INDEX

Numerics

10BaseT cable pinouts
- appliance F-1

802.1q encapsulation for VLAN groups 1-15

A

access control list. See ACL.

accessing
- IPS software C-1
- service account E-5

access list misconfiguration E-26

actions
- ACL changes 1-2
- IP logs 1-3
- multiple packet drop 1-3
- TCP reset 1-2

adaptive security appliance
- ASA 5585-X IPS SSP 5-2
- models 5-2

alternate TCP reset interface
- configuration restrictions 1-11
- designating 1-9
- restrictions 1-5

Analysis Engine
- error messages E-23
- errors E-52
- IDM exits E-55
- sensing interfaces 1-6
- verify it is running E-20

anomaly detection disabling E-19

appliance
- cable pinouts (10BaseT) F-1
- cable pinouts(10BaseT) F-1

appliances
- ACLs 1-2
- described 1-18
- GRUB menu E-8
- initializing B-8
- logging in A-2
- managers 1-18
- models 1-18
- password recovery E-8
- preparing for installation 2-1
- restrictions 1-18
- SPAN 1-18
- TCP reset 1-2
- terminal servers
  - described 1-19, A-3, D-13
  - setting up 1-19, A-3, D-13
- time sources 1-20, E-15
- upgrading recovery partition D-6

application partition image recovery D-12

applying software updates E-52

ARC
- blocking not occurring for signature E-42
- device access issues E-39
- enabling SSH E-41
- inactive state E-37
- misconfigured master blocking sensor E-43
- troubleshooting E-36
- verifying device interfaces E-41
- verifying status E-36

ASA 5500-X IPS SSP
initializing B-13
logging in A-4
memory usage E-68
memory usage values (table) E-68
Normalizer engine E-67
password recovery E-10
resetting the password E-10
session command A-4
sessioning in A-4
setup command B-13
time soruces 1-20, E-16
ASA 5585-X
slide rail kit hardware installation 4-20
ASA 5585-X IPS SSP
adaptive security appliance 5-2
described 5-2
front panel indicators
described 5-7
illustration 5-6
initializing B-17
installing 5-10
installing system image D-22
interfaces 5-2, 5-3
introducing 5-2
logging in A-5
memory requirements 5-9
Normalizer engine E-74
password recovery E-12
reimaging D-21
removing 5-10, 5-14
requirements 5-4
resetting the password E-12
session command A-5
sessioning in A-5
setup command B-17
show module 1 command 5-13
slot 1 5-10
specifications 5-3
time sources 1-20, E-16
verifying status 5-14
ASA 5585-X SSP-10 with IPS SSP-10
described 5-2
memory requirements 5-9
ASA 5585-X SSP-20 with IPS SSP-20
described 5-3
memory requirements 5-9
ASA 5585-X SSP-40 with IPS SSP-40
described 5-3
memory requirements 5-9
ASA 5585-X SSP-60 with IPS SSP-60
described 5-3
memory requirements 5-9
ASA IPS modules
jumbo packet count E-68, E-75
ASDM resetting passwords E-11, E-13
asymmetric traffic and disabling anomaly detection E-18
attack responses for TCP resets 1-2
attempt limit
RADIUS E-21
authenticated NTP 1-20, E-15
automatic setup B-2
automatic upgrade
information required D-7
troubleshooting E-52
auto-upgrade-option command D-7

B

backing up
configuration E-3
current configuration E-4
back panel features
IPS 4345 3-7
IPS 4360 3-8
IPS 4510 4-6
IPS 4520 4-6
basic setup B-4

blocking not occurring for signature E-42
BST
described E-2
URL E-2
Bug Search Tool. See BST.

