



Numerics

802.1q encapsulation for VLAN groups [7-14](#)

A

AAA RADIUS

functionality [6-19](#)

limitations [6-19](#)

accessing

IPS software [25-2](#)

service account [6-18, C-5](#)

access list misconfiguration [C-27](#)

access lists

necessary hosts [5-3](#)

Startup Wizard [5-3](#)

account locking

configuring [6-25](#)

security [6-25](#)

account unlocking configuring [6-26](#)

ACLs

adding [5-6](#)

described [15-3](#)

Post-Block [15-17, 15-18](#)

Pre-Block [15-17, 15-18](#)

ad0 pane

default [12-10](#)

described [12-10](#)

tabs [12-10](#)

Add/Update Trusted Root Certificate dialog box

field descriptions [14-15](#)

Add ACL Entry dialog box field descriptions [5-3](#)

Add Allowed Host dialog box

field descriptions [6-6](#)

user roles [6-6](#)

Add Authorized RSA1 Key dialog box

field descriptions [14-5](#)

user roles [14-4](#)

Add Authorized RSA Key dialog box

field descriptions [14-3](#)

user roles [14-2](#)

Add Blocking Device dialog box

field descriptions [15-15](#)

user roles [15-14](#)

Add Cat 6K Blocking Device Interface dialog box

field descriptions [15-22](#)

user roles [15-21](#)

Add Configured OS Map dialog box

field descriptions [8-31, 11-26](#)

user roles [8-30, 11-23](#)

Add Destination Port dialog box

field descriptions [12-17, 12-23, 12-30](#)

user roles [12-15](#)

Add Device dialog box field descriptions [2-3](#)

Add Device Login Profile dialog box

field descriptions [15-12](#)

user roles [15-12](#)

Add Event Action Filter dialog box

field descriptions [8-21, 11-16](#)

user roles [11-15](#)

Add Event Action Override dialog box

field descriptions [8-12, 11-13](#)

user roles [8-12, 11-13](#)

Add Event Variable dialog box

field descriptions [8-34, 11-29](#)

- user roles [8-33, 11-28](#)
- Add External Product Interface dialog box
 - field descriptions [18-6](#)
 - user roles [18-4](#)
- Add Filter dialog box
 - field descriptions [3-19, 21-3](#)
- Add Histogram dialog box
 - field descriptions [12-17, 12-24, 12-30](#)
 - user roles [12-15](#)
- Add Host Block dialog box field descriptions [16-4](#)
- adding
 - ACLs [5-6](#)
 - a host never to be blocked [15-11](#)
 - anomaly detection policies [12-10](#)
 - blocking devices [15-15](#)
 - CSA MC interfaces [18-7](#)
 - denied attackers [16-2](#)
 - event action filters [8-22, 11-17](#)
 - event action overrides [11-14](#)
 - event action rules policies [11-12](#)
 - event variables [8-35, 11-29](#)
 - external product interfaces [18-7](#)
 - host blocks [16-4](#)
 - IPv4 target value ratings [8-25, 11-20](#)
 - IPv6 target value ratings [8-27, 11-22](#)
 - network blocks [16-7](#)
 - OS maps [8-32, 11-27](#)
 - rate limiting devices [15-15](#)
 - rate limits [16-9](#)
 - risk categories [8-37, 11-32](#)
 - signature definition policies [9-10](#)
 - signatures [9-21](#)
 - signature variables [9-41](#)
 - trusted root certificates [14-15](#)
 - virtual sensors [5-14, 8-12](#)
 - virtual sensors (ASA 5500-X IPS SSP) [8-16](#)
 - virtual sensors (ASA 5585-X IPS SSP) [8-16](#)
- Add Inline VLAN Pair dialog box
 - field descriptions [7-27](#)
 - user roles [7-26](#)
- Add Inline VLAN Pair Entry dialog box field descriptions [5-11](#)
- Add Interface Pair dialog box
 - field descriptions [7-25](#)
 - user roles [7-24](#)
- Add IP Logging dialog box field descriptions [16-11](#)
- Add Known Host RSA1 Key dialog box
 - field descriptions [14-9](#)
 - user roles [14-8](#)
- Add Known Host RSA Key dialog box
 - field descriptions [14-7](#)
 - user roles [14-6](#)
- Add Master Blocking Sensor dialog box
 - field descriptions [15-25](#)
 - user roles [15-24](#)
- Add Network Block dialog box field descriptions [16-6](#)
- Add Never Block Address dialog box
 - field descriptions [15-10](#)
 - user roles [15-7](#)
- Add Policy dialog box
 - field descriptions [9-9, 11-12, 12-9](#)
 - user roles [9-8, 11-11, 12-9](#)
- Add Posture ACL dialog box field descriptions [18-7](#)
- Add Protocol Number dialog box field descriptions [12-18, 12-25, 12-32](#)
- Add Rate Limit dialog box
 - field descriptions [16-8](#)
 - user role [16-7](#)
- Address Resolution Protocol. See ARP.
- Add Risk Level dialog box
 - field descriptions [8-37, 11-31](#)
 - user roles [8-36, 11-31](#)
- Add Router Blocking Device Interface dialog box
 - field descriptions [15-19](#)
 - user roles [15-17](#)
- Add Signature dialog box field descriptions [9-14](#)
- Add Signature Variable dialog box
 - field descriptions [9-40](#)

