* dan serangan UDP *flood*. Simulasi dilakukan dengan cara mengirimkan paket SYN dan paket UDP secara terus-menerus. Gambar 9 adalah hasil dari simulasi serangan TCP SYN flood.

Gambar 5 TCP SYN attack

Pada **Error! Reference source not found.**ambar 9 dapat disimpulkan bahwa perangkat IDPS dapat mendeteksi serangan TCP SYN *flood*. Gambar 10 memperihatkan simulasi serangan UDP *flood*.



Gambar 6 Hasil deteksi serangan UDP flood

Pada Gambar 10 dapat disimpulkan bahwa perangkat IDPS mendeteksi serangan tersebut dan dapat melakukan aksi drop pada paket hingga 250 paket.

3. Simulasi VPN untuk Koneksi SSH

Koneksi SSH diperlukan untuk mengakses dan mengendalikan *server* dari jarak jauh. Koneksi ini harus aman karena koneksi ini memperbolehkan pengguna dari jarak jauh untuk dapat melakukan perubahan sistem pada server. Oleh

sebab itu diperlukan VPN untuk mengamankan koneksi SSH. Gambar 11 adalah pengujian koneksi SSH tanpa VPN.

Gambar 7 Koneksi SSH tanpa VPN

Pada Gambar 11 dapat disimpulkan bahwa koneksi SSH tanpa VPN tidak dapat dilakukan sehingga tidak bisa melakukan melakukan *remote* dan perubahan sistem pada *server*. Setelah dilakukan pengujian koneksi SSH dengan VPN, hasilnya adalah sebagai berikut.

Gambar 8 Koneksi VPN

Gambar 9 Koneksi SSH berhasil dilakukan

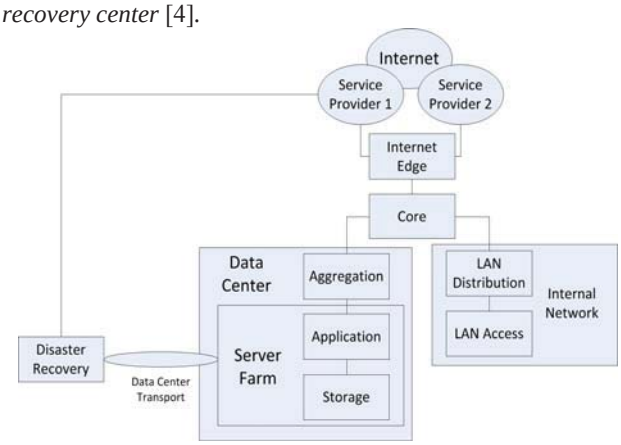
Simulasi dilakukan dengan perangkat lunak Cisco AnyConnect Client. Simulasi ini membutuhkan proses otentikasi sebanyak 2 kali, yaitu otentikasi VPN dan otentikasi SSH. Setelah koneksi VPN berhasil dilakukan, maka pengguna dapat melakukan koneksi SSH pada *server* menggunakan *private* IP *address* milik *server*.

D. Analisis

Setelah dilakukan perancangan dan simulasi, maka dilakukan analisis apakah keamanan jaringan komputer usulan layak dan mampu memenuhi kebutuhan pengguna atau tidak.

1. Analisis Perbandingan *Existing* dengan Usulan

Arsitektur jaringan dan data center yang ideal harus mencakup layanan-layanan seperti layanan *Internet edge, core*, *data center* yang terpisah dengan jaringan internal, *aggregation layer*, *server farm*, *layered access network*, dan *disaster recovery center* [4].



Gambar 10 Diagram layanan ideal

Pada Gambar 14, setiap *layer* memiliki komponen yang redundan, sehingga tidak ada *single point of failure*. Hal ini dibutuhkan agar ketersediaan layanan meningkat.

