ANALISIS DAN PERANCANGAN INFRASTRUKTUR JARINGAN KOMPUTER STUDI KASUS: FAKULTAS TEKNIK UNIVERSITAS NEGERI MANADO

Arje Cerullo Djamen
Pendidikan Teknologi Informasi dan Komunikasi, FakultasTeknik , Universitas Negeri Manado
Kaampus UNIMA Tondano
Email : arjedjamen@unima.ac.id

Abstract— The network security has become more important since people spend most of their time to get connected through computer network. The quick development of Internet and internal networking requires the security towards internal network from external network attacks or even by the internal network itself. Universitas Negeri Manado (UNIMA) is one of the universities in North Sulawesi that has been implementing and adapting information technology and communication. The related problems about the issue of network security, such as, hacker activity, virus attacs, denial of service attack (DoS), spyware, malware, and the other attacks may threaten the network security anytime when there is no good management and control because of the limitation of experts in that infrastructure and network security. In order to overcome and prevent the network security problem, it needs to do the network infrastructure analysis and to design the infrastructure that is suitable with the recent and future demands by using Access/Distribution/Core Architectural Model as the basic research development that will be done. The result of this research is the programming of short term and long term network security.

Key word: Access/Distribution/Core Architectural Model

Intisari*—Keamanan jaringan menjadi semakin penting dengan semakin banyaknya waktu yang dihabiskan orang untuk berhubungan melalui jaringan komputer. Perkembangan Internet dan jaringan internal yang semakin pesat menuntut adanya pengamanan terhadap jaringan internal dari kemungkinan adanya serangan dari jaringan eksternal maupun dari jaringan internal itu sendiri. Universitas Negeri Manado (UNIMA) merupakan salah satu perguruan tinggi negeri yang ada di Sulawesi Utara dan sudah sejak tahun 2009 UNIMA melakukan implementasi dan adaptasi teknologi informasi dan komunikasi. Masalah-masalah terkait isu keamanan jaringan seperti aktivitas hacker, serangan virus, denial of service attack (DoS), spyware, malware serta serangan–serangan lainnya yang bisa mengancam keamanan jaringan dapat terjadi kapan saja jika tidak dilakukan pengelolaan dan pengawasan yang baik serta pengelolaan yang kurang optimal karena keterbatasan tenaga ahli bidang infrastruktur dan keamanan jaringan. Untuk mengatasi dan mencegah masalah keamanan jaringan tersebut perlu dilakukan analisis infrastruktur jaringan dan merancang infrastruktur yang sesuai dengan kebutuhan saat ini dan yang akan datang, dengan menggunkan Access/Distribution/Core Architectural Model [3], sebagai dasar pengembangan penelitian yang akan dilakukan. Adapun hasil penelitian berupa perancangan infrastruktur keamanan jaringan jangka pendek dan jangka panjang.

***Kata Kunci*—Access, Distribution, Core Architectural Model.**

I. PENDAHULUAN

Informasi pada era ini sudah menjadi sebuah komoditas yang sangat penting. Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual. Dengan perkembangan yang pesat di bidang teknologi komputer dan telekomunikasi sekarang, perlu adanya pertimbangan akan bahaya dan kerugian penyalahgunaannnya baik itu dalam layanan jaringan lokal ataupun dalam aplikasi yang berbasis internet, maka bagi para pelaku bisnis atau organisasi yang menerapkan teknologi informasi pada organisasinya perlu menerapkan suatu strategi langkah awal untuk menanggulanginya.

Sebagai lembaga yang melaksanakan pendidikan tinggi, Universitas Negeri Manado mempunyai tiga fungsi utama yaitu pendidikan dan pengajaran penelitian dan pengembangan pengabdian pada masyarakat. Ketiga fungsi tersebut lebih dikenal sebagai TRI DARMA PERGURUAN TINGGI yang harus dikembangkan secara simultan dan bersama-sama. Universitas Negeri Manado sebagai salah satu universitas negeri di Indonesia sudah sejak tahun 2009 melakukan implementasi dan adaptasi teknologi informasi dan komunikasi. Sesuai dengan motto Universitas Negeri Manado “why not the best?” maka UNIMA mengintegrasikan berbasis TI ke dalam layanannya. Puskom UNIMA (Pusat Komputer Universitas Negeri Manado) merupakan salah satu instansi di UNIMA yang merupakan unsur instansi pembantu pimpinan universitas dalam mendukung tugas manajemen sitem informasi di lingkungan Universitas Negeri Manado.

