



INDEX

Symbols

* (asterisk)

- autolearned entries [9-14](#)
- port security wildcard [9-10](#)
- port security wildcards [9-10](#)

Numerics

3DES encryption

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

A

AAA

- authentication process [3-7](#)
- authorization process [3-7](#)
- configuring accounting services [3-53 to 3-54](#)
- default settings [3-58](#)
- description [3-1](#)
- DHCHAP authentication [8-9](#)
- displaying error-enabled status [3-5](#)
- enabling server distribution [3-46](#)
- local services [3-52](#)
- remote services [3-4](#)
- setting authentication [3-52](#)
- starting a distribution session [3-46](#)

AAA servers

- groups [3-4](#)
- monitoring [3-6](#)
- remote authentication [3-4](#)

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

accounting

- configuring services [3-53 to 3-54](#)

administrator passwords

- recovering (procedure) [5-23](#)

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 [3-4](#)
- local [3-3](#)
- remote [3-3, 3-4](#)
- user IDs [3-3](#)

authentication, authorization, and accounting. See AAA

authorization

- role-based [5-1](#)
- rule placement order [5-4](#)

C

CAs

- authenticating [6-8](#)
- certificate download example [6-19](#)
- configuring [6-6 to 6-15](#)
- creating a trust point [6-8](#)
- default settings [6-39](#)
- deleting digital certificates [6-14](#)
- description [6-1 to 6-5](#)
- displaying configuration [6-16](#)

Send documentation comments to mdsfeedback-doc@cisco.com

- enrollment using cut-and-paste [6-4](#)
 - example configuration [6-16 to 6-38](#)
 - identity [6-2](#)
 - maintaining [6-13](#)
 - maximum limits [6-38](#)
 - monitoring [6-13](#)
 - 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 [3-55 to 3-58](#)
 - configuring for TACACS+ [3-55 to 3-58](#)
 - cisco-av-pair
 - specifying for SNMPv3 [3-29](#)
 - Cisco vendor ID
 - description [3-28](#)
 - common roles
 - configuring [5-9](#)
 - common users
 - mapping CLI to SNMP [5-10](#)
 - CRLs
 - configuring [6-14](#)
 - configuring revocation checking methods [6-9](#)
 - description [6-5](#)
 - downloading example [6-34](#)
 - generation example [6-33](#)
 - importing example [?? to 6-38](#)
 - crypto IPv4-ACLs
 - any keyword [7-20](#)
 - configuration guidelines [7-17](#)
 - creating [7-21](#)
 - creating crypto map entries [7-24](#)
 - mirror images [7-19](#)
 - crypto map entries
 - configuring global lifetime values [7-29](#)
 - global lifetime values [7-28](#)
 - setting SA lifetimes [7-25](#)
 - crypto maps
 - auto-peer option [7-26](#)
 - configuration guidelines [7-24](#)
 - configuring autopeer option [7-26](#)
 - configuring perfect forward secrecy [7-27](#)
 - creating entries [7-24](#)
 - entries for IPv4-ACLs [7-23](#)
 - perfect forward secrecy [7-27](#)
 - SA lifetime negotiations [7-25](#)
 - SAs between peers [7-23](#)
 - crypto map sets
 - applying to interfaces [7-27](#)
-
- ## D
- Data Encryption Standard encryption. See DES encryption
 - DES encryption
 - IKE [7-7](#)
 - IPsec [7-6](#)
 - DH
 - IKE [7-7](#)
 - DHCHAP
 - AAA authentication [8-9](#)
 - authentication modes [8-4](#)
 - compatibility with other SAN-OS features [8-3](#)
 - configuring [8-2 to 8-11](#)
 - configuring AAA authentication [8-9](#)
 - default settings [8-13](#)
 - description [8-2](#)
 - displaying security information [8-10](#)
 - enabling [8-4](#)
 - group settings [8-6](#)
 - hash algorithms [8-5](#)
 - licensing [8-2](#)
 - passwords for local switches [8-7](#)
 - passwords for remote devices [8-8](#)
 - sample configuration [8-11 to 8-12](#)

Send documentation comments to mdsfeedback-doc@cisco.com

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 [6-16 to ??](#)

configuring [6-6 to 6-15](#)

default settings [6-39](#)

deleting from CAs [6-14](#)

description [6-1 to 6-5](#)

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 7-10](#)

maintaining [6-13](#)

maximum limits [6-38](#)

monitoring [6-13](#)

peers [6-5](#)

purpose [6-2](#)

requesting identity certificate example [6-24](#)

revocation example [6-30](#)

