



Numerics

802.1q encapsulation for VLAN groups [5-14](#)

A

AAA RADIUS

functionality [4-19](#)

limitations [4-19](#)

accessing

IPS software [21-2](#)

service account [4-18, C-5](#)

access list misconfiguration [C-26](#)

access lists

necessary hosts [3-4](#)

Startup Wizard [3-4](#)

account locking

configuring [4-25](#)

security [4-25](#)

account unlocking configuring [4-26](#)

ACLs

adding [3-6](#)

described [13-2](#)

Post-Block [13-17](#)

Pre-Block [13-17](#)

Active Host Blocks pane

field descriptions [14-3](#)

user roles [14-3](#)

ad0 pane

default [10-10](#)

described [10-10](#)

tabs [10-10](#)

Add ACL Entry dialog box field descriptions [3-4](#)

Add Active Host Block dialog box field descriptions [14-4](#)

Add Allowed Host dialog box

field descriptions [4-6](#)

user roles [4-5](#)

Add Authorized RSA1 Key dialog box

field descriptions [12-5](#)

user roles [12-4](#)

Add Authorized RSA Key dialog box

field descriptions [12-3](#)

user roles [12-2](#)

Add Blocking Device dialog box

field descriptions [13-14](#)

user roles [13-13](#)

Add Cat 6K Blocking Device Interface dialog box

field descriptions [13-22](#)

user roles [13-20](#)

Add Configured OS Map dialog box

field descriptions [6-31, 9-27](#)

user roles [6-30, 9-24](#)

Add Destination Port dialog box field descriptions [10-16](#)

Add Device Login Profile dialog box

field descriptions [13-12](#)

user roles [13-11](#)

Add Event Action Filter dialog box

field descriptions [6-20, 9-16](#)

user roles [6-19, 9-15](#)

Add Event Action Override dialog box

field descriptions [6-11, 9-14](#)

user roles [6-11, 9-13](#)

Add Event Variable dialog box

field descriptions [6-34, 9-30](#)

user roles [9-29](#)

- Add External Product Interface dialog box
 - field descriptions [16-6](#)
 - user roles [16-4](#)
- Add Histogram dialog box field descriptions [10-17](#)
- adding
 - ACLs [3-6](#)
 - a host never to be blocked [13-10](#)
 - anomaly detection policies [10-9](#)
 - blocking devices [13-15](#)
 - CSA MC interfaces [16-7](#)
 - dashboards [2-1](#)
 - denied attackers [14-2](#)
 - event action filters [6-21, 9-18](#)
 - event action overrides [9-14](#)
 - event action rules policies [9-12](#)
 - event variables [6-35, 9-31](#)
 - external product interfaces [16-7](#)
 - gadgets [2-1](#)
 - host blocks [14-4](#)
 - IPv4 target value ratings [6-24, 9-21](#)
 - IPv6 target value ratings [6-27, 9-23](#)
 - network blocks [14-7](#)
 - OS maps [6-31, 9-28](#)
 - rate limiting devices [13-15](#)
 - rate limits [14-9](#)
 - risk categories [6-37, 9-33](#)
 - signature definition policies [7-2](#)
 - signatures [7-13](#)
 - signature variables [7-33](#)
 - virtual sensors [3-14, 6-11](#)
 - virtual sensors (ASA 5500-X IPS SSP) [6-15](#)
 - virtual sensors (ASA 5585-X IPS SSP) [6-15](#)
- Add Inline VLAN Pair dialog box field descriptions [3-11, 5-21](#)
- Add Interface Pair dialog box field descriptions [5-19](#)
- Add IP Logging dialog box field descriptions [14-11](#)
- Add Known Host RSA1 Key dialog box
 - field descriptions [12-9](#)
 - user roles [12-8](#)
- Add Known Host RSA Key dialog box
 - field descriptions [12-7](#)
 - user roles [12-6](#)
- Add Master Blocking Sensor dialog box
 - field descriptions [13-24](#)
 - user roles [13-23](#)
- Add Network Block dialog box field descriptions [14-6](#)
- Add Never Block Address dialog box
 - field descriptions [13-10](#)
 - user roles [13-7](#)
- Add Policy dialog box field descriptions [7-2, 9-12, 10-9](#)
- Add Posture ACL dialog box field descriptions [16-7](#)
- Add Protocol Number dialog box field descriptions [10-18, 10-25](#)
- Add Rate Limit dialog box
 - field descriptions [14-8](#)
 - user role [14-7](#)
- Address Resolution Protocol. See ARP.
- Add Risk Level dialog box field descriptions [6-37, 9-33](#)
- Add Router Blocking Device Interface dialog box
 - field descriptions [13-19](#)
 - user roles [13-16](#)
- Add Signature dialog box field descriptions [7-7](#)
- Add Signature Variable dialog box
 - field descriptions [7-33](#)
 - user roles [7-32](#)
- Add SNMP Trap Destination dialog box field descriptions [15-8](#)
- Add SNMPv3 User dialog box
 - field descriptions [15-4](#)
- Add SNMPv3 user dialog box
 - user roles [15-3](#)
- Add Target Value Rating dialog box field descriptions [9-23](#)
- Add Trusted Host dialog box
 - field descriptions [12-13](#)
 - user roles [12-12](#)
- Add User dialog box
 - field descriptions [4-22](#)
 - user roles [4-19, 4-22](#)

- Add Virtual Sensor dialog box
 - described [3-14, 6-9](#)
 - field descriptions [3-14, 6-9](#)
- Add VLAN Group dialog box field descriptions [5-23](#)
- Advanced Alert Behavior Wizard
 - Alert Dynamic Response Fire All window field descriptions [8-27](#)
 - Alert Dynamic Response Fire Once window field descriptions [8-28](#)
 - Alert Dynamic Response Summary window field descriptions [8-28](#)
 - Alert Summarization window field descriptions [8-27](#)
 - Event Count and Interval window field descriptions [8-26](#)
 - Global Summarization window field descriptions [8-29](#)
- aggregation
 - alert frequency [6-6, 9-5](#)
 - operating modes [6-6, 9-5](#)
- AIC
 - policy [7-44](#)
 - signatures (example) [7-44](#)
- AIC engine
 - AIC FTP [B-11](#)
 - AIC FTP engine parameters (table) [B-12](#)
 - AIC HTTP [B-11](#)
 - AIC HTTP engine parameters (table) [B-11](#)
 - described [B-11](#)
 - features [B-11](#)
 - signature categories [7-36](#)
- AIC policy enforcement
 - default configuration [7-37, B-11](#)
 - described [7-37, B-10](#)
 - sensor oversubscription [7-37, B-11](#)
- Alarm Channel
 - described [9-6, A-26](#)
 - risk rating [11-5](#)
- alert and log actions (list) [9-8](#)
- alert behavior
 - Custom Signature Wizard [8-26](#)
 - normal [8-26](#)
- alert frequency
 - aggregation [7-19](#)
 - configuring [7-19](#)
 - controlling [7-19](#)
 - modes [B-6](#)
- allocate-ips command [6-14](#)
- Allowed Hosts/Networks pane
 - configuring [4-6](#)
 - described [4-6](#)
 - field descriptions [4-6](#)
- alternate TCP reset interface
 - configuration restrictions [5-9](#)
 - designating [5-7](#)
 - restrictions [5-2](#)
- Analysis Engine
 - described [6-2](#)
 - error messages [C-23](#)
 - errors [C-52](#)
 - IDM exits [C-55](#)
 - sensing interfaces [5-3](#)
 - verify it is running [C-19](#)
 - virtual sensors [6-2](#)
- anomaly detection
 - asymmetric traffic [10-2](#)
 - caution [10-2](#)
 - configuration sequence [10-5](#)
 - default anomaly detection configuration [10-4](#)
 - default configuration (example) [10-4](#)
 - described [10-2](#)
 - detect mode [10-4](#)
 - disabling [10-34](#)
 - enabling [10-4](#)
 - event actions [10-7, B-71](#)
 - inactive mode [10-4](#)
 - learning accept mode [10-3](#)
 - learning process [10-3](#)
 - limiting false positives [10-13, 18-8](#)
 - operation settings [10-11](#)

- protocols [10-3](#)
- signatures (table) [10-7, B-72](#)
- signatures described [10-6](#)
- worms
 - attacks [10-13, 18-8](#)
 - described [10-3](#)
 - zones [10-5](#)
- anomaly detection disabling [C-18](#)
- Anomaly Detection pane
 - button functions [18-9](#)
 - described [18-7](#)
 - field descriptions [18-9](#)
 - user roles [18-7](#)
- anomaly detection policies
 - ad0 [10-9](#)
 - adding [10-9](#)
 - cloning [10-9](#)
 - default policy [10-9](#)
 - deleting [10-9](#)
- Anomaly Detections pane
 - described [10-9](#)
 - field descriptions [10-9](#)
 - user roles [10-9](#)
- appliances
 - GRUB menu [17-5, C-8](#)
 - initializing [20-8](#)
 - logging in [19-2](#)
 - password recovery [17-5, C-8, C-9](#)
 - setting system clock [4-16](#)
 - terminal servers
 - described [19-3, 22-16](#)
 - setting up [19-3, 22-16](#)
 - time sources [4-8, C-15](#)
 - upgrading recovery partition [22-7](#)
- Application Inspection and Control see AIC
- application partition
 - described [A-4](#)
 - image recovery [22-14](#)
- application policy enforcement described [7-37, B-10](#)
- applications in XML format [A-4](#)
- applying signature threat profiles [3-17](#)
- applying software updates [C-52](#)
- ARC
 - ACLs [13-17, A-14](#)
 - authentication [A-15](#)
 - blocking
 - connection-based [A-17](#)
 - response [A-13](#)
 - unconditional blocking [A-17](#)
 - blocking application [13-1](#)
 - blocking not occurring for signature [C-41](#)
 - Catalyst switches
 - VACL commands [A-19](#)
 - VACLs [A-16, A-19](#)
 - VLANs [A-16](#)
 - checking status [13-3, 13-4](#)
 - described [A-4](#)
 - design [13-2](#)
 - device access issues [C-39](#)
 - enabling SSH [C-41](#)
 - features [A-14](#)
 - firewalls
 - AAA [A-18](#)
 - connection blocking [A-18](#)
 - NAT [A-18](#)
 - network blocking [A-18](#)
 - postblock ACL [A-16](#)
 - preblock ACL [A-16](#)
 - shun command [A-18](#)
 - TACACS+ [A-18](#)
 - formerly Network Access Controller [13-1](#)
 - functions [13-1](#)
 - illustration [A-13](#)
 - inactive state [C-37](#)
 - interfaces [A-14](#)
 - maintaining states [A-16](#)
 - managed devices [13-7](#)
 - master blocking sensors [A-14](#)

- maximum blocks [13-2](#)
 - misconfigured master blocking sensor [C-42](#)
 - nac.shun.txt file [A-16](#)
 - NAT addressing [A-15](#)
 - number of blocks [A-15](#)
 - postblock ACL [A-16](#)
 - preblock ACL [A-16](#)
 - prerequisites [13-5](#)
 - rate limiting [13-3](#)
 - responsibilities [A-13](#)
 - single point of control [A-15](#)
 - SSH [A-14](#)
 - supported devices [13-5, A-15](#)
 - Telnet [A-14](#)
 - troubleshooting [C-35](#)
 - VACLs [A-14](#)
 - verifying device interfaces [C-40](#)
 - verifying status [C-36](#)
- ARP
- Layer 2 signatures [B-13](#)
 - protocol [B-13](#)
- ARP spoof tools
- dsniff [B-13](#)
 - ettercap [B-13](#)
- ASA 5500-X IPS SSP
- assigning virtual sensors [6-16](#)
 - creating virtual sensors [6-15](#)
 - initializing [20-13](#)
 - IPS reloading messages [C-67, C-73](#)
 - logging in [19-4](#)
 - memory usage [17-16, C-66](#)
 - memory usage values (table) [17-17, C-67](#)
 - no CDP mode support [5-27](#)
 - Normalizer engine [B-39, C-65](#)
 - password recovery [17-6, C-10](#)
 - resetting the password [17-6, C-10](#)
 - sensing interface [6-14](#)
 - session command [19-4](#)
 - sessioning in [19-4](#)
 - setup command [20-13](#)
 - time sources [4-8, C-15](#)
 - virtual sensors
 - assigning policies [6-14](#)
 - assigning the interface [6-14](#)
 - virtual sensor sequence [6-14](#)
- ASA 5585-X IPS SSP
- assigning virtual sensors [6-16](#)
 - creating virtual sensors [6-15](#)
 - initializing [20-17](#)
 - installing system image [22-25](#)
 - IPS reloading messages [C-67, C-73](#)
 - logging in [19-5](#)
 - no CDP mode support [5-27](#)
 - Normalizer engine [B-39, C-72](#)
 - password recovery [17-8, C-11](#)
 - resetting the password [17-8, C-12](#)
 - sensing interface [6-14](#)
 - session command [19-5](#)
 - sessioning in [19-5](#)
 - setup command [20-17](#)
 - time sources [4-8, C-15](#)
 - virtual sensors
 - assigning policies [6-14](#)
 - assigning the interface [6-14](#)
 - sequence [6-14](#)
- ASA IPS modules
- Deny Connection Inline [7-12, 9-10](#)
 - Deny Packet Inline [7-12, 9-10](#)
 - jumbo packet count [C-67, C-73](#)
 - Reset TCP Connection [7-12, 9-10](#)
 - TCP reset packets [7-12, 9-10](#)
- ASDM
- resetting passwords [17-7, 17-9, C-11, C-13](#)
- assigning
- interfaces to virtual sensors (ASA 5500-X IPS SSP) [6-14](#)
 - interfaces to virtual sensors (ASA 5585-X IPS SSP) [6-14](#)