- user roles [9-40](#)
- Add SNMP Trap Destination dialog box field descriptions [17-8](#)
- Add SNMPv3 User dialog box
 - field descriptions [17-5](#)
- Add Start Time dialog box
 - field descriptions [12-14](#)
 - user roles [12-12](#)
- Add Target Value Rating dialog box
 - field descriptions [8-25, 8-27](#)
 - user roles [8-25, 8-26](#)
- Add Trusted Host dialog box
 - field descriptions [14-13](#)
 - user roles [14-13](#)
- Add User dialog box
 - field descriptions [6-22](#)
 - user roles [6-19, 6-22](#)
- Add Virtual Sensor dialog box
 - described [5-13, 8-10](#)
 - field descriptions [5-14, 8-10](#)
 - user roles [8-9](#)
- Add VLAN Group dialog box
 - field descriptions [7-29](#)
 - user roles [7-28](#)
- Advanced Alert Behavior Wizard
 - Alert Dynamic Response Fire All window field descriptions [10-27](#)
 - Alert Dynamic Response Fire Once window field descriptions [10-28](#)
 - Alert Dynamic Response Summary window field descriptions [10-28](#)
 - Alert Summarization window field descriptions [10-27](#)
 - Event Count and Interval window field descriptions [10-26](#)
 - Global Summarization window field descriptions [10-29](#)
- aggregation
 - alert frequency [8-7, 11-5](#)
 - operating modes [8-7, 11-5](#)
- AIC
 - policy [9-52](#)
 - signatures (example) [9-52](#)
- AIC engine
 - AIC FTP [B-11](#)
 - AIC FTP engine parameters (table) [B-12](#)
 - AIC HTTP [B-11](#)
 - AIC HTTP engine parameters (table) [B-12](#)
 - described [B-11](#)
 - features [B-11](#)
 - signature categories [9-44](#)
- AIC policy enforcement
 - default configuration [9-45, B-11](#)
 - described [9-45, B-11](#)
 - sensor oversubscription [9-45, B-11](#)
- Alarm Channel
 - described [11-6, A-26](#)
 - risk rating [13-5](#)
- alert and log actions (list) [9-2, 9-16, 11-7](#)
- alert behavior
 - Custom Signature Wizard [10-26](#)
 - normal [10-26](#)
- alert frequency
 - aggregation [9-27](#)
 - configuring [9-27](#)
 - controlling [9-27](#)
 - modes [B-7](#)
- allocate-ips command [8-15](#)
- Allowed Hosts/Networks pane
 - configuring [6-6](#)
 - described [6-6](#)
 - field descriptions [6-6](#)
- alternate TCP reset interface
 - configuration restrictions [7-9](#)
 - designating [7-7](#)
 - restrictions [7-2](#)
- Analysis Engine
 - described [8-2](#)
 - error messages [C-24](#)

- errors [C-52](#)
- IDM exits [C-56](#)
- sensing interfaces [7-3](#)
- verify it is running [C-20](#)
- virtual sensors [8-2](#)
- anomaly detection
 - asymmetric traffic [12-2](#)
 - caution [12-2](#)
 - configuration sequence [12-5](#)
 - default anomaly detection configuration [12-4](#)
 - default configuration (example) [12-4](#)
 - described [12-2](#)
 - detect mode [12-4](#)
 - enabling [12-4](#)
 - event actions [12-7, B-70](#)
 - inactive mode [12-4](#)
 - learning accept mode [12-3](#)
 - learning process [12-3](#)
 - limiting false positives [12-13, 20-8](#)
 - operation settings [12-11](#)
 - protocols [12-3](#)
 - signatures (table) [12-7, B-70](#)
 - signatures described [12-7](#)
 - worms
 - attacks [12-13, 20-8](#)
 - described [12-3](#)
 - zones [12-5](#)
- anomaly detection disabling [12-35, C-19](#)
- Anomaly Detection pane
 - button functions [20-9](#)
 - described [20-7](#)
 - field descriptions [20-9](#)
 - user roles [20-7](#)
- anomaly detection policies
 - ad0 [12-9](#)
 - adding [12-10](#)
 - cloning [12-10](#)
 - default policy [12-9](#)
 - deleting [12-10](#)
- Anomaly Detections pane
 - described [12-9](#)
 - field descriptions [12-9](#)
 - user roles [12-9](#)
- appliances
 - GRUB menu [19-5, C-8](#)
 - initializing [24-7](#)
 - logging in [23-2](#)
 - password recovery [19-5, C-8](#)
 - setting system clock [6-16](#)
 - terminal servers
 - described [23-3, 26-16](#)
 - setting up [23-3, 26-16](#)
 - time sources [6-11, C-15](#)
 - upgrading recovery partition [26-7](#)
- Application Inspection and Control. See AIC.
- application partition
 - described [A-4](#)
 - image recovery [26-14](#)
- application policy enforcement described [9-45, B-11](#)
- applications in XML format [A-4](#)
- applying
 - threat profiles [9-19](#)
- applying signature threat profiles [5-17](#)
- applying software updates [C-53](#)
- ARC
 - ACLs [15-18, A-14](#)
 - authentication [A-15](#)
 - blocking
 - connection-based [A-17](#)
 - response [A-13](#)
 - unconditional blocking [A-17](#)
 - blocking application [15-2](#)
 - blocking not occurring for signature [C-42](#)
- Catalyst switches
 - VACL commands [A-19](#)
 - VACLs [A-16, A-19](#)
 - VLANs [A-16](#)
- checking status [15-3, 15-4](#)

