ANALISIS PERANCANGAN DAN IMPLEMENTASI IP *SECURITY* (IPSEC) SEBAGAI PROTOKOL KEAMANAN UNTUK *VIRTUAL PRIVATE NETWORK* (VPN) PADA KLIEN PT. XYZ

TUGAS AKHIR

M. BAGUS OKA G.W.

1102001025

FAKULTAS TEKNIK DAN ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

UNIVERSITAS BAKRIE

JAKARTA

2016

HALAMAN PENGESAHAN

Tugas Akhir ini diajukan oleh:

Nama	: M. Bagus Oka G.W.
NIM	: 1102001025
Program Studi	: Informatika
Fakultas	: Fakultas Teknik dan Ilmu Komputer
Judul Skripsi	: Analisis Perancangan dan Implementasi IP *Security* (IPSec) sebagai Protokol Keamanan untuk *Virtual Private Network* (VPN) pada Klien PT. XYZ

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer (S.Kom) pada progam studi Teknik Informatika Fakultas Teknik dan Ilmu Komputer Universitas Bakrie

DEWAN PENGUJI

Pembimbing	: Berkah I. Santoso, ST., MTI.
Penguji I	: Prof. Dr. Hoga Saragih, ST., MT.
Penguji II	: Boy Pasaribu S.Kom., G.D.B.S., M.I.S., M.I.T.

Ditetapkan di : Jakarta

Tanggal : 16 September 2016

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI

Sebagai sivitas akademik Universitas Bakrie, saya yang bertanda tangan di bawah ini,

Nama	: M. Bagus Oka G.W.
NIM	: 1102001025
Program Studi	: Informatika
Fakultas	: Teknik dan Ilmu Komputer
Jenis Tugas Akhir	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Bakrie **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul:

Analisis Perancangan dan Implementasi IP *Security* (IPSec) sebagai Protokol Keamanan untuk *Virtual Private Network* (VPN) pada Klien PT. XYZ

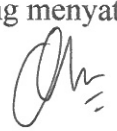
Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Bakrie berhak menyimpan, mengalih mediakan/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan Tugas Akhir saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik Hak Cipta untuk kepentingan akademis.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada Tanggal : 16 September 2016

Yang menyatakan,



(M. Bagus Oka G.W.)

HALAMAN PERNYATAAN ORISINALITAS

Tugas Akhir ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : **M. Bagus Oka G.W.**

NIM : **1102001025**

Tanda Tangan :

Tanggal : **15 September 2016**

O: Benar sekali. Jadi klien membutuhkan jaringan antar *site* yang aman. Nanti untuk koneksi antar *site* menggunakan VPN. Nah di dalam VPN itu kita pakai IPSec sebagai metode keamanannya.

P: Paham Pak. Nanti untuk *hardware*-nya menggunakan apa Pak?

O: Nanti kita pakai *device firewall* saja yang *support* IPSec. Nanti topologi jaringan saya kasih ke kamu. Kamu bikin model penelitian yang detail saja mengenai kelebihan dan fungsionalitas dari IPSec. Mulai dari perancangan jaringan, model VPN, sampai menentukan enkripsinya apa. Nanti setelah kamu analisis kebutuhan tersebut, baru kita implementasi jaringannya bersama-sama.

P: Siap Pak Otto. Saya akan belajar dulu mengenai IPSec. Lalu selanjutnya akan membuat rangka pengerjaan penelitian untuk implementasi jaringan ini.

O: Iya Ka. Nanti saya tunggu ya hasilnya. Kalau ada yang mau ditanyakan lebih lanjut atau butuh bantuan langsuka kontak saya saja ya.

P: Siap Pak Otto. Terima kasih atas usulan dan waktunya. Sampai ketemu lagi. Nanti saya kontak ya.

O: Oke Ka sama-sama.

Interviewer	*Interviewee*
Muhammad Bagus Oka	Otto Kuntowijoyo
Mahasiswa Universitas Bakrie	Divisi Jaringan PT. XYZ

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan kehadirat Allah SWT, karena hanya atas berkat dan karunia-Nya, sehingga Tugas Akhir yang berjudul "Analisis Perancangan dan Implementasi IP *Security* (IPSec) sebagai Protokol Keamanan untuk *Virtual Private Network* (VPN) pada Klien PT. XYZ", dapat terselesaikan dengan baik. Penulisan Tugas Akhir ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Komputer Program Studi Informatika pada Fakultas Teknologi dan Ilmu Komputer Universitas Bakrie. Penyusunan Tugas Akhir ini tidak terlepas dari berbagai hambatan dan kesulitan dari awal hingga akhir penyusunan.

