

**ANALISIS DAN PERANCANGAN KEAMANAN JARINGAN
MENGUNAKAN INTRUSION DETECTION SYSTEM DAN
FIREWALL PADA ROUTERBOARD MIKROTIK
RB951Ui-2HnD BERBASIS SMS GATEWAY**

SKRIPSI



disusun oleh

Ilman Fajar

13.11.7287

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2016**

**ANALISIS DAN PERANCANGAN KEAMANAN JARINGAN
MENGUNAKAN INTRUSION DETECTION SYSTEM DAN
FIREWALL PADA ROUTERBOARD MIKROTIK
RB951Ui-2HnD BERBASIS SMS GATEWAY**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika



disusun oleh

Ilman Fajar

13.11.7287

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2016**

PERSETUJUAN

SKRIPSI

**ANALISIS DAN PERANCANGAN KEAMANAN JARINGAN
MENGUNAKAN INTRUSION DETECTION SYSTEM DAN
FIREWALL PADA ROUTERBOARD MIKROTIK
RB951Ui-2HnD BERBASIS SMS GATEWAY**

yang dipersiapkan dan disusun oleh

Ilman Fajar
13.11.7287

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 30 Maret 2016

Dosen Pembimbing,

Rizqi Sukma Kharisma, M.Kom.

NIK. 190302215

PENGESAHAN

SKRIPSI

ANALISIS DAN PERANCANGAN KEAMANAN JARINGAN MENGUNAKAN INRUSION DETECTION SYSTEM DAN FIREWALL PADA ROUTERBOARD MIKROTIK RB951Ui-2HnD BERBASIS SMS GATEWAY

yang dipersiapkan dan disusun oleh

Ilman Fajar

13.11.7287

telah dipertahankan di depan Dewan Penguji
pada tanggal 24 Agustus 2016

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Kusnawi, S.Kom., M.Eng.
NIK. 190302112

Tonny Hidayat, M.Kom.
NIK. 190302182

Rizqi Sukma Kharisma, M.Kom.
NIK. 190302215



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 29 Agustus 2016

KETUA STMIK AMIKOM YOGYAKARTA



Prof. Dr. M. Suyanto, M.M.
NIK. 190302001


PERYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 26 Agustus 2016




Ilman Fajar
NIM. 13.11.7287

MOTTO

TIADA PRESTASI TANPA DISIPLIN



PERSEMBAHAN

Puji syukur penulis panjatkan kehadirat Allah SWT atas segala limpahan rahmat dan ridho-Nya yang telah memberikan kesehatan, kelancara, keteguhan, dan membekali anugrah ilmu. Skripsi in dipersembahkan untuk :

1. Allah SWT, karena hanya dengan ijin dan pertolongan-Nya lah, saya bisa menyelesaikan skripsi ini.
2. Kedua orang tua saya, Robby Rusmana,dan Uni Widaningsih, yang selalu mendoakan, membimbing, dan mendidik.
3. Rizqi Sukma Kharisma M.Kom, selaku dosen pembimbing skripsi.
4. Mutsana Shafyati A.Md yang selalu memberikan motivasi dan semangat.
5. Aini Aulia, Ciee yang mau ditulis dipersembahkan.
6. Wiwid Trianto yang telah memberikan kesempatan untuk mencetak naskah skripsi.
7. Monalisa Fatmawati Sarifah, yang telah memberikan semangat dalam mencetak skripsi.
8. Faza Ayyasi, Elri Satria, Dimas Prayoga, M. Zaki Firdaus, Alif Abdul Aziz, Java Batara N, Adi Nugraha, Imam Malik, Pahlevi Rabbani, yang selalu memberikan canda tawa serta semangat.
9. Keluarga besar alumni SMKDTBS yang sudah memberikan pengalaman dan motivasi.
10. Keluarga besar 13-S1TI-08 yang sudah menemani masa-masa kuliah saya dan memberikan motivasi.
11. Keluarga Besar HMJTI (Himpunan Mahasiswa Jurusan Teknik Informatika) yang selalu memberikan pengalaman dan kebahagiaan keluarga.
12. Teman-teman kontrakan yang super gila sudah menghibur saya ketika dalam menghadapi kesulitan.

KATA PENGANTAR

Puji syukur penulis panjatkan kehadiran Tuhan Yang Maha Esa yang telah memberikan rahmat serta karunia- Nya sehingga penulis dapat menyelesaikan laporan Skripsi ini. Sholawat serta salam semoga senantiasa terlimpah curahkan kepada Nabi Muhammad SAW, keluarganya, para sahabat, hingga pada umatnya hingga akhir zaman, amin. Laporan Skripsi ini disusun sebagai syarat kelulusan program studi Strata-1 di Sekolah Tinggi Manajemen Informatika dan Komputer “AMIKOM Yogyakarta” Jurusan Teknik Informatika.

