



A

- access VPNs 1
- Aggressive Mode
 - description
 - option 61, 93

B

- benefits 8

C

- Cisco 1720 VPN Router
 - documentation xvi
- Cisco 7100 VPN Router
 - documentation xviii
- Cisco Secure Policy Manager
 - documentation xiii
- Cisco Secure VPN Client
 - description 4
 - documentation xv
- client-initiated VPNs 2
- Connect using Secure Gateway Tunnel
 - option 33, 57
- crypto isakmp policy global configuration command 69, 101

D

- digital certificate 5
- digital certification
 - Entrust

- description 19
- Microsoft
 - description 19
- VeriSign
 - description 19
- dynamic IP addressing
 - description 15

E

- Enable Perfect Forward Secrecy
 - description
 - option 61, 93
- Enable Replay Detection
 - description
 - option 61, 93
- Encrypt Alg
 - option 66
- extranet VPNs 3

H

- Hash Alg
 - option 66, 98

I

- ID Type
 - option 36, 59
- IKE
 - description 4
- IKE Mode Configuration
 - description 15

Internal Network IP Address

- box 36

Internet Key Exchange

- description 4

intranet VPNs 3

IP Network Security

- description 4

IPSec

- description 4

IPSec tunneling protocol

- description 11

L

LDAP

- configuring 105, 110, 112, 114

M

manual configuration

- description 14

mode tunnel command 39, 46

N

NAS-initiated VPNs 2

new and changed information x

P

Port

- option 36, 91

Pre-shared key

- option 37, 92

pre-shared key, configuring

- router 70

pre-shared keys

- description 16

public/private key system 5

S

sample configurations x

sample IP addresses and keys 26

Secure

- option 32

security policy 5

Select Certificate

- option 36, 59

static IP addressing

- description 14

system requirements 7

T

TAC

- TAC, sample configurations x

U

Use Manual Keys

- description

- option 61, 93

V

VPN

- description 1

type

- access 1

- client-initiated 2

- NAS-initiated 2

- extranet 3

- intranet 3

W

wildcard pre-shared key
description 18

