Implementasi Management Network Security Pada Laboratorium CISCO Universitas Bina Darma

Edi Surya Negara
Fakultas Ilmu Komputer
Universitas Bina Darma
Jalan Jenderal Ahmad Yani No.12 Palembang
Pos-el : e.s.negara@mail.binadarma.ac.id

Abstract : *Edi Surya Negara "Management Network Security Implementation At Laboratory CISCO Bina Darma University".*
The development of computer network technology as a medium for data communications to this increase. The need for the use of shared resources on the network both software and hardware has resulted in the emergence of a variety of network technology development itself. Along with the high level of need and the increasing number of network users who want some form of network that can deliver maximum results, in terms of both efficiency and increase network security itself, the improvement efforts continue to be made by the various parties. One measure of the quality of the computer network management and network security is good. By it because they needed a real action to create a system management and network security is good. So with the management and security of the network that will either guide to good computer network.

Keywords:
Computer networks, network management, and network security.

Abstrak : Edi Surya Negara "Implementasi *Management Network Security* Pada Laboratorium CISCO Universitas Bina Darma.
Perkembangan teknologi jaringan komputer sebagai media komunikasi data hingga saat ini semakin meningkat. Kebutuhan atas penggunaan bersama resources yang ada dalam jaringan baik software maupun hardware telah mengakibatkan timbulnya berbagai pengembangan teknologi jaringan itu sendiri. Seiring dengan semakin tingginya tingkat kebutuhan dan semakin banyaknya pengguna jaringan yang menginginkan suatu bentuk jaringan yang dapat memberikan hasil maksimal, baik dari segi efisiensi maupun peningkatan keamanan jaringan itu sendiri, maka upaya-upaya penyempurnaan terus dilakukan oleh berbagai pihak. Salah satu tolak ukur dari jaringan komputer yang berkualitas adalah management dan keamanan jaringan yang baik. Oleh kerena itu dibutuhkan suatu tindak nyata untuk membuat suatu sistem management dan pengamanan jaringan yang baik. Sehingga dengan adanya management dan keamanan jaringan yang baik akan mencipkan jaringan komputer yang berkulitas.

Keyword : Jaringan komputer, Management jaringan , dan Keamanan jaringan

1. PENDAHULUAN

Perkembangan teknologi jaringan komputer telah merubah cara interaksi sosial, komersial, politik, dan pribadi mengikuti evolusi jaringan komputer secara global. Salah satu bentuk nyata evolusi jaringan komputer itu adalah perkembangan jaringan *internet*. Meningkatnya penggunaan *internet* di dunia bisnis mendorong semakin berkembang dan beragam *content-content* di *internet*.

Pada saat sebuah badan usaha atau instansi baik pemerintah atau swasta mengintegrasikan jaringannya ke jaringan publik atau yang lebih kita kenal dengan istilah *internet*,

maka akan timbul suatu masalah baru yang sangat mengancam yaitu masalah keamanan jaringan atau sering disebut dengan *network security*, (Negara, E.S., Rachman, B. and Lutfi, 2013, Edi, S.N., 2014). Ancaman keamanan ini banyak sekali ditemukan oleh pengguna seperti *Virus, Trojan, Worm, DoS, Hacker, Sniffing* dan sebagainya dengan apapun istilah *underground* yang sering kita dengar, yang pasti akan menyusahkan kita pada saat ancaman – ancaman ini menyerang sistem kita. Semakin besar skala suatu jaringan maka semakin kompleks administrasi dari jaringan itu, oleh karena itu diperlukan suatu mekanisme keamanan dan metode untuk dapat mengoptimalkan sumber daya jaringan tersebut.

Sejalan dengan hal di atas, Universitas Bina Darma telah memiliki sistem jaringan komputer yang telah diimplementasikan di masing - masing unit kerja. Seperti sistem jaringan komputer di pusat pengolahan data, atau jaringan komputer di masing – masing laboratorium. Jaringan komputer yang telah diimplementasikan dengan baik di Universitas Bina Darma harus memiliki sistem keamanan yang baik untuk dapat melindungi seluruh data dan informasi penting yang selalu diincar oleh pihak - pihak yang ingin mencoba menyusup atau bahkan merusak sistem informasi dan jaringan komputer Universitas Bina Darma.