Pengelolaan dan resiko keamanan jaringan dianggap penting untuk pengembangan teknologi informasi jaringan komputer di UNIMA, karena jaringan teknologi informasi bisa membantu aktivitas universitas dalam menjalankan tugas dan tanggung jawabnya. Masalah-masalah terkait isu keamanan jaringan seperti diserang oleh hacker, serangan virus, denial of service attack (DoS), spyware adware dan serangan–serangan lainnya yang bisa mengancam keamanan jaringan ini bisa terjadi kapan saja jika tidak dilakukakannya pengawasan yang baik, perawatan yang tidak baik karena keterbatasan tenaga ahli dalam jaringan serta infrastruktur jaringan yang kurang baik. Jika masalah keamanan jaringan

ini terjadi maka akan mempengaruhi layanan kepada civitas UNIMA seperti pemberian informasi, web service, dan layanan lainnya yang menggunakan teknologi jaringan UNIMA serta bisa saja menghambat pengembangan teknologi informasi jaringan komputer di UNIMA. Untuk menghindari dan mencegah masalah keamanan jaringan tersebut solusi yang diberikan adalah dengan melakukan analisis jaringan dan membangun arsitekur yang sesuai dengan kebutuhan serta mendesain teknologi jaringan dengan pendekatan sistem dan hasil nantinya bisa menjadi pedoman atau dokumentasi pihak pengelola dalam mengelola infrastruktur, layanan maupun keamanan terhadap keduanya.

II. TINJAUAN PUSTAKA

Pengaturan akses terhadap peralatan atau tempat-tempat tertentu medapatkan perhatian yang semakin serius oleh para manajer dalam suatu organisasi, baik perusahaan kecil, perusahaan multinasional maupun lembaga-lembaga pemerintahan dalam semua tingkatan. Pengaturan akses terhadap asset dan peralatan organisasi berarti mengontrol akses secara fisik maupun akses secara logic, baik itu akses secara independen maupun akses melalui pendekatan sistem yang telah terintegrasi. Pengamanan terhadap akses secara fisik berarti mengamankan asset organisasi baik asset yang dapat dinilai maupun asset intelektual yang tidak ternilai dari pencurian atau penyadapat. Pengaturan logical akses berarti perusahaan atau organisasi membatasi akses terhadap data, jaringan dan workstation terhadap orang-orang yang berhak saja [8].

Kebutuhan akan Teknologi Informasi yang handal menjadi sangat penting bagi perusahaan untuk menghubungkan kantor pusat dengan kantor cabang didaerah dan mitra dengan perusahaan lain sehingga membentuk suatu jaringan online. Jaringan tersebut membantu dan mempercepat penyebaran informasi, remote, transfer data, video conference (Vicon) dan meningkatkan pelayanan kepada publik, serta efisiensi proses dan manajemen kerja. Teknologi ini memiliki mekanisme pemeliharaan Quality of Service QoS, dan memungkinkan diferensiasi, namun menghadapi masalah pada skalabilitas yang mengakibatkan perlunya investasi tinggi untuk implementasinya. Intranet dan internet yang dengan protokol IP berkembang lebih cepat. IP sangat baik dari segi skalabilitas, yang membuat teknologi Internet menjadi cukup murah. Namun IP memiliki kelemahan serius pada implementasi QoS. Namun kemudian dikembangkan beberapa metode untuk memperbaiki kinerja jaringan IP, antara lain dengan MPLS (Multi Protocol Label Switching). Untuk menjawab kebutuhan perusahaan saat ini dan memberikan solusi yang terbaik sesuai dukungan teknolgi terkini, yaitu layanan VPN IP. VPN IP (Virtual Private Network Internet Protocol) adalah jaringan yang berbasis multimedia dengan platform teknologi IP MPLS (Internet Protocol Multi Protocol Label Switching) [1].

