Symbols

* (asterisk)
  - autolearned entries 9-7
  - port security wildcard 9-5
  - port security wildcards 9-5

Numerics

3DES encryption
  - IKE 7-6
  - IPsec 7-6

A

AAA
  - configuring accounting services 4-14 to ??
  - default settings 4-16
  - description 4-1
  - distributing with CFS (procedure) 4-29
  - enabling server distribution 4-27
  - local services 4-14
  - remote services 4-4
  - setting authentication 4-14
  - starting a distribution session 4-13

AAA servers
  - groups 4-4
  - monitoring 4-5
  - remote authentication 4-15

Access Control Lists. See IPv4-ACLs; IPv6-ACLs

accounting
  - configuring services 4-14 to ??

Advanced Encrypted Standard encryption. See AES encryption

AES encryption
IKE 7-6
IPsec 7-6
AES-XCBC-MAC
IPsec 7-6
authentication
fabric security 8-1
guidelines 4-15
local 4-3
remote 4-3, 4-15
user IDs 4-3
authentication, authorization, and accounting. See AAA
authorization
rule placement order 3-10

C

CAs
authenticating 6-9
certificate download example 6-17
configuring 6-6 to 6-15
creating a trust point 6-8
default settings 6-6
deleting digital certificates 6-14
enrollment using cut-and-paste 6-4
example configuration ?? to 6-20
identity 6-2
maintaining 6-12
maximum limits 6-5
monitoring 6-12
multiple 6-4
multiple trust points 6-3
peer certificates 6-5
purpose 6-2
certificate revocation lists. See CRLs
Cisco Access Control Server. See Cisco ACS
Cisco ACS
configuring for RADIUS 4-30 to 4-34
configuring for TACACS+ 4-30 to 4-34

cisco-av-pair
specifying for SNMPv3 4-10
Cisco vendor ID
description 4-9
common roles
configuring 3-4
deleting (procedure) 3-9
common users
mapping CLI to SNMP 3-5
CRLs
configuring 6-14
configuring revocation checking methods 6-10
description 6-5
downloading example 6-19
generation example 6-19
importing example ?? to 6-20
crypto IPv4-ACLs
any keyword 7-14
configuration guidelines 7-19
mirror images 7-13
crypto map entries
global lifetime values 7-18
setting SA lifetimes 7-28
crypto maps
auto-peer option 7-16
configuration guidelines 7-20
configuring perfect forward secrecy 7-28
entries for IPv4-ACLs 7-15
perfect forward secrecy 7-17
SA lifetime negotiations 7-16
SAs between peers 7-16
crypto map sets
applying to interfaces 7-17

D

Data Encryption Standard encryption. See DES encryption
DES encryption
IKE 7-6

IPsec 7-6
DH
IKE 7-6
DHCHAP
authentication modes 8-3
compatibility with other SAN-OS features 8-3
configuring 8-6 to ??
default settings 8-6
description 8-2
enabling 8-3, 8-6
group settings 8-4
hash algorithms 8-4
licensing 8-2
passwords for local switches 8-4
passwords for remote devices 8-5
timeout values 8-5
See also FC-SP
Diffie-Hellman Challenge Handshake Authentication Protocol. See DHCHAP
Diffie-Hellman protocol. See DH
digital certificates
configuration example 6-16 to 6-17
configuring 6-6 to 6-15
default settings 6-6
deleting from CAs 6-14
exporting 6-5, 6-13
generating requests for identity certificates 6-10
importing 6-5, 6-13
installing identity certificates 6-11
IPsec 7-7 to 7-9
maintaining 6-12
maximum limits 6-5
monitoring 6-12
peers 6-5
purpose 6-2
requesting identity certificate example 6-18
revocation example 6-19
SSH support 3-6
digital signature algorithm. See DSA key pairs
DSA key-pairs

generating 3-14
dsa key pairs
generating 3-14

E

EFMD
fabric binding 10-1
E ports
fabric binding checking 10-2
Exchange Fabric Membership Data. See EFMD 10-1