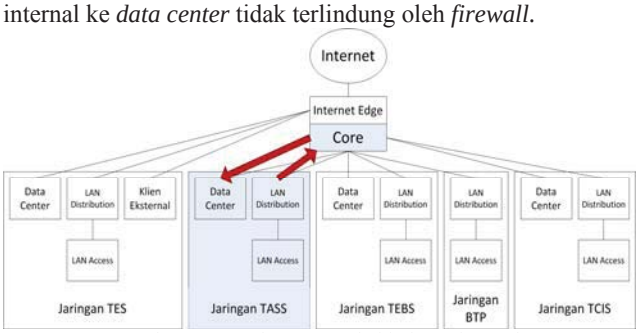
Pada sisi *internet edge*, layanan yang disediakan adalah layanan WAN *routing* dan keamanan. Perangkat yang digunakan meliputi *firewall, intrusion detection system*, dan *intrusion prevention system*. Di sisi *core*, layanan yang disediakan adalah *routing* antara jaringan internal, *data center*, dan *public* WAN atau Internet. Pada layer ini, dibutuhkan layanan *forwarding data* yang cepat dan *redundan* karena menghubungkan tiga layanan kritis. Pada sisi *aggregation*, layanan yang disediakan adalah layanan redundansi *default gateway*, sehingga *data center* dapat mencapai ketersediaan yang tinggi. Pada layer ini pula *intrusion detection system*, *Network Analysis Module* (NAM), dan perlindungan serangan DoS/DDoS diimplementasikan. Di *server farm layer*, adalah layanan-layanan aplikasi dan penyimpanan data yang dibutuhkan oleh organisasi. Pada *layer* ini pula beberapa atau semua aplikasi-aplikasi dan data-data penting dilakukan *backup* ke *disaster recovery*.

Di jaringan yang melayani pengguna jaringan, terdapat *distribution layer* yang memberikan layanan seperti *inter*-VLAN *routing*, *access list*, *quality of service* (QoS), dan redundansi *default gateway* pada pengguna untuk meningkatkan ketersediaan layanan. Pada *access layer*, diterapkan layanan yang menghubungkan langsung dengan pengguna, seperti *power over ethernet* (PoE), *patch panel*, *switch*, dan layanan *wireless*.

Perbandingan antara diagram layanan *existing* dengan diagram layanan ideal memiliki memiliki perbedaan yaitu tidak adanya *aggregation layer*. *Layer* ini penting karena

menyediakan layanan redundansi *default gateway*, *intrusion detection system*, *network analysis module*, dan menyediakan perlindungan terhadap serangan DoS/DDoS. Selain itu, *internet edge layer* tidak redundan dan diletakkan menjadi satu dengan *core layer* sehingga mengakibatkan kondisi *single point of failure* yang menyebabkan ketersediaan layanan tidak terjamin.

Selain itu, jika ada serangan yang dilakukan pada jaringan internal (LAN) maka *data center* yang ada di beberapa fakultas menjadi tidak terlindungi karena lalu lintas data dari jaringan internal ke *data center* tidak terlindung oleh *firewall*.



Gambar 11 Contoh serangan dari jaringan internal

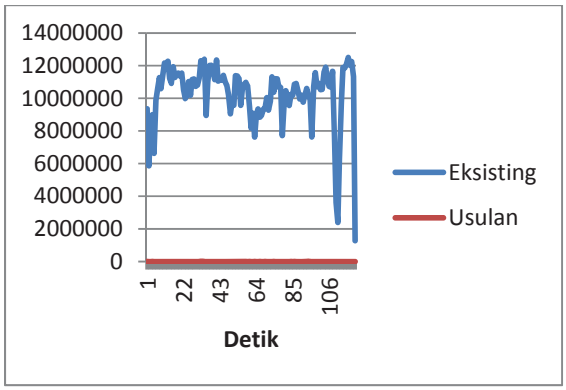
Berdasarkan Gambar 15 terdapat kemungkinan serangan pada jaringan internal (LAN) karena akses menuju *data center* tidak dilindungi oleh *firewall*. Oleh karena itu dibutuhkan desain jaringan yang memungkinkan *data center* dapat terlindung oleh *firewall.*

2. Analisis Hasil Simulasi

Analisis hasil simulasi diperlukan untuk mengetahui apakah keamanan jaringan komputer usulan telah dapat memenuhi kebutuhan keamanan jaringan komputer pada Universitas.

3. Analisis Simulasi Serangan DoS/DDoS

Pada dapat disimpulkan bahwa semakin banyak jumlah host yang berpartisipasi dalam serangan UDP *flood* maka semakin banyak pula lalu lintas paket UDP. Hal ini dapat menghabiskan *bandwidth* yang tersedia sehingga lalu lintas data yang normal tidak mendapat porsi *bandwidth* yang semestinya. Jika dibandingkan dengan lalu lintas paket UDP pada usulan keamanan jaringan komputer adalah sebagai berikut.