Menurut Howard dalam Sofana (2010:306) dalam buku yang berjudul CISCO CCNA & Jaringan Komputer mengemukakan tentang *computer security*. " Computer security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks."(Jhon D. Howard, "An Analysis Of Security Incidents On The *Internet* 1989 – 1995)".

Menurut Garfinkel dalam Sofana (2010:307) keamanan komputer mencakup empat aspek yaitu, *privacy*, *integrity*, *authentication*, dan *availability*.

1. *Privacy atau confidentiality*

   Privacy mencakup kerahasian informasi. Inti aspek *privacy* adalah bagaimana menjaga informasi agar tidak dilihat atau diakses oleh orang yang tidak berhak. Sebagai contoh, *e-mail* seorang pemakai tidak boleh dibaca orang lain bahkan *administrator*. Salah satu usaha yang dapat dilakukan yaitu penggunaan *enkripsi*. Kita dapat menggunakan *enkripsi* untuk setiap dokumen atau informasi lainnya yang dianggap rahasia dan hanya kita sendiri yang dapat membukanya menggunakan kunci yang tepat.

2. *Integrity*

   Integrity atau integritas mencakup keutuhan informasi. Inti aspek *integrity* ini adalah bagaimana menjaga informasia agar tetap utuh. Informasi tidak boleh diubah, baik ditambah atau pun dikurangi, kecuali jika mendapat izin dari pemilik informasi. *Virus, Trojan horse*, atau pemakai lain yang mengubah informasi tanpa izin pemiliknya merupakan contoh masalah yang menggangu aspek ini. Penggunaan anti virus, *enkripsi* , dan *digital signature*, merupakan contoh usaha untuk mengatasi masalah ini.

3. *Authentication*

Authentication atau otentikasi berkaitan dengan keabsahan pemilik informasi. Harus ada cara untuk mengetahui bahwa informasi benar – benar asli, kemudian yang mengakses informasi adalah orang – orang yang berhak, dan hanya yang berhak saja yang boleh memberikan informasi tersebut kepada orang lain. Penggunaan *access control* seperti *login* dan *password* merupakan usaha yang dilakukan untuk memenuhi aspek ini. *Digital signature* dan *watermarking* juga merupakan salah satu usaha untuk melindungi *intellectual property* yang sesuai dengan aspek *authentication*.

4. *Availability*

Aspek ini berhubungan dengan ketersediaan informasi. Informasi harus tersedia manakala dibutuhkan. Contoh serangan terhadap aspek ini yaitu ”*Denial of Service attack*“ atau DoS attack. misalkan, server dikirim *request* palsu sacara bertubi – tubi sehingga tidak dapat melayani permintaan lain. Contoh lain yaitu *mailbomb*, dimana seorang pemakai dikirim ribuan bahkan jutaan *e-mail* sehingga pemakai tidak dapat membuka *e-mail* miliknya atau kesulitan mengakses *e-mail*, terutama jika akses *internet* dilakukan melalui saluran telephon.

Management network security pada Universitas Bina Darma sebagian besar sudah diimplementasikan dengan baik. Akan tepati akan lebih baik lagi apabila seruluh bagian terkercil dari jaringan Universitas Bina Darma diimplementasikan *management network security*, khususnya jaringan intranet yang akan menuju jaringan internet (dari internal *network* ke external *network*) sehingga akan membantu kinerja server yang telah ada di unit kerja MIS_CUT dalam pengamanan *network*.

Salah satu bagian dari jaringan komputer tersebut adalah laboratorium komputer. Laboratorium merupakan salah satu pintu masuk pihak – pihak yang tidak bertanggung jawab untuk merusak jaringan Universitas Bina Darma. Sehingga dibutuhkan mekanisme pengamanan yang nyata pada seluruh laboratorium komputer Universistas Bina Darma. Oleh sebab itu penulis bermaksud untuk mengimplementasikan *management network security* pada salah satu laboratorium komputer di Universitas Bina Darma dengan memanfaatkan berbagai sumber daya jaringan yang ada di laboratorium CISCO seperti Router Cisco 2600 series dan Switch Catalyst 2950 . Adapun judul penelitian ini adalah “Implementasi *Management Network Security* Pada Laboratorium CISCO Universitas Bina Darma”.