SSH support [5-20](#)

digital signature algorithm. See DSA key pairs

documentation

related documents [4-xxi](#)

DSA key-pairs

generating [5-16](#)

dsa key pairs

generating [5-16](#)

E

EFMD

fabric binding [10-1](#)

encrypted passwords

user accounts [5-13](#)

E ports

fabric binding checking [10-2](#)

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

F

fabric binding

activation [10-4](#)

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

clearing statistics [10-6](#)

compatibility with DHCHAP [8-3](#)

configuration [10-3 to 10-6](#)

default settings [10-9](#)

deleting database [10-6](#)

description [10-1 to 10-2](#)

EFMD [10-1](#)

enforcement [10-2](#)

forceful activation [10-5](#)

licensing requirements [10-1](#)

port security comparison [10-1](#)

saving configurations [10-5](#)

verifying configuration [10-6 to 10-9](#)

fabric security

authentication [8-1](#)

default settings [8-13](#)

FCIP

compatibility with DHCHAP [8-3](#)

sample IPsec configuration [7-34 to 7-38](#)

FC-SP

authentication [8-1](#)

enabling [8-4](#)

See also DHCHAP

Federal Information Processing Standards. See FIPS

Fibre Channel

sWWNs for fabric binding [10-4](#)

Fibre Channel Security Protocol. See FC-SP

FICON

fabric binding requirements [10-3](#)

sWWNs for fabric binding [10-4](#)

FIPS

Send documentation comments to mdsfeedback-doc@cisco.com

configuration guidelines [2-1](#)

self-tests [2-2](#)

G

global keys

assigning for RADIUS [3-23](#)

H

high availability

compatibility with DHCHAP [8-3](#)

host keys

assigning [3-21](#)

host names

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

I

ICMP packets

type value [4-4](#)

IDs

Cisco vendor ID [3-28](#)

IKE

algorithms for authentication [7-7](#)

default settings [6-39, 7-40](#)

description [7-3](#)

displaying configurations [7-29](#)

enabling [7-11](#)

initializing [7-10](#)

refreshing SAs [7-16](#)

terminology [7-5](#)

transforms for encryption [7-7](#)

IKE domains

clearing [7-16](#)

configuring [7-11](#)

description [7-11](#)

IKE initiators

configuring version [7-16](#)

displaying configuration [7-30](#)

IKE peers

configuring keepalive times [7-15](#)

displaying keepalive configuration [7-29](#)

IKE policies

configuring lifetime associations [7-15](#)

configuring negotiation parameters [7-13](#)

displaying current policies [7-30](#)

negotiation [7-11](#)

IKE tunnels

clearing [7-16](#)

description [7-11](#)

Internet Key Exchange. See IKE

IP domain names

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

IP filters

contents [4-2](#)

restricting IP traffic [4-1, 4-2](#)

IPsec

algorithms for authentication [7-6](#)

crypto IPv4-ACLs [7-16 to 7-21](#)

default settings [7-40](#)

description [7-2](#)

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

displaying configurations [7-30 to 7-34](#)

fabric setup requirements [7-5](#)

global lifetime values [7-28](#)

hardware compatibility [7-4](#)

licensing requirements [7-4](#)

maintenance [7-28](#)

prerequisites [7-4](#)

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

sample FCIP configuration [7-34 to 7-38](#)

sample iSCSI configuration [7-38 to 7-40](#)

terminology [7-5](#)

transform sets [7-21](#)

transforms for encryption [7-6](#)

unsupported features [7-5](#)

Send documentation comments to mdsfeedback-doc@cisco.com

IP security. See IPsec

IPv4-ACLs

- adding entries [4-7](#)
- applying to interfaces [4-10, 4-12](#)
- clearing counters [4-13](#)
- configuration guidelines [4-2](#)
- crypto [7-16 to 7-21](#)
- crypto map entries [7-23](#)
- defining filters [4-6](#)
- displaying configuration [4-8](#)
- operands [4-7](#)
- reading dump logs [4-9](#)
- removing entries [4-8](#)
- verifying interface configuration [4-12](#)

IPv6-ACLs

- defining [4-7](#)
- operands [4-7](#)

iSCSI

- sample IPsec configuration [7-38 to 7-40](#)

L

logins

- SSH [3-5](#)
- Telnet [3-5](#)

M

MD5 authentication

- IKE [7-7](#)
- 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 [3-50](#)