- described [A-4](#)
- design [15-2](#)
- device access issues [C-40](#)
- enabling SSH [C-42](#)
- 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 [15-1](#)
- functions [15-2](#)
- illustration [A-13](#)
- inactive state [C-38](#)
- interfaces [A-14](#)
- maintaining states [A-16](#)
- managed devices [15-7](#)
- master blocking sensors [A-14](#)
- maximum blocks [15-2](#)
- misconfigured master blocking sensor [C-43](#)
- nac.shun.txt file [A-16](#)
- NAT addressing [A-15](#)
- number of blocks [A-15](#)
- postblock ACL [A-16](#)
- preblock ACL [A-16](#)
- prerequisites [15-5](#)
- rate limiting [15-4](#)
- responsibilities [A-13](#)
- single point of control [A-15](#)
- SSH [A-14](#)
- supported devices [15-5, A-15](#)
- Telnet [A-14](#)
- troubleshooting [C-36](#)
- VACLs [A-14](#)
- verifying device interfaces [C-41](#)
- verifying status [C-37](#)
- 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 [8-18](#)
 - creating virtual sensors [8-16](#)
 - initializing [24-13](#)
 - IPS reloading messages [C-69, C-75](#)
 - logging in [23-4](#)
 - memory usage [19-17, C-68](#)
 - memory usage values (table) [19-17, C-68](#)
 - no CDP mode support [7-33](#)
 - Normalizer engine [B-36, C-67, C-74](#)
 - password recovery [19-6, C-10](#)
 - resetting the password [19-7, C-10](#)
 - sensing interface [8-15](#)
 - session command [23-4](#)
 - sessioning in [23-4](#)
 - setup command [24-13](#)
 - TCP reset differences [9-5, 9-19, 11-10](#)
 - time sources [5-12, 6-11, C-15](#)
 - virtual sensors
 - assigning policies [8-16](#)
 - assigning the interface [8-16](#)
 - virtual sensor sequence [8-15](#)
- ASA 5585-X IPS SSP
 - assigning virtual sensors [8-18](#)
 - creating virtual sensors [8-16](#)
 - initializing [24-17](#)
 - installing system image [26-24](#)
 - IPS reloading messages [C-69, C-75](#)
 - logging in [23-5](#)
 - no CDP mode support [7-33](#)
 - Normalizer engine [B-36, C-67, C-74](#)
 - password recovery [19-8, C-12](#)

- resetting the password [19-9, C-12](#)
- session command [23-5](#)
- sessioning in [23-5](#)
- setup command [24-17](#)
- TCP reset differences [9-5, 9-19, 11-10](#)
- time sources [5-12, 6-11, C-15](#)
- virtual sensors
 - assigning policies [8-16](#)
 - assigning the interface [8-16](#)
 - sequence [8-15](#)
- ASA IPS modules
 - jumbo packet count [C-69, C-75](#)
- ASDM
 - resetting passwords [19-8, 19-10, C-11, C-13](#)
- assigning
 - interfaces to virtual sensors (ASA 5500 AIP SSM) [8-16](#)
 - interfaces to virtual sensors (ASA 5500-X IPS SSP) [8-16](#)
 - interfaces to virtual sensors (ASA 5585-X IPS SSP) [8-16](#)
 - policies to virtual sensors (ASA 5500 AIP SSM) [8-16](#)
 - policies to virtual sensors (ASA 5500-X IPS SSP) [8-16](#)
 - policies to virtual sensors (ASA 5585-X IPS SSP) [8-16](#)
- assigning actions to signatures [9-25](#)
- asymmetric mode
 - described [8-4](#)
 - normalization [8-4](#)
- asymmetric traffic
 - anomaly detection [12-2](#)
 - caution [12-2](#)
- asymmetric traffic and disabling anomaly detection [12-35, C-19](#)
- Atomic ARP engine
 - described [B-13](#)
 - parameters (table) [B-13](#)
- Atomic IP Advanced engine
 - described [B-14](#)
- parameters (table) [B-16](#)
- restrictions [B-15](#)
- Atomic IP engine
 - described [10-13, B-24](#)
 - parameters (table) [B-24](#)
- Atomic IPv6 engine
 - described [B-27](#)
 - Neighborhood Discovery protocol [B-28](#)
 - signatures [B-28](#)
- attack relevance rating
 - calculating risk rating [8-6, 11-3](#)
 - described [8-6, 8-29, 11-3, 11-24](#)
- 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 [8-6, 11-3](#)
 - described [8-6, 11-3](#)
- Attacks Over Time gadgets
 - configuring [3-13](#)
 - described [3-13](#)
- Attacks Over Time Reports described [1-15, 22-2](#)
- attempt limit
 - RADIUS [C-21](#)
- attemptLimit command [6-25](#)
- audit mode
 - described [13-8](#)
 - testing global correlation [13-8](#)
- authenticated NTP [6-11, 6-14, C-15](#)
- authentication
 - local [6-19](#)
 - RADIUS [6-19](#)
- 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 [6-23](#)
 - described [6-19](#)
 - field descriptions [6-20](#)
 - user roles [6-17, A-30](#)
- Authorized RSA1 Keys pane
 - configuring [14-5](#)
 - described [14-4](#)
 - field descriptions [14-4](#)
 - RSA authentication [14-4](#)
 - RSA key generation tool [14-5](#)
- Authorized RSA Keys pane
 - configuring [14-3](#)
 - described [14-2](#)
 - field descriptions [14-2](#)
 - RSA authentication [14-2](#)
 - RSA key generation tool [14-3](#)
- Auto/Cisco.com Update pane
 - configuring [19-23](#)
 - described [5-17, 19-20](#)
 - field descriptions [19-22](#)
 - UNIX-style directory listings [19-21](#)
 - user roles [19-18, 19-20](#)
- automatic reporting configuring (IME) [1-16](#)
- automatic setup [24-2](#)
- automatic updates
 - Cisco.com [5-17, 19-20](#)
 - configuring [5-18, 19-23](#)
 - cryptographic account [5-17, 19-20](#)
 - FTP servers [19-20](#)
 - immediate [26-12](#)
 - SCP servers [5-17, 19-20](#)
- automatic upgrade
 - information required [26-8](#)
 - troubleshooting [C-53](#)
- autoupdatenow command [26-11](#)
- Auto Update window field descriptions [5-18](#)

