ANALISIS DAN PERANCANGAN JARINGAN HOTSPOT PADA SEKOLAH SMK SATYA BAKTI I DAN II JAKARTA TIMUR MENGGUNAKAN ENDIAN FIREWALL COMMUNITY

¹Arisantoso, ²Irfan, dan ³Didin Samsudin Adhuri

¹ Fakultas Teknik Universitas Islam Attahiriyah

Jl. Kampung Melayu Kecil III No. 15, Tebet, Jakarta Selatan, 12840, Telp: 021-836706126

² Fakultas Ilmu komputer Universitas Budi luhur

Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, 12260. DKI Jakarta, Telp: 021-5853753

³ Fakultas Teknik Universitas Islam Attahiriyah

Jl. Kampung Melayu Kecil III No. 15, Tebet, Jakarta Selatan, 12840, Telp: 021-836706126

email: 1arisantoso2008@gmail.com, 2irfan03092008@gmail.com, 3adhuri007@yahoo.com

Abstrak SMK Satya Bakti I dan II mempunyai misi ingin menjadikan sekolah tersebut sebagai CYBER SCHOOL sehingga seluruh area SMK Satya Bakti I dan II yang terhubung jaringan Internet untuk mendukung pembelajaran di tiap-tiap kelas, untuk itu diharapkan setiap Ruang Kelas siswa, Ruang Guru, Ruang Kepala Sekolah, Ruang Tata Usaha atau Administrasi, Kantin dan di koridor sekolah bisa mengakses Internet dengan Hotspot atau internet tanpa kabel (wireless) dengan jumlah pengakses seluruh komunitas sekolah SMK Satya Bakti I dan II. Metode Penelitian ini menggunakan dua metode yaitu metode pengumpulan data yang meliputi survei lapangan, wawancara, observasi dan studi pustaka, metode perancangan yang dilakukan meliputi rancangan topologi jaringan dengan menggunakan Edraw Max 5.1, konfigurasi endian firewall comunity dilakukan pada web browser. Hasil yang dicapai adalah dengan adanya rancangan arsitektur jaringan internet berbasis Wifi (Wireless-Fidelity) yang dapat menjangkau seluruh ruang dan kelas di area sekolah yang terhubung ke hotspot area serta kemudahan untuk melakukan pencarian informasi internet di sekolah khususnya bagi para siswa/siswi, kepala sekolah, guru, para orangtua atau wali murid. Sistim belajar mengajar akan menjadi lebih terdukung dengan ketersediaan akses internet hotspot yang dapat digunakan di mana saja asal masih di lingkungan sekolah yang masih terjangkau oleh access point di area hotspot.

Kata Kunci : Analisis, Perancangan, Hotspot, Endian.

1. Pendahuluan

Jaringan komputer merupakan sistem yang terdiri dari berbagai sumber daya yang digunakan baik hardware dan software yang kesemuanya dapat berkomunikasi dan dapat mengakses semua informasi khususnya di internet.

Jaringan Wireless adalah bidang disiplin yang berkaitan dengan komunikasi antar sistem tanpa menggunakan kabel. Jaringan nirkabel ini sering dipakai untuk jaringan komputer baik pada jarak dekat maupun pada jarak jauh. Jenis jaringan yang popular dalam kategori jaringan nirkabel meliputi Wireless LAN/WLAN dan Wi-Fi. [3]

Sebagian besar sekolah di kota-kota besar di Indonesia terutama di Kota DKI Jakarta rata-rata sudah memiliki komputer yang terhubung dengan internet. Fungsi internet dikalangan sekolah biasanya untuk administrasi sekolah maupun dalam proses pembelajaran. Untuk mempermudah proses komunikasi dan pertukaran data maka setiap komputer harus terhubung ke dalam jaringan. [3]

Menurut Onno W. Purbo [8] Hotspot adalah sebuah wilayah terbatas yang dilayani oleh satu atau sekumpulan Access Point Wireless LAN standar 802.11a/b/g. Dimana pengguna dapat masuk ke dalam Access Point secara bebas dan mobile menggunakan perangkat sejenis notebook, laptop, PDA dan sebangsanya.