Terima kasih juga Penulis sampaikan kepada Universitas Bakrie yang telah memberikan dukungan dan fasilitas yang memadai selama masa perkuliahan. Begitu banyak pihak yang telah memberikan doa, masukan, bantuan, semangat dan nasihat selama penyusunan Tugas Akhir ini. Oleh karena itu, Penulis sampaikan juga terima kasih kepada:

1. Kedua orang tua tercinta, Bapak Arfan Chairudin dan Ibu Ika Saulina atas kasih sayang, dukungan, dan doa yang tidak henti-henti untuk penulis.
2. Anggittya Larasaty, sahabat yang tidak pernah lelah untuk mendukung dan menyemangati penulis dalam penulisan penelitian ini.
3. Dosen pembimbing Tugas Akhir, Bapak Berkah I. Santoso, ST., MTI., yang sudah dua tahun dengan sabar membimbing penulis dalam menyelesaikan penelitian ini.
4. Bapak Prof. Dr. Hoga Saragih, ST., MT., selaku kepala Program Studi Informatika yang membantu penulis dalam penyusunan penelitian ini.
5. Bapak Iqbal, Mas Otto, dan Mas Diki beserta tim divisi jaringan PT. XYZ yang telah mengizinkan penulis melakukan penelitian dalam proyek implementasi jaringan untuk klien.

6. Sahabat- sahabat penulis Ikri, Bagus, Preste, Kak Siska, Kak Eky yang selalu menyemangati dan membantu penulis.
7. Adik-adik dan keluarga penulis, terima kasih untuk doa dan motivasi yang diberikan.
8. Teman-teman Fakultas Teknologi dan Ilmu Komputer Baubau, Said, Adit, Dida, Hamdi, Dipta, dan teman-teman lain yang tidak bisa disebutkan namanya satu per satu.
9. Teman-teman Universitas Bakrie Tria, Seiva, Kenny, Edo, dan teman-teman lain yang tidak bisa disebutkan namanya satu per satu.
10. Ibu Ikri, Ibu Kenny, dan Ibu Anggit untuk doanya.
11. Kakak-kakak Sahabat Anak Manggarai Kak Septi, Kak Vita, Kak Dena, Kak Jane, Kak Suci, Kak Ais, dan kakak-kakak lain yang tidak bisa disebutkan namanya satu per satu.
12. Mbak Rona atas dukungannya yang membuat penulis tetap melanjutkan kuliah di Universitas Bakrie.
13. Teman-teman barista untuk dukungannya kepada penulis.

Semoga Allah SWT membalas kebaikan dan memberikan keberkahan kepada kita semua. Serta semoga Tugas Akhir ini memberi informasi yang berguna dan dapat bermanfaat bagi semua kalangan bidang pendidikan, khususnya bidang Informatika.

Jakarta, 16 September 2016

M. Bagus Oka G.W.

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI

Sebagai sivitas akademik Universitas Bakrie, saya yang bertanda tangan di bawah ini,

Nama : M. Bagus Oka G.W.

NIM : 1102001025

Program Studi : Informatika

Fakultas : Teknik dan Ilmu Komputer

Jenis Tugas Akhir : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Bakrie **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul:

Analisis Perancangan dan Implementasi IP *Security* (IPSec) sebagai Protokol Keamanan untuk *Virtual Private Network* (VPN) pada Klien PT. XYZ

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Bakrie berhak menyimpan, mengalih mediakan/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan Tugas Akhir saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik Hak Cipta untuk kepentingan akademis.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada Tanggal : 16 September 2016

Yang menyatakan,

(M. Bagus Oka G.W.)