Analisis dan implementasi sistem keamanan jaringan komputer dengan IPtables sebagai firewall menggunakan metode port knocking di Universitas Kristen Satya Wacana. Pada penelitian ini membahas bagaimana administrator suatu firewall ditantang untuk menyeimbangkan fleksibilitas dan keamanan saat merancang seperangkat aturan yang komperensif. Penelitian ini menyajikan suatu sistem keamanan yang disebut port knocking, di mana pengguna terpercaya memanipulasi aturan firewall dengan mengirimkan informasi di seluruh port yang tertutup [6].

Suatu aplikasi model sistem keamanan jaringan berbasis De-Militarised Zone, pada pembuatan aplikasi untuk sistem keamanan komputer ini membahas bagaimana seni keamanan jaringan internet menggunakan De-Militarised Zone. DMZ merupakan mekanisme untuk melindungi sistem internal dari serangan hacker atau pihak-pihak lain yang ingin memasuki sistem tanpa mempunyai hak akses[7].

Analisa Traffic Jaringan dan Desain Jaringan untuk Optimalisasi Bandwidth Internet pada Universitas Kanjuruhan Malang. Pada Penelitian ini menitik-beratkan pada pembuatan jaringan yang lebih optimal pada Universitas Kanjuruhan Malang menggunakan perangkat lunak. Untuk mencapai tujuan tersebut, maka perlu dilakukan perancangan dari topologi jaringan Universitas Kanjuruhan Malang. Dalam pembuatan jaringan digunakan topologi jaringan star. Di dalam proyek akhir ini di gunakan perangkat lunak Mikrotik RouterOS. Di dalam implementasi optimasi bandwidth menggunakan queue yang telah disediakan oleh Mikrotik RouterOS. Untuk analisa paket yang lewat digunakan fasilitas Torch di dalam Mikrotik RouterOS [5].

Perancangan Tata Kelola Teknologi Informasi dengan Framework Cobit pada Infrastruktur dan Keamanan Jaringan di Universitas X. Dalam pada peneltian ini membahas bagaimana membuat rancangan tata kelola infrastruktur dan keamanan jaringan yang relevan dengan kegiatan operasional sehari-hari pada Puskom universitas X, sesuai dengan Framework CobIT, [4]. Mengoptimalkan sebuah jaringan warung internet dan keamanan jaringan yaitu dengan cara melakukan proses filterisasi dan pembatasan hak akses pada situs-situs tertentu (situs berbahaya dan mengandung unsur pornografi) dengan menggunakan Mikrotik Routerboard. dan mengimplementasikan proses manajemen bandwidth serta mengoptimalkannya menggunakan Mikrotik Routerboard pada sebuah jaringan warung internet sehingga menghasilkan koneksi internet yang stabil [2].

Metode analisis jaringan adalah metode terstruktur yang secara luas digunakan untuk menganalisis sebuah sistem jaringan komputer.

Salah satu metode yang digunakan adalah metode analisis dan perancangan jaringan dengan pendekatan sistem [3]. Metode ini akan menggunakan beberapa tahap sebagai panduan dalam menganalisi sebuah sistem jaringan.

III. METODE PENELITIAN

3.1. *Network Analysis*

Network analysis merupakan proses analisis terhadap berbagai kebutuhan yang berhubungan dengan jaringan, kebutuhan dari pembangunan dan

pengembangan sistem jaringan yang ada. Dengan analisis jaringan ini maka ada akan diketahui apa saja kebutuhan dari sistem jaringan yang akan diubah atau dikembangkan [3]

3.2. *Network Architecture*

Network Architecture merupakan proses pengembangan struktur jaringan secara konseptual, proses pengembangan dilakukan setelah proses analisis jaringan dilakukan. *Network Architecture* menjelaskan mengenai proses pemilihan topologi antar fungsi jaringan, dan bagaimana melakukan optimisasi antar setiap komponen di dalam arsitektur jaringan yang akan dikembangkan [3].