Saat ini tahun 2012-an SMK Satya Bakti I dan II mempunyai misi ingin menjadikan sekolah tersebut sebagai *CYBER SCHOOL* sehingga seluruh area SMK Satya Bakti I dan II yang terhubung jaringan Internet dapat mendukung pembelajaran di tiap-tiap kelas, untuk itu diharapkan setiap Ruang Kelas siswa, Ruang Guru, Ruang Kepala Sekolah, Ruang Tata Usaha atau Administrasi, Kantin dan di koridor sekolah bisa mengakses Internet tanpa kabel (wireless) dengan jumlah pengakses seluruh komunitas sekolah SMK Satya Bakti I dan II. Karena luasnya lokasi dan banyaknya ruangan di sekolah yang memiliki 2 Lantai maka dibutuhkan suatu rancangan *HotSpot* yang efektif dan efisien dengan biaya yang terjangkau, dapat meng-*cover* seluruh area sekolah SMK Satya Bakti I dan II khususnya para siswa sekolah, guru dan pegawai TU yang berjumlah sekitar ± 500 orang.

2. Permasalahan

Berdasarkan analisa yang telah dilakukan di SMK Satya Bakti I dan II Jakarta Timur maka rumusan masalah yang akan dibahas adalah sebagai berikut: Bagaimana menganalisis dan merancang Internet Hotspot pada SMK Satya Bakti I dan II Jakarta Timur?

3. Literatur Riview

Penelitian Joko Ariyanto, (2008) Universitas Muhammadiyah Surakarta tentang Desain dan Implementasi Autentikasi Jaringan Hotspot Menggunakan Pfsense dan Radius Server di Fakultas Teknik Elektro Universitas Muhammadiyah Surakarta. Implementasi autentikasi jaringan Hotspot dengan menggunakan sistem operasi pfsense sebagai router. [4]

Penelitian Nisfil Mafidah, (2009) Universitas Negeri Malang tentang Perancangan dan implementasi infrastruktur Hotspot di SMK Yasmu Manyar Gresik. Perancangan dan implementasi Hotspot untuk para guru dan siswa dengan menggunakan modem ADSL sebagai router dan access Point Hotspot menggunakan antena kentongan E-Goen. [7]

Penelitian Isaac Wiguna, William Wijaya, Indrawan Cahyadi (2012) Universitas Bina Nusantara Jakarta tentang analisis dan perancangan jaringan hotspot pada sekolah kristen ketapang I dengan menggunakan mikrotik sebagai router dan konfigurasinya dilakukan dengan aplikasi winbox yang digunakan untuk remote akses jaringan menjadi lebih terkontrol. [3]

Dari ketiga peneliti pendahulu terkait dengan permasalahan perancangan jaringan Hotpsot belum ada yang mendalami masalah keamanan jaringan dari ancaman serangan pihak dalam dan luar. Pun demikian pengaksesan terhadap kategori situs tertentu seperti pornografi di internet dapat dikendalikan oleh firewall router berbasis opensource dengan endian firewall community.

4. Pembahasan

Dalam perancangan ini terdiri dari yaitu perangkat keras (*hardware*) dan perangkat lunak berbasis opensource yang bisa didapatkan secara gratis pada alamat website <u>http://www.endian.com/en/community/</u>.