- auto-upgrade-option command [26-8](#)

B

- backing up
 - configuration [C-2](#)
 - current configuration [C-4](#)
- BackOrifice. See BO.
- BackOrifice 2000. See BO2K.
- basic setup [24-4](#)
- blocking
 - described [15-2](#)
 - disabling [15-8](#)
 - master blocking sensor [15-24](#)
 - necessary information [15-3](#)
 - prerequisites [15-5](#)
 - supported devices [15-5](#)
 - types [15-2](#)
- blocking devices
 - adding [15-15](#)
 - deleting [15-15](#)
 - editing [15-15](#)
- Blocking Devices pane
 - configuring [15-15](#)
 - described [15-14](#)
 - field descriptions [15-14](#)
 - ssh host-key command [15-15](#)
- blocking not occurring for signature [C-42](#)
- Blocking Properties pane
 - adding a host never to be blocked [15-11](#)
 - configuring [15-9](#)
 - described [15-7](#)
 - field descriptions [15-8](#)
- BO
 - described [B-72](#)
 - Trojans [B-72](#)
- BO2K
 - described [B-72](#)
 - Trojans [B-72](#)

BST

- described [C-1](#)

- URL [C-1](#)

Bug Search Tool. See BST.

bypass mode

- described [7-31](#)

- signature updates [19-22](#)

Bypass pane

- field descriptions [7-32](#)

- user roles [7-31](#)

C

calculating risk rating

- attack relevance rating [8-6, 11-3](#)

- attack severity rating [8-6, 11-3](#)

- promiscuous delta [8-6, 11-3](#)

- signature fidelity rating [8-5, 11-3](#)

- target value rating [8-6, 11-3](#)

- watch list rating [8-6, 11-3](#)

cannot access sensor [C-25](#)

Cat 6K Blocking Device Interfaces pane

- configuring [15-23](#)

- described [15-21](#)

- field descriptions [15-22](#)

CDP mode

- ASA 5500-X IPS SSP [7-33](#)

- ASA 5585-X IPS SSP [7-33](#)

- described [7-33](#)

- interfaces [7-33](#)

CDP Mode pane

- configuring [7-33](#)

- field descriptions [7-33](#)

- user roles [7-33](#)

certificates

- displaying [14-16](#)

- generating [14-16](#)

certificates (IDM) [14-11](#)

changing

- threat profiles [9-19](#)

changing Microsoft IIS to UNIX-style directory listings [19-21](#)

cidDump obtaining information [C-103](#)

CIDEE

- defined [A-34](#)

- example [A-34](#)

- IPS extensions [A-34](#)

- protocol [A-34](#)

- supported IPS events [A-34](#)

cisco

- default password [23-2](#)

- default username [23-2](#)

Cisco.com

- accessing software [25-2](#)

- downloading software [25-1](#)

- software downloads [25-1](#)

Cisco Bug Search Tool

- described [C-1](#)

Cisco Discovery Protocol. See CDP.

Cisco IOS rate limiting [15-4](#)

Cisco Security Intelligence Operations

- described [25-7](#)

- URL [25-7](#)

Cisco Services for IPS

- service contract [19-13](#)

- supported products [19-13](#)

clear events command [6-12, 6-16, 20-4, C-17, C-103](#)

Clear Flow States pane

- described [20-22](#)

- field descriptions [20-22](#)

clearing

- denied attackers [16-2](#)

- events [6-16, 20-4, C-103](#)

- flow states [20-23](#)

- statistics [C-86](#)

CLI

- described [A-4, A-30](#)