C

cable pinouts
RJ-45 to DB-9 F-3
cannot access sensor E-24
cidDump obtaining information E-101
circuit breaker warning 3-21
cisco
default password A-2
default username A-2
Cisco.com
accessing software C-1
downloading software C-1
software downloads C-1
Cisco ASA 5585-X
described 5-2
installing ASA 5585-X IPS SSP 5-14
models 5-2
removing ASA 5585-X IPS SSP 5-14
Cisco Bug Search Tool
described E-2
Cisco Security Intelligence Operations
described C-8
URL C-8
Cisco Services for IPS
service contract C-9
supported products C-9
clear events command 1-21, E-17, E-101
clearing
events E-101
statistics E-85
CLI password recovery E-14
command and control interface
described 1-5
Ethernet 1-2
list 1-5
commands
auto-upgrade-option D-7
clear events 1-21, E-17, E-101
copy backup-config E-3
copy current-config E-3
copy license-key C-11
downgrade D-11
erase license-key C-14
hw-module module slot_number password-reset E-12
setup B-1, B-4, B-8, B-13, B-17
show events E-98
show health E-76
show module 1 details E-59, E-71
show settings E-14
show statistics E-84
show statistics virtual-sensor E-23, E-84
show tech-support E-77
show version E-81
sw-module module slot_number password-reset E-10
upgrade D-4, D-6
configuration files
backing up E-3
merging E-3
configuration restrictions
alternate TCP reset interface 1-11
inline interface pairs 1-10
inline VLAN pairs 1-10
interfaces 1-10
physical interfaces 1-10
VLAN groups 1-11
configuring
automatic upgrades D-9
upgrades D-5
connecting SFP/SFP+ modules 5-13
copy backup-config command E-3
copy current-config command E-3

copy license-key command C-11
correcting time on the sensor 1-21, E-17
creating the service account E-6
cryptographic account
  Encryption Software Export Distribution Authorization from C-2
  obtaining C-2
current configuration back up E-3

D

DC power supply
  connecting (IPS 4360) 3-23
debug logging enable E-44
defaults
  password A-2
  username A-2
device access issues E-39
disabling
  anomaly detection E-19
  password recovery E-14
disaster recovery E-6
displaying
  events E-99
  health status E-76
  password recovery setting E-14
  statistics E-85
  tech support information E-78
  version E-81
downgrade command D-11
downgrading sensors D-11
downloading Cisco software C-1
duplicate IP addresses E-27

E

electrical safety guidelines 2-3
enabling debug logging E-44
Encryption Software Export Distribution Authorization form
  cryptographic account C-2
  described C-2
erase license-key command C-14
errors (Analysis Engine) E-52
ESD environment working in 2-4
events
  clearing E-101
  displaying E-99
  types E-97
Event Store
  clearing E-101
  clearing events 1-21, E-17
  no alerts E-31
  time stamp 1-21, E-17
examples
  ASA failover configuration E-59, E-70
  SPAN configuration for IPv6 support 1-13
  System Configuration Dialog B-2
external product interfaces
  issues E-21
  troubleshooting E-22

F

false positives
  filtering 1-4
  tuning IPS 1-3
files Cisco IPS (list) C-1
front panel features
  IPS 4510 4-3
  IPS 4520 4-3
front panel indicators
  ASA 5585-X IPS SSP 5-6
  IPS 4345 3-6
  IPS 4360 3-6
FTP servers and software updates D-3

G

global correlation
- license B-5
- troubleshooting E-19

GRUB menu password recovery E-8

guidelines
- electrical safety 2-3
- power supplies 2-6

H

health status display E-76

HTTP/HTTPS servers supported D-3

hw-module module slot_number password-reset command E-12

I

IDM
- Analysis Engine is busy E-55
- described 4-2, 5-2
- web browsers 4-2, 5-2
- will not load E-54

IME
- 10 devices 4-3, 5-2
- described 4-3, 5-2
- password recovery E-14
- time synchronization problems E-57

initializing
- appliances B-8
- ASA 5500-X IPS SSP B-13
- ASA 5585-X IPS SSP B-17
- sensors B-1, B-4
- user roles B-1
- verifying B-21

inline interface pair mode
- configuration restrictions 1-10
- described 1-13
- illustration 1-14

inline mode
- interface cards 1-6
- pairing interfaces 1-6

inline VLAN pair mode
- configuration restrictions 1-10
- described 1-14
- illustration 1-15
- supported sensors 1-14

installation preparation 2-1

installer major version C-5

installer minor version C-5

installing
- DC power supply (IPS 4360) 3-26
- IPS 4345 3-12
- IPS 4360 3-12
- IPS 4510 4-11
- IPS 4520 4-11
- license key C-12
- sensor license C-10
- SFP/SFP+ modules 5-13
- system image
  - ASA 5500-X IPS SSP D-20
  - ASA 5585-X IPS SSP D-22
  - IPS 4345 D-14
  - IPS 4360 D-14
  - IPS 4510 D-18
  - IPS 4520 D-18