ANALISIS PERANCANGAN DAN IMPLEMENTASI IP SECURITY (IPSEC) SEBAGAI PROTOKOL KEAMANAN VIRTUAL PRIVATE NETWORK (VPN) PADA KLIEN PT. XYZ

M. Bagus Oka G.W.

ABSTRAK

Keamanan jaringan merupakan faktor penting dalam suatu organisasi yang menggunakan teknologi informasi dalam kegiatannya. Hal ini menjadikan mekanisme keamanan jaringan harus diimplementasi dengan baik dan efisien untuk memastikan tidak ada data yang dapat diambil oleh penyerang dalam jaringan tersebut. IPSec adalah salah satu protokol keamanan yang diterapkan pada *layer* ketiga dalam OSI *model*. IPSec berjalan di atas VPN dan berfungsi untuk mengenkripsi setiap paket data yang keluar dan masuk dalam suatu jaringan. Penelitian ini bertujuan untuk menganalisis perancangan dan implementasi IPSec sebagai protokol keamanan jaringan klien PT. XYZ. Dari hasil penelitian, diperoleh bahwa konfigurasi yang diusulkan oleh penulis berdasarkan jurnal yang dilampirkan, dapat dilaksanakan dengan baik, dan dapat dijadikan sebagai referensi implementasi IPSec untuk proyek selanjutnya.

Kata kunci: kemanan jaringan, IPSec, analisis perancangan.

DESIGN ANALYSIS AND IMPLEMENTATION OF IP SECURITY (IPSEC) AS SECURITY PROTOKOL ON PT. XYZ CLIENT'S VIRTUAL PRIVATE NETWORK (VPN)

M. Bagus Oka G.W.

ABSTRACT

Network security is an important factor in the organization which relies on information technology. This reason makes network security mechanism must be implemented with good consideration and efficiency, to make sure there are not data that can be stolen by the attacker. IPSec is security protocol in layer three of the OSI model. The purpose of IPSec is to encrypt each data packet either in or out in the network. This study aims for providing design analysis and implementation of IPSec as a security protocol for PT. XYZ's client network. The result of this research is IPSec's configuration who author suggests based on attached journal is properly implemented, and can be referenced for next implementation.

Keywords: network security, IPSec, design analysis.

DAFTAR ISI

DAFTAR SINGKATAN

3DES	*TRIPLE DATA ENCRYPTION STANDARD*
AES	*ADVANCED ENCRYPTION STANDARD*
AH	*AUTHENTICATION HEADER*
ARPANet	*ADVANCED RESEARCH PROJECTS AGENCY NETWORK*
CLI	*COMMAND LINE INTERFACE*
DES	*DATA ENCRYPTION STANDARD*
DOD	*DEPARTMENT OF DEFENSE*
DSA	*DIGITAL SIGNATURE ALGORITHM*
E2E-NATPT	*END TO END NETWORK ADDRESS TRANSLATION PROTOCOL TRANSLATION*
ECDSA	*ELLYPTIC CURVE DIGITAL SIGNATURE ALGORITHM*
ESP	*ENCAPSULATED SECURITY PAYLOAD*
GNS3	*GRAPHICAL NETWORK SIMULATOR-3*
GtG	*GATEWAY TO GATEWAY*
HMAC	*HASH MESSAGE AUTHENTICATION CODE*
HMAC-MD5	*HASH MESSAGE AUTHENTICATION CODE-MESSAGE DIGGEST 5*
HMAC-SHA1	*HASH MESSAGE AUTHENTICATION CODE-SECURE HASH ALGORITHM*
HtG	*HOST TO GATEWAY*

HtH	*HOST TO HOST*
IAB	*INTERNET ARCHITECTURE BOARD*
IDEA	*INTERNATIONAL DATA ENCRYPTION ALGORITHM*
IKE	*INTERNET KEY EXCHANGE*
IP	*INTERNET PROTOCOL*
IPSec	*INTERNET PROTOCOL-SECURITY*
LAN	*LOCAL AREA NETWORK*
NAT-T	*NETWORK ADDRESS TRANSLATION-TRAVERSAL*
NS-2	*NETWORK SIMULATOR-2*
OS	*OPERATING SYSTEM*
OSI	*OPEN SYSTEM INTERCONNECTION*
PKI	*PUBLIC KEY INFRASTRUCTURE*
PSK	*PRE-SHARED KEY*
QoS	*QUALITY OF SERVICE*
RC4	*RIVEST CIPHER 4*
RFC	*REQUEST FOR COMMENTS*
RSA	RIVEST-SHAMIR-ADLEMAN
SA	*SECURITY ASSOCIATION*
SAD	*SECURITY ASSOCIATION DATABASE*
SPD	*SECURITY POLICY DATABASE*

SPI	*SECURITY PARAMETER INDEX*
TCP/IP	*TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL*
UDP-ESP	*USER DATAGRAM PROTOCOL-ENCAPSULATED SECURITY PAYLOAD*
VPN	*VIRTUAL PRIVATE NETWORK*
WAN	*WIDE AREA NETWORK*

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN