**DAFTAR ISI**

HALAMAN JUDUL i

HALAMAN PENGESAHAN ii

ABSTRAK iii

ABSTRACT iv

KATA PENGANTAR v

DAFTAR ISI vi

DAFTAR GAMBAR ix

DAFTAR LISTING xiii

DAFTAR TABEL xv

BAB I PENDAHULUAN 1

1.1 Latar Belakang 1

1.2 Tujuan 2

1.3 Teori Penunjang 3

1.4 Ruang Lingkup 4

1.5 Metodologi 11

1.6 Sistematika Pembahasan 12

BAB II Virtual Private Network 14

2.1 Pengenalan Virtual Private Network 14

2.2 Topologi Virtual Private Network 21

2.2.1 Site to Site Virtual Private Network 22

2.2.1.1 Point-to-Point Tunneling Protocol 24

2.2.1.2 Layer 2 Tunneling Protocol 24

2.2.1.3 Internet Protocol Security 25

2.2.1.4 Multi Protocol Label Switching 25

2.2.2 Remote User Virtual Private Network 26

2.3 Generic Routing Encapsulation (GRE) VPN 28

2.3.1 Konfigurasi Site-to-Site GRE Tunnel 29

2.4 Pengenalan Internet Protocol Security (IPsec) 31

2.4.1 Kerahasiaan (Confidentiality) 34

2.4.1.1 DES (Data Encryption Standard) 36

2.4.1.1.1 Block Cipher Mode 37

2.4.1.1.2 Stream Cipher Mode 39

2.4.1.2 3DES (Triple DES) 39

2.4.1.3 AES (Advanced Encryption Standard) 41

2.4.1.4 SEAL (Software-Optimized Encryption

Algorithm) 42

2.4.2 Keaslian (Integrity) 42

2.4.3 Autentikasi (Authentication) 44

2.4.4 Secure Key Exchange 46

2.5 Protokol Keamanan IPsec 48

2.5.1 Authentication Header 50

2.5.2 Encapsulating Security Payload 51

2.6 Mode Protokol IPsec 54

2.6.1 Transport Mode 54

2.6.2 Tunnel Mode 54

2.7 Internet Key Exchange 55

BAB III IMPLEMENTASI DAN STUDI KASUS 62

3.1 Persiapan 62

3.1.1 Router 62

3.1.2 Koneksi Internet ADSL 69

3.2 Implementasi 70

3.2.1 Jaringan Laboratorium Jaringan Komputer 72

3.2.2 Jaringan Remote 79

BAB IV IPSEC PADA ROUTER CISCO 1841 85

4.1 Skenario Uji Coba 85

4.2 Tolok Ukur 92

4.2.1 PING 92

4.2.2 Aplikasi Sederhana 94

4.2.3 Wireshark 95

4.3 Metode Penelitian 102

4.3.1 ANOVA (Analysis of Variance) 102

4.3.2 Regressi Linear 103

4.4 Uji Coba dan Analisa 104

4.4.1 Uji Coba 104

4.4.1.1 DES-SHA 104

4.4.1.2 DES-MD5 107

4.4.1.3 3DES-SHA 108

4.4.1.4 3DES-MD5 105

4.4.1.5 AES-SHA 106

4.4.1.6 AES-MD5 108

4.4.2 Analisa 113

4.4.2.1 ANOVA 114

4.4.2.2 Regressi Linear 120

4.4.2.3 Analisa Biaya 122

4.4.3 Hasil Analisa 125

4.5 Cisco Configuration Proffesional 126

4.5.1 Pengenalan Cisco Configuration Proffesional 126

4.5.2 VPN IPsec dengan Cisco Configuration Proffesional 132

BAB V PENUTUP 142

5.1 Kesimpulan 142

5.2 Saran 142

DAFTAR PUSTAKA 144

RIWAYAT HIDUP 145

LAMPIRAN A – KONFIGURASI ROUTER 1 A-1

LAMPIRAN B – KONFIGURASI ROUTER 2 B-1

LAMPIRAN C – SEGMEN PROGRAM CLASS CLIENT C-1

LAMPIRAN D – IPSEC SECURITY ASSOCIATION D-1

LAMPIRAN E – HASIL UJI COBA E-1

LAMPIRAN F – TABEL DISTRIBUSI F PROBABILITAS = 0.05 F-1