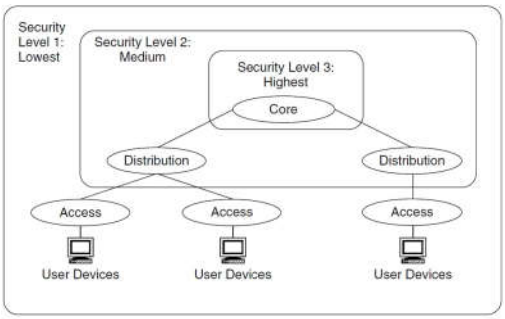
Beberapa tahapan dalam *Network Architecture* [3], yaitu:

a. *Topology Selection*
   Pada bagian ini menjelaskan mengenai topologi jaringan yang digunakan seperti topologi *bus, ring, star, mesh,* atau *hierarki,* beserta penjelasan mengapa topologi tersebut yang pada akhirnya dipilih dan digunakan.
b. *Technology Selection*
   Pada bagian ini menjelaskan mengenai teknologi jaringan yang dipilih (*Ethernet, Fiber Channel, Frame Relay, SONET, ATM,* dll) beserta penjelasan mengapa teknologi-teknologi tersebut yang dipilih dan digunakan.
c. *Equiptment Type/ Class*
   Pada bagian ini menjelaskan mengebai jenis piranti jaringan yang akan dipakai (*hub, switch, router, repeater, bridge, gateway, firewall,* dll).
d. *Component Relationships*
   Pada bagian ini menjelaskan mengenai komponen arsitektur jaringan dan relasinya, baik yang bersifat internal maupun eksternal.

3.3. *Network Design*

Network Design menjelaskan menjelaskan mengenai proses mengembangkan datil fisik dari arsitektur jaringan dalam bentuk *blueprint* (cetak biru), serta pemilihan vendor, piranti dan *service provider* yang digunakan [3]. Selain itu pada bagian ini juga dilakukan proses desain *traceability* unutk meleihat keterkaitan antara *problem statement, requirement analysis, network architecture,* dan *network design.* Tahap ini dibagi lagi menjadi beberapa bagian, yaitu:

a. *Vendor, equipment and Service Provider Selection*
   Pada bagian ini menjelaskan mengenai proses pemilihan *vendor,* piranti, dan *service provider.* Bagian ini diawali dengan menentukan kriteria evaluasi terhadap kandidat *vendor,* piranti, dan *service provider* beserta bobotnya masing-masing.
b. *Existing Network*
   Pada bagian ini menjelaskan mengenai aspek fisik dari jaringan yang telah diimplementasikan secara detil yang terdiri dari lokasi setiap piranti jaringan (termasuk perencanaan pengkabelan) dan bagaimana masing-masing piranti jaringan tersebut saling terhubung.
c. *Network Blueprint*
   Bagian ini menjelaskan mengenai aspek fisik dari jaringan yang akan dirancang secara detil yang terdiri dari setiap piranti jaringan dan bagaimana masing-masing piranti jaringan tersebut saling terhubung.
d. *Design Traceability*
   Pada bagian ini menjelaskan mengenai keterkaitan antra *problem statement, requirement, architecture decisions,* dan *design decisions.*



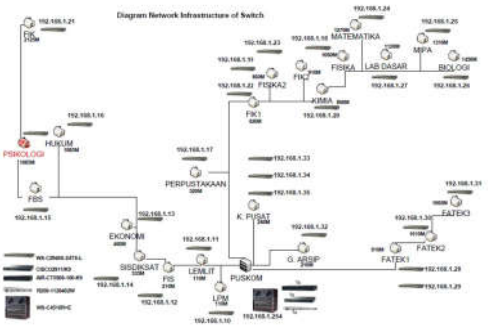
Gambar 1: *The Access/Distribution/Core Architectural Model* [3]

Gambar 1 merupakan *Model Network security* [3], yang akan diimplementasikan di UNIMA. Peneliti mengambil metode perancangan jaringan dari ini sebagai dasar pengembangan penelitian yang akan dilakukan

IV. HASIL DAN PEMBAHASAN

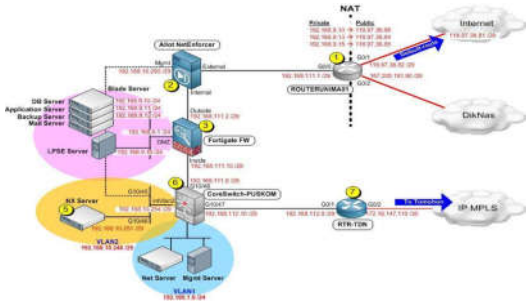
4.1. *Network Analysis* (kondisi awal jaringan UNIMA)