Adapun usulan arsitektur jaringan komputer Hotspot yang diusulkan sebagai berikut Gambar 1 :



Gambar 1. Arsitektur Jaringan Hotspot yang Diusulkan

4.1 Segmentasi Internet Protocol (IP) Address

Segmentasi IP Address yang diusulkan pada implementasi arsitektur jaringan pada SMK Satya Bhakti I, II secara kebutuhan jaringan, segmentasi yang dipakai menggunakan tiga segmentasi, di antaranya adalah:

- 1) Warna Merah (*Red*) adalah segmentasi *Endian Firewall* dengan koneksi internet dari ADSL Router Telkom Speedy dengan IP Address 192.168.121.1
- 2) Warna Hijau (*Green*) adalah segmentasi *Endian Firewall* dengan koneksi antara jaringan lokal (LAN) yang menuju Switch HUB. IP Address yang digunakan adalah 172.19.1.1, IP ini akan menjadi *Gateway* / jembatan untuk komputer client dimana user dapat mengakses internet.
- 3) Warna Biru (*Blue*) adalah segmentasi *Endian Firewall* untuk koneksi Wireless / Hotspot. Disini perlu adanya 3 Access Point untuk dilakukan konfigurasi dengan *Endian Firewall Server* agar dapat dikelola secara terpusat pengaturannya. IP yang digunakan adalah 192.168.2.1. IP ini akan menjadi *Gateway* untuk komputer client yang menggunakan komputer laptob, Handphone atau sejenisnya yang mempunyai perangkat jaringan Wirelless lihat Tabel 1.

Network	IP	Status
INTERNET	192.168.121.4	Connected – (0d 0h 2m 46s)
Gateway	192.168.121.1	
DNS-Server	202.134.0.155	203.130.193.74
LAN	172.19.1.1	Proxy on (transparent)
Wireless	192.168.2.2	Proxy on (transparent)

Tabel 1. Pengaturan Akses Antar Segmen Endian Firewall Community

Segmentasi IP Address

1)	Modem ADSI	L
	IP	: 192.168.121.1
	Subnet Mask	: 255.255.255.0
	DNS	: 202.134.0.155
		203.130.193.74
2)	Endian Firewa	all Server
	IP	: 172.19.1.1
	Subnet Mask	: 255.255.0.240
	Gateway	: 192.168.121.1
	DNS	: 202.134.0.155
		203.130.193.74
3)	IP server Mor	nitoring
	IP	: 172.19.1.2
	Subnet Mask	: 255.255.255.0
	Gateway	: 172.19.1.1
	DNS	: 202.130.196.155
		203.130.193.74
4)	DHCP Client	Hotspot (AP) 1
	IP	: 192.168.2.2 - 80
	Subnet Mask	: 255.255.255.0
	Gateway	: 192.168.2.1
5)	DHCP Client	Hotspot (AP) 2
	IP	: 192.168.2.81 - 160
	Subnet Mask	: 255.255.255.0
	Gateway	: 192.168.2.1
6)	DHCP Client	Hotspot (AP) 3
	IP	: 192.168.2.161 - 254
	Subnet Mask	: 255.255.255.0
	Gateway	: 192.168.2.1
7)	DHCP Client	dengan Kabel LAN
	IP a.t. a.t. i	: 172.19.1.3 - 254
	Subnet Mask	: 255.255.255.0
	Gateway	: 172.19.1.1

5. Pengujian dan Analisa

Pengujian dan analisa hasil perancangan jaringan Hotspot, baik hardware maupun software diperlukan untuk mengetahui kesiapan alat yang dirancang apakah sudah sesuai dengan standar yang telah ditetapkan sehingga pada saat implementasi dapat berjalan sesuai perancangan. Setelah rancangan selesai di install tahapan berikutnya melakukan pengujian terhadap sistem. Skenario pengetesan seperti pada Tabel 2 berikut :

No.	Fitur Aplikasi Endian	Skenario Pengujian
1	Fitur Content Filter	Mengakses situs pornografi yang belum atau telah dimasukkan dalam daftar situs Blacklist berdasarkan alamat web.
2	Fitur Filtering E-mail	Melakukan pengiriman spam pada kotak masuk e-mail jaringan lokal dengan memasukkan ke dalam daftar situs Blacklist
3	Fitur Anti Virus	Memasukkan jenis virus yang berasal dari sumber eicar.com melalui alamat port http.
4	Fitur Instrusion Prevention System	Melakukan serangan icmp postweep pada jaringan lokal.
5	Fitur File Sharing	Melakukan pengiriman file dalam bentuk satuan Gigabyte
6	Fitur Quality of Service (QoS)	Melakukan akses streaming web disalah satu situs video untuk melihat satuan kecepatan data streaming.
7	Fitur DHCP Server	Menghubungkan komputer ke Server Endian untuk melihat apakah pengalamatan IP Address sesuai dengan settingan pada DHCP server.

