 ISSN: 1411-3201

MANAJEMEN KEAMANAN JARINGAN INFORMASI MENGGUNAKAN IDS/IPS STRATAGUARD "STUDI KASUS STMIK AMIKOM YOGYAKARTA"

Joko Dwi Santoso, M. Suyanto, M. Rudyanto Arief
Magister Teknik Informatika STMIK AMIKOM Yogyakarta,
joko@amikom.ac.id, yanto@amikom.ac.id, rudy@amikom.ac.id

ABSTRAKSI

Jaringan komputer terus mengalami perkembangan, baik dari skalabilitas, jumlah node dan teknologi yang digunakan. Hal ini memerlukan pengelolaan jaringan yang baik agar ketersediaan jaringan selalu tinggi. Tugas pengelolaan jaringan yang dilakukan administrator jaringan memiliki banyak permasalahan, diantaranya yang berkaitan dengan keamanan jaringan komputer. Seiring bertambahnya pengguna di dalam sebuah jaringan maka tingkat keamanan jaringan juga menjadi pertanyaan pokok. Apakah dalam mengakses sebuah jaringan internet sudah aman ? Sebagai langkah guna mengantipasi para pengguna yang nakal, maka harus di pilih pola keamanan jaringan yang baik. *Intrusion Detection Sistem (IDS)* merupakan salah satu opsi untuk meningkatkan keamanan jaringan dalam sebuah network baik intranet maupun internet.

Kata Kunci : IDS, IPS, Keamanan Jaringan, Jaringan, IDS/IPS, Jaringan

PENDAHULUAN

Jaringan komputer terus mengalami perkembangan, baik dari skalabilitas, jumlah node dan teknologi yang digunakan. Hal ini memerlukan pengelolaan jaringan yang baik agar ketersediaan jaringan selalu tinggi. Tugas pengelolaan jaringan yang dilakukan administrator jaringan memiliki banyak permasalahan, diantaranya yang berkaitan dengan keamanan jaringan komputer.

Seiring bertambahnya pengguna di dalam sebuah jaringan maka tingkat keamanan jaringan juga menjadi pertanyaan pokok. Apakah dalam mengakses sebuah jaringan internet sudah aman ? Sebagai langkah guna mengantipasi para pengguna yang nakal, maka harus di pilih pola keamanan jaringan yang baik. *Intrusion Detection Sistem (IDS)* merupakan salah satu opsi untuk meningkatkan keamanan jaringan dalam sebuah network baik intranet maupun internet.

Penyusupan (*Intrusion*) usaha merusak dan menyalahgunakan sistem, usaha yang melakukan *compromise* integritas, kepercayaan atau ketersediaan suatu sumberdaya komputer. Definisi ini tidak bergantung pada sukses atau gagalnya aksi tersebut, sehingga berkaitan dengan suatu serangan pada sistem komputer. *Intrusion detection (ID)* singkatnya adalah usaha mengidentifikasi adanya penyusup yang memasuki sistem tanpa otorisasi (misal *cracker*) atau seorang user yang sah tetapi menyalahgunakan *(abuse) privelege* sumberdaya sistem (misal *insider threath*).

Intrusion Detection Sistem (IDS) atau Sistem Deteksi Penyusupan adalah sistem komputer (bisa merupakan kombinasi software dan hardware) yang berusaha melakukan deteksi penyusupan. IDS akan melakukan pemberitahuan saat mendeteksi sesuatu yang dianggap sebagai mencurigakan atau tindakan ilegal. IDS tidak melakukan pencegahan terjadinya penyusupan. Pengamatan untuk melakukan pemberitahuan itu bergantung pada bagaimana baik melakukan konfigurasi IDS.

IDS pada umumnya melakukan dua pekerjaan, yaitu pengumpulan data dan analisis data.Penggolongan IDS bisa dilakukan berdasar banyak karakteristik,
diantaranya adalah:

1. Host Based – Network Based Collection
2. Direct – Indirect Monitoring
3. Internal – External Sensor

Penerapan IDS telah mengalami peningkatan pesat pada tahun-tahun belakangan ini.Salah satu alasannya adalah perkembangan dari internet dan jumlah jaringan yang cukup besar pada setiap organisasi. Peningkatan jumlah mesin pada jaringan ini memunculkan aktivitas yang tidak diinginkan, tidak hanya dari serangan luar, tetapi juga dari dalam seperti disgruntled employes dan orang yang menyalahgunakan privelege untuk keperluan pribadi.

TUJUAN PENELITIAN

Adapun tujuan yang ingin dicapai dalam penelitian tesis ini adalah di jabarkan sebagai berikut :

1. Sebagai syarat kelulusan S2 di STMIK AMIKOM Yogyakarta
2. Untuk merancang sistem IDS di STMIK AMIKOM sebagai solusi permasalahan jaringan.

RUMUSAN MASALAH

Adapun rumusan masalah adalah sebagai berikut:

 ISSN: 1411-3201

1. Bagaimanakah Infrastruktur Jaringan STMIK AMIKOM ?
2. Bagaimanakah menyelesaikan permasalahan keamanan jaringan di Lingkungan STIMIK AMIKOM ?

METODE PENELITIAN

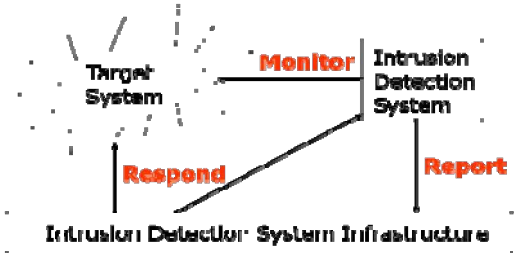
Adapun metode penelitian yang digunakan adalah :

1. Metode pengumpulan data.
   a. Studi Kepustakaan (*Library Research*)
      Metode ini dimaksudkan untuk memperoleh data sekunder dari kepustakaan yang berguna dalam penyusunan landasan teori yang berhubungan dengan permasalahan yang dibahas.
   b. Literature
      Metode ini untuk memperoleh data yang dikutip dari pencarian di Internet.
   c. Alat
      Metode ini untuk memperoleh data dengan menggunakan tools antara lain adalah:
      1. Wireshark
      2. Digiblast
      3. Softperfect Network Scanner
      4. Colasoft Capsa
      5. IDS Sax2
2. Metode analisis Data
   Data yang dikumpulkan akan diolah terlebih dahulu agar dapat disajikan secara lebih jelas. Penyajian data ini dilakukan dalam bentuk deskriptif untuk lebih memperjelas masalah yang dihadapi dan mempermudahkan dalam melakukan suatu analisis.
3. Merancang IDS
   Pada tahap ini dilakukan perancangan IDS yang sesuai. Adapun tahapannya sebagai berikut :
   a. Menginstal IDS / IPS StrataGuard
   b. Konfigurasi IDS / IPS Sebagai Network Policies
      1. Pertama-waktu konfigurasi
      2. Quick Tune
   c. Fisik Deployment
      1. Koneksi ethernet
      2. Mode
4. Pengujian pada sisi server
5. Pengujian pada sisi client
6. Pengujian sistem

LANDASAN TEORI

SISTEM DETEKSI PENYUSUPAN (IDS)

Keamanan Jaringan Komputer Tujuan utama dari keamanan sistem adalah memberikan jalur yang aman antara entitas yang saling bertukar informasi dan untuk menyediakan perlindungan data.