- policies to virtual sensors (ASA 5500-X IPS SSP) [6-14](#)
 - policies to virtual sensors (ASA 5585-X IPS SSP) [6-14](#)
- assigning actions to signatures [7-17](#)
- asymmetric mode
 - described [6-4](#)
 - normalization [6-4](#)
- asymmetric traffic
 - anomaly detection [10-2](#)
 - caution [10-2](#)
 - disabling anomaly detection [10-34](#)
- asymmetric traffic and disabling anomaly detection [C-18](#)
- Atomic ARP engine
 - parameters (table) [B-13](#)
- Atomic ARP engine described [B-13](#)
- Atomic IP Advanced engine
 - described [B-14](#)
 - parameters (table) [B-15](#)
 - restrictions [B-14](#)
- Atomic IP engine
 - described [8-13, B-25](#)
 - parameters (table) [B-25](#)
- Atomic IPv6 engine
 - described [B-29](#)
 - Neighborhood Discovery protocol [B-29](#)
 - signatures [B-29](#)
- attack relevance rating
 - calculating risk rating [6-5, 9-3](#)
 - described [6-5, 6-28, 9-3, 9-25](#)
- Attack Response Controller
 - described [A-4](#)
 - formerly known as Network Access Controller [A-4](#)
- Attack Response Controller. See ARC.
- attack severity rating
 - calculating risk rating [6-5, 9-3](#)
 - described [6-5, 9-3](#)
- attempt limit
 - RADIUS [C-20](#)
- attemptLimit command [4-25](#)
- audit mode
 - described [11-8](#)
 - testing global correlation [11-8](#)
- authenticated NTP [4-8, 4-14, C-15](#)
- authentication
 - local [4-19](#)
 - RADIUS [4-19](#)
- AuthenticationApp
 - authenticating users [A-20](#)
 - described [A-4](#)
 - login attempt limit [A-20](#)
 - method [A-20](#)
 - responsibilities [A-20](#)
 - secure communications [A-21](#)
 - sensor configuration [A-20](#)
- Authentication pane
 - configuring [4-23](#)
 - described [4-19](#)
 - field descriptions [4-20](#)
 - user roles [4-17, A-30](#)
- Authorized RSA1 Keys pane
 - configuring [12-5](#)
 - described [12-4](#)
 - field descriptions [12-4](#)
 - RSA authentication [12-4](#)
 - RSA key generation tool [12-5](#)
- Authorized RSA Keys pane
 - configuring [12-3](#)
 - described [12-2](#)
 - field descriptions [12-2](#)
 - RSA authentication [12-2](#)
 - RSA key generation tool [12-3](#)
- Auto/Cisco.com Update pane
 - configuring [17-23](#)
 - described [3-17, 17-20](#)
 - field descriptions [17-22](#)
 - UNIX-style directory listings [17-21](#)
 - user roles [17-18, 17-20](#)

- automatic setup [20-2](#)
- automatic update
 - immediate [22-12](#)
- automatic updates
 - Cisco.com [3-17, 17-20](#)
 - configuring [3-18, 17-23](#)
 - cryptographic account [3-17, 17-20](#)
 - FTP servers [17-20](#)
 - license [1-8](#)
 - SCP servers [3-17, 17-20](#)
- automatic upgrade
 - information required [22-8](#)
 - troubleshooting [C-52](#)
- autoupdatenow command [22-12](#)
- Auto Update window
 - field descriptions [3-18](#)
 - user roles [3-17](#)
- auto-upgrade-option command [22-8](#)

B

- backing up
 - configuration [C-2](#)
 - current configuration [C-4](#)
- BackOrifice. See BO.
- BackOrifice 2000. See BO2K.
- basic setup [20-4](#)
- blocking
 - described [13-1](#)
 - disabling [13-7](#)
 - master blocking sensor [13-23](#)
 - necessary information [13-3](#)
 - prerequisites [13-5](#)
 - supported devices [13-5](#)
 - types [13-2](#)
- blocking devices
 - adding [13-15](#)
 - deleting [13-15](#)
 - editing [13-15](#)

- Blocking Devices pane
 - configuring [13-15](#)
 - described [13-14](#)
 - field descriptions [13-14](#)
 - ssh host-key command [13-15](#)
- blocking not occurring for signature [C-41](#)
- Blocking Properties pane
 - adding a host never to be blocked [13-10](#)
 - configuring [13-9](#)
 - described [13-7](#)
 - field descriptions [13-8](#)
- BO
 - described [B-74](#)
 - Trojans [B-74](#)
- BO2K
 - described [B-74](#)
 - Trojans [B-74](#)
- BST
 - described [C-1](#)
 - URL [C-1](#)
- Bug Search Tool. See BST.
- bypass mode
 - described [5-25](#)
 - signature updates [17-21](#)
- Bypass pane
 - field descriptions [5-26](#)
 - user roles [5-25](#)

C

- calculating risk rating
 - attack relevance rating [6-5, 9-3](#)
 - attack severity rating [6-5, 9-3](#)
 - promiscuous delta [6-5, 9-3](#)
 - signature fidelity rating [6-5, 9-3](#)
 - target value rating [6-5, 9-3](#)
 - watch list rating [6-5, 9-3](#)
- cannot access sensor [C-24](#)

Cat 6K Blocking Device Interfaces pane

- configuring [13-22](#)
- described [13-20](#)
- field descriptions [13-21](#)

CDP mode

- ASA 5500-X IPS SSP [5-27](#)
- ASA 5585-X IPS SSP [5-27](#)
- described [5-27](#)
- interfaces [5-27](#)

CDP Mode pane

- configuring [5-27](#)
- field descriptions [5-27](#)
- user roles [5-27](#)

certificates

- displaying [12-14](#)
- generating [12-14](#)

certificates (IDM) [1-7, 12-11](#)changing Microsoft IIS to UNIX-style directory listings [17-21](#)cidDump obtaining information [C-99](#)

CIDEE

- defined [A-34](#)
- example [A-34](#)
- IPS extensions [A-34](#)
- protocol [A-34](#)
- supported IPS events [A-34](#)

cisco

- default password [19-2](#)
- default username [19-2](#)

Cisco.com

- accessing software [21-2](#)
- downloading software [21-1](#)
- software downloads [21-1](#)

Cisco Bug Search Tool

- described [C-1](#)

Cisco Discovery Protocol. See CDP.

Cisco IOS rate limiting [13-3](#)

Cisco Security Intelligence Operations

- described [21-7](#)

URL [21-7](#)

Cisco Services for IPS

- service contract [1-9, 17-12](#)
- supported products [1-9, 17-12](#)

clear events command [4-12, 4-16, 18-4, C-16, C-99](#)

Clear Flow States pane

- described [18-18](#)
- field descriptions [18-19](#)

clearing

- denied attackers [14-2](#)
- events [4-16, 18-4, C-99](#)
- flow states [18-19](#)
- statistics [C-82](#)

CLI

- described [A-4, A-30](#)
- password recovery [17-10, C-13](#)

client manifest described [A-28](#)clock set command [4-16](#)Clone Event Action Rules dialog box field descriptions [9-12](#)Clone Policy dialog box field descriptions [7-2, 10-9](#)Clone Signature dialog box field descriptions [7-7](#)

cloning

- anomaly detection policies [10-9](#)
- event action rules policies [9-12](#)
- signature definition policies [7-2](#)
- signatures [7-15](#)

CollaborationApp described [A-4, A-27](#)

command and control interface

- described [5-2](#)
- list [5-2](#)

commands

- allocate-ips [6-14](#)
- attemptLimit [4-25](#)
- autoupdatenow [22-12](#)
- auto-upgrade-option [22-8](#)
- clear events [4-12, 4-16, 18-4, C-16, C-99](#)
- clock set [4-16](#)
- copy backup-config [C-3](#)

- copy current-config [C-3](#)
- downgrade [22-12](#)
- erase license-key [17-15](#)
- hw-module module slot_number password-reset [17-8, C-12](#)
- setup [4-1, 20-1, 20-4, 20-8, 20-13, 20-17](#)
- show events [C-96](#)
- show health [C-74](#)
- show module 1 details [C-58, C-69](#)
- show settings [17-11, C-14](#)
- show statistics [C-82](#)
- show statistics virtual-sensor [C-23, C-82](#)
- show tech-support [C-75](#)
- show version [C-79](#)
- sw-module module slot_number password-reset [17-6, C-10](#)
- unlock user username [4-26](#)
- upgrade [22-5, 22-7](#)
- virtual-sensor name [6-14](#)
- Compare Knowledge Bases dialog box field descriptions [18-11](#)
- comparing KBs [18-11, 18-12](#)
- configuration files
 - backing up [C-2](#)
 - merging [C-2](#)
- configuration restrictions
 - alternate TCP reset interface [5-9](#)
 - inline interface pairs [5-8](#)
 - inline VLAN pairs [5-9](#)
 - interfaces [5-8](#)
 - physical interfaces [5-8](#)
 - VLAN groups [5-9](#)
- Configure Summertime dialog box field descriptions [3-5, 4-10](#)
- configuring
 - account locking [4-25](#)
 - account unlocking [4-26](#)
 - AIC policy parameters [7-44](#)
 - allowed hosts [4-6](#)
 - allowed networks [4-6](#)
 - anomaly detection operation settings [10-11](#)
 - application policy signatures [7-44](#)
 - authorized keys [12-5](#)
 - authorized RSA keys [12-3](#)
 - automatic updates [3-18, 17-23](#)
 - automatic upgrades [22-10](#)
 - blocking devices [13-15](#)
 - blocking properties [13-9](#)
 - Cat 6K blocking device interfaces [13-22](#)
 - CDP mode [5-27](#)
 - CPU, Memory, & Load gadget [2-12](#)
 - CSA MC IPS interfaces [16-3](#)
 - device login profiles [13-12](#)
 - event action filters [6-21, 9-18](#)
 - events [18-3](#)
 - event variables [6-35, 9-31](#)
 - external zone [10-31](#)
 - general settings [6-40, 9-36](#)
 - Global Correlation Health gadget [2-8](#)
 - Global Correlation Reports gadget [2-7](#)
 - host blocks [14-4](#)
 - illegal zone [10-25](#)
 - inline VLAN pairs [3-12](#)
 - inspection/reputation [11-9](#)
 - inspection load statistics display [18-5](#)
 - interface pairs [5-19](#)
 - interfaces [5-17](#)
 - interface statistics display [18-6](#)
 - Interface Status gadget [2-7](#)
 - internal zone [10-19](#)
 - IP fragment reassembly signatures [7-48](#)
 - IP logging [14-12](#)
 - IPv4 target value ratings [6-24, 9-21](#)
 - IPv6 target value ratings [6-27, 9-23](#)
 - known host RSA1 keys [12-9](#)
 - known host RSA keys [12-7](#)
 - learning accept mode [10-14](#)
 - Licensing gadget [2-6](#)
 - local authentication [4-23](#)