- password recovery [19-10, C-14](#)
- client manifest described [A-28](#)
- clock set command [6-16](#)
- Clone Policy dialog box
 - field descriptions [9-9, 11-12, 12-9](#)
 - user roles [9-8, 11-11, 12-9](#)
- Clone Signature dialog box field descriptions [9-14](#)
- cloning
 - anomaly detection policies [12-10](#)
 - event action rules policies [11-12](#)
 - signature definition policies [9-10](#)
 - signatures [9-23](#)
- CollaborationApp described [A-4, A-27](#)
- color rules
 - described [21-2](#)
 - events (IME) [21-2](#)
- Color Rules tab
 - described [21-2](#)
 - filters [21-2](#)
- command and control interface
 - described [7-2](#)
 - list [7-2](#)
- commands
 - allocate-ips [8-15](#)
 - attemptLimit [6-25](#)
 - autoupdatenow [26-11](#)
 - auto-upgrade-option [26-8](#)
 - clear events [6-12, 6-16, 20-4, C-17, C-103](#)
 - clock set [6-16](#)
 - copy backup-config [C-3](#)
 - copy current-config [C-3](#)
 - downgrade [26-12](#)
 - erase license-key [19-15](#)
 - hw-module module slot_number password-reset [19-8, C-12](#)
 - setup [6-1, 24-1, 24-4, 24-7, 24-13, 24-17](#)
 - show events [C-99](#)
 - show health [C-76](#)
 - show module 1 details [C-60, C-71](#)
 - show settings [19-11, C-14](#)
 - show statistics [C-85](#)
 - show statistics virtual-sensor [C-24, C-85](#)
 - show tech-support [C-77](#)
 - show version [C-82](#)
 - sw-module module slot_number password-reset [19-7, C-10](#)
 - unlock user username [6-26](#)
 - upgrade [26-4, 26-7](#)
 - virtual-sensor name [8-16](#)
- Compare Knowledge Bases dialog box field descriptions [20-11](#)
- comparing KBs [20-11, 20-12](#)
- configuration files
 - backing up [C-2](#)
 - merging [C-2](#)
- configuration restrictions
 - alternate TCP reset interface [7-9](#)
 - inline interface pairs [7-8](#)
 - inline VLAN pairs [7-8](#)
 - interfaces [7-8](#)
 - physical interfaces [7-8](#)
 - VLAN groups [7-9](#)
- Configure Summertime dialog box field descriptions [5-5, 6-8](#)
- configuring
 - account locking [6-25](#)
 - account unlocking [6-26](#)
 - AIC policy parameters [9-52](#)
 - allowed hosts [6-6](#)
 - allowed networks [6-6](#)
 - anomaly detection operation settings [12-11](#)
 - application policy signatures [9-52](#)
 - Attacks Over Time gadgets [3-13](#)
 - authorized keys [14-5](#)
 - authorized RSA keys [14-3](#)
 - automatic updates [5-18, 19-23](#)
 - automatic upgrades [26-10](#)
 - blocking devices [15-15](#)
 - blocking properties [15-9](#)

- Cat 6K blocking device interfaces [15-23](#)
- CDP mode [7-33](#)
- CSA MC IPS interfaces [18-3](#)
- device login profiles [15-13](#)
- event action filters [8-22, 11-17](#)
- events [20-3](#)
- event variables [8-35, 11-29](#)
- external zone [12-32](#)
- general settings [8-40, 11-34](#)
- Global Correlation Health gadget [3-8](#)
- Global Correlation Reports gadget [3-6](#)
- host blocks [16-4](#)
- illegal zone [12-25](#)
- inline VLAN pairs [5-11](#)
- inspection/reputation [13-9](#)
- inspection load statistics display [20-5](#)
- interface pairs [7-25](#)
- interfaces [7-19](#)
- interface statistics display [20-6](#)
- Interface Status gadget [3-6](#)
- internal zone [12-19](#)
- IP fragment reassembly signatures [9-56](#)
- IP logging [16-12](#)
- IPv4 target value ratings [8-25, 11-20](#)
- IPv6 target value ratings [8-27, 11-22](#)
- known host RSA1 keys [14-9](#)
- known host RSA keys [14-7](#)
- learning accept mode [12-14](#)
- Licensing gadget [3-5](#)
- local authentication [6-23](#)
- master blocking sensor [15-25](#)
- Memory & Load gadget [3-11](#)
- network blocks [16-7](#)
- network participation [13-11](#)
- Network Security gadget [3-9](#)
- network settings [6-3](#)
- NTP servers [6-13](#)
- OS maps [8-32, 11-27](#)
- RADIUS authentication [6-23](#)
- rate limiting [16-9](#)
- rate limiting device interfaces [15-20](#)
- risk categories [8-37, 11-32](#)
- router blocking device interfaces [15-20](#)
- RSS Feed gadgets [3-11](#)
- RSS feeds [4-2](#)
- Sensor Health gadget [3-4](#)
- Sensor Information gadget [3-3](#)
- Sensor Setup window [5-5](#)
- sensor to use NTP [6-14](#)
- signature variables [9-41](#)
- SNMP [17-3](#)
- SNMP traps [17-8](#)
- SNMPv3 users [17-6](#)
- time [6-9](#)
- Top Applications gadget [3-9](#)
- Top Attackers gadgets [3-12](#)
- Top Signatures gadgets [3-13](#)
- Top Victims gadgets [3-12](#)
- traffic flow notifications [7-32](#)
- trusted hosts [14-13](#)
- upgrades [26-5](#)
- users [6-23](#)
- VLAN groups [7-30](#)
- VLAN pairs [7-27](#)
- control transactions
 - characteristics [A-9](#)
 - request types [A-8](#)
- copy backup-config command [C-3](#)
- copy current-config command [C-3](#)
- correcting time on the sensor [6-12, C-17](#)
- creating
 - Atomic IP Advanced engine signature [9-33, 10-14](#)
 - custom signatures
 - not using signature engines [10-4](#)
 - Service HTTP [10-17](#)
 - String TCP [10-22](#)
 - using signature engines [10-1](#)
 - event views [21-4](#)