N

network administrators

- additional roles [3-3](#)
- permissions [3-3](#)

network operators

- permissions [3-3](#)

O

Online Certificate Status Protocol. See OSCP

OSCP

- support [6-5](#)

P

passwords

- DHCHAP [8-7, 8-8](#)
- encrypted [5-13](#)
- recovering (procedure) [5-23](#)
- strong characteristics [5-12](#)

persistent domain ID

- FICON VSANs [10-3](#)

PKI

- enrollment support [6-4](#)

PortChannels

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

port security

- activating [9-6](#)
- activation [9-3](#)
- activation rejection [9-6](#)
- adding authorized pairs [9-11](#)
- auto-learning [9-2](#)
- cleaning up databases [9-17](#)
- compatibility with DHCHAP [8-3](#)
- configuration guidelines [9-3](#)
- configuring CFS distribution [9-12 to 9-14](#)
- copying databases [9-16](#)
- database interactions [9-15](#)

Send documentation comments to mdsfeedback-doc@cisco.com

- database merge guidelines [9-14](#)
- data scenarios [9-15](#)
- deactivating [9-6](#)
- default settings [9-20](#)
- deleting databases [9-17](#)
- disabling [9-5](#)
- displaying configuration [9-18, 9-18 to 9-20](#)
- enabling [9-5](#)
- enforcement mechanisms [9-2](#)
- fabric binding comparison [10-1](#)
- forcing activation [9-6](#)
- license requirement [9-2](#)
- manual configuration guidelines [9-5](#)
- preventing unauthorized accesses [9-2](#)
- unauthorized accesses prevented [9-2](#)
- WWN identification [9-10](#)
- port security auto-learning
 - description [9-2](#)
 - device authorization [9-8](#)
 - disabling [9-8](#)
 - distributing configuration [9-13](#)
 - enabling [9-7](#)
 - guidelines for configuring with CFS [9-4](#)
 - guidelines for configuring without CFS [9-4](#)
- port security databases
 - cleaning up [9-17](#)
 - copying [9-16](#)
 - deleting [9-17](#)
 - displaying configuration [9-18 to 9-19](#)
 - displaying violations [9-20](#)
 - interactions [9-15](#)
 - manual configuration guidelines [9-5](#)
 - merge guidelines [9-14](#)
 - reactivating [9-7](#)
 - scenarios [9-15](#)
- preshared keys
 - RADIUS [3-23](#)
 - TACACS+ [3-32](#)
- profiles

- configuring [5-2](#)

- modifying [5-3](#)

Public Key Infrastructure. See PKI

R

RADIUS

- AAA protocols [3-1](#)

- assigning host keys [3-21](#)

- CFS merge guidelines [3-49](#)

- clearing configuration distribution sessions [3-48](#)

- configuring Cisco ACS [3-55 to 3-58](#)

- configuring server groups [3-43](#)

- configuring server monitoring parameters [3-25](#)

- configuring test idle timer [3-26](#)

- configuring test user name [3-27](#)

- default settings [3-59](#)

- description [3-21](#)

- discarding configuration distribution changes [3-48](#)

- displaying configured parameters [3-29](#)

- enabling configuration distribution [3-46](#)

- sending test messages for monitoring [3-27](#)

- setting preshared keys [3-23](#)

- specifying servers [3-21 to 3-23](#)

- specifying server timeout [3-24](#)

- starting a distribution session [3-46](#)

role databases

- clearing distribution sessions [5-7](#)

- committing changes to fabric [5-6](#)

- disabling distribution [5-7](#)

- discarding database changes [5-6](#)

- enabling distribution [5-7](#)

roles

- authentication [5-1](#)

- configuring [5-2](#)

- configuring rules [5-2](#)

- default permissions [3-3](#)

- default setting [5-25](#)

- displaying information [5-7](#)

Send documentation comments to mdsfeedback-doc@cisco.com

- distributing configurations [5-5 to 5-9](#)
- modifying profiles [5-3](#)
- user profiles [3-3](#)
- See also command roles
- roles database
 - displaying information [5-7](#)
- roles databases
 - description [5-6](#)
 - locking in the fabric [5-6](#)
 - merge guidelines [5-7](#)
- RSA key-pairs
 - deleting [6-15](#)
 - description [6-3](#)
 - displaying configuration [6-16](#)
 - exporting [6-5, 6-13](#)
 - generating [6-6](#)
 - importing [6-5, 6-13](#)
 - multiple [6-4](#)
- rsa key pairs
 - generating [5-16](#)
- rules
 - configuring [5-2](#)