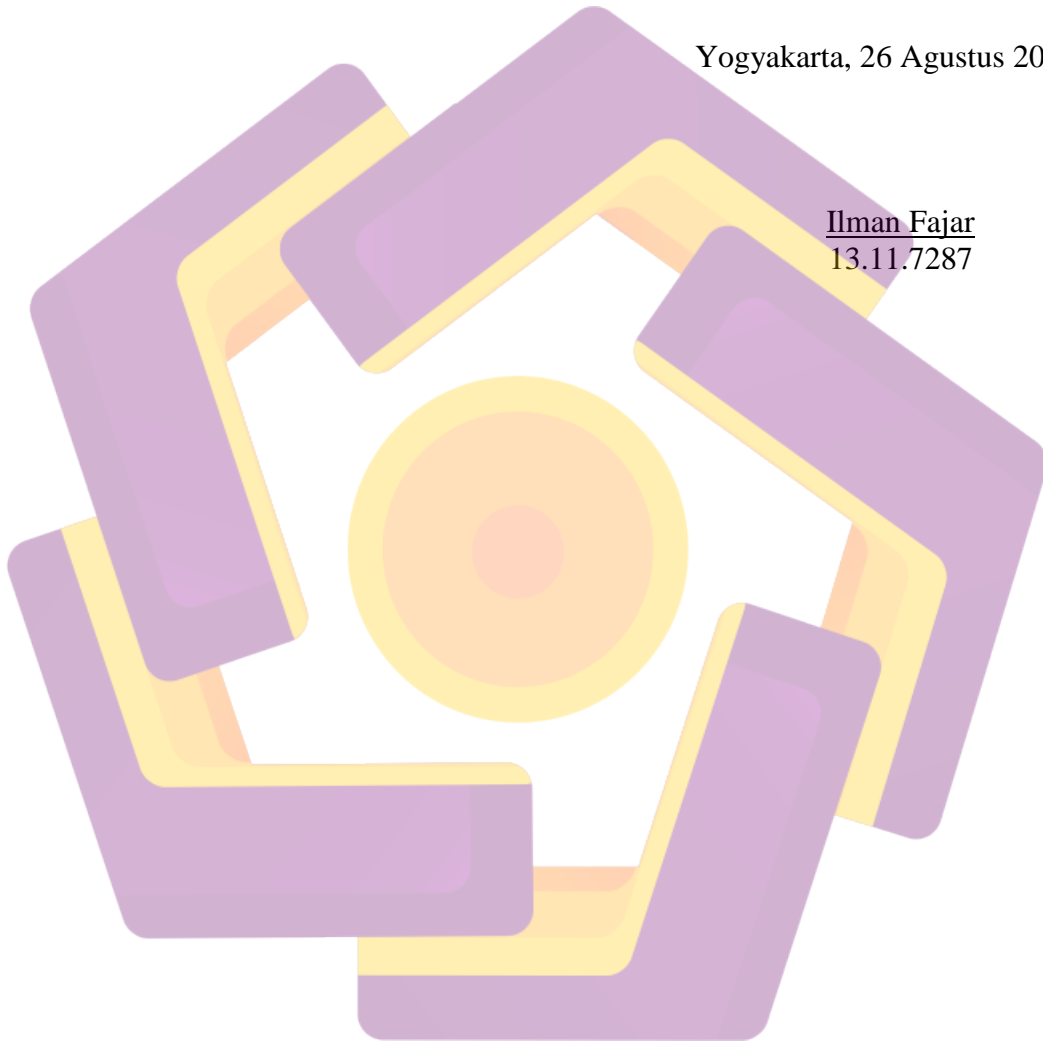
Pada kesempatan kali ini penulis menyampaikan rasa hormat dan terimakasih kepada:

1. Bapak Prof. Dr. M. Syuanto, M.M, selaku ketua STMIK AMIKOM Yogyakarta.
2. Bapak Sudarmawan, M.Kom, selaku ketua jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.
3. Bapak Rizqi Sukma Kharisma, M.Kom, selaku dosen pembimbing atas bimbingannya dan ilmu pengetahuannya yang telah diberikan selama penyusunan skripsi ini.
4. Bapak Joko Dwi Santoso, M.Kom, yang sudah membantu dalam penyelesaian penyusunan skripsi ini.
5. Bapak Ibu Dosen dan seluruh staff serta pegawai STMIK AMIKOM Yogyakarta yang telah memberikan ilmu dan kemudahan-kemudahan selama masa perkuliahan.
6. Seluruh teman-teman yang telah membantu penulis dalam menyelesaikan penyusunan skripsi ini.