Gambar 2 merupakan skema jaringan yang terimplementasi sekarang di UNIMA. Jaringan UNIMA menggunakan teknologi *fiber optic*. Dari skema jaringan tersebut UNIMA menggunakan topologi jaringan *star* dengan PUSKOM sebagai pusat dari jaringan yang ada. Terdapat dua pengguna dalam jaringan UNIMA yaitu pengguna LAN dan WLAN. Topologi jaringan yang berbentuk *extended star* yaitu koneksi dari server puskom ke setiap gedung dan juga dari setiap gedung (kantor dan fakultas) ke *switch serta j*aringan *wireless access point..*



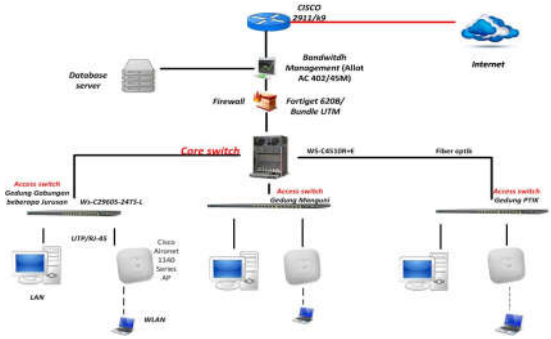
Gambar 2: Kondisi awal Jaringan UNIMA

Gambar 3 merupakan *Logical diagram* (*full view*) jaringan UNIMA yang terimplementasi di Pusat Komputer (Pusat Komputer) UNIMA. Infrastruktur jaringan di Puskom menggunakan teknologi yang cukup modern sudah menggunakan *firewall* (keamanan sistem), *bandwidth management,* dan *core switch.* Namun terdapat perancangan yang kurang baik pada infrstruktur jaringan di Puskom, yaitu koneksi dari *bandwidth management* ke *firewall* terjadi *bottle neck* (leher botol) atau terjadi pengecilan *bandwidth* dari *firewall* ke *core switch,* ini terjadi karena pengaktifan anti virus di *firewall* sehingga mengakibatkan akses data internet yang masuk jaringan internal menjadi lambat.



Gambar 3: *Logical diagram* (*full view*) jaringan kampus UNIMA

Gambar 4 merupakan skema jaringan yang terimplementasi dari server (Puskom) ke Fakultas Teknik (Fatek). Koneksi dari setiap *client* ke internet masih bersifat koneksi langsung *(direct connection)*, tanpa ada *filtering*, proses *caching* atau otentikasi melalui *proxy server*. Hal ini selain akan mengakibatkan kesulitan dalam melakukan monitoring ataupun audit penggunaan jaringan komputer di UNIMA, juga mengakibatkan *bandwidth* terpakai banyak yang terbuang percuma atau tidak optimal pemanfaatannya. Infrastruktur jaringan seperti ini juga menjadi rentan dan *vulnerable*



Gambar 4: Skema jaringan yang terimplementasi di Fakultas Teknik UNIMA

4.2. *Network Architecture*

Setelah proses analisis jaringan dilakukan maka proses selanjutnya adalah pada bagian *network architecture*. Tahapan-tahapan yang akan dilakukan adalah:

a. *Topology Selection*

Untuk topologi tidak ada perubahan yaitu tetap menggunakan topologi *star*

b. *Technology Selection*

Teknologi untuk jaringan LAN dari Puskom ke fakultas dan kantor menggunakan teknologi *fiber optic*. Teknologi ini dipilih karena *fiber optic* memiliki jangkauan yang jauh, tahan terhadap interferensi elektromagnetik, dan dapat mengirim data pada kecepatan yang lebih tinggi dari jenis kabel lainnya. Sementara untuk menghubungkan antar piranti jaringan yaitu dalam gedung, menggunakan teknologi *fast Ethernet* yaitu untuk menghubungkan perangkat jaringan. Dimana teknologi *fast Ethernet* dapat mendukung semua jenis topologi jaringan. Penggunaan teknologi *fast Ethernet* didasarkan pada kondisi berikut. Kapasitas maksimal data aplikasi universitas yang masih dibawah 100 MB, jarak anatar piranti dalam suatu gedung di bawah 100 meter serta harga teknologi *fast ethernet* juga masih terjangkau dibandingkan dengan teknologi lain. Selain itu instalasi *fast ethernet* juga mudah. Sedangkan untuk teknologi WLAN menggunakan cisco aironet yang sudah mendukung vlan.