Tabel 2. Skenario Pengetesan Sistem Keamanan Router Endian

6. Pengujian terhadap Fitur Content Filter

Pemblokiran dilakukan terhadap situs-situs yang dianggap berbahaya (situs porno, hacking, dan judi) dapat dilakukan dengan mengkonfigurasi panel Content Filtering. Klik pada tanda icon yang berwarna hijau (allow) pada keyword yang diinginkan sampai icon berubah warna menjadi merah (deny). Fitur ini digunakan untuk melakukan pemeriksaan apakah situs tersebut berbahaya atau tidak. Pemblokiran juga dapat dilakukan berdasarkan pemeriksaan alamat URL situs yang ingin dikunjungi. Dengan mengubah icon yang berwarna hijau (allow) menjadi merah (deny) Gambar 2 dan 3.

388 | Arisantoso, et al.

 Adult 	⇒i	 Advertisements 	->1
Porn	⇒i	Ads	⇒i
- Audio	⇒i	Drugs	⇒i
<u>Audio-video</u>	아	Drugs	⇒i
Gambling	아	Hacking	⇔ i
Gambling	⇔ i	Warez	아
		Hacking	⇒i
Violence	⇒i	Web-based	\rightarrow
Violence	⇔∎	Mail	\Rightarrow
Aggressive	⇒i		

Gambar 2. Tampilan Pengaktifan Fitur Content Filtering Akhir

← → C © www.porn.com	\$
🛓 Laman ini dalam bahasa Inggris 🗸 Apakah Anda ingin menerjemahkannya? 🛛 Terjemahkan 🕅 Nggak	Opsi 🗸
ERROR	
The requested URL could not be retrieved While trying to retrieve the URL: http://www.porn.com/	
The following error was encountered:	
Unable to forward this request at this time.	
Sorry, you are not currently allowed to request: http://www.porn.com/ from this cache undi you have authenticated yourself.	
This request could not be forwarded to the origin server or to any parent caches. The most likely cause for this error is that: The cache administrator does not allow this cache to make direct connections to origin servers, and All configured parent caches are currently unreachable.	
Your cache administrator is <u>webmaster</u> .	
Endian Erevall - Powered by Souid	

Gambar 3. Pengujian Akses internet dengan Fitur Content Filtering

6.1 Pengujian Fitur Intrusion Prevention System (IPS)

Terdapat pada menu "Services" panel atas kemudian pilih "Intrusion Prevention" di panel samping. Menggunakan varian SNORT sebagai Intrusion Prevention System Gambar 4 dan 5.

C (8 Daps://1/2.	19.1.1.1.0443/cgi-bin/ias.cgi	
	System Status Network Services Firewall Proxy VPN Logs	
	Intrusion Prevention System	
DHCP server	>> Intrusion Prevention System Rules Editor	
Dynamic DNS		
Antivirus Engine	D Intrusion Prevention System	
Time server	Earthin Interview Derivative Contemport	
Spam Training	Enable initiation Prevention System	
Intrusion Prevention	SNORT Bulas Satisas	
Traffic Monitoring	onoki kuita atuinga	
SNMP Server	Emerging Threats SNORT rules *	
Quality of Service	Automatically fetch SNORT rules Update rules now	
	Choose update schedule "	
	Daily 💌	
	Custom SHORT Rules * Pib Berkas Tidak ada beryang dipilih Upload custom rules. You may either use a tar.gz, z(p, or angleules file containing the rules	