- IPv6 signatures [9-33, 10-14](#)
 - Meta signatures [9-30](#)
 - Post-Block VACLs [15-21](#)
 - Pre-Block VACLs [15-21](#)
 - reports (IME) [22-3](#)
 - String TCP XL signatures [9-38](#)
 - creating the service account [C-6](#)
 - cryptographic account
 - automatic updates [5-17, 19-20](#)
 - Encryption Software Export Distribution Authorization from [25-2](#)
 - obtaining [25-2](#)
 - cryptographic features (IME) [1-2](#)
 - CSA MC
 - adding interfaces [18-7](#)
 - configuring IPS interfaces [18-3](#)
 - host posture events [18-1, 18-3](#)
 - quarantined IP address events [18-1](#)
 - supported IPS interfaces [18-3](#)
 - CtlTransSource
 - described [A-4, A-11](#)
 - illustration [A-12](#)
 - current configuration back up [C-2](#)
 - current KB setting [20-13](#)
 - custom signatures
 - Custom Signature Wizard [10-5](#)
 - described [9-2](#)
 - IPv6 signature [9-33, 10-14](#)
 - Meta signature [9-30](#)
 - sensor performance [10-4](#)
 - String TCP XL [9-35, 9-38](#)
 - Custom Signature Wizard
 - alert behavior [10-26](#)
 - Alert Response window field descriptions [10-26](#)
 - Atomic IP Engine Parameters window field descriptions [10-13](#)
 - described [10-1](#)
 - ICMP Traffic Type window field descriptions [10-12](#)
 - Inspect Data window field descriptions [10-12](#)
 - MSRPC Engine Parameters window field descriptions [10-11](#)
 - no signature engine sequence [10-4](#)
 - Protocol Type window field descriptions [10-10](#)
 - Service HTTP Engine Parameters window field descriptions [10-16](#)
 - Service RPC Engine Parameters window field descriptions [10-19](#)
 - Service Type window field descriptions [10-13](#)
 - signature engine sequence [10-1](#)
 - Signature Identification window field descriptions [10-11](#)
 - State Engine Parameters window field descriptions [10-20](#)
 - String ICMP Engine Parameters window field descriptions [10-21](#)
 - String TCP Engine Parameters window field descriptions [10-21](#)
 - String UDP Engine Parameters window field descriptions [10-24](#)
 - supported signature engines [10-2](#)
 - Sweep Engine Parameters window field descriptions [10-25](#)
 - TCP Sweep Type window field descriptions [10-13](#)
 - TCP Traffic Type window field descriptions [10-12](#)
 - UDP Sweep Type window field descriptions [10-12](#)
 - UDP Traffic Type window field descriptions [10-12](#)
 - using [10-5](#)
 - Welcome window field descriptions [10-10](#)
-
- ## D
- dashboards
 - adding [3-1](#)
 - deleting [3-1](#)
 - Data Archive dialog box
 - configuring [1-10](#)
 - described [1-9](#)
 - field descriptions [1-9](#)
 - data archiving configuring [1-10](#)
 - data nodes [10-25, B-67](#)

- data structures (examples) [A-8](#)
- DDoS
 - protocols [B-72](#)
 - Stacheldraht [B-72](#)
 - TFN [B-72](#)
- debug logging enable [C-45](#)
- default policies
 - ad0 [12-9](#)
 - rules0 [11-2, 11-11](#)
 - sig0 [9-9](#)
- defaults
 - KB filename [12-12](#)
 - password [23-2](#)
 - restoring [19-28](#)
 - username [23-2](#)
 - virtual sensor vs0 [8-2](#)
- deleting
 - anomaly detection policies [12-10](#)
 - blocking devices [15-15](#)
 - denied attackers [16-2](#)
 - event action filters [8-22, 11-17](#)
 - event action overrides [11-14](#)
 - event action rules policies [11-12](#)
 - event variables [8-35, 11-29](#)
 - host blocks [16-4](#)
 - imported OS values [20-18](#)
 - IPv4 target value ratings [8-25, 11-20](#)
 - IPv6 target value ratings [8-27, 11-22](#)
 - KBs [20-14](#)
 - learned OS values [20-17](#)
 - network blocks [16-7](#)
 - OS maps [8-32, 11-27](#)
 - rate limiting devices [15-15](#)
 - rate limits [16-9](#)
 - risk categories [8-37, 11-32](#)
 - signature definition policies [9-10](#)
 - signature variables [9-41](#)
 - virtual sensors [8-12](#)
- Demo mode (IME) [1-4](#)
- demo reports described [22-1](#)
- Denial of Service. See DoS.
- denied attackers
 - adding [16-2](#)
 - clearing [16-2](#)
 - deleting [16-2](#)
 - hit count [16-1](#)
 - resetting hit counts [16-2](#)
 - viewing hit counts [16-2](#)
 - viewing list [16-2](#)
- Denied Attackers pane
 - described [16-1](#)
 - field descriptions [16-2](#)
 - user roles [16-1](#)
 - using [16-2](#)
- deny actions (list) [9-3, 9-16, 11-8](#)
- Deny Packet Inline described [9-5, 9-18, 11-10](#)
- detect mode (anomaly detection) [12-4](#)
- device access issues [C-40](#)
- Device Details pane described [2-1](#)
- Device List pane
 - described [2-1](#)
 - field descriptions [2-2](#)
- Device Login Profiles pane
 - configuring [15-13](#)
 - described [15-12](#)
 - field descriptions [15-12](#)
- devices
 - adding [2-4](#)
 - deleting [2-4](#)
 - editing [2-4](#)
- device tools
 - DNS lookup [2-6](#)
 - ping [2-6](#)
 - traceroute [2-6](#)
 - whois [2-6](#)
- Diagnostics Report pane
 - button functions [20-25](#)
 - described [20-24](#)