S

- SAs
 - displaying for IKE [7-30](#)
 - displaying global lifetime values [7-34](#)
 - establishing between IPsec peers [7-23](#)
 - global lifetime values [7-29](#)
 - lifetime negotiations [7-25](#)
 - refreshing [7-16](#)
 - setting lifetime [7-25](#)
- Secure Hash Algorithm. See SHA-1
- security
 - accounting [3-4](#)
 - managing on the switch [3-2](#)
- security associations. See SAs
- security control

- local [3-2, 3-52](#)
- remote [3-2, 3-31](#)
- remote AAA servers [3-21](#)
- server groups
 - configuring [3-42](#)
- SHA-1
 - IKE [7-7](#)
 - IPsec [7-7](#)
- SNMP
 - creating roles [5-10](#)
 - mapping CLI operations [5-10](#)
 - security features [3-2](#)
- SNMPv3
 - specifying cisco-av-pair [3-29](#)
- SSH
 - clearing hosts [5-18](#)
 - default service [5-15](#)
 - description [5-16](#)
 - digital certificate authentication [5-20](#)
 - displaying status [5-19](#)
 - enabling [5-19](#)
 - generating server key-pairs [1-2, 5-16](#)
 - logins [3-5](#)
 - overwriting server key-pairs [5-17](#)
 - protocol status [5-19](#)
 - specifying keys [5-16](#)
- SSH key pairs
 - overwriting [5-17](#)
- switch security
 - default settings [3-58, 5-25](#)
- sWWNs
 - configuring for fabric binding [10-3](#)

T

- TACACS+
 - AAA protocols [3-1](#)
 - CFS merge guidelines [3-49](#)
 - clearing configuration distribution sessions [3-48](#)

Send documentation comments to mdsfeedback-doc@cisco.com

- configuring Cisco ACS [3-55 to 3-58](#)
- configuring server groups [3-44](#)
- default settings [3-59](#)
- description [3-31](#)
- discarding configuration distribution changes [3-48](#)
- displaying information [3-41](#)
- enabling [3-32](#)
- enabling configuration distribution [3-46](#)
- global keys [3-32](#)
- sending test messages for monitoring [3-38](#)
- setting default server timeout [3-34](#)
- setting global secret keys [3-34](#)
- setting preshared key [3-32](#)
- setting server addresses [3-32](#)
- setting server monitoring parameters [3-35](#)
- setting timeout value [3-34](#)
- specifying server at login [3-39](#)
- starting a distribution session [3-46](#)
- validating [3-39](#)
- TCP ports
 - IPv4-ACLs [4-4](#)
- Telnet
 - enabling [5-19](#)
 - logins [3-5](#)
- TE ports
 - fabric binding checking [10-2](#)
- transform sets
 - configuring for IPsec [7-22](#)
 - creating crypto map entries [7-24](#)
 - description [7-21](#)
- 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 [11-2](#)
 - Best Practices [11-9](#)
 - enabling [11-2](#)

- ESP Modes [11-6](#)
- ESP Settings [11-4](#)
- Information [11-7](#)
- Security Association Parameters [11-3](#)
- Security Associations [11-3](#)
- Supported Modules [11-2](#)
- Terminology [11-1](#)

U

- UDP ports
 - IPv4-ACLs [4-4](#)
- user accounts
 - configuring [5-11 to 5-15](#)
 - configuring profiles [5-2](#)
 - configuring roles [5-2](#)
 - displaying information [5-14](#)
 - password characteristics [5-12](#)
- user IDs
 - authentication [3-3](#)
- user profiles
 - role information [3-3](#)
- users
 - configuring [5-13](#)
 - deleting [5-13](#)
 - description [5-12](#)
 - displaying account information [5-14](#)
 - logging out other users [5-14](#)

V

- vendor-specific attributes. See VSAs
- VSAN policies
 - default roles [5-25](#)
 - licensing [5-4](#)
 - modifying [5-5](#)
- VSANs
 - compatibility with DHCHAP [8-3](#)

Send documentation comments to mdsfeedback-doc@cisco.com

configuring policies [5-4](#)

IP routing [4-1, 4-2](#)

policies [5-4](#)

VSAs

communicating attributes [3-28](#)

protocol options [3-28](#)

W

WWNs

port security [9-10](#)

Send documentation comments to mdsfeedback-doc@cisco.com