Send documentation comments to fm-docfeedback@cisco.com

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
  - default settings 4-30
  - description 4-1
  - DHCHAP authentication 8-10
  - distributing with CFS (procedure) 4-24
  - enabling server distribution 4-22
  - local services 4-26
  - remote services 4-4
  - service configuration options 4-4
  - setting authentication 4-26
  - starting a distribution session 4-23

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

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

administrator passwords
  - recovering 3-19

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 4-4
  - local 4-3
  - remote 4-3, 4-4
  - user IDs 4-3

authentication, authorization, and accounting. See AAA

C

CAs
  - authenticating 6-9
  - certificate download example 6-18
  - configuring 6-5 to 6-16
  - creating a trust point 6-7
  - 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
  - identity 6-2
  - maintaining 6-13
  - maximum limits 6-35
  - monitoring 6-13

Send documentation comments to fm-docfeedback@cisco.com

multiple 6-4
multiple trust points 6-3
peer certificates 6-4
purpose 6-2
certificate authorities. See CAs
certificate revocation lists. See CRLs
Cisco Access Control Server. See Cisco ACS
Cisco ACS
configuring for RADIUS 4-27 to 4-30
configuring for TACACS+ 4-27 to 4-30
cisco-av-pair
specifying for SNMPv3 4-13
Cisco vendor ID
description 4-13
common roles
deleting (procedure) 3-3
CRLs
configuring 6-15
configuring revocation checking methods 6-11
description 6-5
downloading example 6-33
generation example 6-32
importing example 6-35, ?? 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 7-6
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 6-16 to 6-18
configuring 6-5 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 6-11
importing 6-5, 6-14

Send documentation comments to fm-docfeedback@cisco.com

installing identity certificates 6-12
IPsec 7-7 to 7-10
maintaining 6-13
maximum limits 6-35
monitoring 6-13
peers 6-4
purpose 6-2
requesting identity certificate example 6-23
revocation example 6-29
digital signature algorithm. See DSA key pairs
documentation
related documents 4-xix
dsa key pairs
generating 3-15

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 4-8

H

high availability
compatibility with DHCHAP 8-3
host names
configuring for digital certificates 6-6

I

ICMP packets
type value 5-4
IDs
Cisco vendor ID 4-13
IKE
algorithms for authentication 7-6
default settings 6-36, 7-39

Send documentation comments to fm-docfeedback@cisco.com

description 7-3
initializing 7-13
refreshing SAs 7-20
terminology 7-5
transforms for encryption 7-6
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 5-2
restricting IP traffic 5-1
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 7-4
global lifetime values 7-37
hardware compatibility 7-4
licensing requirements 7-3
maintenance 7-37
prerequisites 7-3
RFC implementations 7-1
terminology 7-5
transform sets 7-25
transforms for encryption 7-6
unsupported features 7-4
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 4-4
Telnet 4-4

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 4-25

Send documentation comments to fm-docfeedback@cisco.com

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

persistent domain ID
- FICON VSANs 10-3

PKI
- enrollment support 6-3

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
- deactivating 9-9
- default settings 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 9-13
- 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 9-22
- interactions 9-20
- manual configuration guidelines 9-4
- merge guidelines 9-20
- reactivating 9-11
- scenarios 9-21

preshared keys
- RADIUS 4-8
- TACACS+ 4-15

Public Key Infrastructure. See PKI

R

RADIUS
- AAA protocols 4-1
- CFS merge guidelines 4-24
- clearing configuration distribution sessions 4-24
- configuring Cisco ACS 4-27 to 4-30

Send documentation comments to fm-docfeedback@cisco.com

configuring test idle timer 4-11
configuring test user name 4-11
default settings 4-31
description 4-7
discarding configuration distribution changes 4-24
enabling configuration distribution 4-22
setting preshared keys 4-8
specifying server at user login 4-12
specifying time-out 4-9
starting a distribution session 4-23
recovering passwords 3-19
roles
default permissions 4-3
deleting (procedure) 3-3
user profiles 4-3
rsa1 key pairs
generating 3-15
RSA key-pairs
deleting 6-16
description 6-2
exporting 6-5, 6-14
generating 6-6
importing 6-5, 6-14
multiple 6-4
rsa key pairs
generating 3-15

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 4-3
managing on the switch 4-1
security associations. See SAs
security control
local 4-2
remote 4-2, 4-14
remote AAA servers 4-7
server groups
configuring 4-20
SHA-1
IKE 7-7
IPsec 7-6
SNMP
security features 4-2
SNMPv3
specifying cisco-av-pair 4-13
SSH
default service 3-17
host key pair 3-15
logins 4-4
SSH key pair
overwriting 3-17
switch security
default settings 3-23, 4-30
sWWNs
configuring for fabric binding 10-3

T

TACACS+
AAA protocols 4-1
CFS merge guidelines 4-24
clearing configuration distribution sessions 4-24
configuring Cisco ACS 4-27 to 4-30
default settings 4-31
description 4-14
discarding configuration distribution changes 4-24
displaying server statistics 4-18
enabling configuration distribution 4-22
global keys 4-15
setting default server encryption 4-15
setting default server timeout 4-15

Send documentation comments to fm-docfeedback@cisco.com

setting preshared key 4-15
specifying server at login 4-18
starting a distribution session 4-23
validating 4-17
TCP ports
IPv4-ACLs 5-3
Telnet
default service 3-15
logins 4-4
TE ports
fabric binding checking 10-2
transform sets
description 7-25
Triple DES. See 3DEC encryption
trust points
creating 6-7
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 11-7
Security Association Parameters 11-3
Security Associations 11-3
Statistics 11-11
Supported Modules 11-2
Terminology 11-1

U

UDP ports
IPv4-ACLs 5-3
user IDs
authentication 4-3
user profiles
role information 4-3
users
deleting (procedure) 3-14

V

vendor-specific attributes. See VSAs
VSANs
compatibility with DHCHAP 8-3
IP routing 5-1
Rules and features 3-4
VSAs
communicating attributes 4-13
protocol options 4-13

W

WWNs
port security 9-16

Send documentation comments to fm-docfeedback@cisco.com