- user roles [20-24](#)
- using [20-25](#)
- diagnostics reports [20-25](#)
- Differences between knowledge bases KB_Name and KB_Name window field descriptions [20-11](#)
- disabling
 - anomaly detection [12-35, C-19](#)
 - blocking [15-8](#)
 - event action filters [8-22, 11-17](#)
 - global correlation [13-12](#)
 - interfaces [7-19](#)
 - password recovery [19-10, C-14](#)
 - signatures [9-21](#)
- disaster recovery [C-6](#)
- displaying
 - events [20-3, C-100](#)
 - health status [C-76](#)
 - imported OS maps [20-18](#)
 - inspection load statistics [20-5](#)
 - interface statistics [20-6](#)
 - LACP internals [20-20](#)
 - LACP neighbors [20-19](#)
 - learned OS maps [20-17](#)
 - password recovery setting [19-11, C-14](#)
 - sensor statistics [20-26](#)
 - statistics [C-86](#)
 - tech support information [C-78](#)
 - version [C-82](#)
- Distributed Denial of Service. See DDoS.
- DNS lookup device tool (IME) [1-3, 2-6, 3-15, 3-16, 21-6](#)
- DoS tools
 - Stacheldraht [B-72](#)
 - stick [B-7](#)
 - TFN [B-72](#)
- downgrade command [26-12](#)
- downgrading sensors [26-12](#)
- downloading
 - Cisco software [25-1](#)
 - KBs [20-15](#)

- Download Knowledge Base From Sensor dialog box
 - described [20-15](#)
 - field descriptions [20-15](#)
- duplicate IP addresses [C-27](#)

E

- Edit ACL Entry dialog box field descriptions [5-3](#)
- Edit Allowed Host dialog box
 - field descriptions [6-6](#)
 - user roles [6-6](#)
- Edit Authorized RSA1 Key dialog box
 - field descriptions [14-5](#)
 - user roles [14-4](#)
- Edit Authorized RSA Key dialog box
 - field descriptions [14-3](#)
 - user roles [14-2](#)
- Edit Blocking Device dialog box
 - field descriptions [15-15](#)
 - user roles [15-14](#)
- Edit Cat 6K Blocking Device Interface dialog box
 - field descriptions [15-22](#)
 - user roles [15-21](#)
- Edit Configured OS Map dialog box
 - field descriptions [8-31, 11-26](#)
 - user roles [8-30, 11-23](#)
- Edit Destination Port dialog box
 - field descriptions [12-17, 12-23, 12-30](#)
 - user roles [12-15](#)
- Edit Device dialog box field descriptions [2-3](#)
- Edit Device Login Profile dialog box
 - field descriptions [15-12](#)
 - user roles [15-12](#)
- Edit Event Action Filter dialog box
 - field descriptions [8-21, 11-16](#)
 - user roles [11-15](#)
- Edit Event Action Override dialog box
 - field descriptions [8-12, 11-13](#)
 - user roles [8-12, 11-13](#)

- Edit Event Variable dialog box
 - field descriptions [8-34, 11-29](#)
 - user roles [8-33, 11-28](#)
- Edit External Product Interface dialog box
 - field descriptions [18-6](#)
 - user roles [18-4](#)
- Edit Filter dialog box field descriptions [3-19](#)
- Edit Histogram dialog box
 - field descriptions [12-17, 12-24, 12-30](#)
 - user roles [12-15](#)
- editing
 - blocking devices [15-15](#)
 - event action filters [8-22, 11-17](#)
 - event action overrides [11-14](#)
 - event variables [8-35, 11-29](#)
 - interfaces [7-20](#)
 - IPv4 target value ratings [8-25, 11-20](#)
 - IPv6 target value ratings [8-27, 11-22](#)
 - OS maps [8-32, 11-27](#)
 - rate limiting devices [15-15](#)
 - risk categories [8-37, 11-32](#)
 - signatures [9-24](#)
 - signature variables [9-41](#)
 - virtual sensors [8-12](#)
- Edit Inline VLAN Pair dialog box
 - field descriptions [7-27](#)
 - user roles [7-26](#)
- Edit Inline VLAN Pair Entry dialog box field descriptions [5-11](#)
- Edit Interface dialog box
 - field descriptions [7-19](#)
 - user roles [7-17](#)
- Edit Interface Pair dialog box
 - field descriptions [7-25](#)
 - user roles [7-24](#)
- Edit IP Logging dialog box field descriptions [16-11](#)
- Edit Known Host RSA1 Key dialog box
 - field descriptions [14-9](#)
 - user roles [14-8](#)
- Edit Known Host RSA Key dialog box
 - field descriptions [14-7](#)
 - user roles [14-6](#)
- Edit Master Blocking Sensor dialog box
 - field descriptions [15-25](#)
 - user roles [15-24](#)
- Edit Never Block Address dialog box
 - field descriptions [15-10](#)
 - user roles [15-7](#)
- Edit Posture ACL dialog box field descriptions [18-7](#)
- Edit Protocol Number dialog box field descriptions [12-18, 12-25, 12-32](#)
- Edit Risk Level dialog box
 - field descriptions [8-37, 11-31](#)
 - user roles [8-36, 11-31](#)
- Edit Router Blocking Device Interface dialog box
 - field descriptions [15-19](#)
 - user roles [15-17](#)
- Edit Signature dialog box field descriptions [9-14](#)
- Edit Signature Variable dialog box
 - field descriptions [9-40](#)
 - user roles [9-40](#)
- Edit SNMP Trap Destination dialog box field descriptions [17-8](#)
- Edit SNMPv3 User dialog box
 - field descriptions [17-5](#)
- Edit Start Time dialog box
 - field descriptions [12-14](#)
 - user roles [12-12](#)
- Edit Target Value Rating dialog box
 - field descriptions [8-25, 8-27](#)
 - user roles [8-25, 8-26](#)
- Edit User dialog box
 - field descriptions [6-22](#)
 - user roles [6-19, 6-22](#)
- Edit Virtual Sensor dialog box
 - field descriptions [8-10](#)
 - user roles [8-9](#)