Gambar 2.4 Skema IDS

Insiden keamanan jaringan komputer adalah suatu aktivitas yang berkaitan denganjaringan komputer, dimana aktivitas tersebut memberikan implikasi terhadap keamanan.Secara garis besar insiden dapat diklasifikasikan menjadi:

1. *Probe/scan*: Usaha-usaha yang tidak lazim untuk memperoleh akses ke dalamsuatu sistem, atau untuk menemukan informasi tentang sistem tersebut. Kegiatanprobe dalam jumlah besar dengan menggunakan tool secara otomatis biasadisebut Scan. Bermacam-macam tool yang dipergunakan untuk keperluan ini seperti : *network mapper, port mapper network scanner, port scanner, atau vulnerability scanner*. Informasi yang diperoleh misalkan :
   a. Topologi dari jaringan target
   b. Tipe traffic yang melewati firewall
   c. Hosts yang aktif
   d. Sistem operasi pada host
   e. Software yang berjalan pada server dan versinya.
2. *Account Compromisse* : Penggunaan account sebuah komputer secara ilegal oleh seseorang yang bukan pemilik account, dimana account tersebut tidak mempunyai *privelege* sebagai administrator sistem.
3. *Root Compromisse* : Mirip account compromisse tetapi mempunyai privilege sebagai administrator sistem.
4. *Packet sniffer* :Perangkat lunak/keras yang digunakan untuk memperoleh informasi yang melewati jaringan komputer, biasanya dengan NIC bermodepromiscuous.
5. *Denial of service (DOS)* : Membuat sumberdaya jaringan maupun komputer tidakbekerja, sehingga tidak mampu memberikan layanan kepada user. Misalkan

 ISSN: 1411-3201

sajadengan membanjiri sumber daya komputer, misal CPU,memori,ruang disk,bandwith jaringan. Serangan dapat dilakukan dari satu komputer atau beberapa komputer *(Distributed DOS)*.

6. Eksploitasi perintah : Menyalahgunakan perintah yang bisa dieksekusi.
7. Malicious code : Program yang bila dieksekusi akan menyebabkan sesuatu yangtidak diinginkan didalam sistem. Misal trojan horse, virus dan worm.
8. Penetration : Pengubahan data, privelege, atau sumber daya. Beberapa jenisnya:
   a. *User to Root* : User lokal pada suatu host memperoleh hak admin
   b. *Remote to user* : Pengakses luar memperoleh account lokal di host target
   c. *Remote to Root* : Pengakses luar memperoleh account admin di host target
   d. *Remote to Disk Read* : Pengakses luar bisa membaca file di host target
   e. *Remote Disk write* : Pengakses luar bisa menulis file di host target

Privelege Escalation : User Publik bisa memperoleh akses sebagai user lokal,yang nantinya bisa dilanjutkan ke hak akses sebagai admin.

Pengumpulan Data Dan Hasil Analisisnya

Untuk mendapatkan data yang akurat maka perlu melakukan beberapa sample penetrasi dalam infrastruktur jaringan amikom dengan menggunakan tools sebagai berikut :

a. Intrusion Detection System – Sax2
b. Digiblast Ddos
c. Wireshark
d. Colasoft
e. Softperfect Network Scanner

Adapun hasil dari capture data dan log data dari lapangan dan IC (INNOVATION CENTER) adalah sebagai berikut :

Tabel 3.1. Pengujian Jaringan Wifi dan Lan STMIK AMIKOM Yogyakarta

Tanggal	Jam	Lokasi	SSID	Jenis Serangan
11 - 09 - 2010	13:20	Pengajaran Lama	• Gejayan • Selat 2 dan 3	SYN ACK ATTACK
IDS Sax2				BruteForce
Colasoft				Thresold
Wireshark				Floodder
11 - 09 - 2010	16:00	LAN Pengajaran Lama	-	
Colasoft				
IDS Sax2				Malware Decoder
02 – 02 - 2010	10:15	MSV Studio	-	
IDS Sax2				
Wireshark				Malware Decoder
03 - 08 - 2010	14:00	Wifi	Selat 2 dan 3	SYN ACK ATTACK
IDS Sax2				BruteForce
Colasoft				Thresold
Wireshark				Floodder
Digiblast				Ddos
11 - 10 - 2010	18:00	Wifi	Unit III	Trojan
IDS Sax2				Malware
Colasoft				SYN ACK ATTACK
12 - 03 - 2010	09:00	Wifi	Unit III	BruteForce
IDS Sax2				Thresold
Colasoft				Floodder
Wireshark				Ddos
Digiblast				Trojan
				Malware
				SYN ACK ATTACK
02 - 12 - 2010	10:00	Pengajaran Baru	Pengajaran Baru	Floodder

 ISSN: 1411-3201

IDS Sax2				Ddos
Colasoft				Trojan
Wireshark				Malware
Digiblast				SYN ACK ATTACK
				Duplicated MAC
12 - 12 - 2010	12:20	Basemant Unit II	Basemant Unit II	Ddos
IDS Sax2				SSH Tunneling
Colasoft				SYN ACK ATTACK
Wireshark				Duplicated MAC

IDENTIFIKASI MASALAH

Tinjauan kasus yang telah di identifikasi berdasarkan bukti dari MasterPlan yang di berikan oleh pihak IC (innovation Center) adalah sebagai berikut :