- master blocking sensor [13-25](#)
- network blocks [14-7](#)
- network participation [11-11](#)
- Network Security gadget [2-9](#)
- network settings [4-3](#)
- NTP servers [4-13](#)
- OS maps [6-31, 9-28](#)
- RADIUS authentication [4-23](#)
- rate limiting [14-9](#)
- rate limiting device interfaces [13-19](#)
- risk categories [6-37, 9-33](#)
- router blocking device interfaces [13-19](#)
- Sensor Health gadget [2-5](#)
- Sensor Information gadget [2-4](#)
- Sensor Setup window [3-5](#)
- sensor to use NTP [4-14](#)
- signature variables [7-33](#)
- SNMP [15-2](#)
- SNMP traps [15-8](#)
- SNMPv3 users [15-5](#)
- time [4-11](#)
- Top Applications gadget [2-10](#)
- traffic flow notifications [5-26](#)
- trusted hosts [12-13](#)
- upgrades [22-5](#)
- users [4-23](#)
- VLAN groups [5-24](#)
- VLAN pairs [5-21](#)
- control transactions
 - characteristics [A-9](#)
 - request types [A-8](#)
- cookies IDM [1-6](#)
- copy backup-config command [C-3](#)
- copy current-config command [C-3](#)
- correcting time on the sensor [4-12, C-16](#)
- CPU, Memory, & Load gadget
 - configuring [2-12](#)
 - described [2-11](#)
- creating
 - Atomic IP Advanced engine signature [7-25, 8-14](#)
 - custom signatures
 - not using signature engines [8-4](#)
 - Service HTTP [8-17](#)
 - String TCP [8-22](#)
 - using signature engines [8-1](#)
 - IPv6 signatures [7-25, 8-14](#)
 - Meta signatures [7-22](#)
 - Post-Block VACLs [13-21](#)
 - Pre-Block VACLs [13-21](#)
 - String TCP XL signatures [7-30](#)
- creating the service account [C-5](#)
- cryptographic account
 - automatic updates [3-17, 17-20](#)
 - Encryption Software Export Distribution Authorization from [21-2](#)
 - obtaining [21-2](#)
- cryptographic features (IDM) [1-1](#)
- CSA MC
 - adding interfaces [16-7](#)
 - configuring IPS interfaces [16-3](#)
 - host posture events [16-1, 16-3](#)
 - quarantined IP address events [16-1](#)
 - supported IPS interfaces [16-3](#)
- CtlTransSource
 - described [A-4, A-11](#)
 - illustration [A-12](#)
- current configuration back up [C-2](#)
- current KB setting [18-14](#)
- customizing
 - dashboards [2-1](#)
 - gadgets [2-1](#)
- custom signatures
 - Custom Signature Wizard [8-5](#)
 - described [7-4](#)
 - IPv6 signature [7-25, 8-14](#)
 - Meta signature [7-22](#)
 - sensor performance [8-4](#)

- String TCP XL [7-27, 7-30](#)
 - Custom Signature Wizard
 - alert behavior [8-26](#)
 - described [8-1](#)
 - no signature engine sequence [8-4](#)
 - signature engine sequence [8-1](#)
 - supported signature engines [8-2](#)
 - using [8-5](#)
- ## D
-
- Dashboard pane gadgets [2-2](#)
 - dashboards
 - adding [2-1](#)
 - customizing [2-1](#)
 - data nodes [8-25, B-69](#)
 - data structures (examples) [A-8](#)
 - DDoS
 - protocols [B-74](#)
 - Stacheldraht [B-74](#)
 - TFN [B-74](#)
 - debug logging enable [C-44](#)
 - default policies
 - ad0 [10-9](#)
 - rules0 [9-12](#)
 - sig0 [7-2](#)
 - defaults
 - KB filename [10-12](#)
 - password [19-2](#)
 - restoring [17-27](#)
 - username [19-2](#)
 - virtual sensor vs0 [6-2](#)
 - deleting
 - anomaly detection policies [10-9](#)
 - blocking devices [13-15](#)
 - denied attackers [14-2](#)
 - event action filters [6-21, 9-18](#)
 - event action overrides [9-14](#)
 - event action rules policies [9-12](#)
 - event variables [6-35, 9-31](#)
 - host blocks [14-4](#)
 - imported OS values [18-18](#)
 - IPv4 target value ratings [6-24, 9-21](#)
 - IPv6 target value ratings [6-27, 9-23](#)
 - KBs [18-14](#)
 - learned OS values [18-17](#)
 - network blocks [14-7](#)
 - OS maps [6-31, 9-28](#)
 - rate limiting devices [13-15](#)
 - rate limits [14-9](#)
 - risk categories [6-37, 9-33](#)
 - signature definition policies [7-2](#)
 - signature variables [7-33](#)
 - virtual sensors [6-11](#)
 - Denial of Service. See DoS.
 - denied attackers
 - adding [14-2](#)
 - clearing [14-2](#)
 - deleting [14-2](#)
 - hit count [14-1](#)
 - resetting hit counts [14-2](#)
 - viewing hit counts [14-2](#)
 - viewing list [14-2](#)
 - Denied Attackers pane
 - described [14-1](#)
 - field descriptions [14-2](#)
 - user roles [14-1](#)
 - using [14-2](#)
 - deny actions (list) [9-8](#)
 - Deny Packet Inline described [7-11, 9-10](#)
 - detect mode (anomaly detection) [10-4](#)
 - device access issues [C-39](#)
 - Device Login Profiles pane
 - configuring [13-12](#)
 - described [13-11](#)
 - field descriptions [13-12](#)
 - Diagnostics Report pane
 - button functions [18-21](#)

- described [18-21](#)
 - user roles [18-20](#)
 - using [18-21](#)
 - diagnostics reports [18-21](#)
 - Differences between knowledge bases KB_Name and KB_Name window field descriptions [18-12](#)
 - Difference Thresholds between knowledge base KB_Name and KB_Name window field descriptions [18-12](#)
 - disabling
 - anomaly detection [10-34, C-18](#)
 - blocking [13-7](#)
 - event action filters [6-21, 9-18](#)
 - global correlation [11-12](#)
 - interfaces [5-17](#)
 - password recovery [17-10, C-13](#)
 - signatures [7-12](#)
 - disaster recovery [C-6](#)
 - displaying
 - events [18-3, C-97](#)
 - health status [C-74](#)
 - imported OS maps [18-18](#)
 - inspection load statistics [18-5](#)
 - interface statistics [18-6](#)
 - learned OS maps [18-17](#)
 - password recovery setting [17-11, C-14](#)
 - sensor statistics [18-22](#)
 - statistics [C-82](#)
 - tech support information [C-76](#)
 - version [C-79](#)
 - Distributed Denial of Service. See DDoS.
 - DoS tools
 - Stacheldraht [B-74](#)
 - stick [B-6](#)
 - TFN [B-74](#)
 - downgrade command [22-12](#)
 - downgrading sensors [22-13](#)
 - downloading
 - Cisco software [21-1](#)
 - KBs [18-15](#)
 - Download Knowledge Base From Sensor dialog box
 - described [18-15](#)
 - field descriptions [18-15](#)
 - duplicate IP addresses [C-26](#)
-
- ## E
- Edit Allowed Host dialog box
 - field descriptions [4-6](#)
 - user roles [4-5](#)
 - Edit Authorized RSA1 Key dialog box
 - field descriptions [12-5](#)
 - user roles [12-4](#)
 - Edit Authorized RSA Key dialog box
 - field descriptions [12-3](#)
 - user roles [12-2](#)
 - Edit Blocking Device dialog box
 - field descriptions [13-14](#)
 - user roles [13-13](#)
 - Edit Cat 6K Blocking Device Interface dialog box
 - field descriptions [13-22](#)
 - user roles [13-20](#)
 - Edit Configured OS Map dialog box
 - field descriptions [6-31, 9-27](#)
 - user roles [6-30, 9-24](#)
 - Edit Destination Port dialog box field descriptions [10-16](#)
 - Edit Device Login Profile dialog box
 - field descriptions [13-12](#)
 - user roles [13-11](#)
 - Edit Event Action Filter dialog box
 - field descriptions [6-20, 9-16](#)
 - user roles [6-19, 9-15](#)
 - Edit Event Action Override dialog box
 - field descriptions [6-11, 9-14](#)
 - user roles [6-11, 9-13](#)
 - Edit Event Variable dialog box
 - field descriptions [6-34, 9-30](#)
 - user roles [9-29](#)

- Edit External Product Interface dialog box
 - field descriptions [16-6](#)
 - user roles [16-4](#)
- Edit Histogram dialog box field descriptions [10-17](#)
- editing
 - blocking devices [13-15](#)
 - event action filters [6-21, 9-18](#)
 - event action overrides [9-14](#)
 - event variables [6-35, 9-31](#)
 - interfaces [5-17](#)
 - IPv4 target value ratings [6-24, 9-21](#)
 - IPv6 target value ratings [6-27, 9-23](#)
 - OS maps [6-31, 9-28](#)
 - rate limiting devices [13-15](#)
 - risk categories [6-37, 9-33](#)
 - signatures [7-16](#)
 - signature variables [7-33](#)
 - virtual sensors [6-11](#)
- Edit Inline VLAN Pair dialog box field descriptions [3-11, 5-21](#)
- Edit Interface dialog box field descriptions [5-16](#)
- Edit Interface Pair dialog box field descriptions [5-19](#)
- Edit IP Logging dialog box field descriptions [14-11](#)
- Edit Known Host RSA1 Key dialog box
 - field descriptions [12-9](#)
 - user roles [12-8](#)
- Edit Known Host RSA Key dialog box
 - field descriptions [12-7](#)
 - user roles [12-6](#)
- Edit Master Blocking Sensor dialog box
 - field descriptions [13-24](#)
 - user roles [13-23](#)
- Edit Never Block Address dialog box
 - field descriptions [13-10](#)
 - user roles [13-7](#)
- Edit Posture ACL dialog box field descriptions [16-7](#)
- Edit Protocol Number dialog box field descriptions [10-18, 10-25](#)
- Edit Risk Level dialog box field descriptions [6-37, 9-33](#)
- Edit Router Blocking Device Interface dialog box
 - field descriptions [13-19](#)
 - user roles [13-16](#)
- Edit Signature dialog box field descriptions [7-7](#)
- Edit Signature Variable dialog box
 - field descriptions [7-33](#)
 - user roles [7-32](#)
- Edit SNMP Trap Destination dialog box field descriptions [15-8](#)
- Edit SNMPv3 User dialog box
 - field descriptions [15-4](#)
- Edit SNMPv3 user dialog box
 - user roles [15-3](#)
- Edit User dialog box
 - field descriptions [4-22](#)
 - user roles [4-19, 4-22](#)
- Edit Virtual Sensor dialog box
 - field descriptions [6-9](#)
 - user roles [6-9](#)
- Edit VLAN Group dialog box field descriptions [5-23](#)
- efficacy
 - described [11-4](#)
 - measurements [11-4](#)
- enabling
 - anomaly detection [10-4](#)
 - event action filters [6-21, 9-18](#)
 - event action overrides [9-14](#)
 - interfaces [5-17](#)
 - packet logging [17-3](#)
 - signatures [7-12](#)
- enabling debug logging [C-44](#)
- Encryption Software Export Distribution Authorization form
 - cryptographic account [21-2](#)
 - described [21-2](#)
- engines
 - AIC [B-10](#)
 - AIC FTP [B-11](#)
 - AIC HTTP [B-11](#)