Gambar 4. Tampilan Awal Konfigurasi IPS

🕞 Open	- Barrow - 18	Manufact in	×	← → × 🚯 bttp5://172.19	📓 detiketo × 🔣 BIXIAN Firewall - does en: × 🗋 Sekolah Kehidupan: Menya × 🔶 📼 🖬 👘 🕰 🛝
Organize Vew folder	Documents	earch Documents		endian fr	Difine Efficient
Favorites	Documents library Includes: 4 locations	Arrange by: Fol	der 🕶		System Status Network Services Frenal Prox VPN Logs
Downloads	Name	Date modified	Туре 🔺	DHCP server Dynamic DNS Antivirus Engine	Intrusion Prevention System Rules Editor Intrusion Prevention System
Documents	C:\Users\LABKOM	24/12/2011 9:25	E File fol	Time server Spam Training Intrusion Prevention	Enable Intrusion Prevention System
Music Fictures	[www.indowebster.com]-VmWare_Work ENDIAN Second	15/11/2011 13:08 14/03/2012 17:05	WinRA Micros	Traffic Monitoring SNMP Server Quality of Service	Emerging Threats SIORT rules * (2) Automotody feto: SIORT rules (3) Bigdete rules new:
Computer	snort thata	14/03/2012 17:04 13/01/2012 21:23	Text D CoreIE		Caston SIGIT Rules *
Local Disk (C:)	<				Betaal soot.rar Lipbad casten nies You may either use a for gr. zijs, or aingte .nite file containing the soles
File n	ame: snort 🗸 Ser	mua Jenis Berkas	•		Seve and restort
N	Custom SNORT Rules *	Open 🛛 Ca	incei		Status: Connected: main (bil db 24m 7b) Uppfine: 11 03 43 up 25 min, 0 users, laad average: 172, 1.54, 1.07

Gambar 5. File Snort dan simpan Settingan IPS

6.2 Pengujian Fitur Quality of Service (QoS)

Untuk membatasi kecepatan downlink dan uplink pada komputer client dapat menggunakan fitur Quality of Service yang telah disediakan oleh sistem Endian Firewall. Pilih menu "Services" pada panel atas, kemudian pilih "Quality of Service" pada panel samping. Klik icon panah hijau "Add Quality of Service Device" Gambar 6.

	firewall, MUNITY							
	System St	atus Network	Services	Firewall	Proxy	VPN	Logs	
	Quality of S	Service Devices	5					
DHCP server	>> Devices	Classes Rules						
Dynamic DNS	@ Add Out	ne of Conica Davica						
Antivirus Engine	Add Quan	LY OF SERVICE DEVICE						
Time server	Device	Upstream Bandwid	ith (kbit/s)		Downs	tream Ba	ndwidth (kbit/s)	Actions
Spam Training				No	entries to d	isplay		
Intrusion Prevention								
Traffic Monitoring								
SNMP Server								
Quality of Service								

Gambar 6. Tampilan Konfigurasi Awal Quality of Service

Pada tampilan layar berikutnya ditampilkan berapa kecepatan upstream dan downstream yang ingin diberlakukan pada tiap user. Area pembatasan kecepatan juga dapat diatur pada drop-down menu "target device". Klik tombol "Add" untuk menyelesaikan pengaturan QoS Gambar 7 dan 8.

	System	Status Network		Firewall	Proxy VP1		
	Quality of	f Service Device	s				
DHCP server	>> Device	s Classes Rules					
Antivirus Engine	Add Qua	lity of Service Device					
Time server							
Spam Training	Target I	Device					
Intrusion Prevention	Uplink	main 19					
Traffic Monitoring	Upstream	n Bandwidth (kbit/s)	3	_	Downstream	Bandwidth (kbit/s)	
SNMP Server	128			_	10000		
Quality of Service	Enabled						
	Add	or <u>Cancel</u>					* This Field is require
	Device	Upstream Bandwi	dth (kbit/s)		Downstream	Bandwidth (kbit/s)	Actions
				No e	ntries to display		