1. Jaringan Komputer STMIK Amikom dikembangkan dengan sistem jaringan yang bersifat tradisional yakni memanfaatkan PC router sebagai pembagi broadcast domain ke setiap unit kerja atau group pengguna jaringan di setiap gedung STMIK Amikom Yogyakarta. Hal ini menyebabkan setiap penambahan unit kerja atau group tertentu maka akan membutuhkan sebuah PC router atau minimal sebuah kartu jaringan agar mampu membentuk jaringan (subnetwork) yang baru sehingga manajemen jaringan dan *maintenance* lebih kompleks dan cenderung kesulitan untuk menerapkan standart *policy* pada setiap jaringan.
2. Pada beberapa subnet (jaringan) atau kelompok user (group), terdapat jaringan yang hanya di*manage* menggunakan *ip aliases* melalui interface pc router, hal ini membuat performance jaringan tidak bekerja dengan optimal. Penggunaan lebih dari satu subnet pada jaringan yang memiliki *broadcast domain* yang sama mengakibatkan *broadcast* yang lebih besar, disamping terdapat permasalahan keamanan karena *administrator* tidak dapat mengontrol komunikasi kedua jaringan yang masih berada pada broadcast domain yang sama. Pembagian subnet jaringan yang hanya memanfaatkan *IP aliases* justru akan mengurangi kinerja atau performa jaringan komputer itu sendiri.
3. Distribusi Internet Protokol Public (IP Public) ke setiap PC Router yang dimaksudkan untuk membagi koneksi internet ke setiap unit/lab menjadikan sistem keamanan jaringan *intranet* STMIK Amikom menjadi rentan dan *vulnerable*. Hal ini karena IP Public yang digunakan oleh setiap PC router otomatis terpublikasi di Internet yang harusnya menjadi jaringan yang tidak dapat dipercaya (*untrust network)*. Dengan kondisi sekarang, maka setiap pengguna internet dimungkinkan untuk melakukan penyerangan ke jaringan Intranet STMIK Amikom, padahal jaringan intranet menjadi jaringan yang aman dari jaringan di luar Jaringan Kampus STMIK Amikom (termasuk Internet).
4. Penggunaan IP Private dan IP Public di setiap PC router di unit-unit/laboratorium, menyebabkan routing jaringan internal dan jaringan public (internet) menjadi satu (digabung), hal ini membuat manajemen dan monitoring komunikasi data antar jaringan intranet atau antar unit/lab sulit dilakukan, karena adanya pemanfaatan fungsi *masquarade (NAT)* atau penyembunyian identitas internet protokol pengguna jaringan. Selain itu komunikasi antar ip public dan ip private sudah tidak sesuai aturan RFC, dimana IP Private seharusnya tidak dapat di routingkan melalui IP Public (non-routabel)
5. Pemberian alamat Internet Protokol pada beberapa unit kerja tidak seragam atau berada pada kelas IP yang berbeda, selain mengakibatkan kesulitan menjamin skalabilitas dan kemampuan untuk dapat diakses dari mana saja, juga membuat administrasi jaringan semakin rumit.
6. Saat ini server-server intranet pada kampus STMIK Amikom dipasangkan IP public yang menyebabkan kemungkinan terpublikasikan atau dapat diaksesnya informasi server internal tersebut dari *Internet*.
7. 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 STMIK Amikom Yogyakarta, juga mengakibatkan

 ISSN: 1411-3201

bandwidth terpakai banyak yang terbuang percuma atau tidak optimal pemanfaatannya.

8. Pemasangan Wireless Access Point untuk mendistribusikan koneksi internet di lingkungan luar gedung kampus STMIK Amikom sebaiknya dipertimbangkan kembali. Jaringan wireless merupakan jaringan yang memiliki tingkat vulnerable yang sangat tinggi, diperlukan monitoring yang terus-menerus dan pemanfaatan teknologi keamanan jaringan wireless berlapis untuk menjamin pengguna benar benar memiliki otorisasi menggunakan akses tersebut.
9. Saat ini, beberapa jaringan wireless (AP) digunakan sebagai *bridge* yang terhubung secara langsung ke pengguna pada jaringan kabel tanpa ada proteksi (filtering), hal ini akan sangat mengganggu trafik yang terjadi pada kedua jaringan tersebut karena masih menggunakan broadcast domain yang sama. Sebaiknya broadcast domain untuk jaringan *wireless* dipisahkan dengan *broadcast domain* jaringan kabel *(wired network)*.
10. Pendistribusian koneksi jaringan kabel UTP melalui switch secara bertingkat (koneksi dari switch yang satu ke switch yang lain karena harus menjangkau lebih dari 100 meter) perlu mendapatkan perhatian atau pengukuran kembali. Karena jika sudah melalui beberapa switch, signal koneksi jaringan akan melemah dan mengakibatkan akses yang lambat atau bahkan terputus.
11. Penggunaan kanal frekwensi dalam pemasangan Access Point atau HotSpot umumnya belum melakukan site-survey terlebih dahulu, sehingga jangkauan atau pemanfaatan hotspot kurang maksimal, akibat terjadi interference antar wireless yang satu dengan yang lainnya. Penempatan Wireless Access point sebaiknya mengukuti kaidah frekwensi yang bersifat re-usable dan dapat dialokasikan pada lokasi yang berdekatan seperti aturan penggunan kanal 1, kanal 6 dan kanal 11 di lokasi yang berdekatan.