- Atomic [B-12](#)
- Atomic ARP [B-13](#)
- Atomic IP [8-13, B-25](#)
- Atomic IP Advanced [B-14](#)
- Atomic IPv6 [B-29](#)
- Fixed [B-30](#)
- Fixed ICMP [B-30](#)
- Fixed TCP [B-30](#)
- Fixed UDP [B-30](#)
- Flood [B-33](#)
- Flood Host [B-33](#)
- Flood Net [B-33](#)
- Master [B-4](#)
- Meta [7-22, B-34](#)
- Multi String [B-36](#)
- Normalizer [B-37](#)
- Service [B-41](#)
- Service DNS [B-41](#)
- Service FTP [B-42](#)
- Service Generic [B-43](#)
- Service H225 [B-45](#)
- Service HTTP [8-16, B-47](#)
- Service IDENT [B-49](#)
- Service MSRPC [8-11, B-50](#)
- Service MSSQL [B-52](#)
- Service NTP [B-53](#)
- Service P2P [B-54](#)
- Service RPC [8-19, B-54](#)
- Service SMB Advanced [B-56](#)
- Service SNMP [B-58](#)
- Service SSH [B-59](#)
- Service TNS [B-59](#)
- State [8-20, B-61](#)
- String [8-21, 8-24, B-63](#)
- String ICMP [8-21, 8-24, B-63](#)
- String TCP [8-21, 8-24, B-63](#)
- String UDP [8-21, 8-24, B-63](#)
- Sweep [8-24, B-68](#)
- Sweep Other TCP [B-70](#)
- Traffic Anomaly [B-71](#)
- Traffic ICMP [B-73](#)
- Trojan [B-74](#)
- erase license-key command [17-15](#)
- errors (Analysis Engine) [C-52](#)
- evAlert [A-9](#)
- event action filters
 - adding [6-21, 9-18](#)
 - configuring [6-21, 9-18](#)
 - deleting [6-21, 9-18](#)
 - described [6-18, 9-5](#)
 - disabling [6-21, 9-18](#)
 - editing [6-21, 9-18](#)
 - enabling [6-21, 9-18](#)
 - moving [6-21, 9-18](#)
- Event Action Filters tab
 - configuring [6-21, 9-18](#)
 - described [6-19, 9-15](#)
 - field descriptions [6-19, 9-16](#)
- event action overrides
 - adding [9-14](#)
 - deleting [9-14](#)
 - described [6-4, 9-4](#)
 - editing [9-14](#)
 - enabling [9-14](#)
 - risk rating range [6-4, 9-4](#)
- Event Action Overrides tab
 - described [9-13](#)
 - field descriptions [9-13](#)
- event action rules
 - described [9-2](#)
 - functions [9-2](#)
- Event Action Rules (rules0) pane described [9-13](#)
- Event Action Rules pane
 - described [9-12](#)
 - field descriptions [9-12](#)
 - user roles [9-11](#)
- event action rules policies
 - adding [9-12](#)

- cloning [9-12](#)
- deleting [9-12](#)
- event action rules variables [6-19, 9-15](#)
- event actions
 - risk ratings [6-6, 9-4](#)
 - threat ratings [6-6, 9-4](#)
- events
 - clearing [4-16, 18-4, C-99](#)
 - displaying [C-97](#)
 - host posture [16-2](#)
 - quarantined IP address [16-2](#)
- Events pane
 - configuring [18-3](#)
 - described [18-1](#)
 - field descriptions [18-2](#)
- Event Store
 - clearing [4-16, 18-4, C-99](#)
 - clearing events [4-12, C-16](#)
 - data structures [A-8](#)
 - described [A-4](#)
 - examples [A-7](#)
 - no alerts [C-31](#)
 - responsibilities [A-7](#)
 - time stamp [4-12, C-16](#)
 - timestamp [A-7](#)
- event types [C-95](#)
- event variables
 - adding [6-35, 9-31](#)
 - configuring [6-35, 9-31](#)
 - deleting [6-35, 9-31](#)
 - described [6-33, 9-29](#)
 - editing [6-35, 9-31](#)
 - example [6-34, 9-30](#)
- Event Variables tab
 - configuring [6-35, 9-31](#)
 - field descriptions [6-34, 9-30](#)
- Event Viewer pane
 - displaying events [18-3](#)
 - field descriptions [18-2](#)
- evError [A-9](#)
- evLogTransaction [A-9](#)
- evShunRqst [A-9](#)
- evStatus [A-9](#)
- example custom signatures
 - Atomic IP Advanced [7-25, 8-14](#)
 - Meta [7-22](#)
 - Service HTTP [8-17](#)
 - String TCP [8-22](#)
 - String TCP XL [7-27](#)
- examples
 - AIC engine signature [7-44](#)
 - ASA failover configuration [C-58, C-68](#)
 - Atomic IP Advanced engine signature [7-25, 8-14](#)
 - automatic update [17-24](#)
 - configured OS maps [6-30, 9-25](#)
 - default anomaly detection configuration [10-4](#)
 - IP Fragment Reassembly signature [7-48](#)
 - IPv6 attacker address [6-20, 9-17](#)
 - IPV6 victim address [6-21, 9-17](#)
 - KB histogram [10-13, 18-8](#)
 - Meta engine signature [7-22](#)
 - Service HTTP engine signature [8-17](#)
 - SPAN configuration for IPv6 support [5-11](#)
 - String TCP engine signature [8-22](#)
 - String TCP XL engine signature [7-27, 7-30](#)
 - System Configuration Dialog [20-2](#)
 - TCP Stream Reassembly signature [7-55](#)
- external product interfaces
 - adding [16-7](#)
 - described [16-1](#)
 - issues [16-3, C-21](#)
 - troubleshooting [16-10, C-22](#)
 - trusted hosts [16-4](#)
- External Product Interfaces pane
 - described [16-4](#)
 - field descriptions [16-5](#)
- external zone
 - configuring [10-31](#)

protocols [10-29](#)

user roles [10-28](#)

External Zone tab

described [10-29](#)

tabs [10-29](#)

user roles [10-28](#)

F

false positives described [7-4](#)

files

Cisco IPS (list) [21-1](#)

Fixed engine described [B-30](#)

Fixed ICMP engine parameters (table) [B-30](#)

Fixed TCP engine parameters (table) [B-31](#)

Fixed UDP engine parameters (table) [B-32](#)

Flood engine described [B-33](#)

Flood Host engine parameters (table) [B-33](#)

Flood Net engine parameters (table) [B-34](#)

flow states clearing [18-19](#)

FTP servers

automatic updates [17-20](#)

signature updates [17-25](#)

FTP servers and software updates [17-20, 22-3](#)

G

gadgets

adding [2-1](#)

CPU, Memory, & Load [2-11](#)

customizing [2-1](#)

Dashboard pane [2-2](#)

Global Correlation Health [2-8](#)

Global Correlation Reports [2-7](#)

IDM [2-2](#)

IDM home pane [1-4](#)

Interface Status [2-6](#)

Licensing [2-6](#)

Network Security [2-9](#)

Sensor Health [2-4](#)

Sensor Information [2-3](#)

Top Applications [2-10](#)

general settings

configuring [6-40, 9-36](#)

described [6-39, 9-35](#)

General tab

configuring [6-40, 9-36](#)

described [6-39, 9-35, 10-16, 10-23](#)

enabling zones [10-16, 10-23](#)

field descriptions [6-40, 9-36](#)

user roles [9-35](#)

generating diagnostics reports [18-21](#)

global correlation

described [1-1, 11-1, 11-2](#)

disabling [11-12](#)

disabling about [11-12](#)

DNS server [11-6](#)

error messages [A-29](#)

features [11-5](#)

goals [11-5](#)

health metrics [11-7](#)

health status [11-7](#)

HTTP proxy server [11-6](#)

IPS reloading messages [C-67, C-73](#)

license [1-8, 4-3, 11-6, 11-8, 20-1, 20-5](#)

no IPv6 support [6-20, 6-21, 6-26, 6-27, 6-33, 6-35, 9-15, 9-16, 9-18, 9-22, 9-23, 9-29, 9-31, 11-6](#)

Produce Alert [7-9, 9-8](#)

requirements [11-6](#)

risk rating [11-5](#)

troubleshooting [11-11, C-20](#)

update client (illustration) [11-8](#)

Global Correlation Health gadget

configuring [2-8](#)

described [2-8](#)

Global Correlation Reports gadget

configuring [2-7](#)

described [2-7](#)

Global Correlation Update

client described [A-28](#)server described [A-28](#)GRUB menu password recovery [17-5, C-8](#)**H**H.225.0 protocol [B-45](#)H.323 protocol [B-45](#)

health status

global correlation [11-7](#)metrics [2-4](#)sensor [2-4](#)health status display [C-74](#)

Home pane

gadgets [1-4](#)updating [1-4](#)

host blocks

adding [14-4](#)deleting [14-4](#)managing [14-4](#)

Host Blocks pane

configuring [14-4](#)described [14-3](#)

host posture events

CSA MC [16-3](#)described [16-2](#)HTTP/HTTPS servers supported [17-20, 22-3](#)

HTTP deobfuscation

ASCII normalization [8-16, B-47](#)described [8-16, B-47](#)hw-module module slot_number password-reset
command [17-8, C-12](#)**I**

IDAPI

communications [A-4, A-32](#)described [A-4](#)functions [A-32](#)illustration [A-32](#)responsibilities [A-32](#)

IDCONF

described [A-33](#)example [A-33](#)RDEP2 [A-33](#)XML [A-33](#)

IDIOM

defined [A-32](#)messages [A-32](#)

IDM

Analysis Engine is busy [C-55](#)certificates [1-7, 12-11](#)cookies [1-6](#)cryptographic features [1-1](#)Custom Signature Wizard supported signature
engines [8-2](#)described [1-4, 1-5](#)gadgets [2-2](#)GUI [1-4](#)known host key retrieval [12-6, 12-7, 12-8](#)logging in [1-6](#)password recovery [17-10, C-14](#)supported platforms [1-3](#)system requirements [1-2](#)TLS [1-7, 12-11](#)user interface [1-4](#)web browsers [1-4, 1-5](#)will not load [C-54](#)

illegal zone

configuring [10-25](#)user roles [10-22](#)

Illegal Zone tab

described [10-22](#)user roles [10-22](#)

Imported OS pane

clearing [18-18](#)described [18-18](#)

- field descriptions [18-18](#)
- imported OS values
 - clearing [18-18](#)
 - deleting [18-18](#)
- inactive mode (anomaly detection) [10-4](#)
- initializing
 - appliances [20-8](#)
 - ASA 5500-X IPS SSP [20-13](#)
 - ASA 5585-X IPS SSP [20-17](#)
 - sensors [4-1, 20-1, 20-4](#)
 - user roles [20-1](#)
 - verifying [20-21](#)
- inline interface pair mode
 - configuration restrictions [5-8](#)
 - described [5-12](#)
 - illustration [5-12](#)
- Inline Interface Pair window
 - described [3-10](#)
 - Startup Wizard [3-10](#)
- inline mode
 - interface cards [5-3](#)
 - normalization [6-4](#)
 - pairing interfaces [5-3](#)
- inline TCP session tracking modes described [6-3](#)
- inline VLAN pair mode
 - configuration restrictions [5-9](#)
 - configuring [3-12](#)
 - described [5-13](#)
 - illustration [5-13](#)
 - supported sensors [5-13](#)
- Inline VLAN Pairs window
 - described [3-11](#)
 - field descriptions [3-11](#)
 - Startup Wizard [3-11](#)
- Inspection/Reputation pane
 - configuring [11-9](#)
 - described [11-8](#)
 - field descriptions [11-9](#)
- Inspection Load Statistics pane
 - configuring [18-5](#)
 - described [18-4](#)
 - field descriptions [18-4](#)
 - user roles [18-4](#)
- installer major version [21-5](#)
- installer minor version [21-5](#)
- installing
 - sensor license [1-10, 17-14](#)
 - system image
 - ASA 5500-X IPS SSP [22-23](#)
 - ASA 5585-X IPS SSP [22-25](#)
 - IPS 4345 [22-17](#)
 - IPS 4360 [22-17](#)
 - IPS 4510 [22-20](#)
 - IPS 4520 [22-20](#)
 - IPS 4520-XL [22-20](#)
- IntelliShield
 - alerts [7-5](#)
 - MySDN [7-5](#)
- InterfaceApp described [A-4](#)
- interface pairs
 - configuring [5-19](#)
 - described [5-18](#)
- Interface Pairs pane
 - configuring [5-19](#)
 - described [5-18](#)
 - field descriptions [5-18](#)
 - user roles [5-18](#)
- interfaces
 - alternate TCP reset [5-2](#)
 - command and control [5-2](#)
 - configuration restrictions [5-8](#)
 - configuring [5-17](#)
 - described [3-8, 5-1](#)
 - disabling [5-17](#)
 - editing [5-17](#)
 - enabling [5-17](#)
 - logical [3-8](#)