interfaces
- alternate TCP reset 1-5
- command and control 1-5
- configuration restrictions 1-10
- described 1-4
- port numbers 1-4
- sensing 1-5, 1-6
- slot numbers 1-4
- support (table) 1-6
- TCP reset 1-9

introducing
ASA 5585-X IPS SSP 5-2
IPS 4345 3-2
IPS 4360 3-2
IPS 4510 4-2
IPS 4520 4-2
IPS appliances 1-18
Intrusion Prevention System Device Manager. See IDM. 4-2, 5-2
Intrusion Prevention System Manager Express. See IME. 5-2
Intrusion Prevention System Manager Express. See IME. 4-3
IPS
restrictions 1-18
supported
appliances 1-16
modules 1-16
tuning 1-3
IPS 4345
AC power supply (V01) 3-15
back panel features 3-7
back panel features (illustration) 3-7
described 3-2
front panel (llustration) 3-5
front panel indicators described 3-6
indicators 3-6
installation 3-12
installing system image D-14
packing box contents 3-4
password recovery E-8, E-9
power supplies 3-16
power supplies (illustration) 3-17
power supply indicator 3-17
rack mounting 3-10
reimaging D-14
specifications 3-2
V01 power supply limitations 3-15
IPS 4360
AC power supply
installing 3-19
removing 3-19
AC power supply (V02) 3-15
back panel features 3-8
back panel features (illustration) 3-8
connecting DC power supplies 3-23
described 3-2
front panel (illustration) 3-5
front panel indicators described 3-6
indicators 3-6
installation 3-12
installing DC power supplies 3-26
installing system image D-14
packing box contents 3-4
password recovery E-8, E-9
power supplies 3-16
power supplies(illustration) 3-17
power supply indicator 3-17
reimaging D-14
removing DC power supplies 3-26
specifications 3-2
V01 power supply limitations 3-15
IPS 4510
back panel features 4-6
back panel features (illustration) 4-6
cable management brackets
described 4-33
installing 4-33
chassis features 4-3
connecting cables 4-11
described 4-2
Ethernet port indicators 4-7
fan modules
hot-pluggable 4-18
installing 4-19
OIR 4-18
removing 4-19

front panel indicators
described 4-5
illustration 4-4
front panel view 4-3
installing
core IPS SSP 4-14
SFP/SFP+ modules 4-12
slide rail kit hardware 4-20
installing system image D-18
Management 0/0 4-11
management port described 4-11
memory requirements 4-10
OIR
fan supply modules 4-2
not supported 4-2
power supply modules 4-2
SFP/SFP+ 4-2
packing box contents 4-9
password recovery E-8, E-9
power module indicators
described 4-7
illustration 4-6
power supply modules
installing 4-17
removing 4-17
requirements 4-10
rack mounting 4-30
reimaging D-18
removing core IPS SSP 4-14
SFP ports 4-12
slide rail kit hardware installation 4-20
specifications 4-8
supported SFP+ modules 4-11, 5-10
supported SFP modules 4-11, 5-10
SwitchApp 4-35
IPS 4520
back panel features 4-6
back panel features (illustration) 4-6
cable management brackets
described 4-33
installing 4-33
chassis features 4-3
connecting cables 4-11
described 4-2
Ethernet port indicators 4-7
fan modules
hot-pluggable 4-18
installing 4-19
OIR 4-18
removing 4-19
front panel indicators
described 4-5
illustration 4-4
front panel view 4-3
installing
core IPS SSP 4-14
SFP/SFP+ modules 4-12
slide rail kit hardware 4-20
installing system image D-18
Management 0/0 4-11
management port described 4-11
memory requirements 4-10
OIR
fan supply modules 4-2
not supported 4-2
power supply modules 4-2
SFP/SFP+ 4-2
packing box contents 4-9
password recovery E-8, E-9
power module indicators
described 4-7
illustration 4-6
power supply modules
installing 4-17
removing 4-17
requirements 4-10
rack mounting 4-30