Penulis menyadari bahwa dalam penyusunan skripsi ini masih terdapat banyak kekurangan. Oleh karena itu, dengan segala kerendahan hati, penulis sangat mengharapkan kritik serta saran yang dapat membangun agar dapat menghasilkan karya yang lebih baik dikemudian hari. Akhir kata semoga skripsi ini dapat bermanfaat bagi semua pihak.

Yogyakarta, 26 Agustus 2016

Ilman Fajar
13.11.7287



DAFTAR ISI

JUDUL	i
PERSETUJUAN	ii
PENGESAHAN	iii
PERNYATAAN	iv
MOTTO	v
PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR TABEL	xiii
DAFTAR GAMBAR	xiv
INTISARI	xvi
ABSTRACT	xvii
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	2
1.5 Manfaat Penelitian	3
1.6 Metode Penelitian	3
1.6.1 Pengumpulan Data	3
1.6.2 Metode Perancangan Sistem Menggunakan PPDIOO	4
1.7 Sistematika Penulisan	5
BAB II LANDASAN TEORI	7
2.1 Tinjauan Pustaka	7
2.2 Pengertian Analisis Sistem.....	9
2.3 Pengertian Design	9
2.4 Definisi Jaringan Komputer	9
2.5 Jenis-jenis Jaringan Komputer	10
2.5.1 <i>Local Area Network</i>	10
2.5.2 <i>Wide Area Network</i>	10

2.6	Internet	11
2.7	Protokol	11
2.8	Jenis Koneksi Antar Jaringan	11
2.8.1	<i>Peer to Peer</i>	11
2.8.2	Client Server	12
2.9	Topologi Jaringan	13
2.9.1	Topologi <i>Bus</i>	13
2.9.2	Topologi <i>Star</i>	13
2.9.3	Topologi <i>Ring</i>	14
2.9.4	Topologi <i>Mesh</i>	15
2.10	Referensi Model OSI	15
2.11	Referensi Model DOD TCP/IP	17
2.11.1	<i>Aplication Layer</i>	18
2.11.2	<i>Host-to-Host Layer</i>	18
2.11.3	<i>Internet Layer</i>	18
2.11.4	<i>Network Access Layer</i>	19
2.12	IP Address	20
2.13	Keamanan Komputer	20
2.14	Kebijakan Keamanan Jaringan	23
2.15	Aspek-aspek Ancaman Keamanan	23
2.15.1	<i>Intrruption</i>	23
2.15.2	<i>Interception</i>	24
2.15.3	<i>Modification</i>	24
2.15.4	<i>Fabrication</i>	24
2.16	<i>Intrusion Detection System (IDS)</i>	24
2.17	Tipe <i>Intrusion Detection System (IDS)</i>	25
2.17.1	<i>Network-Based Intrusion Detection System (NIDS)</i>	25
2.17.2	<i>Host-Based Intrusion Detection System (HIDS)</i>	26
2.18	Metodology Deteksi	26
2.18.1	<i>Signature-Based Detection</i>	26
2.18.2	<i>Anomaly-Based Detection</i>	27

2.18.3	<i>Passive Detection</i>	27
2.18.4	<i>Reactive Detection</i>	28
2.19	Mikrotik	28
2.19.1	<i>Routerboard</i> Mikrotik	28
2.19.2	Winbox Mikrotik	29
2.20	<i>Firewall</i>	29
2.21	<i>Ports</i>	30
2.22	<i>Short Message Service (SMS)</i>	31
2.23	<i>PPDIOO Network LifeCycle</i>	31
BAB III	ANALISIS DAN PERANCANGAN	32
3.1	Gambaran Umum Sistem	32
3.2	Metode Penelitian	33
3.3	Tahapan Persiapan (<i>Prepare</i>)	33
3.3.1	Analisis	33
3.3.2	Identifikasi Masalah	35
3.3.3	Hipotesis Solusi	36
3.4	Tahap Perencanaan (<i>Plan</i>)	37
3.4.1	Analisis Kebutuhan	37
3.4.2	Analisis Kebutuhan Fungsional	38
3.4.3	Analisis Kebutuhan Non-Fungsional	38
3.4.3.1	Perangkat Keras (<i>Hardware</i>)	38
3.4.3.2	Perangkat Lunak (<i>Software</i>)	41
3.5	Perancangan <i>Testing</i>	42
3.6	Desain (<i>Design</i>)	42
3.6.1	Rancangan <i>Intrusion Detection System</i>	42
3.6.2	Perancangan Topologi IDS	42
3.6.3	Perancangan <i>Firewall</i>	43
BAB IV	IMPLEMENTASI DAN PEMBAHASAN	46
4.1	Tahapan Implementasi (<i>Implement</i>)	46
4.1.1	Implementasi Topologi	46
4.1.2	Implementasi Sistem NIDS	47