- physical [3-8](#)
- port numbers [5-1](#)
- sensing [5-2, 5-3](#)
- slot numbers [5-1](#)
- support (table) [5-4](#)
- TCP reset [5-6](#)
- Interface Selection window
 - described [3-10](#)
 - Startup Wizard [3-10](#)
- Interfaces pane
 - configuring [5-17](#)
 - described [5-15](#)
 - field descriptions [5-15](#)
- Interface Statistics pane
 - configuring [18-6](#)
 - described [18-5](#)
 - field descriptions [18-6](#)
- Interface Status gadget
 - configuring [2-7](#)
 - described [2-6](#)
- Interface Summary window
 - described [3-8](#)
- internal zone
 - configuring [10-19](#)
 - user roles [10-15](#)
- Internal Zone tab
 - described [10-15](#)
 - user roles [10-15](#)
- IP fragmentation described [B-38](#)
- IP fragment reassembly
 - configuring [7-47](#)
 - described [7-45](#)
 - mode [7-47](#)
 - parameters (table) [7-46](#)
 - signatures [7-48](#)
 - signatures (example) [7-48](#)
 - signatures (table) [7-46](#)
- IP logging
 - described [7-55, 14-10](#)
 - event actions [14-10](#)
 - system performance [14-10](#)
- IP Logging pane
 - configuring [14-12](#)
 - described [14-10](#)
 - field descriptions [14-11](#)
 - user roles [14-10](#)
- IP Logging Variables pane
 - described [17-18](#)
 - field description [17-18](#)
- IP logs
 - circular buffer [14-10](#)
 - states [14-10](#)
 - TCPDUMP [14-10](#)
 - viewing [14-12](#)
 - WireShark [14-10](#)
- IPS 4345
 - installing system image [22-17](#)
 - password recovery [C-8](#)
 - reimaging [22-17](#)
- IPS 4360
 - installing system image [22-17](#)
 - password recovery [C-8](#)
 - reimaging [22-17](#)
- IPS 4510
 - installing system image [22-20](#)
 - reimaging [22-20](#)
 - SwitchApp [A-29](#)
- IPS 4520
 - installing system image [22-20](#)
 - reimaging [22-20](#)
 - SwitchApp [A-29](#)
- IPS 4520-XL
 - installing system image [22-20](#)
 - reimaging [22-20](#)
 - SwitchApp [A-29](#)
- IPS appliances
 - Deny Connection Inline [7-12, 9-10](#)
 - Deny Packet Inline [7-12, 9-10](#)

- Reset TCP Connection [7-12, 9-10](#)
- TCP reset packets [7-12, 9-10](#)
- IPS applications
 - summary [A-35](#)
 - table [A-35](#)
 - XML format [A-4](#)
- IPS clock synchronization [4-8, C-15](#)
- IPS data
 - types [A-8](#)
 - XML document [A-9](#)
- IPS events
 - evAlert [A-9](#)
 - evError [A-9](#)
 - evLogTransaction [A-9](#)
 - evShunRqst [A-9](#)
 - evStatus [A-9](#)
 - list [A-9](#)
 - types [A-9](#)
- IPS internal communications [A-32](#)
- IPS modules unsupported features [3-2](#)
- IPS Policies pane
 - described [6-7](#)
 - Event Action Rules [6-8](#)
 - field descriptions [6-8](#)
- IPS software
 - application list [A-4](#)
 - available files [21-1](#)
 - configuring device parameters [A-5](#)
 - directory structure [A-34](#)
 - Linux OS [A-1](#)
 - obtaining [21-1](#)
 - retrieving data [A-5](#)
 - security features [A-5](#)
 - tuning signatures [A-5](#)
 - updating [A-5](#)
 - user interaction [A-5](#)
 - versioning scheme [21-3](#)
- IPS software file names
 - major updates (illustration) [21-4](#)
 - minor updates (illustration) [21-4](#)
 - patch releases (illustration) [21-4](#)
 - service packs (illustration) [21-4](#)
- IPv4
 - address format [6-33, 9-30](#)
 - event variables [6-33, 9-30](#)
- IPv4 Add Target Value Rating dialog box
 - field descriptions [6-24, 9-21](#)
 - user roles [6-24, 9-20](#)
- IPv4 Edit Target Value Rating dialog box
 - field descriptions [6-24, 9-21](#)
 - user roles [6-24, 9-20](#)
- IPv4 target value ratings
 - adding [6-24, 9-21](#)
 - deleting [6-24, 9-21](#)
 - editing [6-24, 9-21](#)
- IPv4 Target Value Rating tab
 - configuring [6-24, 9-21](#)
 - field descriptions [6-24, 9-21](#)
- IPv6
 - address format [6-34, 9-30](#)
 - described [B-29](#)
 - event variables [6-34, 9-30](#)
 - SPAN ports [5-11](#)
 - switches [5-11](#)
- IPv6 Add Target Value Rating dialog box
 - field descriptions [6-26](#)
 - user roles [6-25, 9-22](#)
- IPv6 Edit Target Value Rating dialog box
 - field descriptions [6-26, 9-23](#)
 - user roles [6-25, 9-22](#)
- IPv6 target value ratings
 - adding [6-27, 9-23](#)
 - configuring [6-27, 9-23](#)
 - deleting [6-27, 9-23](#)
 - editing [6-27, 9-23](#)
- IPv6 Target Value Rating tab
 - configuring [6-27, 9-23](#)
 - field descriptions [6-26, 9-22](#)

K

KBs

- comparing [18-12](#)
- default filename [10-12](#)
- deleting [18-14](#)
- described [10-3](#)
- downloading [18-15](#)
- histogram [10-12, 18-8](#)
- initial baseline [10-3](#)
- learning accept mode [10-12](#)
- loading [18-14](#)
- monitoring [18-11](#)
- renaming [18-15](#)
- saving [18-14](#)
- scanner threshold [10-12, 18-8](#)
- tree structure [10-12, 18-8](#)
- uploading [18-16](#)

Knowledge Base. See KB.

Known Host RSA1 Keys pane

- configuring [12-9](#)
- described [12-8](#)
- field descriptions [12-9](#)

Known Host RSA Keys pane

- configuring [12-7](#)
- described [12-6](#)
- field descriptions [12-7](#)

L

Learned OS pane

- clearing [18-17](#)
- described [18-17](#)
- field descriptions [18-17](#)

learned OS values

- clearing [18-17](#)
- deleting [18-17](#)

learning accept mode

- anomaly detection [10-3](#)

configuring [10-14](#)

user roles [10-12](#)

Learning Accept Mode tab

- described [10-12](#)
- field descriptions [10-13, 10-14](#)
- user roles [10-12](#)

license key

- obtaining [1-8, 17-12](#)
- trial [1-8, 17-12](#)
- uninstalling [17-15](#)
- viewing status of [1-8, 17-12](#)

licensing

- described [1-8, 17-12](#)
- IPS device serial number [1-8, 17-12](#)

Licensing gadget

- configuring [2-6](#)
- described [2-6](#)

Licensing pane

- configuring [1-10, 17-14](#)
- described [1-8, 17-12](#)
- field descriptions [1-10, 17-13](#)
- user roles [1-10, 17-11](#)

limitations for concurrent CLI sessions [19-1](#)

listings UNIX-style [17-21](#)

loading KBs [18-14](#)

local authentication configuring [4-23](#)

Logger

- described [A-4, A-19](#)
- functions [A-19](#)
- syslog messages [A-19](#)

logging in

- appliances [19-2](#)
- ASA 5500-X IPS SSP [19-4](#)
- ASA 5585-X IPS SSP [19-5](#)
- IDM [1-6](#)
- sensors
 - SSH [19-6](#)
 - Telnet [19-6](#)
- service role [19-2](#)

terminal servers [19-3, 22-16](#)

user role [19-1](#)

LOKI

described [B-74](#)

protocol [B-73](#)

loose connections on sensors [C-22](#)

M

MainApp

components [A-6](#)

described [A-4, A-6](#)

host statistics [A-6](#)

responsibilities [A-6](#)

show version command [A-6](#)

major updates described [21-3](#)

managing

host blocks [14-4](#)

network blocks [14-7](#)

rate limiting [14-9](#)

manifests

client [A-28](#)

server [A-28](#)

manually updating sensor [17-25](#)

master blocking sensor

described [13-23](#)

not set up properly [C-42](#)

verifying configuration [C-43](#)

Master Blocking Sensor pane

configuring [13-25](#)

described [13-23](#)

field descriptions [13-24](#)

Master engine

alert frequency [B-6](#)

alert frequency parameters (table) [B-7](#)

described [B-4](#)

event actions [9-8, B-7](#)

general parameters (table) [B-4](#)

universal parameters [B-4](#)

master engine parameters

obsoletes [B-6](#)

promiscuous delta [B-6](#)

vulnerable OSes [B-6](#)

merging configuration files [C-2](#)

Meta engine

described [7-22, B-34](#)

parameters (table) [B-35](#)

Signature Event Action Processor [7-22, B-34](#)

Meta Event Generator described [6-39, 9-35](#)

metrics for sensor health [17-16](#)

MIBs supported [15-9, C-18](#)

minor updates described [21-3](#)

Miscellaneous tab

application policy parameters [7-34](#)

button functions [7-35](#)

configuring

application policy [7-44](#)

IP fragment reassembly mode [7-47](#)

IP logging [7-56](#)

TCP stream reassembly mode [7-54](#)

described [7-34](#)

field descriptions [7-35](#)

IP fragment reassembly options [7-34](#)

IP logging options [7-35](#)

TCP stream reassembly [7-34](#)

user roles [7-34](#)

modes

anomaly detection detect [10-4](#)

anomaly detection learning accept [10-3](#)

asymmetric [6-4](#)

bypass [5-25](#)

inactive (anomaly detection) [10-4](#)

inline interface pair [5-12](#)

inline TCP tracking [6-3](#)

inline VLAN pair [5-13](#)

Normalizer [6-4](#)

promiscuous [5-10](#)

VLAN groups [5-13](#)

- monitoring
 - displaying statistics [18-6](#)
 - events [18-3](#)
 - inspection load statistics [18-4, 18-5](#)
 - KBs [18-11](#)
 - moving
 - event action filters [6-21, 9-18](#)
 - OS maps [6-31, 9-28](#)
 - Multi String engine
 - described [B-36](#)
 - parameters (table) [B-36](#)
 - Regex [B-36](#)
 - MySDN
 - described [7-5](#)
 - Intellishield [7-5](#)
-
- N**
- NAS-ID
 - described [4-23](#)
 - RADIUS authentication [4-23](#)
 - Neighborhood Discovery
 - options [B-30](#)
 - types [B-30](#)
 - network blocks
 - adding [14-7](#)
 - deleting [14-7](#)
 - managing [14-7](#)
 - Network Blocks pane
 - configuring [14-7](#)
 - described [14-6](#)
 - field descriptions [14-6](#)
 - user roles [14-6](#)
 - Network pane
 - configuring [4-3](#)
 - described [4-2](#)
 - field descriptions [4-2](#)
 - TLS/SSL [4-4](#)
 - user roles [4-2](#)
 - network participation
 - data gathered [11-3](#)
 - data use (table) [1-2, 11-2](#)
 - described [11-3](#)
 - health metrics [11-7](#)
 - modes [11-4](#)
 - requirements [11-3](#)
 - SensorBase Network [11-4](#)
 - statistics [11-4](#)
 - network participation data
 - improving signature fidelity [11-4](#)
 - understanding sensor deployment [11-4](#)
 - Network Participation pane
 - configuring [11-11](#)
 - described [11-10](#)
 - field descriptions [11-10](#)
 - Network Security gadget
 - configuring [2-9](#)
 - described [2-9](#)
 - never block
 - hosts [13-7](#)
 - networks [13-7](#)
 - normalization described [6-4](#)
 - Normalizer engine
 - ASA 5500-X IPS SSP [B-39, C-65](#)
 - ASA 5585-X IPS SSP [B-39, C-72](#)
 - described [B-38](#)
 - IPv6 fragments [B-38](#)
 - modify packets inline [6-3](#)
 - parameters (table) [B-39](#)
 - NotificationApp
 - alert information [A-9](#)
 - described [A-4](#)
 - functions [A-9](#)
 - SNMP gets [A-9](#)
 - SNMP traps [A-9](#)
 - SNMPv3 [A-9](#)
 - statistics [A-11](#)
 - system health information [A-10](#)

NTP

- authenticated [4-8, 4-14, C-15](#)
- configuring servers [4-13](#)
- described [4-8, C-15](#)
- incorrect configuration [4-9, C-16](#)
- sensor time source [4-13, 4-14](#)
- time synchronization [4-8, C-15](#)
- unauthenticated [4-8, 4-14, C-15](#)
- verifying configuration [4-9](#)

