



**ANALISIS PERBANDINGAN KEAMANAN DATA DENGAN MENGGUNAKAN MODE IPSEC DAN
AUTENTIKASIHEADER AH-SHA-HMAC**

SAYED AFDHAL
41512110183

UNIVERSITAS
MERCU BUANA

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2014



**ANALISIS PERBANDINGAN KEAMANAN DATA DENGAN MENGGUNAKAN MODE IPSEC DAN
AUTENTIKASI HEADER AH-SHA-HMAC**

Laporan Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:
SAYED AFDHAL
41512110183

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2014

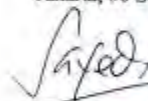
LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM : 41512110183
Nama : SAYED AFDHAL
Judul Skripsi : ANALISIS PERBANDINGAN KEAMANAN DATA DENGAN
MENGUNAKAN MODE IPSEC DAN *AUTENTIKASI*
HEADER AH-SHA-HMAC

Menyatakan bahwa skripsi tersebut diatas adalah hasil karya saya sendiri danbukan plagiat. Apabila ternyata ditemukan didalam laporan skripsi saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 30 Sept 2014


Sayed Afdhal



LEMBAR PENGESAHAN

NIM : 41512110183
Nama : Sayed Afdhal
Judul Skripsi : Analisis Perbandingan Keamanan Data Dengan Menggunakan Mode IPSEC dan Autentikasi Header AH-SHA-HMAC

SKRIPSI INI TELAH DISETUJUI DAN DISIDANGKAN

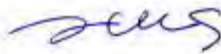
JAKARTA, OKTOBER 2014



Ida Nurhaida, S.T., MT.
Pembimbing Tugas Akhir



Umiy Salamah, S.T., MMSI.
Koord. Tugas Akhir Teknik
Informatika



Sabar Rudiarto, M.Kom.
KaProdi Teknik Informatika

KATA PENGANTAR

Puji syukur Alhamdulillah kehadiran Allah SWT yang telah melimpahkan segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Jurusan Teknik Informatika Universitas Mercu Buana.

Penulis menyadari bahwa laporan tugas akhir ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadari pula bahwa laporan tugas akhir ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Ibu Ida Nurhaida selaku dosen pembimbing tugas akhir pada Jurusan Teknik Informatika Universitas Mercu Buana yang telah membantu membimbing selama proses pembuatan skripsi ini.
2. Ibu dan ayah tersayang yang telah mendukung penulis baik moril maupun materiil.
3. Sahabat dan rekan kerja yang telah memberikan dukungan moral untuk menyelesaikan tugas akhir ini.
4. Rekan-rekan seperjuangan atas kebersamaan dan dukungan moral sejak selama masa kuliah hingga dalam penyelesaian tugas akhir ini.
5. Pihak-pihak lain yang tidak dapat penulis sebutkan satu per satu atas semua dukungannya baik secara langsung maupun tidak langsung.

Semoga Allah SWT membalas kebaikan dan selalu mencurahkan hidayah serta taufik-Nya,
Amin.

Jakarta, 30Juni 2014

Penulis



DAFTAR ISI

LEMBAR PERNYATAAN	Error! Bookmark not defined.
LEMBAR PERSETUJUAN	3
KATA PENGANTAR.....	5
ABSTRACT	Error! Bookmark not defined.
ABSTRAK	Error! Bookmark not defined.
DAFTAR ISI	7
DAFTAR GAMBAR.....	9
DAFTAR LAMPIRAN	Error! Bookmark not defined.
BAB I PENDAHULUAN.....	Error! Bookmark not defined.
1.1 LATAR BELAKANG.....	Error! Bookmark not defined.
1.2 RUMUSAN MASALAH	Error! Bookmark not defined.
1.3 BATASAN MASALAH	2
1.4 TUJUAN DAN MANFAAT	3
1.4.1 <i>Tujuan Penelitian</i>	3
1.4.2 <i>Manfaat Penelitian</i>	3
1.5 METODE PENELITIAN	4
1.6 SISTEMATIKA PENULISAN	5
BAB II LANDASAN TEORI	7
2.1 KONSEP DASAR JARINGAN	7
2.1.1 <i>Local Area Network (LAN)</i>	7
2.1.2 <i>Metropolitan Area Network (WAN)</i>	8
2.1.3 <i>Wide Area Network (WAN)</i>	9
2.2 TOPOLOGI JARINGAN	9
2.3 MEDIA TRANSMISI	15
2.4 Perangkat Pendukung Implementasi VPN	17
2.4.1 <i>Cisco ASA SERIES</i>	17
2.4.2 <i>Cisco Router</i>	18
2.4.3 <i>Switch</i>	19
2.4.4 <i>Graphical Network Simulator 3 (GNS3)</i>	20