reimaging D-18
removing core IPS SSP 4-14
SFP ports 4-12
slide rail kit hardware installation 4-20
specifications 4-8
supported SFP+ modules 4-11, 5-10
supported SFP modules 4-11, 5-10
SwitchApp 4-35
two power supply modules 4-16, 4-18
IPS software
available files C-1
obtaining C-1
IPS software file names
major updates (illustration) C-4
minor updates (illustration) C-4
patch releases (illustration) C-4
service packs (illustration) C-4
IPS SSP-10 front panel features (illustration) 5-4
IPS SSP-20 front panel features (illustration) 5-4
IPS SSP-40 front panel features (illustration) 5-5
IPS SSP-60 front panel features (illustration) 5-5
IPS SSP in the ASA 5585-X 5-2
IPS SSPs (core)
slot 0 4-14
IPv6
SPAN ports 1-13
switches 1-13

L

license key
installing C-12
obtaining C-9
trial C-9
uninstalling C-14
viewing status of C-9
licensing
described C-9
IPS device serial number C-9
Licensing pane
configuring C-10
described C-9
logging in
appliances A-2
ASA 5500-X IPS SSP A-4
ASA 5585-X IPS SSP A-5
sensors
SSH A-6
Telnet A-6
service role A-1
terminal servers 1-19, A-3, D-13
user role A-1
loose connections on sensors 4-34, E-23

M

major updates described C-3
Management 0/0 port described 4-11
Management 0/1 described 4-11
manual block to bogus host E-41
master blocking sensor
not set up properly E-43
verifying configuration E-43
merging configuration files E-3
MIBs supported E-18
minor updates described C-3
modes
IDS 1-1
inline interface pair 1-13
inline VLAN pair 1-14
IPS 1-1
promiscuous 1-12
VLAN groups 1-15
modules
ASA 5585-X IPS SSP 5-2

N

NTP
- authenticated 1-20, E-15
- described 1-20, E-15
- incorrect configuration 1-20, E-16
- time synchronization 1-20, E-15
- unauthenticated 1-20, E-15
- verifying configuration 1-21

O

obtaining
- cryptographic account C-2
- IPS software C-1
- license key C-9
- sensor license C-10

OIR
- not supported for modules 4-2
- supported
  - fan modules 4-2
  - power supply modules 4-2
  - SFP/SFP+ 4-2

online insertion and removal. See OIR. 5-2

P

password recovery
- appliances E-8
- ASA 5500-X IPS SSP E-10
- ASA 5585-X IPS SSP E-12
- CLI E-14
- described E-8
- disabling E-14
- displaying setting E-14
- GRUB menu E-8
- IME E-14
- IPS 4345 E-8, E-9
- IPS 4360 E-8, E-9
- IPS 4510 E-8, E-9
- IPS 4520 E-8, E-9
- platforms E-8
- ROMMON E-9
- troubleshooting E-15
- verifying E-14

patch releases described C-3

physical connectivity issues E-30

physical interfaces configuration restrictions 1-10

ports
- Management 0/0 4-11
- Management 0/1 4-11
- SFP 4-12
- SFP/SFP+ 5-13

power supplies
- described (IPS 4345) 3-16
- describes (IPS 4360) 3-16
- illustration (IPS 4345) 3-17
- illustration (IPS 4560) 3-17

power supply guidelines 2-6

power supply indicator
- IPS 4345 3-17
- IPS 4360 3-17

power supply indicators
- IPS 4510 4-6
- IPS 4520 4-6

power supply modules
- hot-pluggable 4-16
- installing (IPS 4510) 4-17
- installing (IPS 4520) 4-17
- OIR 4-16
- redundant configuration 4-16
- removing (IPS 4510) 4-17
- removing (IPS 4520) 4-17