c. *Equiptment Type/ Class*

Adapun jenis piranti jaringan yang akan dipakai *yaitu router, switch, core switch, firewall, server*, *bandwidth management*. Piranti jaringan sudah tersedia dan akan dimanfaatkan sesuai kebutuhan.

d. *Component Relationships*

Pembangunan komponen relasi ekternal dan internal dibedakan pada proses *addressing/ routing* dan penerapan akses kontrol (VLAN) yang sesuai dengan kebutuhan jaringan UNIMA. Dalam perencanaan dan implementasi skema jaringan diperlukan *redesign* alamat logikal atau IP Addressing seluruh jaringan yang ada. Pemilihan pengalamatan jaringan (IP *addressing*) harus benar-benar dipertimbangkan secara baik, agar disesuaikan kebutuhan sekarang dan mendatang jadi kedepan tidak perlu ada perubahan yang signifikan lagi.

IP *address* untuk jaringan UNIMA mengggunakan IP *address* kelas b, dibagi dalam lima bagian yaitu kantor pusat, fakultas, kantor instansi, *wifi* dan lab. Untuk akses sistem informasi atau jaringan internet di lingkungan kampus UNIMA seharusnya sudah memiliki kebijakan *(policy)* dan prosedur *(procedure)* yang sejalan dengan visi misi kampus. Oleh karena itu itu rekomendasi yang diusulkan adalah sebagai pembuatan kebijakan (*policy*)

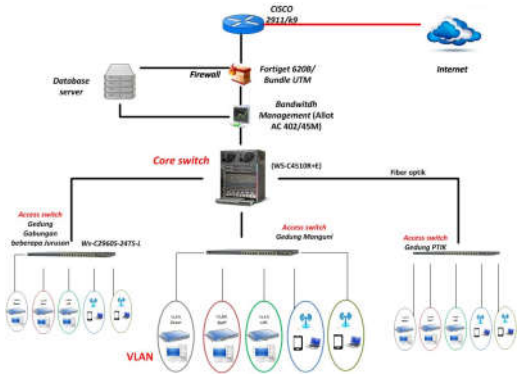
dan prosedur (*procedure*) pemanfaatan dan penggunaan sistem informasi secara tertulis untuk dipublikasikan serta disosialisasikan kepada seluruh civitas akademika kampus UNIMA. Kebijakan dan prosedur harus mencakup topik area keamanan kunci atau *password*, manajemen resiko, identifikasi aset kritis, keamanan fisik, manajemen sistem dan jaringan, otentikasi dan otorisasi, kontrol akses *(access-control)*, manajemen kelemahan *(weakness management)*, manajemen insiden *(incident response)*, kesadaran *(awareness)* dan pelatihan *(training)*, dan privasi *(privacy)*.

4.3. *Network Design*

Setelah proses *network architecture masuk pada proses network design.* Tahap ini dibagi lagi menjadi beberapa bagian yaitu:

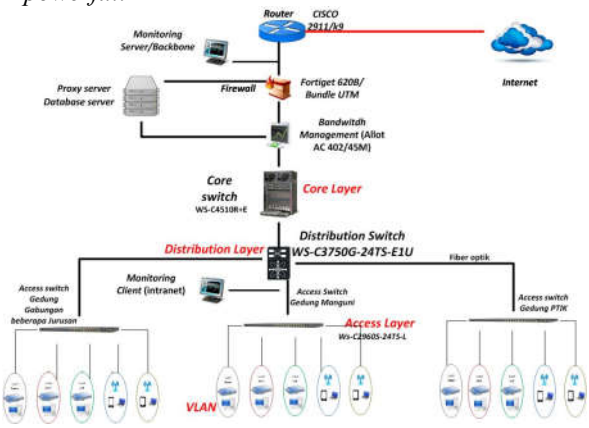
a. *Vendor, equipment* dan *Service Provider Selection*
Pemilihan vendor, *equipment and service provider* di sesuaikan dan dengan kebutuhan jaringan dan biaya untuk membangun jaringan kebutuhan jangka pendek dan jangka panjang dan sesuai kesepakatan dari pihak pengelola jaringan (puskom), penanggung jawab (rektorat), dan vendor.

