



INDEX

Symbols

* (asterisk)

- autolearned entries [9-20](#)
- port security wildcard [9-15](#)
- port security wildcards [9-15](#)

Numerics

3DES encryption

- IKE [7-7](#)
- IPsec [7-6](#)

A

AAA

- authentication process [4-6](#)
- authorization process [4-6](#)
- configuring accounting services [4-33 to ??](#)
- default settings [4-37](#)
- description [4-1](#)
- DHCHAP authentication [8-10](#)
- distributing with CFS (procedure) [4-30](#)
- enabling server distribution [4-28](#)
- local services [4-33](#)
- remote services [4-4](#)
- setting authentication [4-33](#)
- starting a distribution session [4-29](#)

AAA servers

- groups [4-5](#)
- monitoring [4-5](#)
- remote authentication [4-4](#)

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

accounting

- configuring services [4-33 to ??](#)

administrator passwords

- recovering (procedure) [3-21](#)

Advanced Encrypted Standard encryption. See AES encryption

AES encryption

- IKE [7-7](#)
- IPsec [7-6](#)

AES-XCBC-MAC

- IPsec [7-7](#)

authentication

- fabric security [8-1](#)
- guidelines [4-4](#)
- local [4-3](#)
- remote [4-3, 4-4](#)
- user IDs [4-3](#)

authentication, authorization, and accounting. See AAA

authorization

- rule placement order [3-5](#)

C

CAs

- authenticating [6-10](#)
- certificate download example [6-18](#)
- configuring [6-6 to 6-16](#)
- creating a trust point [6-8](#)
- default settings [6-36](#)
- deleting digital certificates [6-15](#)
- description [6-1 to 6-5](#)
- enrollment using cut-and-paste [6-4](#)
- example configuration [6-16 to 6-35](#)

Send documentation comments to mdsfeedback-doc@cisco.com

- identity [6-2](#)
- maintaining [6-14](#)
- maximum limits [6-35](#)
- monitoring [6-14](#)
- multiple [6-4](#)
- multiple trust points [6-3](#)
- peer certificates [6-5](#)
- purpose [6-2](#)
- certificate authorities. See CAs
- certificate revocation lists. See CRLs
- Cisco Access Control Server. See Cisco ACS
- Cisco ACS
 - configuring for RADIUS [4-34 to 4-37](#)
 - configuring for TACACS+ [4-34 to 4-37](#)
- cisco-av-pair
 - specifying for SNMPv3 [4-17](#)
- Cisco vendor ID
 - description [4-16](#)
- common roles
 - configuring [3-10](#)
 - deleting (procedure) [3-3](#)
- common users
 - mapping CLI to SNMP [3-11](#)
- CRLs
 - configuring [6-15](#)
 - configuring revocation checking methods [6-11](#)
 - description [6-5](#)
 - downloading example [6-33](#)
 - generation example [6-32](#)
 - importing example [?? to 6-35](#)
- crypto IPv4-ACLs
 - any keyword [7-25](#)
 - configuration guidelines [7-22](#)
 - creating [7-25](#)
 - mirror images [7-24](#)
- crypto map entries
 - global lifetime values [7-37](#)
 - setting SA lifetimes [7-31](#)
- crypto maps

- auto-peer option [7-32](#)
- configuration guidelines [7-29](#)
- configuring perfect forward secrecy [7-35](#)
- entries for IPv4-ACLs [7-28](#)
- perfect forward secrecy [7-34](#)
- SA lifetime negotiations [7-30](#)
- SAs between peers [7-28](#)
- crypto map sets
 - applying to interfaces [7-36](#)

D

- Data Encryption Standard encryption. See DES encryption
- DES encryption
 - IKE [7-7](#)
 - IPsec [7-6](#)
- DH
 - IKE [7-7](#)
- DHCHAP
 - AAA authentication [8-10](#)
 - authentication modes [8-4](#)
 - compatibility with other SAN-OS features [8-3](#)
 - configuring [8-2 to 8-10](#)
 - configuring AAA authentication [8-10](#)
 - default settings [8-10](#)
 - description [8-2](#)
 - enabling [8-4](#)
 - group settings [8-6](#)
 - hash algorithms [8-6](#)
 - licensing [8-2](#)
 - passwords for local switches [8-7](#)
 - passwords for remote devices [8-8](#)
 - timeout values [8-9](#)
 - See also FC-SP
- Diffie-Hellman Challenge Handshake Authentication Protocol. See DHCHAP
- Diffie-Hellman protocol. See DH
- digital certificates
 - configuration example [6-17 to 6-18](#)