F

fabric binding
checking for Ex ports 10-2
compatibility with DHCHAP 8-3
default settings 10-3
description ?? to 10-2
EFMD 10-1
enforcement 10-2
port security comparison 10-1
fabric security
authentication 8-1
default settings 8-6
FCIP
compatibility with DHCHAP 8-3
FC-SP
authentication 8-1
enabling 8-6
enabling on ISLs 8-5
See also DHCHAP
Federal Information Processing Standards. See FIPS
Fibre Channel interfaces
default settings 3-7, 4-16, 6-6, 7-21, 8-6, 9-9, 10-3
Fibre Channel Security Protocol. See FC-SP
FIPS

G

global keys
- assigning for RADIUS 4-8

H

high availability
- compatibility with DHCHAP 8-3

host names
- configuring for digital certificates 6-7

I

ICMP packets
- type value 5-4

IDs
- Cisco vendor ID 4-9

IKE
- algorithms for authentication 7-6
- default settings 6-6, 7-21
- description 7-4
- initializing 7-9
- refreshing SAs 7-26
- terminology 7-5
- transforms for encryption 7-6
- viewing configuration (procedure) 7-23

IKE domains
- clearing 7-25
- description 7-10

IKE initiators
- configuring version 7-25

IKE peers
- configuring keepalive times 7-24

IKE policies
- configuring negotiation parameters 7-24
- negotiation 7-10

IKE tunnels
- clearing 7-25

description 7-10
interfaces
default settings 3-7, 4-16, 6-6, 7-21, 8-6, 9-9, 10-3
Internet Key Exchange. See IKE
IP domain names
configuring for digital certificates 6-7
IP filters
contents 5-2
restricting IP traffic 5-1, 5-2
using IP-ACL Wizard (procedure) 5-6
IPsec
algorithms for authentication 7-6
crypto IPv4-ACLs 7-12 to 7-26
default settings 7-21
digital certificate support 7-7 to 7-9
enabling with FCIP Wizard (procedure) 7-21
fabric setup requirements 7-4
global lifetime values 7-18
hardware compatibility 7-4
licensing requirements 7-18
maintenance 7-18
RFC implementations 7-1
terminology 7-5
transform sets 7-14
transforms for encryption 7-6
unsupported features 7-4
viewing configuration (procedure) 7-23
IP security. See IPsec
IPv4-ACLs
adding entries 5-7
applying to interfaces 5-9, 5-10
configuration guidelines 5-5
creating complex IPv4-ACLs (procedure) 5-7
creating with IP-ACL Wizard (procedure) 5-6
crypto 7-12 to 7-26
crypto map entries 7-15
example configuration 5-11
reading dump logs 5-9
removing entries 5-8

L

logins
SSH 4-5
Telnet 4-5

M

management interfaces
default settings 3-7, 4-16, 6-6, 7-21, 8-6, 9-9, 10-3
MD5 authentication
IKE 7-7
IPsec 7-6
Message Authentication Code using AES. See AES-XCBC-MAC
Message Digest 5. See MD5 authentication
mgmt0 interfaces
default settings 3-7, 4-16, 6-6, 7-21, 8-6, 9-9, 10-3
Microsoft Challenge Handshake Authentication Protocol. See MSCHAP
MSCHAP
description 4-14

N

network administrators
additional roles 4-4
permissions 4-4
network operators
permissions 4-4

O

Online Certificate Status Protocol. See OCSP
OSCP
support 6-5

P

passwords

DHCHAP 8-4, 8-5
strong characteristics 3-6
PKI
enrollment support 6-4
PortChannels
compatibility with DHCHAP 8-3
port security
activating 9-13
activation 9-3
activation rejection 9-3
auto-learning 9-2
cleaning up databases 9-20
compatibility with DHCHAP 8-3
configuring CFS distribution ?? to 9-7
copying databases 9-19
database interactions 9-7
database merge guidelines 9-9
data scenarios 9-8
deactivating 9-13
default settings 9-9
deleting databases 9-20
deleting entries from database (procedure) 9-17
disabling 9-13
displaying settings (procedure) 9-21
displaying statistics (procedure) 9-21
enabling 9-13
enforcement mechanisms 9-2
fabric binding comparison 10-1
forcing activation 9-14
manual configuration guidelines 9-11
WWN identification 9-5
port security auto-learning
description 9-2
device authorization 9-4
disabling 9-16
distributing configuration 9-6
enabling 9-3
guidelines for configuring with CFS 9-10
guidelines for configuring without CFS 9-10