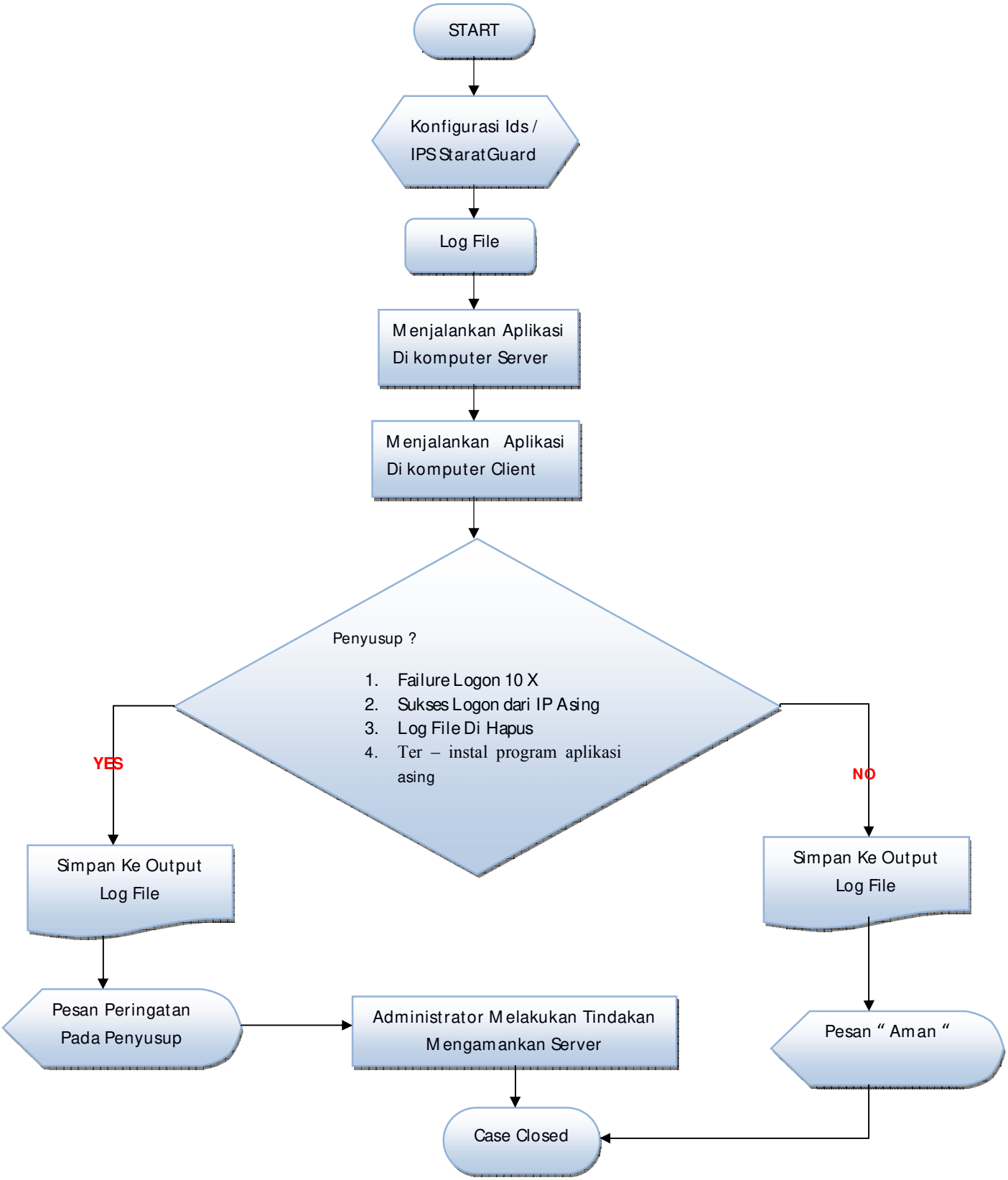
Kondisi saat ini, monitoring traffic hanya dilakukan di *backbone* internet saja, hal ini dapat menyulitkan penelusuran jika terdapat anomali traffik seperti malware yang menginfeksi sebuah komputer client. *Monitoring traffic* hingga ke level pengguna sebaiknya dapat dilakukan agar jika terjadi suatu anomali atau gangguan trafik pada jaringan, dapat langsung ditelusuri penyebab dan permasalahannya..

Strategi Program Deteksi Penyusupan

Sesuai dengan tujuan penelitian ini yaitu mengidentifikasi adanya usaha penyusupan yang berusaha masuk ke system jaringan, membuat pintu belakang untuk masuk kembali ke sistem, dan menghilangkan jejak pada sistem operasi IDS/IPS StrataGuard dengan cara *remote login*, install *backdoor*, dan menghapus *log file*, dengan menganalisa *log file* sesuai dengan aturan pada penelitian ini.

Perancangan sistem keamanan jaringan *StratGuard IDS/IPS* ini merupakan filterisasi suatu pelewatan data melalui jaringan computer baik intranet maupun internet. Hasil identifikasi sistem dikirimkan berupa *alert*, seperti pada Gambar 3.6.

 ISSN: 1411-3201



Gambar 3.6 Diagram Alir Strategi Sistem Deteksi Penyus

 ISSN: 1411-3201

Pengalamatan Jaringan (IP Addressing)

Dalam perencanaan dan implementasi skema jaringan diatas, akan 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.

Berikut Rencana Pengalamatan Internet Protokol pada jaringan Intranet berbasis VLAN:

Tabel 4.1. Alokasi IP Address Intranet STMIK AMIKOM

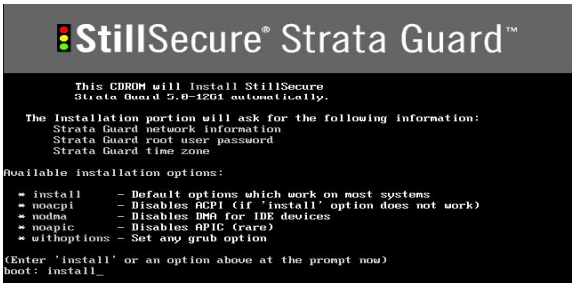
Alokasi IP Address Jaringan Komputer Lokal STMIK AMIKOM (172.16.0.0/16)				
No	**Nama VLAN**	**No VLAN**	**IP Network**	**IP Gateway**
1	BAAK	11	172.16.11.0/24	172.16.11.254
2	BAU	12	172.16.12.0/24	172.16.12.254
3	CustomerService	13	172.16.13.0/24	172.16.13.254
4	IT Dept	14	172.16.14.0/24	172.16.14.254
5	PSDM	15	172.16.15.0/24	172.16.15.254
6	CNAP	16	172.16.16.0/24	172.16.16.254
7	Dosen(r.dosen)	17	172.16.17.0/24	172.16.17.254
8	Pengajaran	18	172.16.18.0/24	172.16.18.254
9	PengelolaEksekutif	19	172.16.19.0/24	172.16.19.254
10	SIPUS	20	172.16.20.0/24	172.16.20.254
11	PublicPerpustakaan	21	172.16.21.0/24	172.16.21.254
12	AnjunganUnit3	22	172.16.22.0/24	172.16.22.254
13	AnjunganUnit2	23	172.16.23.0/24	172.16.23.254
14	Server Intranet	24	172.16.24.0/24	172.16.24.254
15	Print Server	25	172.16.25.0/26	172.16.25.254
16	StaffUPT	26	172.16.26.0/24	172.16.26.254
17	UPT Lab1	101	172.16.101.0/24	172.16.101.254
18	UPT Lab2	102	172.16.102.0/24	172.16.102.254
19	UPT Lab3	103	172.16.103.0/24	172.16.103.254
20	UPT Lab4	104	172.16.104.0/24	172.16.104.254
21	UPT Lab5	105	172.16.105.0/24	172.16.105.254
22	UPT Lab6	106	172.16.106.0/24	172.16.106.254
23	UPT Lab7	107	172.16.107.0/24	172.16.107.254
24	UPT Lab8	108	172.16.108.0/24	172.16.108.254
25	UPT Lab9	109	172.16.109.0/24	172.16.109.254
26	UPT Lab10	110	172.16.110.0/24	172.16.110.254
27	UPT Lab11	111	172.16.111.0/24	172.16.111.254
28	UPT Lab12	112	172.16.112.0/24	172.16.112.254
29	Wifi 1	201	172.16.201.0/24	172.16.201.254
30	Wifi 2	202	172.16.202.0/24	172.16.202.254
31	Wifi 3	203	172.16.203.0/24	172.16.203.254
32	Wifi 4	204	172.16.204.0/24	172.16.204.254
33	Wifi 5	205	172.16.205.0/24	172.16.205.254
34	Wifi 6	206	172.16.206.0/24	172.16.206.254
35	Wifi 7	207	172.16.207.0/24	172.16.207.254
36	Wifi 8	208	172.16.208.0/24	172.16.208.254
37	Wifi 9	209	172.16.209.0/24	172.16.209.254
38	Wifi 10	210	172.16.210.0/24	172.16.210.254
39	Wifi 11	211	172.16.211.0/24	172.16.211.254
40	Wifi 12	212	172.16.212.0/24	172.16.212.254