Send documentation comments to mdsfeedback-doc@cisco.com

- configuring [6-6 to 6-16](#)
- default settings [6-36](#)
- deleting from CAs [6-15](#)
- description [6-1 to 6-5](#)
- exporting [6-5, 6-14](#)
- generating requests for identity certificates [6-12](#)
- importing [6-5, 6-14](#)
- installing identity certificates [6-12](#)
- IPsec [7-7 to 7-10](#)
- maintaining [6-14](#)
- maximum limits [6-35](#)
- monitoring [6-14](#)
- peers [6-5](#)
- purpose [6-2](#)
- requesting identity certificate example [6-23](#)
- revocation example [6-29](#)
- SSH support [3-20](#)

digital signature algorithm. See DSA key pairs

documentation

- related documents [4-xix](#)

DSA key-pairs

- generating [3-17](#)

dsa key pairs

- generating [3-17](#)

E

EFMD

- fabric binding [10-1](#)

E ports

- fabric binding checking [10-2](#)

Exchange Fabric Membership Data. See EFMD [10-1](#)

F

fabric binding

- activation [10-3](#)
- checking for Ex ports [10-2](#)

- compatibility with DHCHAP [8-3](#)
- configuration [10-3 to ??](#)
- default settings [10-4](#)
- description [10-1 to 10-2](#)
- EFMD [10-1](#)
- enforcement [10-2](#)
- licensing requirements [10-1](#)
- port security comparison [10-1](#)
- saving configurations [10-4](#)

fabric security

- authentication [8-1](#)
- default settings [8-10](#)

FCIP

- compatibility with DHCHAP [8-3](#)

FC-SP

- authentication [8-1](#)
- enabling [8-4](#)
- enabling on ISLs [8-10](#)

See also DHCHAP

Federal Information Processing Standards. See FIPS

Fibre Channel Security Protocol. See FC-SP

FICON

- fabric binding requirements [10-3](#)

FIPS

- configuration guidelines [2-1](#)
- self-tests [2-3](#)

G

global keys

- assigning for RADIUS [4-10](#)

H

high availability

- compatibility with DHCHAP [8-3](#)

host names

- configuring for digital certificates [6-6](#)

Send documentation comments to mdsfeedback-doc@cisco.com

I

ICMP packets

type value [5-4](#)

IDs

Cisco vendor ID [4-16](#)

IKE

algorithms for authentication [7-7](#)

default settings [6-36, 7-39](#)

description [7-3](#)

initializing [7-13](#)

refreshing SAs [7-20](#)

terminology [7-5](#)

transforms for encryption [7-7](#)

viewing configuration (procedure) [7-11](#)

IKE domains

clearing [7-20](#)

description [7-13](#)

IKE initiators

configuring version [7-18](#)

IKE peers

configuring keepalive times [7-17](#)

IKE policies

configuring negotiation parameters [7-15](#)

negotiation [7-14](#)

IKE tunnels

clearing [7-20](#)

description [7-13](#)

Internet Key Exchange. See IKE

IP domain names

configuring for digital certificates [6-6](#)

IP filters

contents [5-3](#)

restricting IP traffic [5-1, 5-2](#)

using IP-ACL Wizard (procedure) [5-5](#)

IPsec

algorithms for authentication [7-6](#)

crypto IPv4-ACLs [7-21 to 7-25](#)

default settings [7-39](#)

description [7-2](#)

digital certificate support [7-7 to 7-10](#)

enabling with FCIP Wizard (procedure) [7-10](#)

fabric setup requirements [7-5](#)

global lifetime values [7-37](#)

hardware compatibility [7-4](#)

licensing requirements [7-4](#)

maintenance [7-37](#)

prerequisites [7-4](#)