Penelitian ini bertujuan untuk mengimplementasikan *managemet network security* pada laboratorium CISCO Universitas Bina Darma agar keamanan jaringan pada laboratorium tersebut semakin meningkat dan meminimalisir ancaman – ancaman keamanaan

jaringan pada Universitas Bina Darma serta mengevaluasi secara singkat dampak dari implementasi.

Keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis *(business continuity)*, meminimasi risiko bisnis *(reduce business risk)* dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis (Negara, E.S. and Andryani, R., 2014, ISO 27001 dalam Sarno dan Iffano, 2009, 27). Menurut Syafrizal, M, (2007)Keamanan informasi terdiri dari perlindungan terhadap aspek-aspek berikut:

1. *Confidentiality (kerahasiaan)* aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
2. *Integrity (integritas)* aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin fihak yang berwenang *(authorized)*, menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.
3. *Availability* (ketersediaan) aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).

Gambar 1. Information Assurance Model

Target *network security* adalah bagaimana mencegah dan menghentikan berbagai *threats* (potensi serangan) agar tidak memasuki dan menyebar pada suatu *network* (Sofana 2010:310). Pada dasarnya banyak *threats* (potensi serangan) yang mengancam *network security* , seperti yang telah dipaparkan oleh Sofana dalam bukunya yang berjudul Cisco CCNA & Jaringan Komputer (2010: 310) berbagai *threats* yang mengancam *network security* dapat digolongkan menjadi beberapa golongan, diantaranya adalah :

1. *Viruses, Worms, and Trojan horses*
2. *Spyware and adware*
3. *Zero-day attacks (zero-hour) attacks*
4. *Hacker attacks*
5. *Denial of service attacks (DoS)*
6. *Data interception and theft*
7. *Identity theft*

Implementasi Management Network Security pada Laboratorium CISCO Universitas Bina Darma meliputi aspek – aspek sebagai berikut :

A. Implementasi *Access Control* pada seluruh komputer *client* yang ada di laboratorium CISCO Universitas Bina Darma.

B. Implementasi dan konfigurasi *Network Address Translation* (NAT) pada Router Cisco 2600 series.

C. Implementasi dan konfigurasi *Virtual Local Area Network* (VLAN) pada Router Cisco 2600 series dan implementasi *Metode Variabel Length Subnet Mask* (VLSM) untuk penghematan *host*.

D. Implementasi dan konfigurasi sistem keamanan pada *Router Cisco 2600 series* dan *Switch Cisco Catalyst 2960* antara lain :

   1. Membatasi *Control Access* ke Router dan Switch
   2. Membatasi *access telnet* ke Router dan Switch
   3. *Block spoof* / paket – paket berbahaya. Seperti *block traffic virus* pada *Router Cisco 2600 series*
   4. Membatasi *Simple Network Management Protocol* (SNMP) pada *Router Cisco 2600 series*
   5. Mengenskripsi semua password pada Router dan Switch
   6. Menonaktifkan semua layanan yang tidak digunakan
   7. Membuat LOG pada *Router Cisco 2600 series* untuk memcatat seluruh kegiatan router.

2. METODOLOGI PENELITIAN

Metodologi adalah ilmu yang digunakan untuk memperoleh kebenaran mengggunakan penelusuran dengan tatacara tertentu dalam menemukan kebenaran, tergantung dari realitas yang sedang dikaji. Dalam penelitian ini metode yang digunakan adalah penelitian tindakan atau *action research*, dalam penelitian tindakan mendeskripsikan, mengiterpretasi dan menjelaskan suatu situasi pada waktu yang bersamaan dengan melakukan perubahan atau intervensi dengan tujuan perbaikan atau partisipasi.