O

- obsoletes field described [B-6](#)
- obtaining
 - cryptographic account [21-2](#)
 - IPS software [21-1](#)
 - license key [1-8, 17-12](#)
 - sensor license [1-10, 17-14](#)
- one-way TCP reset described [6-39, 9-35](#)
- Operation Settings tab
 - described [10-11](#)
 - field descriptions [10-11](#)
 - user roles [10-11](#)
- OS Identifications tab
 - described [6-30, 9-25](#)
 - field descriptions [6-30, 9-27](#)
- OS information sources [6-29, 9-25](#)
- OS maps
 - adding [6-31, 9-28](#)
 - configuring [6-31, 9-28](#)
 - deleting [6-31, 9-28](#)
 - editing [6-31, 9-28](#)
 - moving [6-31, 9-28](#)
- other actions (list) [9-9](#)
- Other Protocols tab
 - described [10-18, 10-24, 10-30](#)
 - enabling other protocols [10-18](#)
 - external zone [10-30](#)
 - field descriptions [10-18, 10-30](#)

illegal zone [10-24](#)

P

- P2P networks described [B-54](#)
- Packet Logging pane
 - described [17-3](#)
 - field descriptions [17-3](#)
- partitions
 - application [A-4](#)
 - recovery [A-4](#)
- passive OS fingerprinting
 - components [6-28, 9-25](#)
 - configuring [6-29, 9-26](#)
 - described [6-28, 9-25](#)
 - enabled (default) [6-29, 9-26](#)
- password policy caution [17-3](#)
- password recovery
 - appliances [17-5, C-8, C-9](#)
 - ASA 5500-X IPS SSP [17-6, C-10](#)
 - ASA 5585-X IPS SSP [17-8, C-11](#)
 - CLI [17-10, C-13](#)
 - described [17-4, C-8](#)
 - disabling [17-10, C-13](#)
 - displaying setting [17-11, C-14](#)
 - GRUB menu [17-5, C-8](#)
 - IDM [17-10, C-14](#)
 - IPS 4345 [C-8](#)
 - IPS 4360 [C-8](#)
 - platforms [17-4, C-8](#)
 - ROMMON [17-5, C-9](#)
 - troubleshooting [17-10, C-14](#)
 - verifying [17-11, C-14](#)
- password requirements configuring [17-2](#)
- Passwords pane
 - configuring [17-2](#)
 - described [17-1](#)
 - field descriptions [17-2](#)
- patch releases described [21-3](#)

peacetime learning (anomaly detection) [10-3](#)

Peer-to-Peer. See P2P.

physical connectivity issues [C-29](#)

physical interfaces configuration restrictions [5-8](#)

platforms concurrent CLI sessions [19-1](#)

Post-Block ACLs [13-17](#)

Pre-Block ACLs [13-17](#)

prerequisites for blocking [13-5](#)

promiscuous delta

 calculating risk rating [6-5, 9-3](#)

 described [6-5, 9-3](#)

promiscuous delta described [B-6](#)

promiscuous mode

 atomic attacks [5-10](#)

 described [5-10](#)

 illustration [5-11](#)

 packet flow [5-10](#)

 SPAN ports [5-11](#)

 TCP reset interfaces [5-7](#)

 VACL capture [5-11](#)

protocols

 ARP [B-13](#)

 CDP [5-27](#)

 CIDEE [A-34](#)

 DCE [8-11, B-50](#)

 DDoS [B-74](#)

 H.323 [B-45](#)

 H225.0 [B-45](#)

 ICMPv6 [B-14](#)

 IDAPI [A-32](#)

 IDCONF [A-33](#)

 IDIOM [A-32](#)

 IPv6 [B-29](#)

 LOKI [B-73](#)

 MSSQL [B-52](#)

 Neighborhood Discovery [B-29](#)

 Q.931 [B-45](#)

 RPC [8-11, B-50](#)

 SDEE [A-33](#)

Signature Wizard [8-10](#)

Q

Q.931 protocol

 described [B-45](#)

 SETUP messages [B-45](#)

quarantined IP address events described [16-2](#)

R

RADIUS

 attempt limit [C-20](#)

 multiple cisco av-pairs [4-21, 4-24](#)

RADIUS authentication

 configuring [4-23](#)

 described [4-19](#)

 NAS-ID [4-23](#)

 service account [4-19](#)

 shared secret [4-24](#)

rate limiting

 ACLs [13-4](#)

 configuring [14-9](#)

 described [13-3](#)

 managing [14-9](#)

 percentages [14-8](#)

 routers [13-3](#)

 service policies [13-4](#)

 supported signatures [13-4](#)

rate limiting devices

 adding [13-15](#)

 deleting [13-15](#)

 editing [13-15](#)

rate limits

 adding [14-9](#)

 deleting [14-9](#)

Rate Limits pane

 configuring [14-9](#)

 described [14-7](#)

- field descriptions [14-8](#)
- raw expression syntax
 - described [B-65](#)
 - expert mode [B-65](#)
- Raw Regex
 - described [7-28, 7-31, B-65](#)
 - expert mode [7-28, 7-31, B-65](#)
- rebooting the sensor [17-28](#)
- Reboot Sensor pane
 - configuring [17-28](#)
 - described [17-28](#)
 - user roles [17-28](#)
- recover command [22-14](#)
- recovering the application partition image [22-14](#)
- recovery partition
 - described [A-4](#)
- recovery partition upgrade [22-7](#)
- Regex
 - Multi String engine [B-36](#)
 - standardized [B-1](#)
- Regular Expression. See also [Regex](#).
- regular expression syntax
 - raw Regex [7-28, 7-31, B-65](#)
 - signatures [B-9](#)
- reimaging
 - ASA 5500-X IPS SSP [22-23](#)
 - described [22-3](#)
 - IPS 4345 [22-17](#)
 - IPS 4360 [22-17](#)
 - IPS 4510 [22-20](#)
 - IPS 4520 [22-20](#)
 - IPS 4520-XL [22-20](#)
 - sensors [22-3, 22-14](#)
- removing
 - last applied
 - service pack [22-13](#)
 - signature update [22-13](#)
- renaming KBs [18-15](#)
- reputation
 - described [11-2](#)
 - illustration [11-3](#)
 - servers [11-3](#)
- Reset Network Security Health pane
 - described [18-20](#)
 - field descriptions [18-20](#)
 - resetting data [18-20](#)
 - user roles [18-20](#)
- reset not occurring for a signature [C-50](#)
- resetting
 - hit counts for denied attackers [14-2](#)
 - network security health data [18-20](#)
 - passwords
 - ASDM [17-7, 17-9, C-11, C-13](#)
 - hw-module command [17-8, C-12](#)
 - sw-module command [17-6, C-10](#)
- resetting the password
 - ASA 5500-X IPS SSP [17-6, C-10](#)
 - ASA 5585-X IPS SSP [17-8, C-12](#)
- Restore Default Interface dialog box field descriptions [3-9](#)
- Restore Defaults pane
 - configuring [17-27](#)
 - described [17-27](#)
 - user roles [17-27](#)
- restoring
 - current configuration [C-4](#)
 - defaults [17-27](#)
- retiring signatures [7-12](#)
- risk categories
 - adding [6-37, 9-33](#)
 - configuring [6-37, 9-33](#)
 - deleting [6-37, 9-33](#)
 - editing [6-37, 9-33](#)
- Risk Category tab
 - configuring [6-37, 9-33](#)
 - described [6-36, 9-33](#)
 - field descriptions [6-37, 9-33](#)

- risk rating
 - Alarm Channel [11-5](#)
 - calculating [6-4, 9-2](#)
 - described [6-28, 9-25](#)
 - global correlation [11-5](#)
 - reputation score [11-5](#)
 - ROMMON
 - appliances [17-5, C-9](#)
 - ASA 5585-X IPS SSP [22-27](#)
 - described [22-15](#)
 - IPS 4345 [22-17](#)
 - IPS 4360 [22-17](#)
 - IPS 4510 [22-20](#)
 - IPS 4520 [22-20](#)
 - IPS 4520-XL [22-20](#)
 - password recovery [17-5, C-9](#)
 - remote sensors [22-15](#)
 - serial console port [22-16](#)
 - TFTP [22-16](#)
 - round-trip time. See [RTT](#).
 - Router Blocking Device Interfaces pane
 - configuring [13-19](#)
 - described [13-16](#)
 - field descriptions [13-18](#)
 - RPC portmapper [8-19, B-54](#)
 - RTT
 - described [22-16](#)
 - TFTP limitation [22-16](#)
-
- S**
- Save Knowledge Base dialog box
 - described [18-13](#)
 - field descriptions [18-13](#)
 - saving KBs [18-14](#)
 - scheduling automatic upgrades [22-10](#)
 - SDEE
 - described [A-33](#)
 - HTTP [17-19, A-33](#)
 - protocol [A-33](#)
 - server requests [17-19, A-34](#)
 - SDEE Subscription pane
 - user roles [17-18](#)
 - SDEE Subscriptions pane
 - field descriptions [17-19](#)
 - security
 - account locking [4-25](#)
 - information on Cisco Security Intelligence Operations [21-7](#)
 - information on MySDN [7-5](#)
 - SSH [12-2](#)
 - security policies described [6-1, 7-1, 9-1, 10-1](#)
 - sensing interface
 - ASA 5500-X IPS SSP [6-14](#)
 - ASA 5585-X IPS SSP [6-14](#)
 - sensing interfaces
 - Analysis Engine [5-3](#)
 - described [5-3](#)
 - interface cards [5-3](#)
 - modes [5-3](#)
 - SensorApp
 - Alarm Channel [A-24](#)
 - Analysis Engine [A-24](#)
 - described [A-4](#)
 - event action filtering [A-25](#)
 - inline packet processing [A-24](#)
 - IP normalization [A-24](#)
 - packet flow [A-25](#)
 - processors [A-23](#)
 - responsibilities [A-23](#)
 - risk rating [A-25](#)
 - Signature Event Action Processor [A-23](#)
 - signature updates [17-21](#)
 - TCP normalization [A-24](#)
 - SensorBase Network
 - described [1-1, 11-1, 11-2](#)
 - network participation [11-4](#)
 - participation [1-2, 11-2](#)

- servers [1-2, 11-2](#)
- sensor health
 - critical settings [17-16](#)
 - metrics [17-16](#)
- Sensor Health gadget
 - configuring [2-5](#)
 - described [2-4](#)
 - metrics [2-4](#)
 - status [2-4](#)
- Sensor Health pane
 - described [17-16](#)
 - field descriptions [17-17](#)
- Sensor Information gadget
 - configuring [2-4](#)
 - described [2-3](#)
- Sensor Key pane
 - button functions [12-10](#)
 - described [12-10](#)
 - field descriptions [12-10](#)
 - sensor SSH host key
 - displaying [12-11](#)
 - generating [12-11](#)
 - user roles [12-10](#)
- sensor license
 - installing [1-10, 17-14](#)
 - obtaining [1-10, 17-14](#)
- sensors
 - access problems [C-24](#)
 - application partition image [22-14](#)
 - asymmetric traffic and disabling anomaly detection [10-34, C-18](#)
 - blocking self [13-7](#)
 - command and control interfaces (list) [5-2](#)
 - configuring to use NTP [4-14](#)
 - corrupted SensorApp configuration [C-34](#)
 - diagnostics reports [18-21](#)
 - disaster recovery [C-6](#)
 - downgrading [22-13](#)
 - incorrect NTP configuration [4-9, C-16](#)
 - initializing [4-1, 20-1, 20-4](#)
 - interface support [5-4](#)
 - IP address conflicts [C-26](#)
 - logging in
 - SSH [19-6](#)
 - Telnet [19-6](#)
 - loose connections [C-22](#)
 - misconfigured access lists [C-26](#)
 - no alerts [C-31, C-56](#)
 - not seeing packets [C-33](#)
 - NTP time source [4-14](#)
 - NTP time synchronization [4-8, C-15](#)
 - partitions [A-4](#)
 - physical connectivity [C-29](#)
 - preventive maintenance [C-2](#)
 - rebooting [17-28](#)
 - reimaging [22-3](#)
 - restoring defaults [17-27](#)
 - sensing process not running [C-28](#)
 - setup command [4-1, 20-1, 20-4, 20-8](#)
 - shutting down [17-28](#)
 - statistics [18-22](#)
 - system information [18-23](#)
 - time sources [4-8, C-15](#)
 - troubleshooting software upgrades [C-53](#)
 - updating [17-26](#)
 - upgrading [22-5](#)
 - using NTP time source [4-13](#)
- Sensor Setup window
 - described [3-2, 3-4](#)
 - Startup Wizard [3-2, 3-4](#)
- Server Certificate pane
 - button functions [12-14](#)
 - certificate
 - displaying [12-14](#)
 - generating [12-14](#)
 - described [12-14](#)
 - field descriptions [12-14](#)
 - user roles [12-14](#)