ISSN: 1411-3201

Konfigurasi pada sisi server
Instalasi IDS/IPS StrataGuard

Berikut ini adalah langkah-langkah instalasi IDS/IPS StratGuard *server* :

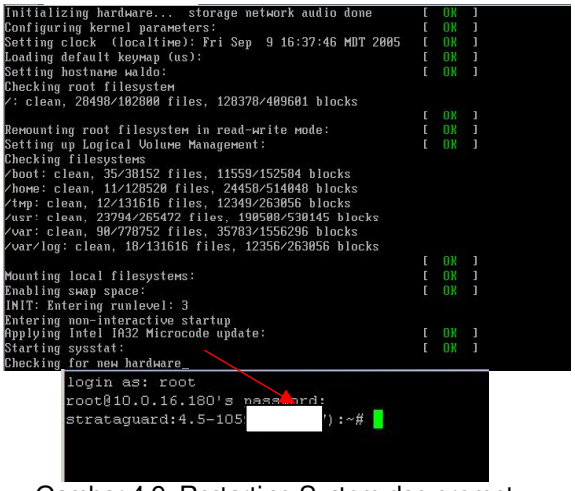
1. Konfigurasi *boot device priority* pada *bios* agar melakukan booting pada cdroom.
2. *Booting* menggunakan cd-room berhasil dengan muncul pada layar seperti pada Gambar 4.8 kemudian tekan *enter*.



Gambar 4.8 Booting IDS/IPS StratGuard

3. Proses Instalasi setelah selesai dan restarting system

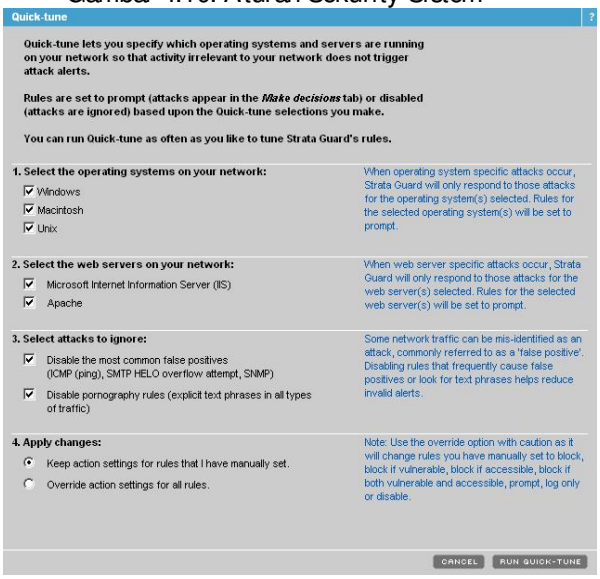
Pada proses kali ini menunjukkan bahwa instalasi sudah selasai dan pada proses akhir instalasi maka system akan restart untuk tahap penyempurnaan instalasi setelah itu system akan menampilkan console untuk login pertama kali.



Gambar 4.9 Restarting System dan prompt login StrataGuard[1]

4. *Restart interface network* dengan mengetikkan perintah pada *konsole/etc/init.d/network restart*.
5. *Remote server* dengan mengetikkan IP address *server* pada *web browsure* maka akan muncul tampilan *user mode* kemudian dapat melakukan *login* sehingga menjadi *privilege user*.

Gambar 4.10. Aturan Sekurity Sistem

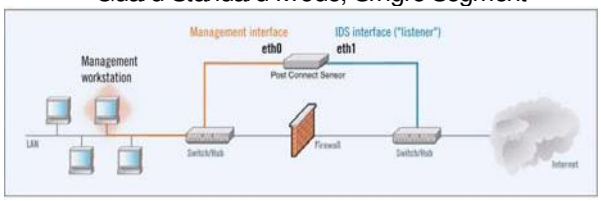


Gambar 4.11. Quick-tune

Quick Tune digunakan untuk memilih jenis sistem operasi apa yang kita pakai, dan konfigurasi jenis serangan serta autentifikasi login apakah itu berbahaya atau tidak.

4.7. Jenis – jenis Rancangan Penggunaan IDS / IPS StrataGuard

a. Default NIC Connections for Strata Guard Standard Mode, Single Segment

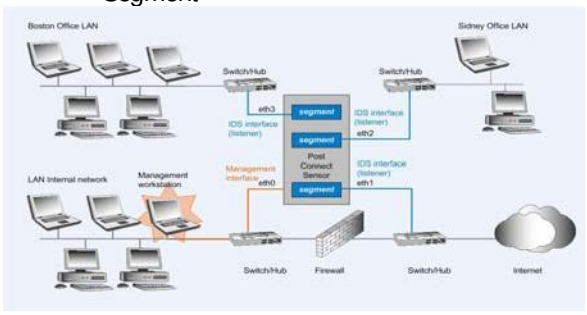


Gambar 4.12. Default NIC Connections for Strata Guard Standard Mode, Single Segment

[1] http://www.stillsecure.com/

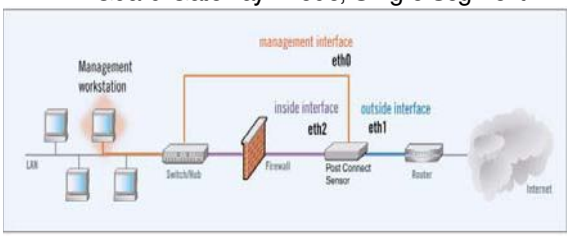
 ISSN: 1411-3201

b. Default NIC Connections for Strata Guard Standard Mode, Multiple Segment[2]



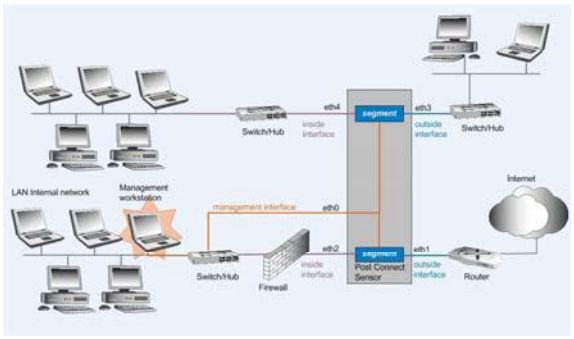
Gambar 4.13. Default NIC Connections for Strata Guard Standard Mode, Multiple Segment

c. Default NIC Connections for Strata Guard Gateway Mode, Single Segment



Gambar 4.14. Default NIC Connections for Strata Guard Gateway Mode, Single Segment