Menurut Halilintar dalam Davison, Martinson & Kock (2004), menyebutkan penelitian tindakan sebagai metode penelitian, didirikan atas asumsi bahwa teori dan praktek dapat secara tertutup diintegrasikan dengan pembelajaran dari hasil intervensi yang direncanakan setelah diagnosis yang rinci terhadap konteks masalahnya. 5 tahapan yang merupakan siklus dari action research :

1. Melakukan diagnose (Diagnosing)

   Melakukan identifikasi masalah – masalah pokok yang ada guna menjadi dasar kelompok atau organisasi sehingga terjadi perubahan.

2. Membuat rencana tindakan (Action Planning)

   Penelitian dan partisipan bersama – sama memahami pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada.

3. Melakukan tindakan (Action Taking)

   Peneliti dan partisipan bersama – sama mengimplementasikan rencana tindakan denga harapan dapat menyelesaikan masalah.

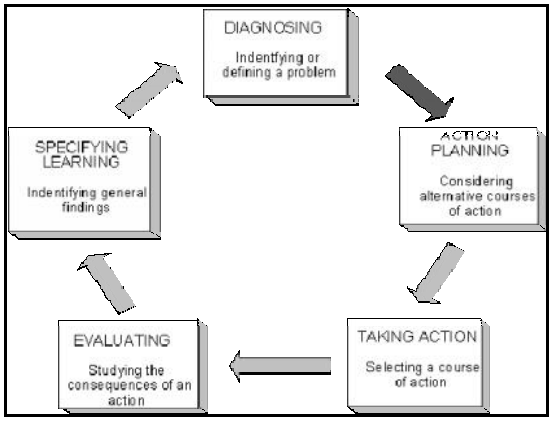
4. Melakukan evaluasi (Evaluating)

   Setalah masa implementasi (action taking) dianggap cukup kemudian peneliti bersama partisipan melaksanakan evaluasi hasil dari implementasi.

5. Pembelajaran (Learning)

   Tahap ini merupakan bagian akhir siklus yang telah dilalui dengan melaksanakan review tahap pertahap yang telah barakhir kemudian penelitian ini dapat berakhir.

Seluruh kriteria dalam prinsip pembelajaran harus dipelajari, perubahan dalam situasi organisasi dievaluasi oleh peneliti dan dikomunikasikan kepada *client*, peneliti dan *client* merefleksikan terhadap hasil proyek, yang nampak akan dilaporkan secara lengkap dan hasilnya secara eksplisit dipertimbangkan dalam hal implikasinya terhadap penerapan *Canonical Action Research* (CAR). Untuk hal tertentu, hasilnya dipertimbangkan dalam hal implikasinya untuk tindakan berikutnya dalam situasi organisasi lebih – lebih kesulitan yang dapat dikaitkan dengan pengimplementasian perubahan proses.



Gambar 2. ***Action Research Mode***

Sumber : O'Brien, R.(2001)

3. HASIL

3.1. Analisis Kebutuhan Perangkat Keras (*Hardware*)

Perangakat keras yang dibutuhkan untuk mengimplementasikan management network security pada laboratorium CISCO Universitas Bina Darma antara lain :

1. Cisco Router 2600 Series.
2. Switch Cisco Catalyst 2950.
3. Switch D-link 16 Port.
4. Personal Computer.

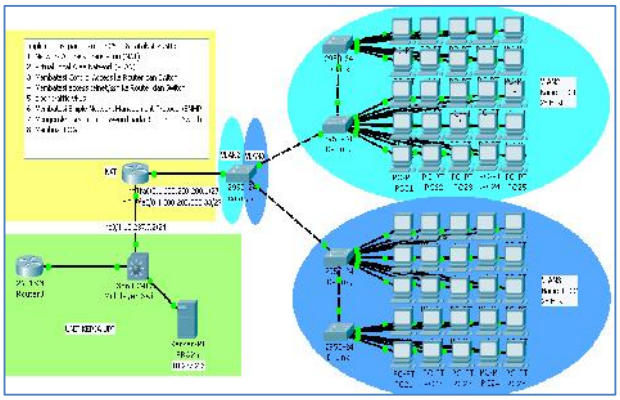
3.2. Analisis Kebutuhan Perangkat Lunak (*Software*)

a. *Microsoft Windows XP SP-2* dan
b. *Ubuntu 10.04* sebagai sistem operasi *client*
c. *Cisco Internetwork Operating System Software (IOS) version 12.0(5)T1 (Router 2600 series)*
d. *Cisco Internetwork Operating System Software (IOS) version 12.1(22)EA1 (Swtich catalyst 2950)*