preparing for appliance installation 2-1

promiscuous mode
- atomic attacks 1-12
- described 1-12
- illustration 1-12

packet flow 1-12
SPAN ports 1-13
TCP reset interfaces 1-9
VACL capture 1-13

R

rack mounting
IPX 4345 3-10
rack-mounting
IPS 4510 4-30
IPS 4520 4-30
RADIUS
attempt limit E-21
recover command D-11
recovering the application partition image D-12
recovery partition upgrade D-6
reimaging
ASA 5500-X IPS SSP D-20
ASA 5585-X IPS SSP D-21
described D-2
IPS 4345 D-14
IPS 4360 D-14
IPS 4510 D-18
IPS 4520 D-18
sensors D-2, D-11
removing
ASA 5585-X IPS SSP 5-14
DC power supply (IPS 4360) 3-26
last applied
service pack D-11
signature update D-11
requirements
ASA 5585-X IPS SSP 5-4
reset not occurring for a signature E-50
resetting
passwords
ASDM E-11, E-13
hw-module command E-12
sw-module command E-10
resetting the password
ASA 5500-X IPS SSP E-10
ASA 5585-X IPS SSP E-12
restoring the current configuration E-5
RJ-45 to DB-9 cable pinouts F-3
ROMMON
ASA 5585-X IPS SSP D-24
described D-13
IPS 4345 D-14, E-9
IPS 4360 D-14, E-9
IPS 4510 D-18, E-9
IPS 4520 D-18, E-9
password recovery E-9
remote sensors D-13
serial console port D-13
TFTP D-13
round-trip time. See RTT.
RTT
described D-13
TFTP limitation D-13

S

scheduling automatic upgrades D-9
security
information on Cisco Security Intelligence Operations C-8
sensing interfaces
Analysis Engine 1-6
described 1-6
interface cards 1-6
modes 1-6
sensor license
installing C-10
obtaining C-10
sensors
access problems E-24
application partition image D-12

asymmetric traffic and disabling anomaly detection E-18
capturing traffic 1-1
command and control interfaces (list) 1-5
comprehensive deployment 1-1
Comprehensive Deployment Solutions (illustration) 1-1
corrupted SensorApp configuration E-35
disaster recovery E-6
downgrading D-11
electrical guidelines 2-3
IDS mode 1-1
incorrect NTP configuration 1-20, E-16
initializing B-1, B-4
interface support 1-6
IP address conflicts E-27
IPS mode 1-1
IPS tuning tips 1-3
logging in
  SSH A-6
  Telnet A-6
loose connections 4-34, E-23
misconfigured access lists E-26
models 1-16
network topology 1-3
no alerts E-31, E-57
not seeing packets E-33
NTP time synchronization 1-20, E-15
physical connectivity E-30
power supply guidelines 2-6
preventive maintenance E-2
reimaging D-2
sensing process not running E-28
setup command B-1, B-4, B-8
site guidelines 2-5
supported 1-16
TCP reset 1-2
time sources 1-20, E-15
troubleshooting software upgrades E-53
  upgrading D-5
service account
  accessing E-5
  cautions E-5
  creating E-6
  described E-5
service packs described C-3
service role A-1
session command
  ASA 5500-X IPS SSP A-4
  ASA 5585-X IPS SSP A-5
sessioning in
  ASA 5500-X IPS SSP A-4
  ASA 5585-X IPS SSP A-5
setting up terminal servers 1-19, A-3, D-13
setup
  automatic B-2
  command B-1, B-4, B-8, B-13, B-17
  simplified mode B-2
SFP+ modules
  described 4-10, 5-9
  supported (table) 4-11, 5-10
SFP+ modules described 5-4
SFP/SFP+ port (illustration) 5-13
SFP modules
  described 4-10, 5-4, 5-9
  supported (table) 4-11, 5-10
SFP port (illustration) 4-12
show events command E-97, E-98
show health command E-76
show interfaces command E-96
show module 1 details command E-59, E-71
show settings command E-14
show statistics command E-84
show statistics virtual-sensor command E-23, E-84
show tech-support command E-77
show version command E-81
signature engine update files described C-5