4.1.2.1	Konfigurasi <i>System Identity</i>	48
4.1.2.2	Konfigurasi <i>Network Time Protokol</i>	48
4.1.2.3	Konfigurasi Tool SMS	49
4.1.2.4	<i>System Logging</i>	50
4.1.2.5	<i>System Script</i>	51
4.1.2.6	Konfigurasi <i>Network-Based IDS</i>	52
4.1.2.6.1	Konfigurasi Rule <i>ICMP Flood</i>	52
4.1.2.6.2	Konfigurasi Rule <i>SSH Bruteforce</i>	54
4.1.2.6.3	Konfigurasi Rule <i>FTP Bruteforce</i>	56
4.1.2.6.4	Konfigurasi Rule <i>Scanning Port</i>	59
4.2	Tahapan Pengoprasian (<i>Operate</i>)	61
4.2.1	Pengujian Serangan <i>ICMP Flood</i>	61
4.2.2	Pengujian Serangan <i>SSH Bruteforce</i>	65
4.2.3	Pengujian Serangan <i>FTP Bruteforce</i>	69
4.2.4	Pengujian Serangan <i>Scanning Port</i>	73
4.3	Tahapan Pengoptimalan (<i>Optimize</i>)	76
BAB V	PENUTUP	78
5.1	Kesimpulan	78
5.2	Saran	79
DAFTAR PUSTAKA	80

DAFTAR TABEL

Tabel 3. 1 Spesifikasi Laptop Yang Digunakan Dalam Penelitian	38
Tabel 3. 2 Spesifikasi Mikrotik RB951Ui-2HnD	39
Tabel 4. 1 <i>Respon Time</i> Sistem <i>Logging</i> ICMP	64
Tabel 4. 2 <i>Respon Time</i> SMS Gateway ICMP	64
Tabel 4. 3 <i>Respon Time</i> Sistem <i>Logging</i> SSH	68
Tabel 4. 4 <i>Respon Time</i> SMS Gateway SSH	68
Tabel 4. 5 <i>Respon Time</i> Sistem <i>Logging</i> FTP	73
Tabel 4. 6 <i>Respon Time</i> SMS Gateway FTP	73
Tabel 4. 7 <i>Respon Time</i> System <i>Logging</i> Port Scanning	76
Tabel 4. 8 <i>Respon Time</i> SMS Gateway Port Scanning	76
Tabel 5. 1 <i>Respon Time</i>	79



DAFTAR GAMBAR

Gambar 1. 1 PPDIOO <i>Network Life-Cycle</i>	4
Gambar 2. 1 Jaringan LAN (<i>workgroups</i>)	10
Gambar 2. 2 Jaringan <i>Peer to Peer</i>	12
Gambar 2. 3 Jaringan <i>Client Server</i>	12
Gambar 2. 4 Model Topologi <i>Bus</i>	13
Gambar 2. 5 Model Topologi <i>Star</i>	14
Gambar 2. 6 Model Topologi <i>Ring</i>	14
Gambar 2. 7 Model Topologi <i>Mesh</i>	15
Gambar 2. 8 <i>OSI Layer</i>	16
Gambar 2. 9 Lapisan Atas OSI	16
Gambar 2. 10 Lapisan Bawah OSI.....	17
Gambar 2. 11 Model DoD TCP/IP	20
Gambar 2. 12 Model MD-IDS <i>system</i>	25
Gambar 2. 13 Model <i>Network-Based IDS system</i>	26
Gambar 2. 14 Logo Mikrotik	28
Gambar 2. 15 <i>Firewall</i>	29
Gambar 3. 1 <i>Network-Based IDS</i>	32
Gambar 3. 2 <i>Top Network Attack</i>	34
Gambar 3. 3 Persentasi Jenis Serangan	35
Gambar 3. 4 Mikrotik RB951Ui-2HnD	39
Gambar 3. 5 Topologi NIDS	43
Gambar 3. 6 Proses Deteksi IDS dan <i>Firewall</i>	45
Gambar 4. 1 Implementasi NIDS	47
Gambar 4. 2 Konfigurasi <i>System Identity</i>	48
Gambar 4. 3 Konfigurasi <i>SNTP Client</i>	49
Gambar 4. 4 <i>Setting Tool SMS</i> Mikrotik	49
Gambar 4. 5 Pengiriman SMS ke <i>Mobile Adminstrator</i>	50
Gambar 4. 6 Menambahkan <i>Rule Logging</i>	50
Gambar 4. 7 Menampilkan <i>Log Router</i>	50
Gambar 4. 8 <i>Script</i> Pengiriman SMS Waktu dan Tanggal	51