Gambar 12 Perbandingan *existing* dengan usulan

Gambar 16 menyatakan bahwa perbandingan antara lalu lintas paket UDP pada jaringan *existing* dengan usulan memiliki perbedaan sebesar 99,98% sehingga dapat disimpulkan bahwa usulan keamanan jaringan komputer dapat memenuhi kebutuhan pertahanan terhadap DoS/DDoS.

3. Analisis Simulasi Pengukuran Efektivitas IDPS

Analisis simulasi pengukuran efektivitas IDPS diperlukan untuk mengetahui apakah perangkat IDPS yang diusulkan dapat memenuhi kebutuhan deteksi penyerangan pada *data center*. Berdasarkan data pada Gambar 8 dan Gambar 9 menyatakan bahwa perangkat IDPS mampu mengenali beberapa serangan dan dapat mendeteksi maupun mencegah serangan tersebut terjadi. Keamanan jaringan komputer usulan telah mampu untuk memenuhi kebutuhan keamanan jaringan komputer.

4. Analisis Simulasi VPN untuk Koneksi SSH

Analisis simulasi VPN untuk koneksi SSH diperlukan untuk mengetahui apakah teknologi VPN mampu untuk meningkatkan keamanan koneksi SSH dari jaringan publik atau Internet. Hasil pengujian menunjukkan bahwa koneksi SSH tanpa menggunakan VPN tidak dimungkinkan. Sedangkan koneksi SSH setelah penerapan teknologi VPN dapat dilakukan.

IV. KESIMPULAN

Dari penelitian yang telah dilakukan, maka dapat ditarik kesimpulan sebagai berikut.

1) Pada tahap identifikasi keamanan jaringan komputer Universitas Telkom dengan menggunakan metode NDLC untuk tahap analisis didapat hasil sebagai berikut:
   a. Telah menerapkan layanan keamanan untuk jaringan internal dan DMZ, tetapi beberapa *server* di beberapa fakultas tidak terlindung dari serangan yang berasal dari jaringan internal.
   b. Lokasi *data center* yang terpisah menyebabkan pengelolaan keamanan pada *data center* menjadi sulit dilakukan.
   c. Jaringan komputer pada Universitas Telkom belum menerapkan perlindungan terhadap DoS/DDoS, oleh karena itu pada keamanan jaringan komputer usulan dilakukan penambahan perlindungan terhadap DoS/DDoS.
2) Rancangan keamanan jaringan komputer di Universitas Telkom diusulkan dengan menggunakan metode NDLC pada tahap desain dan simulator adalah sebagai berikut:
   a. data center di Universitas Telkom belum diberikan layanan untuk mendeteksi dan mencegah serangan, oleh karena itu diberikan usulan penambahan layanan IDPS untuk mendeteksi dan mencegah serangan terjadi. Hasil pengujian menunjukkan bahwa perangkat usulan dapat memenuhi kebutuhan tersebut.
   b. Koneksi SSH ke *server* dari jaringan publik tidak diberikan keamanan tambahan, sehingga diperlukan teknologi VPN untuk meningkatkan keamanan

koneksi SSH. Hasil pengujian pada kondisi *existing* maupun usulan keamanan jaringan komputer menunjukkan bahwa koneksi SSH tidak dimungkinkan jika pengguna belum terkoneksi dengan VPN, sedangkan setelah dilakukan koneksi dengan VPN, maka koneksi SSH dapat dilakukan.

3) Pada tahap *monitoring* pada metode NDLC didapat usulan sebagai berikut
   a. Diberikan usulan agar *server* tersebut terlindung oleh firewall.
   b. Diberikan usulan untuk penempatan *data center* secara terpusat agar memudahkan pengelolaan.

DAFTAR PUSTAKA

[1] Kementrian Pendidikan Nasional, *Kamus Besar Bahasa Indonesia*. Jakarta: Balai Pustaka, 2008.

[2] University of Nebraska. (2012, May) University of Nebraska. [Online]. http://nebraska.edu/media-resource-center/news-releases/486-university-of-nebraska-investigating-security-breach-into-student-information-system.html

[3] ames E. Goldman and Phillip T. Rawles, *Applied Data Communication: A Business-Oriented Approach*. New York: Wiley, 2004.

[4] Mauricio Arregoces and Maurizio Portolani, *Data Center Fundamentals*. Indiana: Cisco Press, 2003.