- server manifest described [A-28](#)
- service account
 - accessing [4-18, C-5](#)
 - cautions [4-18, C-5](#)
 - creating [C-5](#)
 - described [4-18, A-31, C-5](#)
 - RADIUS authentication [4-19](#)
 - TAC [A-31](#)
 - troubleshooting [A-31](#)
- Service Activity pane
 - described [17-18](#)
 - field descriptions [17-18](#)
- Service DNS engine
 - described [B-41](#)
 - parameters (table) [B-41](#)
- Service engine
 - described [B-41](#)
 - Layer 5 traffic [B-41](#)
- Service FTP engine
 - described [B-42](#)
 - parameters (table) [B-43](#)
 - PASV port spoof [B-42](#)
- Service Generic engine
 - described [B-43](#)
 - no custom signatures [B-43](#)
 - parameters (table) [B-44](#)
- Service H225 engine
 - ASN.1PER validation [B-45](#)
 - described [B-45](#)
 - features [B-45](#)
 - parameters (table) [B-46](#)
 - TPKT validation [B-45](#)
- Service HTTP engine
 - custom signature [8-17](#)
 - described [8-16, B-47](#)
 - example signature [8-17](#)
 - parameters (table) [B-48](#)
- Service IDENT engine
 - described [B-49](#)
- parameters (table) [B-50](#)
- Service MSRPC engine
 - DCS/RPC protocol [8-11, B-50](#)
 - described [8-11, B-50](#)
 - parameters (table) [B-51](#)
- Service MSSQL engine
 - described [B-52](#)
 - MSSQL protocol [B-52](#)
 - parameters (table) [B-53](#)
- Service NTP engine
 - described [B-53](#)
 - parameters (table) [B-53](#)
- Service P2P engine described [B-54](#)
- service packs described [21-3](#)
- service role [4-18, 19-2, A-30](#)
- Service RPC engine
 - described [8-19, B-54](#)
 - parameters (table) [B-54](#)
 - RPC portmapper [8-19, B-54](#)
- Service SMB Advanced engine
 - described [B-56](#)
 - parameters (table) [B-56](#)
- Service SNMP engine
 - described [B-58](#)
 - parameters (table) [B-58](#)
- Service SSH engine
 - described [B-59](#)
 - parameters (table) [B-59](#)
- Service TNS engine
 - described [B-59](#)
 - parameters (table) [B-60](#)
- session command
 - ASA 5500-X IPS SSP [19-4](#)
 - ASA 5585-X IPS SSP [19-5](#)
- sessioning in
 - ASA 5500-X IPS SSP [19-4](#)
 - ASA 5585-X IPS SSP [19-5](#)
- setting
 - current KB [18-14](#)

- system clock [4-16](#)
- setting up
 - terminal servers [19-3, 22-16](#)
- setup
 - automatic [20-2](#)
 - command [4-1, 20-1, 20-4, 20-8, 20-13, 20-17](#)
 - simplified mode [20-2](#)
- shared secret
 - described [4-24](#)
 - RADIUS authentication [4-24](#)
- show events command [C-96](#)
- show health command [C-74](#)
- show interfaces command [C-94](#)
- show module 1 details command [C-58, C-69](#)
- show settings command [17-11, C-14](#)
- show statistics command [C-81, C-82](#)
- show statistics virtual-sensor command [C-23, C-82](#)
- show tech-support command [C-75](#)
- show version command [C-78, C-79](#)
- Shut Down Sensor pane
 - configuring [17-28](#)
 - described [17-28](#)
 - user roles [17-28](#)
- shutting down the sensor [17-28](#)
- sig0 pane
 - column heads [7-3](#)
 - configuration buttons [7-3](#)
 - default [7-3](#)
 - described [7-3](#)
 - field descriptions [7-6](#)
 - signatures
 - assigning actions [7-17](#)
 - cloning [7-15](#)
 - tuning [7-16](#)
 - tabs [7-3](#)
- signature definition policies
 - adding [7-2](#)
 - cloning [7-2](#)
 - default policy [7-2](#)
 - deleting [7-2](#)
 - sig0 [7-2](#)
- Signature Definitions pane
 - described [7-2](#)
 - field descriptions [7-2](#)
- signature engines
 - AIC [B-10](#)
 - Atomic [B-12](#)
 - Atomic ARP [B-13](#)
 - Atomic IP [8-13, B-25](#)
 - Atomic IP Advanced [B-14](#)
 - Atomic IPv6 [B-29](#)
 - creating custom signatures [8-1](#)
 - described [B-1](#)
 - Fixed [B-30](#)
 - Flood [B-33](#)
 - Flood Host [B-33](#)
 - Flood Net [B-34](#)
 - list [B-2](#)
 - Master [B-4](#)
 - Meta [7-22, B-34](#)
 - Multi String [B-36](#)
 - Normalizer [B-38](#)
 - Regex
 - patterns [B-9](#)
 - syntax [B-9](#)
 - Service [B-41](#)
 - Service DNS [B-41](#)
 - Service FTP [B-42](#)
 - Service Generic [B-43](#)
 - Service H225 [B-45](#)
 - Service HTTP [8-16, B-47](#)
 - Service IDENT [B-49](#)
 - Service MSRPC [8-11, B-50](#)
 - Service MSSQL [B-52](#)
 - Service NTP [B-53](#)
 - Service P2P [B-54](#)
 - Service RPC [8-19, B-54](#)
 - Service SMB Advanced [B-56](#)

- Service SNMP [B-58](#)
- Service SSH engine [B-59](#)
- Service TNS [B-59](#)
- State [8-20](#), [B-61](#)
- String [8-21](#), [8-24](#), [B-63](#)
- supported by IDM [8-2](#)
- Sweep [8-24](#), [B-68](#)
- Sweep Other TCP [B-70](#)
- Traffic Anomaly [B-71](#)
- Traffic ICMP [B-73](#)
- Trojan [B-74](#)
- signature engine update files described [21-4](#)
- Signature Event Action Filter
 - described [9-6](#), [A-26](#)
 - parameters [9-6](#), [A-26](#)
- Signature Event Action Handler described [9-7](#), [A-26](#)
- Signature Event Action Override described [9-6](#), [A-26](#)
- Signature Event Action Processor
 - Alarm Channel [9-6](#), [A-26](#)
 - components [9-6](#), [A-26](#)
 - described [9-6](#), [A-23](#), [A-26](#)
- signature fidelity rating
 - calculating risk rating [6-5](#), [9-3](#)
 - described [6-4](#), [9-3](#)
- signatures
 - adding [7-13](#)
 - alert frequency [7-19](#)
 - assigning actions [7-17](#)
 - cloning [7-15](#)
 - custom [7-4](#)
 - default [7-4](#)
 - described [7-4](#)
 - disabling [7-12](#)
 - editing [7-16](#)
 - enabling [7-12](#)
 - false positives [7-4](#)
 - rate limits [13-4](#)
 - retiring [7-12](#)
 - String TCP XL [7-30](#)
 - subsignatures [7-4](#)
 - TCP reset [C-50](#)
 - tuned [7-4](#)
 - tuning [7-16](#)
- Signatures window
 - field descriptions [3-16](#)
 - user roles [3-15](#)
- Signatures window described [3-16](#)
- signature threat profiles
 - applying [3-17](#)
 - platform support [3-16](#)
- signature update
 - IPS reloading messages [C-67](#), [C-73](#)
- signature updates
 - bypass mode [17-21](#)
 - files [21-4](#)
 - FTP server [17-25](#)
 - installation time [17-21](#)
 - SensorApp [17-21](#)
- signature variables
 - adding [7-33](#)
 - configuring [7-33](#)
 - deleting [7-33](#)
 - described [7-32](#)
 - editing [7-33](#)
- Signature Variables tab
 - configuring [7-33](#)
 - field descriptions [7-33](#)
- Signature Wizard
 - Alert Response window field descriptions [8-26](#)
 - Atomic IP Engine Parameters window field descriptions [8-13](#)
 - ICMP Traffic Type window field descriptions [8-12](#)
 - Inspect Data window field descriptions [8-12](#)
 - MSRPC Engine Parameters window field descriptions [8-11](#)
 - protocols [8-10](#)
 - Protocol Type window field descriptions [8-10](#)
 - Service HTTP Engine Parameters window field descriptions [8-16](#)

- Service RPC Engine Parameters window field descriptions [8-19](#)
- Service Type window field descriptions [8-12](#)
- signature identification [8-10](#)
- Signature Identification window field descriptions [8-11](#)
- State Engine Parameters window field descriptions [8-20](#)
- String ICMP Engine Parameters window field descriptions [8-21](#)
- String TCP Engine Parameters window field descriptions [8-21](#)
- String UDP Engine Parameters window field descriptions [8-24](#)
- Sweep Engine Parameters window field descriptions [8-25](#)
- TCP Sweep Type window field descriptions [8-13](#)
- TCP Traffic Type window field descriptions [8-12](#)
- UDP Sweep Type window field descriptions [8-12](#)
- UDP Traffic Type window field descriptions [8-12](#)
- Welcome window field descriptions [8-10](#)
- SNMP
 - configuring [15-2](#)
 - described [15-1](#)
 - General Configuration pane
 - field descriptions [15-2](#)
 - user roles [15-2](#)
 - Get [15-1](#)
 - GetNext [15-1](#)
 - Set [15-1](#)
 - supported MIBs [15-9, C-18](#)
 - Trap [15-1](#)
 - Traps Configuration pane
 - field descriptions [15-7](#)
 - user roles [15-7](#)
- SNMP General Configuration pane
 - configuring [15-2](#)
 - described [15-2](#)
- SNMP traps
 - configuring [15-8](#)
 - described [15-1](#)
- SNMPv3 protocol
 - described [15-4](#)
- SNMPv3 users
 - configuring [15-5](#)
- SNMPv3 Users pane
 - configuring [15-5](#)
 - described [15-4](#)
 - field descriptions [15-4](#)
- software architecture
 - ARC (illustration) [A-13](#)
 - IDAPI (illustration) [A-32](#)
- software downloads Cisco.com [21-1](#)
- software file names
 - recovery (illustration) [21-5](#)
 - signature/virus updates (illustration) [21-4](#)
 - system image (illustration) [21-5](#)
- software release examples
 - platform identifiers (table) [21-6](#)
 - table [21-5](#)
- software updates
 - supported FTP servers [17-20, 22-3](#)
 - supported HTTP/HTTPS servers [17-20, 22-3](#)
- SPAN port issues [C-29](#)
- SSH
 - described [12-1](#)
 - security [12-2](#)
- SSH Server
 - private keys [A-21](#)
 - public keys [A-21](#)
- standards
 - CIDEE [A-34](#)
 - IDCONF [A-33](#)
 - IDIOM [A-32](#)
 - SDEE [17-19, A-33](#)
- Startup Wizard
 - access lists [3-4](#)
 - adding ACLs [3-6](#)
 - adding virtual sensors [3-14](#)
 - Add Virtual Sensor dialog box [3-14](#)

- ASA 5500-X IPS SSP [3-2](#)
- ASA 5585-X IPS SSP [3-2](#)
- Auto Update configuring [3-18](#)
- described [3-1](#)
- Inline Interface Pair window
 - described [3-10](#)
 - field descriptions [3-10](#)
- Inline VLAN Pairs window configuring [3-12](#)
- Interface Selection window [3-10](#)
- Interface Summary window [3-8](#)
- Sensor Setup window
 - configuring [3-5](#)
 - described [3-4](#)
 - field descriptions [3-3, 3-4](#)
- Signatures window described [3-16](#)
- Traffic Inspection Mode window [3-10](#)
- Virtual Sensors window
 - field descriptions [3-13](#)
- Virtual Sensors window described [3-13](#)
- VLAN groups unsupported [3-1, 3-9](#)
- State engine
 - Cisco Login [8-20, B-61](#)
 - described [8-20, B-61](#)
 - LPR Format String [8-20, B-61](#)
 - parameters (table) [B-61](#)
 - SMTP [8-20, B-61](#)
- statistic display [C-82](#)
- Statistics pane
 - categories [18-21](#)
 - described [18-21](#)
 - using [18-22](#)
- statistics viewing [18-22](#)
- String engine described [8-21, 8-24, B-63](#)
- String ICMP engine parameters (table) [B-63](#)
- String TCP engine
 - custom signature [8-22](#)
 - example signature [8-22](#)
 - parameters (table) [B-63](#)
- String TCP XL signature (example) [7-27, 7-30](#)
- String UDP engine parameters (table) [B-64](#)
- String XL engine
 - description [B-65](#)
 - hardware support [8-3, B-3, B-65](#)
 - parameters (table) [B-66](#)
 - unsupported parameters [B-68](#)
- subinterface 0 described [5-14](#)
- subsignatures described [7-4](#)
- summarization
 - described [6-6, 9-5](#)
 - Fire All [6-7](#)
 - Fire Once [6-7, 9-6](#)
 - Global Summarization [6-7, 9-6](#)
 - global-summarization [9-6](#)
 - Meta engine [6-6, 9-5](#)
 - Summary [6-7, 9-6](#)
- Summarizer described [6-39, 9-35](#)
- Summary pane
 - button functions [5-14](#)
 - described [5-14](#)
 - field descriptions [3-9, 5-14](#)
- supported
 - FTP servers [17-20, 22-3](#)
 - HTTP/HTTPS servers [17-20, 22-3](#)
 - IDM platforms [1-3](#)
 - IPS interfaces for CSA MC [16-3](#)
- supported sensors
 - signature threat profiles [3-16](#)
- Sweep engine [8-25, B-69](#)
 - described [8-24, B-68](#)
 - parameters (table) [B-69](#)
- Sweep Other TCP engine
 - described [B-70](#)
 - parameters (table) [B-71](#)
- SwitchApp
 - described [A-29](#)
 - IPS 4510 [A-29](#)
 - IPS 4520 [A-29](#)
 - IPS 4520-XL [A-29](#)

switches

- TCP reset interfaces [5-7](#)

sw-module module slot_number password-reset command [17-6, C-10](#)

system architecture

- directory structure [A-34](#)