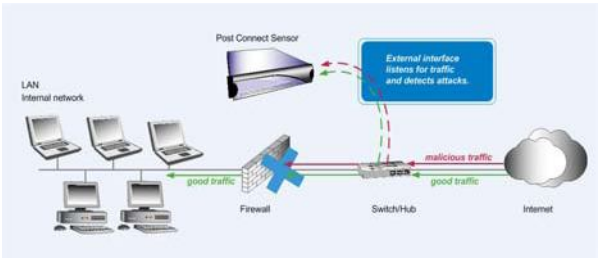
d. Default NIC Connections for Strata Guard Gateway Mode, Multiple Segment[3]



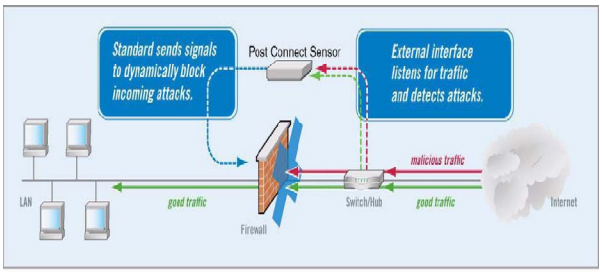
Gambar 4.15. Default NIC Connections for Strata Guard Gateway Mode, Multiple Segment

Strata Guard produk dapat dijalankan dalam mode berikut:

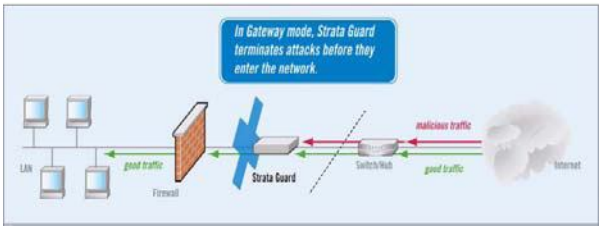
- Modus standar, firewall no - An "out-of-band" intrusion detection system (IDS) yang monitor lalu lintas jaringan.
- Modus standar, dengan firewall - An "out-of-band" gangguan sistem pencegahan (IPS) yang memantau lalu lintas jaringan dan serangan blok dengan memasukkan kebijakan ke firewall.
- Gateway mode - An "in-line" IPS yang dapat diposisikan baik di depan atau belakang firewall kita.