2.4.5	Wireshark	21
2.5	PROTOCOL JARINGAN	21
2.5.1	Refensi OSI Layer	22
2.5.2	Internet Protocol	24
2.5.3	Address Resolution Protocol (ARP).....	25
2.5.4	Reserve Address Resolution Protocol (RARP)	25
2.5.5	Dynamic Host Configuration Protocol (DHCP)	25
2.5.6	Internet Control Message Protocol (ICMP).....	26
2.6	VPN.....	26
2.6.1	IPSec.....	28
2.6.2	Tahapan Konfigurasi VPN.....	32
2.7	VPNSite to site	35
BAB III	DESAIN SISTEM	Error! Bookmark not defined.
3.1	<i>SITE TO SITE</i>	37
3.1.1	Flowchart <i>Site to site</i>	36
3.1.2	<i>Site to site</i> Physical Topologi	37
3.1.2	Logical Topologi <i>Site to site</i>	39
3.2	MODE <i>AUTENTIKASI</i>	40
3.3	PEMETAAN IP PENGUJIAN.....	42
BAB IV	IMPLEMENTASI SISTEM.....	Error! Bookmark not defined.
4.1	KEBUTUHAN APLIKASI.....	44
4.2	<i>SITE TO SITE</i> MENGGUNAKAN IPSec.....	44
4.3	MODE <i>AUTENTIKASI</i> HEADER	52
BAB V	KESIMPULAN DAN SARAN	59
5.1	KESIMPULAN.....	60
5.2	SARAN.....	60
DAFTAR	PUSTAKA.....	61
LAMPIRAN		63

DAFTAR GAMBAR

1. Gambar 2.1: Topologi Local Area Network.....	8
2. Gambar 2.2: Topologi Ring.....	12
3. Gambar 2.3: Cisco Asa Series	18
4. Gambar 2.4: Cisco Switch	20
5. Gambar 2.5: Remote VPN	27
6. Gambar 2.6: Mode Encapsulation Data.....	29
7. Gambar 2.7: Mode Encapsulation Data menggunakan AH	30
8. Gambar 2.8: Fase Interesting Traffic	32
9. Gambar 2.9: Fase 1	33
10. Gambar 2.10: Fase 2	33
11. Gambar 2.11: IPSec SA.....	34
12. Gambar 2.12: Terminal Tunnel	34
13. Gambar 2.13: <i>Site to site</i>	35
14. Gambar 3.1: Flowchart <i>Site to site</i>	36
15. Gambar 3.2: <i>Site to site</i> Physical Topologi.....	37
16. Gambar 3.3: <i>Site to site</i> Logical Topologi.....	38
17. Gambar 3.4: <i>Autentikasi</i> Header.....	39
18. Gambar 3.5: Format Header	39
19. Gambar 4.1: Format header data mode tunnel.....	42
20. Gambar 4.2: Topologi <i>Site to site</i> mode tunnel	42
21. Gambar 4.3: IPconfig1	42
22. Gambar 4.4: IPconfig2	42
23. Gambar 4.5: Hasil Ping.....	42
24. Gambar 4.6: Hasil Tracert Route	42
25. Gambar 4.7: Kofigurasi Interface tunnel	43
26. Gambar 4.8: Hasil show crypto Isakmp Policy	43
27. Gambar 4.9: show crypto ipsec sa sebelum data dikirim	45
28. Gambar 4.10: show crypto ipsec sa sesudah data dikirim	45
29. Gambar 4.11: data mode IPsec	46

30. Gambar 4.12: Protocol Frame Header Data	46
31. Gambar 4.13: Header data internert protocol.....	47
32. Gambar 4.14: Encapsulation Security Palyload	47
33. Gambar 4.15: Header Data IPsec	48
34. Gambar 4.16: Format data mode AH	48
35. Gambar 4.17: <i>Autentikasi</i> Header	49
36. Gambar 4.18: Format <i>Autentikasi</i> Header	49
37. Gambar 4.19: Protocol data.....	49
38. Gambar 4.20: Source port telnet	50
39. Gambar 4.21: Header secara keseluruhan	50
40. Gambar 4.22: Header data telnet	51
41. Gambar 4.23: protocol data.....	51
42. Gambar 4.24: Protocol ICMP dan Telnet.....	56
43. Gambar 4.25: hasil capture	57
44. Gambar 4.26: status IPsec	57
45. Gambar 4.27: Header SPI.....	59