port security databases
cleaning up 9-20
copying 9-19
copying active to config (procedure) 9-15
deleting 9-20
interactions 9-7
manual configuration guidelines 9-11
merge guidelines 9-9
reactivating 9-14
scenarios 9-8
preshared keys
RADIUS 4-8
TACACS+ 4-11
Public Key Infrastructure. See PKI

R

RADIUS
AAA protocols 4-1
CFS merge guidelines 4-15
clearing configuration distribution sessions 4-29
configuring Cisco ACS 4-30 to 4-34
configuring test idle timer 4-8
configuring test user name 4-8
default settings 4-16
description 4-16
discarding configuration distribution changes 4-28
enabling configuration distribution 4-27
setting preshared keys 4-8
specifying time-out 4-19
starting a distribution session 4-13
role databases
disabling distribution 3-11
enabling distribution 3-11
viewing with Fabric Manager 3-17
roles
configuring rules 3-2
default permissions 4-4
default setting 3-8

deleting (procedure) 3-9
distributing configurations ?? to 3-18
user profiles 4-4
See also command roles
RSA key-pairs
deleting 6-15
description 6-3
exporting 6-5, 6-13
generating 6-7
importing 6-5, 6-13
multiple 6-4
rsa key pairs
generating 3-14
rules
configuring 3-2

S

SAs
establishing between IPsec peers 7-16
lifetime negotiations 7-16
refreshing 7-26
setting lifetime 7-28
Secure Hash Algorithm. See SHA-1
security
accounting 4-4
managing on the switch 4-1
security associations. See SAs
security control
local 4-2
remote 4-2, 4-17
remote AAA servers 4-16
SHA-1
IKE 7-7
IPsec 7-6
SNMP
creating roles 3-4
mapping CLI operations 3-5
security features 4-3

SNMPv3
specifying cisco-av-pair 4-10
SSH
default service 3-14
description 3-6
digital certificate authentication 3-6
enabling 3-16
generating server key-pairs 3-14
logins 4-5
overwriting server key-pairs 3-15
SSH key pairs
overwriting 3-15
switch security
default settings 3-7, 4-16

T

TACACS+
AAA protocols 4-1
CFS merge guidelines 4-15
clearing configuration distribution sessions 4-29
configuring Cisco ACS 4-30 to 4-34
default settings 4-16
description 4-11
discarding configuration distribution changes 4-28
displaying server statistics 4-35
enabling configuration distribution 4-27
global keys 4-11
setting default server encryption 4-24
setting default server timeout 4-24
setting preshared key 4-11
specifying server at login 4-13
starting a distribution session 4-13
validating 4-12
TCP ports
IPv4-ACLs 5-3
Telnet
enabling 3-16
logins 4-5

TE ports
fabric binding checking 10-2
transform sets
description 7-14
Triple DES. See 3DEC encryption
trust points
creating 6-8
description 6-2
multiple 6-3
saving configuration across reboots 6-12
TrustSec FC Link Encryption 11-1
enabling 11-3
ESP Settings 11-4
ESP Wizard 11-5
Security Association Parameters 11-3
Security Associations 11-3
Supported Modules 11-1
Terminology 11-2

U

UDP ports
IPv4-ACLs 5-3
user accounts
configuring ?? to 3-18
displaying information 3-18
password characteristics 3-6
user IDs
authentication 4-3
user profiles
role information 4-4
users
configuring 3-12
deleting (procedure) 3-13
description 3-5
displaying account information 3-18

V

vendor-specific attributes. See VSAs
VSAN policies
default roles 3-8
VSANs
compatibility with DHCHAP 8-3
IP routing 5-1, 5-2
Rules and features 3-2
VSAs
communicating attributes 4-9
protocol options 4-9

W

WWNs
port security 9-5