Gambar 4.16. Strata Guard Standard Mode, No Firewall



Gambar 4.17. Strata Guard Standard Mode, with Firewall

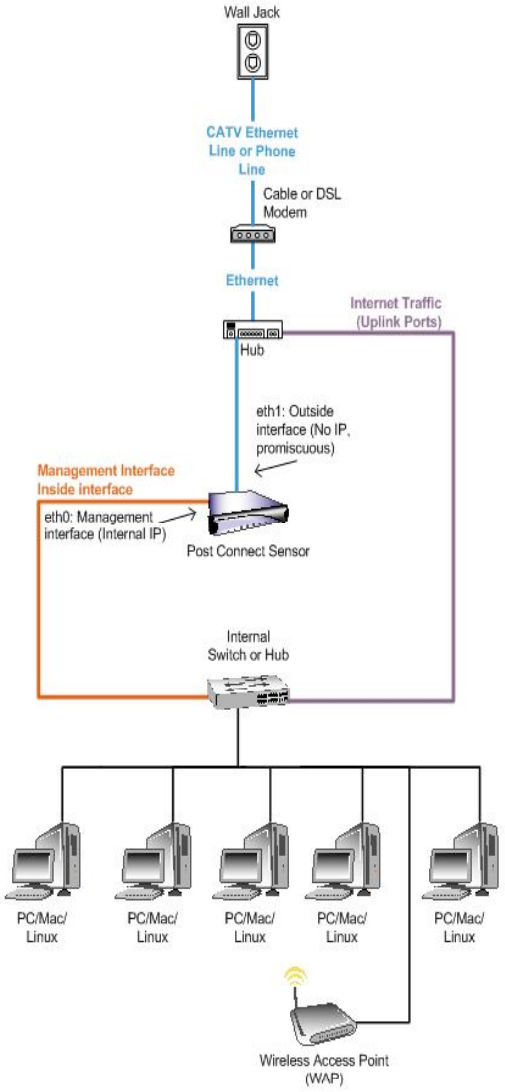


Gambar 4.18. Strata Guard Gateway Mode

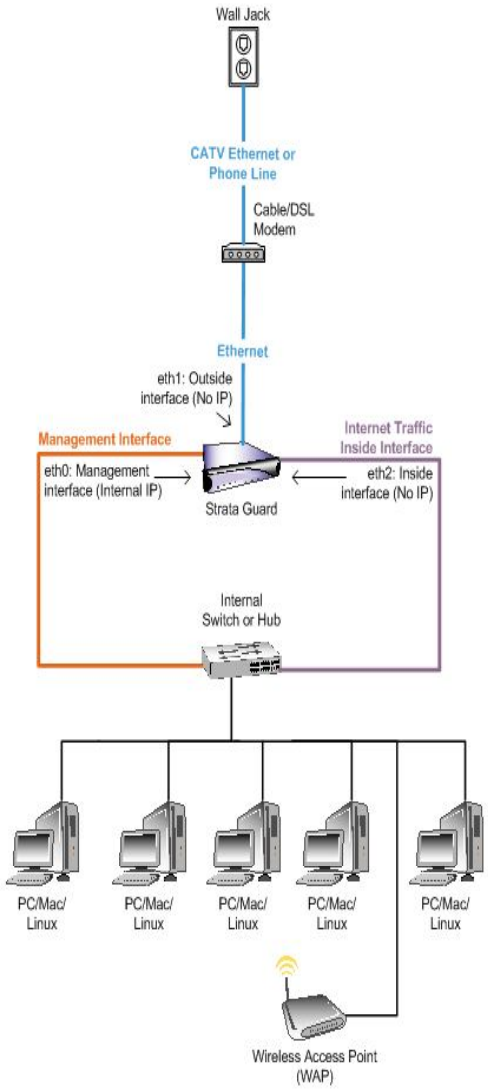
[2] http://www.stillsecure.com/

[3] http://www.stillsecure.com/

 ISSN: 1411-3201



Gambar 4.19. Strata Guard Standard Mode, Cable/DSL Modem Installation



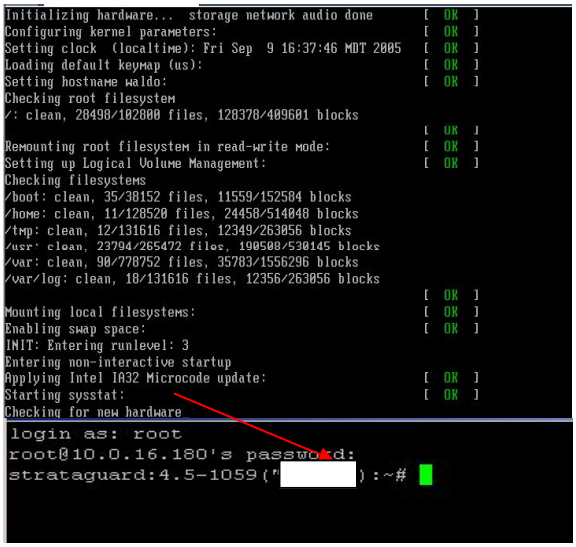
Gambar 4.20. Strata Guard Gateway Mode, Cable/DSL Modem Installation[4]

[4] http://www.stillsecure.com/

ISSN: 1411-3201

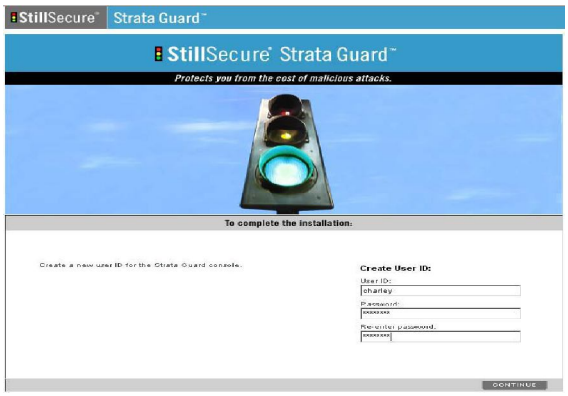
Indikator Pengujian Server

Pada layar komputer akan muncul tampilan awal login seperti pada Gambar 4.14 Menunjukkan proses *booting* pada komputer *server* berjalan dengan normal dan siap untuk dilakukan konfigurasi

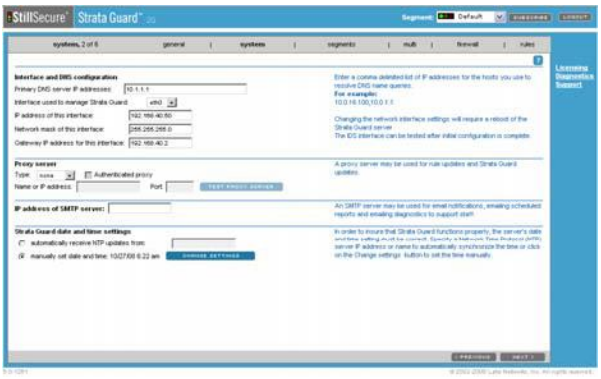


Gambar 4.23. Tampilan Login *StrataGuard*

a) Komputer *server* akan dikonfigurasi melalui *remote web base* sehingga pada tampilan *web browsure* akan muncul seperti pada Gambar 4.48 sebagai tampilan *user mode* kemudian dapat melakukan *login* sehingga menjadi *privilege user* seperti pada gambar 4.48



Gambar 4.24. Tampilan Awal Login



Gambar 4.25 Tampilan Ketika Sudah *Login* Sebagai *User Privilege*[5]

b) Komputer *server* dapat menambahkan gateway dan firewall mode baru dengan login sebagai *privilege user* pada *web base*.

c) *OpenVPN* dapat dijalankan dengan mengetahui status ketika diaktifkan seperti pada Gambar 4.58

```
[tesis.mti ~]#/etc/init.d/openvpn start
Starting openvpn:                                          [
                                OK ]
```

Gambar 4.26. Menjalankan *Openvpn*

Pada Gambar 4.50 *OpenVPN* dijalankan secara manual dengan cara men-*start* di perintah *console* */etc/init.d/openvpn start*. Jika status yang ditampilkan OK maka OpenVPN dapat berjalan sebagai *server* VPN dengan baik.

[5] http://www.stillsecure.com/

 ISSN: 1411-3201

Tabel 4.4. Tabel Pengujian Sisi Server

No	Nama Pengujian	Indikator Pengujian	Manfaat Pengujian	Status Pengujian
1	Komputer *Server* Booting dengan normal	Muncul halaman *login* pada layar monitor	Mengetahui server berjalan dengan baik	Muncul halaman *login*
2	Komputer *Server* dapat dikonfigurasi melalui *remote web base*	Muncul tampilan pada *web browser* halaman *Stratguard Mode*	Mempermudah konfigurasi strataguard	Muncul halaman *stratguard user mode*
3	Komputer *Server* dapat menambahkan serta *teregister extension* dari vlan dan backbone *client* ketika dikonfigurasi melalui *remote web base*	Pada *konsole* ketik *strataguard –r*, kemudian ketik *sip show peers*	Mempermudah manajemen user IDS/IPS Stratguard	Muncul status dari Stratguard
4	Komputer *Server* dapat menjalankan *OpenVPN Server*	Pada *konsole* mengetikkan perintah */etc/init.d/openvpn start* , kemudian *ifconfig*	Paket data yang berlebihan akan di amankan	Muncul *interface* dan *IP address virtual* untuk koneksi VPN,Vlan,Backbone

Ketika *server* VPN telah aktif kemudian dijalankan perintah *ifconfig* pada *konsole* maka akan muncul *interface virtual* baru seperti berikut :

tun0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

inet addr:10.10.10.1 P-t-P:10.10.10.2 Mask:255.255.255.255

UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1

RX packets:0 errors:0 dropped:0 overruns:0 frame:0

TX packets:0 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:100

RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

KESIMPULAN

Dari hasil pengujian dalam tesis ini , dapat diambil kesimpulan sebagai berikut :