b. *Existing Network*
Pada bagian ini menjelaskan mengenai aspek fisik dari jaringan yang telah diimplementasikan secara detil yang terdiri dari lokasi setiap piranti jaringan (termasuk perencanaan pengkabelan) dan bagaimana masing-masing piranti jaringan tersebut saling terhubung. Gambar 5 merupakan perancangan infrastruktur jaringan jangka pendek Fakultas Teknik UNIMA dengan memanfaatkan perangkat jaringan yang sudah ada tanpa harus mengeluarkan biaya. Perubahan tempat antara *firewall* dan *bandwidth management* karena adanya "*bottle neck" atau* terjadi penyaringan antivirus pada *firewall* yang mengakibatkan akses data internet melambat. Infrastruktur jaringan Fatek UNIMA dirancang dengan *design Modern Campus Network* atau jaringan komputer terorganisir dan sistematis yang sudah bersifat modern, memanfaatkan perangkat *manageable switch* baik yang mendukung layer 2 maupun layer 3 pada layer OSI. Pemanfaatan *manageable switch* yang mampu membagi *broadcast domain* atau VLAN (*Virtual Local Area Network*), mengakibatkan pengaturan *(control)* dan pemanfaatan *(utilitas)* komunikasi data melalui jaringan komputer semakin efektif dengan performance yang sangat baik. Keuntungan pemanfaatan VLAN pada jaringan UNIMA antara lain: *Flexibility*, *Scalability* dan *Security*.



Gambar 5: Perancangan infrastruktur jaringan jangka pendek Fakultas Teknik UNIMA

c. *Network Blueprint*
Pada bagian ini menjelaskan mengenai aspek fisik dari jaringan yang akan dirancang secara detil yang terdiri dari setiap piranti jaringan (termasuk perencanaan penkabelan) dan bagaimana masing-masing piranti jaringan tersebut saling terhubung.
Pada rancangan topologi jaringan dan perangkat keras untuk jangka panjang pada gambar 6, akan di implementasikan *modern campus network* yang seutuhnya, dengan ditandai adanya bagian yang berfungsi sebagai *Core Switch*, *Distribution Switch* dan *Access Switch*. Semua perangkat *switching* diharapkan sudah menggunakan perangkat yang manageable, sehingga dapat dilakukan management VLAN, *routing* inter VLAN berbasis *Routing Protocol* (*Dynamic*), *Filtering*, *Monitoring* dan penerapan *policy* setiap komunikasi data lebih *powerfull* dan dilakukan lebih baik.



Gambar 6: Perancangan infrastruktur keamanan jaringan Fakultas Teknik UNIMA

i. Kebutuhan Perangkat

Pada rancangan tersebut, akan ditambahkan sebuah *Multilayer Switch* yang berfungsi sebagai *Distribution Switch* untuk menghubungkan antara *Access Switch dengan Backbone* atau *Core Switch. Core Switch* dimaksudkan untuk melakukan *packet switching* atau *routing* dengan kecepatan penuh tanpa adanya *policy filtering* atau pembatasan. Proses *filtering* akan dilakukan pada *distribution switch*. *Distribution*

switch dirancang menggunakan *Cisco catalyst* seri 3750G-24TS-E1U. Keunggulan dari *Cisco catalyst* model ini adalah selain sudah mendukung *full routing*, juga mendukung BGPv4, EIGRP, OSPF, dan PIM. Sebagai a*ccess switch*, di gedung-gedung cisco seri catalyst 2960. Setiap *Access switch* nanti akan terhubung ke *distribution switch* dengan menggunakan gigabit *ethernet* (UTP Cat 6 atau Cat 5E). Pada access switch ini akan diimplementasikan port VLAN, sesuai dengan fungsi atau unit kerja dimana suatu pengguna (*user*) akan di-*assign* oleh *administrator*.

ii. Pengelolaan Jaringan Terdistribusi dan menggunakan *Protokol Routing* dinamis