- supported platforms [A-1](#)

system clock setting [4-16](#)

system components IDAPI [A-32](#)

System Configuration Dialog

- described [20-2](#)

- example [20-2](#)

system design (illustration) [A-2, A-3](#)

system images

installing

- ASA 5500-X IPS SSP [22-23](#)

- IPS 4345 [22-17](#)

- IPS 4360 [22-17](#)

- IPS 4510 [22-20](#)

- IPS 4520 [22-20](#)

- IPS 4520-XL [22-20](#)

System Information pane

- described [18-22](#)

- using [18-23](#)

system information viewing [18-23](#)

system requirements for IDM [1-2](#)

T

TAC

- contact information [18-22](#)

- service account [4-18, A-31, C-5](#)

- show tech-support command [C-75](#)

- troubleshooting [A-31](#)

target value rating

- calculating risk rating [6-5, 9-3](#)

- described [6-5, 6-24, 6-26, 9-3, 9-20, 9-22](#)

TCP fragmentation described [B-38](#)

TCP Protocol tab

- described [10-16, 10-23, 10-29](#)

- enabling TCP [10-16](#)

- external zone [10-29](#)

- field descriptions [10-16](#)

- illegal zone [10-23](#)

TCP reset interfaces

- conditions [5-7](#)

- described [5-6](#)

- list [5-7](#)

- promiscuous mode [5-7](#)

- switches [5-7](#)

TCP resets

- not occurring [C-50](#)

TCP stream reassembly

- described [7-48](#)

- parameters (table) [7-49](#)

- signatures (table) [7-49](#)

TCP stream reassembly mode [7-54](#)

tech support information display [C-76](#)

terminal server setup [19-3, 22-16](#)

TFN2K

- described [B-73](#)

- Trojans [B-74](#)

TFTP servers

- maximum file size limitation [22-16](#)

- RTT [22-16](#)

Threat Category tab

- described [6-38, 9-34](#)

- field descriptions [6-38, 9-34](#)

threat rating

- described [6-6, 9-4](#)

- risk rating [6-6, 9-4](#)

Thresholds for KB Name window

- described [18-10](#)

- field descriptions [18-10](#)

- filtering information [18-10](#)

time

- correction on the sensor [4-12, C-16](#)

- sensors [4-8, C-15](#)
- synchronizing IPS clocks [4-8, C-15](#)
- Time pane
 - configuring [4-11](#)
 - described [4-7](#)
 - field descriptions [4-9](#)
 - user roles [4-7](#)
- time sources
 - appliances [4-8, C-15](#)
 - ASA 5500-X IPS SSP [4-8, C-15](#)
 - ASA 5585-X IPS SSP [4-8, C-15](#)
- TLS
 - described [4-4](#)
 - handshaking [1-7, 12-11](#)
 - IDM [1-7, 12-11](#)
 - web server [1-7, 12-11](#)
- Top Applications gadget
 - configuring [2-10](#)
 - described [2-10](#)
- Traffic Anomaly engine
 - described [B-71](#)
 - protocols [B-71](#)
 - signatures [B-71](#)
- traffic flow notifications
 - configuring [5-26](#)
 - described [5-26](#)
- Traffic Flow Notifications pane
 - configuring [5-26](#)
 - field descriptions [5-26](#)
 - user roles [5-26](#)
- Traffic ICMP engine
 - DDoS [B-73](#)
 - described [B-73](#)
 - LOKI [B-73](#)
 - parameters (table) [B-74](#)
 - TFN2K [B-73](#)
- Traffic Inspection Mode window described [3-10](#)
- Traps Configuration pane
 - configuring [15-8](#)
- described [15-7](#)
- trial license key [1-8, 17-12](#)
- Tribe Flood Network. See TFN.
- Tribe Flood Network 2000. See TFN2K.
- Trojan engine
 - BO2K [B-74](#)
 - described [B-74](#)
 - TFN2K [B-74](#)
- Trojans
 - BO [B-74](#)
 - BO2K [B-74](#)
 - LOKI [B-74](#)
 - TFN2K [B-74](#)
- troubleshooting
 - Analysis Engine busy [C-55](#)
 - applying software updates [C-52](#)
 - ARC
 - blocking not occurring for signature [C-41](#)
 - device access issues [C-39](#)
 - enabling SSH [C-41](#)
 - inactive state [C-37](#)
 - misconfigured master blocking sensor [C-42](#)
 - verifying device interfaces [C-40](#)
 - ASA 5500-X IPS SSP
 - commands [C-58](#)
 - failover scenarios [C-57](#)
 - ASA 5585-X IPS SSP
 - commands [C-69](#)
 - failover scenarios [C-68](#)
 - traffic flow stopped [C-69](#)
 - automatic updates [C-52](#)
 - cannot access sensor [C-24](#)
 - cidDump [C-99](#)
 - cidLog messages to syslog [C-49](#)
 - communication [C-23](#)
 - corrupted SensorApp configuration [C-34](#)
 - debug logger zone names (table) [C-48](#)
 - debug logging [C-44](#)
 - disaster recovery [C-6](#)

- duplicate sensor IP addresses [C-26](#)
- enabling debug logging [C-44](#)
- external product interfaces [16-10, C-22](#)
- gathering information [C-74](#)
- global correlation [11-11, C-20](#)
- IDM
 - cannot access sensor [C-55](#)
 - will not load [C-54](#)
- IPS clock time drift [4-8, C-15](#)
- misconfigured access list [C-26](#)
- no alerts [C-31, C-56](#)
- password recovery [17-10, C-14](#)
- physical connectivity issues [C-29](#)
- preventive maintenance [C-2](#)
- RADIUS
 - attempt limit [C-20](#)
- reset not occurring for a signature [C-50](#)
- sensing process not running [C-28](#)
- sensor events [C-95](#)
- sensor loose connections [C-22](#)
- sensor not seeing packets [C-33](#)
- sensor software upgrade [C-53](#)
- service account [4-18, C-5](#)
- show events command [C-95](#)
- show interfaces command [C-94](#)
- show statistics command [C-81](#)
- show tech-support command [C-75, C-76](#)
- show version command [C-78](#)
- software upgrades [C-51](#)
- SPAN port issue [C-29](#)
- upgrading [C-51](#)
- verifying Analysis Engine is running [C-19](#)
- verifying ARC status [C-36](#)

Trusted Hosts pane

- configuring [12-13](#)
- described [12-12](#)
- field descriptions [12-13](#)

tuned signatures described [7-4](#)

- tuning
 - AIC signatures [7-44](#)
 - IP fragment reassembly signatures [7-48](#)
 - signatures [7-16](#)
 - TCP fragment reassembly signatures [7-55](#)

U

UDP Protocol tab

- described [10-17, 10-23, 10-24, 10-29](#)
- enabling UDP [10-17](#)
- external zone [10-29](#)
- field descriptions [10-30](#)
- illegal zone [10-23, 10-24](#)

unassigned VLAN groups described [5-14](#)

unauthenticated NTP [4-8, 4-14, C-15](#)

uninstalling

- license key [17-15](#)

UNIX-style directory listings [17-21](#)

unlocking accounts [4-26](#)

unlock user username command [4-26](#)

Update Sensor pane

- configuring [17-26](#)
- described [17-25](#)
- field descriptions [17-25](#)
- user roles [17-25](#)

updating

- Home pane [1-4](#)

- sensors [17-26](#)

updating the sensor immediately [22-12](#)

upgrade command [22-5, 22-7](#)

upgrade notes and caveats

- upgrading IPS software [22-1](#)

upgrading

- application partition [22-14](#)

- latest version [C-51](#)

- recovery partition [22-7](#)

- sensors [22-5](#)

- upgrading IPS software
 - upgrade notes and caveats [22-1](#)
 - uploading KBs
 - FTP [18-16](#)
 - SCP [18-16](#)
 - Upload Knowledge Base to Sensor dialog box
 - described [18-16](#)
 - field descriptions [18-16](#)
 - URLs for Cisco Security Intelligence Operations [21-7](#)
 - user roles authentication [4-19](#)
 - users
 - configuring [4-23](#)
 - using
 - debug logging [C-44](#)
 - TCP reset interfaces [5-7](#)
-
- V**
- VACLs
 - described [13-2](#)
 - Post-Block [13-21](#)
 - Pre-Block [13-21](#)
 - verifying
 - NTP configuration [4-9](#)
 - password recovery [17-11, C-14](#)
 - sensor initialization [20-21](#)
 - sensor setup [20-21](#)
 - version display [C-79](#)
 - viewing
 - denied attacker hit counts [14-2](#)
 - denied attackers list [14-2](#)
 - IP logs [14-12](#)
 - license key status [1-8, 17-12](#)
 - statistics [18-22](#)
 - system information [18-23](#)
 - virtualization
 - advantages [6-3, C-17](#)
 - restrictions [6-3, C-17](#)
 - supported sensors [C-17](#)
 - traffic capture requirements [6-3, C-17](#)
 - virtual-sensor name command [6-14](#)
 - virtual sensors
 - adding [3-14, 6-11](#)
 - adding (ASA 5500-X IPS SSP) [6-15](#)
 - adding (ASA 5585-X IPS SSP) [6-15](#)
 - ASA 5500-X IPS SSP [6-16](#)
 - ASA 5585-X IPS SSP [6-16](#)
 - creating (ASA 5500-X IPS SSP) [6-15](#)
 - creating (ASA 5585-X IPS SSP) [6-15](#)
 - default virtual sensor [6-2, 6-7](#)
 - deleting [6-11](#)
 - described [6-2, 6-7](#)
 - editing [6-11](#)
 - options [6-14](#)
 - Virtual Sensors window
 - described [3-13](#)
 - VLAN groups
 - 802.1q encapsulation [5-14](#)
 - configuration restrictions [5-9](#)
 - configuring [5-24](#)
 - deploying [5-23](#)
 - switches [5-23](#)
 - VLAN IDs [5-22](#)
 - VLAN groups mode
 - described [5-13](#)
 - VLAN Groups pane
 - configuring [5-24](#)
 - described [5-22](#)
 - field descriptions [5-23](#)
 - user roles [5-22](#)
 - VLAN Pairs pane
 - configuring [5-21](#)
 - described [5-20](#)
 - field descriptions [5-20](#)
 - user roles [5-20](#)
 - vulnerable OSeS field described [B-6](#)

W

watch list rating

calculating risk rating [6-5, 9-3](#)

described [6-5, 9-3](#)

web server

described [A-4, A-22](#)

HTTP 1.0 and 1.1 support [A-22](#)

private keys [A-21](#)

public keys [A-21](#)

SDEE support [A-22](#)

TLS [1-7, 12-11](#)

worms

Blaster [10-2](#)

Code Red [10-2](#)

histograms [10-13, 18-8](#)

Nimble [10-2](#)

protocols [10-3](#)

Sasser [10-2](#)

scanners [10-3](#)

Slammer [10-2](#)

SQL Slammer [10-2](#)

Z

zones

external [10-5](#)

illegal [10-5](#)

internal [10-5](#)