RFC implementations [7-1, 7-2](#)

terminology [7-5](#)

transform sets [7-25](#)

transforms for encryption [7-6](#)

unsupported features [7-5](#)

viewing configuration (procedure) [7-11](#)

IP security. See IPsec

IPv4-ACLs

adding entries [5-7](#)

applying to interfaces [5-10, 5-11](#)

configuration guidelines [5-2](#)

creating complex IPv4-ACLs (procedure) [5-6](#)

creating with IP-ACL Wizard (procedure) [5-5](#)

crypto [7-21 to 7-25](#)

crypto map entries [7-28](#)

example configuration [5-12](#)

reading dump logs [5-9](#)

removing entries [5-8](#)

L

logins

SSH [4-5](#)

Telnet [4-5](#)

M

MD5 authentication

IKE [7-7](#)

Send documentation comments to mdsfeedback-doc@cisco.com

IPsec [7-6](#)

Message Authentication Code using AES. See
AES-XCBC-MAC

Message Digest 5. See MD5 authentication

Microsoft Challenge Handshake Authentication Protocol.
See MSCHAP

MSCHAP

description [4-31](#)

N

network administrators

additional roles [4-3](#)

permissions [4-3](#)

network operators

permissions [4-3](#)

O

Online Certificate Status Protocol. See OCSP

OSCP

support [6-5](#)

P

passwords

DHCHAP [8-7, 8-8](#)

recovering (procedure) [3-21](#)

strong characteristics [3-13](#)

persistent domain ID

FICON VSANs [10-3](#)

PKI

enrollment support [6-4](#)

PortChannels

compatibility with DHCHAP [8-3](#)

port security

activating [9-9](#)

activation [9-3](#)

activation rejection [9-10](#)

auto-learning [9-2](#)

cleaning up databases [9-23](#)

compatibility with DHCHAP [8-3](#)

configuration guidelines [9-3](#)

configuring CFS distribution [9-17 to 9-20](#)

copying databases [9-22](#)

database interactions [9-20](#)

database merge guidelines [9-20](#)

data scenarios [9-21](#)

deactivating [9-9](#)

default settings [9-24](#)

deleting databases [9-23](#)

deleting entries from database (procedure) [9-17](#)

disabling [9-8](#)

displaying settings (procedure) [9-11](#)

displaying statistics (procedure) [9-12](#)

enabling [9-8](#)

enforcement mechanisms [9-2](#)

fabric binding comparison [10-1](#)

forcing activation [9-10](#)

license requirement [9-2](#)

manual configuration guidelines [9-4](#)

preventing unauthorized accesses [9-1](#)

unauthorized accesses prevented [9-1](#)

WWN identification [9-16](#)

port security auto-learning

description [9-2](#)

device authorization [9-14](#)

disabling [9-13](#)

distributing configuration [9-19](#)

enabling [9-12](#)

guidelines for configuring with CFS [9-3](#)

guidelines for configuring without CFS [9-4](#)

port security databases

cleaning up [9-23](#)

copying [9-22](#)

copying active to config (procedure) [9-11](#)

deleting [9-23](#)

interactions [9-20](#)

Send documentation comments to mdsfeedback-doc@cisco.com

manual configuration guidelines [9-4](#)

merge guidelines [9-20](#)

reactivating [9-11](#)

scenarios [9-21](#)

preshared keys

RADIUS [4-10](#)

TACACS+ [4-19](#)

Public Key Infrastructure. See PKI

R

RADIUS

AAA protocols [4-1](#)

CFS merge guidelines [4-30](#)

clearing configuration distribution sessions [4-30](#)

configuring Cisco ACS [4-34 to 4-37](#)

configuring server monitoring parameters [4-12](#)

configuring test idle timer [4-14](#)

configuring test user name [4-15](#)

default settings [4-38](#)

description [4-10](#)

discarding configuration distribution changes [4-30](#)

enabling configuration distribution [4-28](#)

sending test messages for monitoring [4-16](#)

setting preshared keys [4-10](#)

specifying time-out [4-11](#)

starting a distribution session [4-29](#)

role databases

disabling distribution [3-9](#)

enabling distribution [3-9](#)

viewing with Fabric Manager [3-10](#)

roles

configuring rules [3-3](#)

default permissions [4-3](#)

default setting [3-22](#)

deleting (procedure) [3-3](#)

distributing configurations [?? to 3-10](#)

user profiles [4-4](#)