Gambar 4. 9 Melakukan <i>Check Rule Firewall ICMP</i>	53
Gambar 4. 10 Melakukan <i>Check Rule Firewall SSH</i>	52
Gambar 4. 11 Melakukan <i>Check Rule Firewall FTP</i>	57
Gambar 4. 12 Melakukan <i>Check Rule Firewall Port Scanning</i>	59
Gambar 4. 13 Melakukan Ping sesuai <i>Rule Firewall</i>	61
Gambar 4. 14 Firewall Melakukan <i>Packet Drop</i>	62
Gambar 4. 15 IP Address tercatat pada <i>Address-list Firewall</i>	62
Gambar 4. 16 Sistem <i>Logging</i> Mencatat Serangan ICMP FLOOD	63
Gambar 4. 17 Laporan SMS <i>Warning ICMP</i>	63
Gambar 4. 18 Melakukan Koneksi SSH	65
Gambar 4. 19 Gagal Melakukan Serangan SSH	66
Gambar 4. 20 <i>Address-list SSH Bruteforce</i>	66
Gambar 4. 21 <i>System Logging</i> Serangan SSH	67
Gambar 4. 22 Laporan SMS <i>Warning SSH</i>	67
Gambar 4. 23 Percobaan Serangan FTP <i>Bruteforce</i>	69
Gambar 4. 24 Serangan FTP <i>Bruteforce</i>	70
Gambar 4. 25 Gagal melakukan Serangan FTP <i>Bruteforce</i>	70
Gambar 4. 26 <i>Address-list</i> Serangan FTP <i>Bruteforce</i>	71
Gambar 4. 27 <i>System Logging</i> Serangan FTP <i>Bruteforce</i>	72
Gambar 4. 28 Laporan SMS <i>Warning FTP</i>	72
Gambar 4. 29 Percobaan <i>Scanning Port</i>	74
Gambar 4. 30 <i>Address-list Scanning Port</i>	74
Gambar 4. 31 <i>System Logging Scanning Port</i>	75
Gambar 4. 32 Laporan SMS <i>Warning Scanning Port</i>	75

INTISARI

Jaringan nirkabel merupakan media transmisi yang pada saat ini sangat ramai digunakan. Semakin ramai jumlah *node* yang terhubung pada jaringan maka akan semakin rentan terhadap keamanan. Administrator memiliki peran penting untuk melindungi keamanan jaringan. Proses *monitoring* yang panjang sangat menyita waktu seorang administrator dalam mengawasi dan melindungi jaringan.

IDS *intrusion detection system* dikombinasikan dengan *firewall* dapat membantu memaksimalkan perlindungan dan pengawasan pada jaringan. *System* ini bekerja dengan cara mendeteksi serangan dan memberikan peringatan kepada administrator ketika terjadi suatu serangan.

Uji sistem dilakukan dengan menggunakan beberapa jenis serangan ke jaringan untuk dapat mengetahui fungsi sistem bekerja, dengan memberikan *report* berupa sms yang dikirim pada *handphone* administrator berisi informasi IP *address* penyerang dan jenis serangan. dengan sistem ini administrator dapat terbantu dalam melakukan *monitoring* jaringan.

Kata Kunci : IDS, *firewall*, jaringan, keamanan, administrator.

ABSTRACT

Wireless is a medium transmission that is very often used. The crowded number of nodes that are connected on the network, it will be more vulnerable to security. The administrator has an important role to protect the security network. The process of monitoring that are very time consuming an administrator in overseeing and protecting the network.

IDS intrusion detection system combined with a firewall can help to maximize protection and surveillance on the network. System works by detecting attacks and to give warning to the administrator when a strike.

Testing the system are carried out using some kind of attack to the network to be able to know the function of the system works, by giving report in the form of a text message sent on the administrator's phone that contains the informations, that are IP address of the attacker and the type of attack. With this system, admninstrator can be helpful in monitoring the network.

Keyword : *IDS, Firewall, Network, Security, Administrator.*