Jika pada rancangan jaringan untuk jangka pendek pengelolaan jaringan semua terpusat pada *core switch*, maka pada rancangan jaringan untuk jangka panjang, pengelolaan jaringan nantinya dapat dilakukan secara terdistribusi, yakni pengelola disetiap gedung dapat membagi atau menambah jaringan VLAN sesuai kebutuhan masing-masing tanpa mempengaruhi jaringan di gedung yang lain. Rancangan ini dimaksudkan untuk mengantisipasi peningkatan jumlah pengguna dan utilitas jaringan di setiap gedung, termasuk perkembangan unit-unit kerja yang tentu saja akan banyak mengalami kemajuan. Perbedaan lain antara rancangan jaringan jangka pendek dan jangka panjang adalah bahwa pada rancangan jaringan jangka pendek, belum mengharuskan implementasi *protokol routing* yang *dynamic* seperti RIP, IGRP atau EIGRP. Sedangkan pada rancangan jaringan jangka panjang, sudah harus implementasi protokol routing dynamic seperti RIP, IGRP atau EIGRP. Jika nantinya semua distribution switch sudah menggunakan product dari vendor Cisco, maka Protokol EIGRP merupakan pilihan terbaik untuk mengelola routing jaringan intranet.

.

V. KESIMPULAN

Hasil analisis jaringan, terdapat dua pengguna dalam jaringan UNIMA yaitu pengguna LAN dan WLAN, masalah pada infrastruktur keamanan di setiap fakultas dan kantor yang terhubung dengan server di Puskom, karena jaringan dari setiap kantor dan fakultas ke Puskom masih bersifat *flat* atau jaringan tradisional dan tidak adanya filtering atau akses kontrol dari setiap kantor dan fakultas yang terhubung dengan server yang terdapat di Puskom. Dari hasil analisis dibuat dua perancangan jaringan dengan yaitu perancangan jangka pendek (pemanfaatan piranti yang sudah ada) dan perancangan jaringan jangka panjang yang merupakan pengembangan dari rancangan jaringan jangka pendek (penambahan piranti jaringan) untuk kebutuhan masa yang akan datang.

Suatu sistem keamanan jaringan bisa dibuat lebih baik tapi keamanan jaringan tidak ada jaminan apakah suatu sistem jaringan dapat dikatakan *secure* atau *reliable*. Namun, keamanan dapat ditingkatkan dalam skala berkelanjutan dari 0 hinggga 1, atau dari kondisi tidak *secure* menjadi relative *secure*.

REFERENSI

[1] Aswandi. (2009). Infrastruktur Jaringan Komunikasi Antar Perusahaan Menggunakan Analisa Top-Down Model Untuk Mendukung Data Center. *Jurnal Ilmiah Abdi Ilmu*, 171-181.

[2] [2]Hizbullah, A. (2012). Optimalisasi Bandwiidth dan Keamanan Jaringan dengan Filterisasi pada Warung Internet menggunakan Mikrotik Routerboard. *Jurnal Komputasi*, 103-116.

[3] McCabe, J. D. (2007). *Network Analysis, Architecture, and Design.* Amsterdam, Boston, Tokyo, Heidelberg, London, Neew York, Oxford, Sidney: Morgan Kaufmann Publishers is an imprint of Elsevier.

[4] Nangoi, F. Y. (2011). Perancangan Tata Kelola Teknologi Informasi dengan Framework Cobit pada Infrastruktur dan Keamanan Jaringan di Universitas X. *Master Thesis of Magister Management Technology*, 2-5.

[5] Rochman, E. F. (2009). Analisa Traffic Jaringan dan Desain Jaringan untuk Optimalisasi Bandwith Internet pada Universitas Kanjuruhan Malang. *Jurnal Matematika dan Komputer Indonesia*, 25-32.

[6] Sembiring, I., Widiasari, I. R., & Prasetyo, S. D. (2009). Analisa dan Implementasi Sistem Keamanan Jaringan Komputer. *Jurnal Informatika*, 1-15.

[7] Suyatno, A. (2009). Aplikasi Model Sistem Keamanan Jaringan Berbasis De-Militarised Zone. *Jurnal Informatika Mulawarman*, 6-12.

[8] Wibowo, A. (2008). Perancangan Sistem Keamanan Komputer Berbasis Jaringan Waktu Nyata. *Jurnal Artificial, ICT Research Center UNAS*, 36-52.