signatures
TCP reset E-50
update files C-4
site guidelines for sensor installation 2-5
SNMP supported MIBs E-18
software downloads Cisco.com C-1
software file names
recovery (illustration) C-5
signature/virus updates (illustration) C-4
signature engine updates (illustration) C-5
system image (illustration) C-5
software release examples
platform identifiers C-7
platform-independent C-6
software updates
supported FTP servers D-3
supported HTTP/HTTPS servers D-3
SPAN
appliances 1-18
port issues E-30
specifications
IPS 4345 3-2
IPS 4360 3-2
IPS 4510 4-8
IPS 4520 4-8
SSP-10
components 5-2
described 5-2
SSP-20
components 5-3
described 5-3
SSP-40
components 5-3
described 5-3
SSP-60
components 5-3
described 5-3
SSP in slot 2 5-10
statistic display E-85
subinterface 0 described 1-15
supported
FTP servers D-3
HTTP/HTTPS servers D-3
SwitchApp described 4-35
Switched Port Analyzer. See SPAN.
switches and TCP reset interfaces 1-9
sw-module module slot_number password-reset command E-10
System Configuration Dialog
described B-2
example B-2
system images
installing
ASA 5500-X IPS SSP D-20
ASA 5585-X IPS SSP D-21
IPS 4345 D-14
IPS 4360 D-14
IPS 4510 D-18
IPS 4520 D-18

T

TAC
service account E-5
show tech-support command E-77
TCP reset interfaces
conditions 1-9
described 1-9
list 1-9
promiscuous mode 1-9
switches 1-9
TCP resets
not occurring E-50
signature actions 1-2
tech support information display E-78
terminal server setup 1-19, A-3, D-13

TFTP servers
recommended
UNIX D-13
Windows D-13
RTT D-13
time
correction on the sensor 1-21, E-17
sensors 1-20, E-15
time sources
appliances 1-20, E-15
ASA 5500-X IPS SSP 1-20, E-16
ASA 5585-X IPS SSP 1-20, E-16
trial license key C-9
troubleshooting E-1
Analysis Engine busy E-55
applying software updates E-52
ARC
blocking not occurring for signature E-42
device access issues E-39
enabling SSH E-41
inactive state E-37
misconfigured master blocking sensor E-43
verifying device interfaces E-41
ASA 5500-X IPS SSP
commands E-59
failover scenarios E-58
ASA 5585-X IPS SSP
commands E-71
failover scenarios E-70
traffic flow stopped E-71
automatic updates E-52
cannot access sensor E-24
cidDump E-101
cidLog messages to syslog E-49
communication E-24
corrupted SensorApp configuration E-35
debug logger zone names (table) E-48
debug logging E-44
disaster recovery E-6
duplicate sensor IP addresses E-27
enabling debug logging E-44
external product interfaces E-22
gathering information E-76
global correlation E-19
IDM
cannot access sensor E-56
will not load E-54
IME time synchronization E-57
IPS clock time drift 1-20, E-16
manual block to bogus host E-41
misconfigured access list E-26
no alerts E-31, E-57
NTP E-50
password recovery E-15
physical connectivity issues E-30
preventive maintenance E-2
RADIUS
attempt limit E-21
reset not occurring for a signature E-50
sensing process not running E-28
sensor events E-97
sensor loose connections 4-34, E-23
sensor not seeing packets E-33
sensor software upgrade E-53
service account E-5
show events command E-97
show interfaces command E-96
show statistics command E-84
show tech-support command E-77, E-78
show version command E-81
software upgrades E-51
SPAN
port issue E-30
upgrading E-52
verifying Analysis Engine is running E-20
verifying ARC status E-36
tuning
IPS 1-3

tips 1-3

U

unassigned VLAN groups described 1-15
unauthenticated NTP 1-20, E-15
uninstalling the license key C-14
upgrade command D-4, D-6
upgrade notes and caveatsu(pgrading IPS software) D-1
upgrading
  application partition D-11
  latest version E-52
  recovery partition D-6
  sensors D-5
upgrading IPS software (upgrade notes and caveats) D-1
URLs for Cisco Security Intelligence Operations C-8
using
  debug logging E-44
  TCP reset interfaces 1-9

V

verifying
  ASA 5585-X IPS SSP installation 5-14
  NTP configuration 1-21
  password recovery E-14
  sensor initialization B-21
  sensor setup B-21
version display E-81
viewing
  license key status C-9
virtualization
  advantages E-17
  restrictions E-17
  supported sensors E-18
  traffic capture requirements E-18
VLAN groups
  802.1q encapsulation 1-15
  configuration restrictions 1-11
  deploying 1-16
  described 1-15
  switches 1-16

W

warning
  circuit breaker 3-21
  exposed DC wire 3-23