Gambar 7. Tampilan Konfigurasi Pembatasan Kecepatan QoS

	System Statu	s Network	Services	Firewall	Proxy		Logs	
	Quality of Ser	vice Devices						
DHCP server	» Devices C	lasses Rules						
Dynamic DNS		_						
Antivirus Engine		100	The confi	iguration h	as been c	hanged	and needs to be applied	
			in order (to make th	a change	active		
Time server			in order i	to make th	e changes			
Time server ipam Training			Analy	to make th	e change:			
ime server ipam Training ntrusion Prevention			Apply	to make th	e unanye:			
Time server Epam Training Intrusion Prevention Fraffic Monitoring		1	(Apply)	to make th	e unanges			
Time server ipam Training ntrusion Prevention fraffic Monitoring INMP Server	C Add Quality o		Apply		e changes			
Time server ipam Training ntrusion Prevention fraffic Monitoring iNMP Server Quality of Service	Add Quality of	f Service Device	Apply		e thanges			
Time server Spam Training Intrusion Prevention Traffic Monitoring SNMP Server Quality of Service	C Add Quality o	If Service Device	Apply)	s)	Down	stream B	andwidth (kbit/s)	Actions

Gambar 8. Tampilan Konfigurasi QoS yang Berhasil Dibuat

7. Kesimpulan

Atas dasar analisis dan pembahasan yang telah dilakukan sebelumnya, dapat ditarik beberapa kesimpulan sebagai berikut :

- 1) Dengan dirancangnya *Internet Hotspot/Wireless* pada SMK Satya Bakti I dan II Jakarta Timur dapat menjangkau seluruh area seperti ruang dan kelas, kantin, laboratorium dengan jarak maksimal 100 meter.
- 2) Setiap user dibatasi akses internetnya dengan menggunakan content filter atau URL filter di komputer server endian firewall yang berfungsi untuk memblokir situs-situr terlarang serta mengatur management bandwidth yang digunakan untuk membagi bandwidth akses internet kepada semua pengguna khususnya pada SMK Satya Bakti I dan II Jakarta Timur.

8. Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada LPPM Universitas Islam Bandung atas terlaksananya acara Seminar Nasional Penelitian dan Pengabdian 2012 ini dan kepada pihak Panitia Prosiding atas kerjasamanya untuk memuat makalah seminar terpilih.

9. Daftar Pustaka

Arifin, Z., (2007). Mengenal Wireless LAN (WLAN). Yogyakarta : Penerbit ANDI Publisher.

Gunadi, (2006), Teknologi wireless LAN dan Aplikasinya, Jakarta : PT. Elex Media Komputindo.

Wiguna, I., Wijaya, W. Cahyadi. I., (2012). Analisis Dan Perancangan Jaringan Hotspot Pada Sekolah Kristen Ketapang I Dengan Menggunakan Mikrotik, diakses tanggal 27 september 2012 dari <u>http://library.binus.ac.id/eColls/eThesis/Lain-lain/2012-1-00134-IF%20Ringkasan.pdf</u>

Ariyanto. J., (2008). Desain dan Implementasi Autentikasi Jaringan Hotspot Menggunakan Pfsense dan Radius Server. Tugas Akhir, Jurusan Teknik Elektro S1, Universitas Muhammadiyah Jakarta.

Kuntoro, T. (2005). Jaringan Wi-Fi. Yogyakarta : Penerbit ANDI Publisher.

- Mafidah, N. (2009). Perancangan dan Implementasi Infrastruktur Hotspot di SMK Yasmu Manyar Gresik. Tugas Akhir, Jurusan Teknik Elektro D3 TKJ, Universitas Negeri Malang.
- Purbo. O.W. (2006). Buku Pengangan Internet Wireless dan Hotspot. Jakarta : PT. Elex Media Komputindo.

Onno. P (2006). Internet Wireless dan Hotspot. Jakarta : Elex Media Komputindo.

Iwan. S. (2005). Wirelless Lan untuk Rumah dan Kantor kecil", Jakarta : Info Komputer, Gramedia.

Mulyanta, E. S. (2006). Pengenalan Protokol Jaringan *Wireless* Komputer. Yogyakarta: Penerbit ANDI Publisher.