1. Bagaimanakah Infrastruktur Jaringan STMIK AMIKOM :
   a. Jaringan Komputer STMIK Amikom dikembangkan dengan sistem jaringan yang bersifat tradisional yakni memanfaatkan PC router sebagai pembagi broadcast domain ke setiap unit kerja atau group pengguna jaringan di setiap gedung STMIK Amikom Yogyakarta. Hal ini menyebabkan setiap penambahan unit kerja atau group tertentu maka akan membutuhkan sebuah PC router atau minimal sebuah kartu jaringan agar mampu membentuk jaringan (subnetwork) yang baru sehingga manajemen jaringan dan *maintenance* lebih kompleks dan cenderung kesulitan untuk menerapkan standart *policy* pada setiap jaringan.
   b. Pada beberapa subnet (jaringan) atau kelompok user (group), terdapat jaringan yang hanya di*manage* menggunakan *ip aliases* melalui interface pc router, hal ini membuat performance jaringan tidak bekerja dengan optimal. Penggunaan lebih dari satu subnet pada jaringan yang memiliki *broadcast domain* yang sama mengakibatkan *broadcast* yang lebih besar, disamping terdapat permasalahan keamanan karena *administrator* tidak dapat mengontrol komunikasi kedua jaringan yang masih berada pada broadcast domain yang sama. Pembagian subnet jaringan yang hanya memanfaatkan *IP aliases* justru akan mengurangi kinerja atau performa jaringan komputer itu sendiri.
   c. Distribusi Internet Protokol Public (IP Public) ke setiap PC Router yang dimaksudkan untuk membagi koneksi

 ISSN: 1411-3201

internet ke setiap unit/lab menjadikan sistem keamanan jaringan *intranet* STMIK Amikom menjadi rentan dan *vulnerable*. Hal ini karena IP Public yang digunakan oleh setiap PC router otomatis terpublikasi di Internet yang harusnya menjadi jaringan yang tidak dapat dipercaya (*untrust network)*. Dengan kondisi sekarang, maka setiap pengguna internet dimungkinkan untuk melakukan penyerangan ke jaringan Intranet STMIK Amikom, padahal jaringan intranet menjadi jaringan yang aman dari jaringan di luar Jaringan Kampus STMIK Amikom (termasuk Internet).

d. Penggunaan IP Private dan IP Public di setiap PC router di unit-unit/laboratorium, menyebabkan routing jaringan internal dan jaringan public (internet) menjadi satu (digabung), hal ini membuat manajemen dan monitoring komunikasi data antar jaringan intranet atau antar unit/lab sulit dilakukan, karena adanya pemanfaatan fungsi *masquarade (NAT)* atau penyembunyian identitas internet protokol pengguna jaringan. Selain itu komunikasi antar ip public dan ip private sudah tidak sesuai aturan RFC, dimana IP Private seharusnya tidak dapat di routingkan melalui IP Public (non-routabel)
e. Pemberian alamat Internet Protokol pada beberapa unit kerja tidak seragam atau berada pada kelas IP yang berbeda, selain mengakibatkan kesulitan menjamin skalabilitas dan kemampuan untuk dapat diakses dari mana saja, juga membuat administrasi jaringan semakin rumit.
f. Saat ini server-server intranet pada kampus STMIK Amikom dipasangkan IP public yang menyebabkan kemungkinan terpublikasikan atau dapat diaksesnya informasi server internal tersebut dari *Internet*.
g. 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 STMIK Amikom Yogyakarta, juga mengakibatkan bandwidth terpakai banyak yang terbuang percuma atau tidak optimal pemanfaatannya.
h. Pemasangan Wireless Access Point untuk mendistribusikan koneksi internet di lingkungan luar gedung kampus STMIK Amikom sebaiknya dipertimbangkan kembali. Jaringan wireless merupakan jaringan yang memiliki tingkat vulnerable yang sangat tinggi, diperlukan monitoring yang terus-menerus dan pemanfaatan teknologi keamanan jaringan wireless berlapis untuk menjamin pengguna benar benar memiliki otorisasi menggunakan akses tersebut.
i. Saat ini, beberapa jaringan wireless (AP) digunakan sebagai *bridge* yang terhubung secara langsung ke pengguna pada jaringan kabel tanpa ada proteksi (filtering), hal ini akan sangat mengganggu trafik yang terjadi pada kedua jaringan tersebut karena masih menggunakan broadcast domain yang sama. Sebaiknya broadcast domain untuk jaringan *wireless* dipisahkan dengan *broadcast domain* jaringan kabel *(wired network).*
j. Pendistribusian koneksi jaringan kabel UTP melalui switch secara bertingkat (koneksi dari switch yang satu ke switch yang lain karena harus menjangkau lebih dari 100 meter) perlu mendapatkan perhatian atau pengukuran kembali. Karena jika sudah melalui beberapa switch, signal koneksi jaringan akan melemah dan mengakibatkan akses yang lambat atau bahkan terputus.
k. Penggunaan kanal frekwensi dalam pemasangan Access Point atau HotSpot umumnya belum melakukan site-survey terlebih dahulu, sehingga jangkauan atau pemanfaatan hotspot kurang maksimal, akibat terjadi interference antar wireless yang satu dengan yang lainnya. Penempatan Wireless Access point sebaiknya mengukuti kaidah frekwensi yang bersifat re-usable dan dapat dialokasikan pada lokasi yang berdekatan seperti aturan penggunan kanal 1, kanal 6 dan kanal 11 di lokasi yang berdekatan.
l. Kondisi saat ini, monitoring traffic hanya dilakukan di *backbone* internet saja, hal ini dapat menyulitkan penelusuran jika terdapat anomali traffik seperti malware yang menginfeksi sebuah komputer client. *Monitoring traffic* hingga ke level pengguna sebaiknya dapat dilakukan agar jika terjadi suatu anomali atau gangguan

 ISSN: 1411-3201

trafik pada jaringan, dapat langsung ditelusuri penyebab dan permasalahannya.
2. Solusi bagi jaringan STMIK AMIKOM adalah dengan membangun IDS / IPS StrataGuard, sehingga bisa dilakukan pencegahan pada saat intruder melakukan penetrasi.
3. Cara merancang IDS / IPS di STMIK AMIKOM adalah dengan meletakkan IDS / IPS StrataGuard pada HostBase.
4. IDS / IPS StratGuard mampu berjalan disemua platform sistem operasi.

IDS/IPS StrataGuard mampu menggantikan peranan firewall dan proxy.

DAFTAR PUSTAKA

http://www.stillsecure.com/

Andalep, S.S. dan Basu, K.A. (1994), 'Technical Complexity and Consumer Knowledge as Moderators of Service Quality Evaluation in Automobile Service Industry', *Journal of Retailing,* Vol.70, No.4:367-381.

Anonymous, *Maximum Linux Security: A Hacker's Guide to Protecting Your Linux Server and Workstation*, Sams Publishing, 2000.

Aquilano (1992), *Production and Operation Management,* Sixth Edition, IRWIN, Boston.

Babakus, E. dan Boller (1992),'An Empirical Assesment of The SERVQUAL Scale', *Journal of Business Research,* Vol. 24: 253-268.

Bill Cheswick, "*An Evening with Berferd: in which a cracker is lured, endured, and studied*," 1991.

Bounds, G., Yorks, L., Adams, M. dan Ranney, G. (1994), *Beyond Total Quality Management, Toward the Emerging Paradigm*, McGrawhill Inc, New York