See also command roles

RSA key-pairs

deleting [6-16](#)

description [6-3](#)

exporting [6-5, 6-14](#)

generating [6-6](#)

importing [6-5, 6-14](#)

multiple [6-4](#)

rsa key pairs

generating [3-17](#)

rules

configuring [3-3](#)

S

SAs

establishing between IPsec peers [7-28](#)

lifetime negotiations [7-30](#)

refreshing [7-20](#)

setting lifetime [7-31](#)

Secure Hash Algorithm. See SHA-1

security

accounting [4-4](#)

managing on the switch [4-2](#)

security associations. See SAs

security control

local [4-2](#)

remote [4-2, 4-18](#)

remote AAA servers [4-9](#)

server groups

configuring [4-26](#)

SHA-1

IKE [7-7](#)

IPsec [7-7](#)

SNMP

creating roles [3-11](#)

mapping CLI operations [3-11](#)

security features [4-2](#)

SNMPv3

specifying cisco-av-pair [4-17](#)

Send documentation comments to mdsfeedback-doc@cisco.com

SSH

- default service [3-16](#)
- description [3-17](#)
- digital certificate authentication [3-20](#)
- enabling [3-20](#)
- generating server key-pairs [3-17](#)
- logins [4-5](#)
- overwriting server key-pairs [3-18](#)
- specifying keys [3-18](#)

SSH key pairs

- overwriting [3-18](#)

switch security

- default settings [3-22, 4-37](#)

sWWNs

- configuring for fabric binding [10-3](#)

T

TACACS+

- AAA protocols [4-1](#)
- CFS merge guidelines [4-30](#)
- clearing configuration distribution sessions [4-30](#)
- configuring Cisco ACS [4-34 to 4-37](#)
- default settings [4-38](#)
- description [4-18](#)
- discarding configuration distribution changes [4-30](#)
- displaying server statistics [4-25](#)
- enabling [4-19](#)
- enabling configuration distribution [4-28](#)
- global keys [4-19](#)
- sending test messages for monitoring [4-24](#)
- setting default server encryption [4-19](#)
- setting default server timeout [4-20](#)
- setting global secret keys [4-20](#)
- setting preshared key [4-19](#)
- setting server addresses [4-19](#)
- setting server monitoring parameters [4-22](#)
- setting timeout value [4-20](#)
- specifying server at login [4-25](#)

- starting a distribution session [4-29](#)

- validating [4-24](#)

TCP ports

- IPv4-ACLs [5-4](#)

Telnet

- enabling [3-20](#)

- logins [4-5](#)

TE ports

- fabric binding checking [10-2](#)

transform sets

- description [7-25](#)

Triple DES. See 3DEC encryption

trust points

- creating [6-8](#)
- description [6-2](#)
- multiple [6-3](#)
- saving configuration across reboots [6-13](#)

TrustSec FC Link Encryption [11-2](#)

- Best Practices [11-13](#)
- enabling [11-2](#)
- ESP Settings [11-5](#)
- ESP Wizard [11-8](#)
- Information [11-11](#)
- Security Association Parameters [11-3](#)
- Security Associations [11-3](#)
- Supported Modules [11-2](#)
- Terminology [11-1](#)

U

UDP ports

- IPv4-ACLs [5-4](#)

user accounts

- configuring [3-12 to 3-16](#)
- displaying information [3-16](#)
- password characteristics [3-13](#)

user IDs

- authentication [4-3](#)

user profiles

Send documentation comments to mdsfeedback-doc@cisco.com

role information [4-4](#)

users

configuring [3-14](#)

deleting (procedure) [3-15](#)

description [3-13](#)

displaying account information [3-16](#)

V

vendor-specific attributes. See VSAs

VSAN policies

default roles [3-22](#)

VSANs

compatibility with DHCHAP [8-3](#)

IP routing [5-1, 5-2](#)

Rules and features [3-4](#)

VSAs

communicating attributes [4-16](#)

protocol options [4-17](#)

W

WWNs

port security [9-16](#)