3.3. Perancangan Management Network Security Pada Laboratorium CISCO

Analisis yang dilakukan terhadap peta jaringan laboratorium CISCO menghasilkan beberapa rancangan pengembangan. Salah satu rancangan pengembangan yang akan diimplementasikan adalah pengembangan management network security laboratorium CISCO. Rancangan pengembangan ini bertujuan untuk meningkatkan keamanan network pada laboratorium tersebut, sehingga nantinya diharapkan dapat membantu kinerja firewall yang telah diimplementasi pada unit pelayanan teknis (UPT). Disamping itu implementasi ini diharapkan memberikan efek yang baik untuk peningkatan proses belajar mengajar pada laboratorium CISCO. Pengembangan yang akan dilakukan antara lain adalah :

1. Pengembangan network topologi dengan menggunakan Cisco Router 2600 series dan Switch catalyst 2950.
2. Implementasi *Access Control* pada seluruh komputer *client* yang ada di laboratorium CISCO Universitas Bina Darma.
3. Implementasi dan konfigurasi *Network Address Translation* (NAT) pada Router Cisco 2600 series.
4. Implementasi dan konfigurasi *Virtual Local Area Network* (VLAN) pada Router Cisco 2600 series dan implementasi *Metode Variabel Length Subnet Mask* (VLSM) untuk penghematan *host.*
5. Implementasi dan konfigurasi sistem keamanan pada *Router Cisco 2600 series* dan *Switch Cisco Catalyst 2960* .



Gambar 3. Rancangan Implementasi Management Network Security Pada Laboratorium CISCO

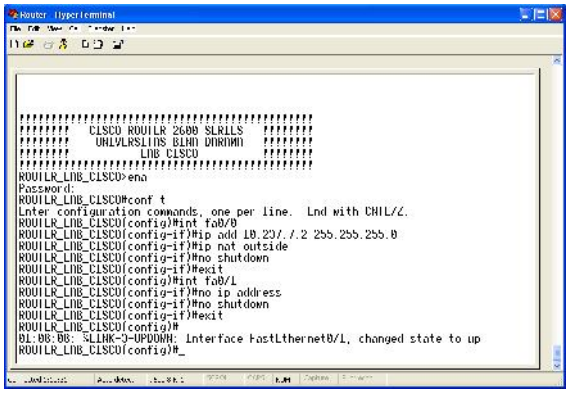
Untuk mengimplementasikan Management Network Security pada jaringan computer laboratorium CISCO ada beberapa tahapan yang harus konfigurasi. Tahapan – tahapan tersebut antara lain :

1. Konfigurasi Hostname, Line Console, Line VTY serta Banner dan mengenskripsi semua password
2. Konfigurasi Network Address Translation (NAT)
3. Konfigurasi Virtual Local Area Network (VLAN)
4. Konfigurasi Control Access ke Router dan Switch
5. Membatasi access telnet ke Router dan Switch
6. Block traffic virus
7. Membatasi Simple Network Management Protocol (SNMP)
8. Membuat LOG

Konfigurasi Network Address Translation atau yang lebih biasa disebut dengan NAT adalah suatu metode untuk menghubungkanlebih darisatu komputer ke jaringan internet dengan menggunakan satu alamat IP.

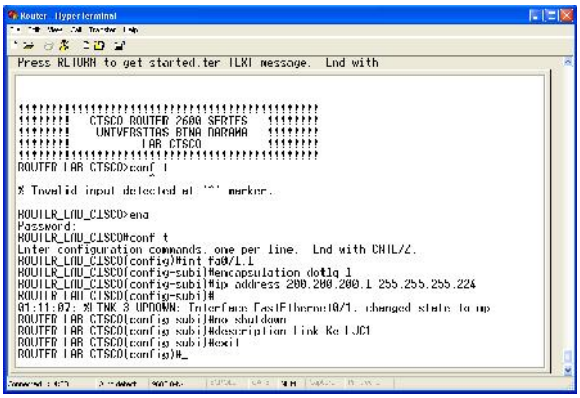
Metode NAT ini diimplementasikan pada laboratorium CISCO sehingga seluruh client bisa mengakses internet melalui satu IP yang didaftarkan pada ROUTER_LAB_CISCO. Ide utama dari implementasi ini adalah untuk meninggkatkan keamanan jaringan dengan menyembunyikan alamat IP internal dari luar network.

Pada ROUTER_LAB_CISCO terdapat dua buah interface fastethernet yaitu interface fastethernet 0/0 dan fastethernet 0/1. Fastethernet 0/0 dikonfigurasi sebagai IP NAT Outside dengan IP Address 10.237.7.234/24. Sedangakan untuk interface fastehternet 0/1 dikonfigurasi sebagai IP NAT Inside dengan IP Address 200.200.200.1/27 dan 200.200.200.33/27.



Gambar 4. Konfigurasi Network Address Translation (NAT)

Pada laboratorium CISCO diimplementasi dua buah VLAN yaitu VLAN_LJC1 dan VLAN_LJC2. Implementasi ini bertujuan untuk memudahkan administrator jaringan dalam memanagement seluruh jaringan yang ada di laboratorium tersebut.



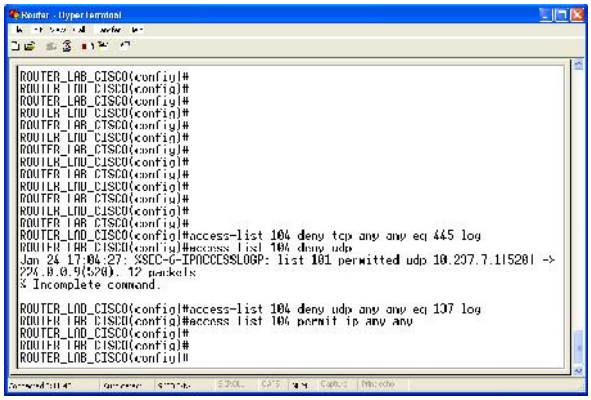
Gambar 5. Konfigurasi VLAN

Router merupakan sebuah device yang berfungsi untuk meneruskan paket-paket dari sebuah network ke network yang lainnya (baik LAN ke LAN atau LAN ke WAN) sehingga host-host yang ada pada sebuah network bisa berkomunikasi dengan host-host yang ada pada network yang lain. Router menghubungkan network-network tersebut pada network layer dari model OSI, sehingga secara teknis Router adalah Layer 3 Gateway. Selain itu juga router dapat menangkap dan melihat aktivitas trafik dalam jaringan, sehingga memudahkan kita untuk mengklasifikasikan trafik dan membuang paket-paket yang tidak diperlukan. Berkembangnya virus jaringan yang sangat cepat, cukup merugikan para penyedia jaringan dan pengguna komputer. Serangan virus ini telah banyak mengkonsumsi bandwidth sehingga trafik aplikasi yang sebenarnya tidak bisa

dilewatkan melalui jaringan karena jaringan telah dipenuhi oleh paket-paket virus.

PC yang terkena virus akan selalu mengirimkan paket-paket ke jaringan dalam jumlah besar dalam waktu singkat. Jika pada saat kita menangkap trafik pada suatu interface, terdapat pola paket yang sangat banyak dan menggunakan port TCP, UDP atau ICMP yang sama, kemungkinan jaringan ini terkena virus.

Implementasi yang dilakaukan pada laboratorium CISCO adalah melakukan filter dan blocking terhadap beberapa port TCP dan UDP yang diidentifikasi sebagai port yang sering digunakan virus untuk membroadcast packet – packet virus.



Gambar 6. Blocking Trafic Virus

3.4. Hasil Implementasi

Hasil dari penelitian yang dilakukan dengan judul Implementasi *Management Network Security* Pada Laboratorium CISCO Universitas Bina Darma dengan memanfaatkan Cisco Router 2600 dan Switch Catalyst 2950 adalah sebagai berikut :

1. Seluruh komputer client yang ada di laboratorium CISCO Universitas Bina Darma telah diinstal dengan sistem operasi tunggal yaitu Ubuntu 10.10 yang diharapkan dapat meminimalisir ancaman keamanan pada network laborarotium CISCO dengan mengatur access control terhadap setiap user yang masuk pada laboratorium tersebut. Selain itu penggunaan sitem operasi ubuntu 10.10 diharapkan sebagai usaha untuk mendukung penggunaan sistem operasi open source kepada seluruh mahasiswa Universitas Bina Darma.
2. Jaringan *Virtual Local Area Network* pada laboratorium CISCO terkoneksi ke internet dengan menggunakan Network Address Translation (NAT) dengan IP Address 10.237.7.234 Subnet Mask 255.255.255.0 sebagai IP NAT Outside dan IP Address 200.200.200.1 Subnet Mask 255.255.255.224 dan IP Address 200.200.200.33 Sunet Mask 255.255.255.224 sebagai IP NAT Inside.
3. Jaringan Virtual Local Area Network telah diimplementasikan *Variabel Length Subnet Mask* (VLSM) dengan menggunakan network 255.255.255.224.
4. Jaringan *Virtual Local Area Network* (VLAN) telah dibangun pada Laboratorium CISCO Universitas Bina Darma yaitu VLAN 10 name LJC1 dan VLAN 20 name LJC2.
5. Pada Cisco Router 2600 Series dan Switch Catalyst 2950 telah dikonfigurasi

Management Networik security untuk membantu pengamanan network pada laboratorium CISCO.

4. SIMPULAN

Kesimpulan yang didapat dari penelitian implementasi *management network security* dengan memanfaatkan Cisco Router 2600 Series dan Switch Catalyst 2950 untuk meningkat keamanan *network* pada laboratorium CISCO adalah :

1. Cisco Router 2600 Series mampu mentranslasikan komputer client yang ada di laboratorium dengan menggunakan alamat privete ke jaringan public dengan menggunakan Network Address Translation.
2. Cisco Router 2600 Series dan Switch Catalyst 2950 mampu melakukan management terhadap network dengan menggunakan virtual local area network.
3. Cisco Router 2600 Series mampu melakukan filter trafic terhadap packet – packet yang tidak diinginkan seperti packet virus dll.
4. Implementasi Management Network Security pada laboratorium CISCO meningkatkan keamanan network pada laboratorium CISCO Universitas Bina Darma.

DAFTAR RUJUKAN

Edi, S.N., 2014, Optimasi End Users Awareness of Data and System Securities Using IT Audit Methodology and Tools. *In Seminar Nasional Teknologi Informasi dan Komunikasi (SNASTIKOM 2014)* (Vol. 2, pp. 269-274). Sekolah Tinggi Teknik Harapan (STTH) Medan.

Negara, E.S., Rachman, B. and Lutfi, 2013, A., *Analysis and Design of Information Security Management System (ISMS) at Computer Network Infrastructure of Bina Darma University.*

Negara, E.S. and Andryani, R., 2014. *A Review: Security Framework Information Technology for University Based on Cloud Computing.*

Odom. 2005. *Computer Networking First-Step.* Yogyakarta: Andi

Sopandi, Dede. 2005. *Instalasi dan Konfigurasi Jaringan Komputer Edisi Revisi*. Bandung: Informatika Bandung.

Sofana. 2010. *CISCO CCNA & Jaringan Komputer.* Bandung: Informatika Bandung.

Lammle. 2005. *CCNA Cisco Certified Network Associate.* Jakarta: Gramedia.

Rafiudin. 2004. *Mengupas Tuntas Cisco Router.* Jakarta: Elex Media Komputindo.

Anonymous,(http://id.wikipedia.org/wiki/Simple_Netwo k_Management_Protocol)

Anonymous,(http://pandawa.ipb.ac.id/ilmukomputer.org/2006/09/27/monitor-dan-memblok-trafik-virus-pada-cisco-router/index.html).http://www.web.net/~robrien/papers/arfinal.html