- Edit VLAN Group dialog box
 - field descriptions [7-29](#)
 - user roles [7-28](#)
- efficacy
 - described [13-4](#)
 - measurements [13-4](#)
- email notification
 - configuring (IME) [1-13](#)
 - example (IME) [1-12](#)
- email setup (IME) [1-11](#)
- Email Setup dialog box
 - configuring [1-11](#)
 - described [1-11](#)
 - field descriptions [1-11](#)
- enabling
 - anomaly detection [12-4](#)
 - event action filters [8-22, 11-17](#)
 - event action overrides [11-14](#)
 - interfaces [7-19](#)
 - LACP [7-23](#)
 - packet logging [19-3](#)
 - signatures [9-21](#)
- enabling debug logging [C-45](#)
- Encryption Software Export Distribution Authorization form
 - cryptographic account [25-2](#)
 - described [25-2](#)
- engines
 - AIC [B-10](#)
 - AIC FTP [B-11](#)
 - AIC HTTP [B-11](#)
 - Atomic ARP [B-13](#)
 - Atomic IP [10-13, B-24](#)
 - Atomic IP Advanced [B-14](#)
 - Atomic IPv6 [B-27](#)
 - Fixed [B-28](#)
 - Fixed ICMP [B-28](#)
 - Fixed TCP [B-28](#)
 - Fixed UDP [B-28](#)
 - Flood [B-31](#)
 - Flood Host [B-31](#)
 - Flood Net [B-31](#)
 - Master [B-4](#)
 - Meta [9-29, B-32](#)
 - Multi String [B-34](#)
 - Normalizer [B-35](#)
 - Service [B-39](#)
 - Service DNS [B-39](#)
 - Service FTP [B-40](#)
 - Service Generic [B-41](#)
 - Service H225 [B-43](#)
 - Service HTTP [10-16, B-45](#)
 - Service IDENT [B-47](#)
 - Service MSRPC [10-11, B-48](#)
 - Service MSSQL [B-50](#)
 - Service NTP [B-51](#)
 - Service P2P [B-52](#)
 - Service RPC [10-19, B-52](#)
 - Service SMB Advanced [B-54](#)
 - Service SNMP [B-56](#)
 - Service SSH [B-57](#)
 - Service TNS [B-57](#)
 - State [10-20, B-59](#)
 - String [10-21, 10-24, B-61](#)
 - String ICMP [10-21, 10-24, B-61](#)
 - String TCP [10-21, 10-24, B-61](#)
 - String UDP [10-21, 10-24, B-61](#)
 - Sweep [10-24, B-66](#)
 - Sweep Other TCP [B-68](#)
 - Traffic Anomaly [B-69](#)
 - Traffic ICMP [B-71](#)
 - Trojan [B-72](#)
- EPS
 - described [1-3](#)
 - IME Home pane [1-3](#)
- erase license-key command [19-15](#)
- errors (Analysis Engine) [C-52](#)
- evAlert [A-9](#)

- event action filters
 - adding [8-22, 11-17](#)
 - configuring [8-22, 11-17](#)
 - deleting [8-22, 11-17](#)
 - described [8-20, 11-4](#)
 - disabling [8-22, 11-17](#)
 - editing [8-22, 11-17](#)
 - enabling [8-22, 11-17](#)
 - moving [8-22, 11-17](#)
- Event Action Filters tab
 - configuring [8-22, 11-17](#)
 - described [8-20, 11-15](#)
 - field descriptions [8-20, 11-15](#)
- event action overrides
 - adding [11-14](#)
 - deleting [11-14](#)
 - described [8-5, 11-4](#)
 - editing [11-14](#)
 - enabling [11-14](#)
 - risk rating range [8-5, 11-4](#)
- Event Action Overrides tab
 - described [11-13](#)
 - field descriptions [11-13](#)
- Event Action Rules (rules0) pane described [11-12](#)
- Event Action Rules pane
 - described [11-2, 11-11](#)
 - field descriptions [11-11](#)
 - user roles [11-11](#)
- event action rules policies
 - adding [11-12](#)
 - cloning [11-12](#)
 - deleting [11-12](#)
- event action rules variables [8-20, 11-15](#)
- event actions
 - risk ratings [8-6, 11-4](#)
 - threat ratings [8-6, 11-4](#)
- event connection status
 - displaying [2-5](#)
 - starting [2-5](#)
 - stopping [2-5](#)
- Event Monitoring pane
 - described [21-1](#)
 - filters [21-2](#)
- events
 - clearing [6-16, 20-4, C-103](#)
 - color rules [21-2](#)
 - displaying [C-100](#)
 - grouping [21-2](#)
 - host posture [18-2](#)
 - quarantined IP address [18-2](#)
- Events pane
 - configuring [20-3](#)
 - described [20-1](#)
 - field descriptions [20-2](#)
- events per second. See EPS.
- Event Store
 - clearing [6-16, 20-4, C-103](#)
 - clearing events [6-12, C-17](#)
 - data structures [A-8](#)
 - described [A-4](#)
 - examples [A-7](#)
 - no alerts [C-32](#)
 - responsibilities [A-7](#)
 - time stamp [6-12, C-17](#)
 - timestamp [A-7](#)
- event types [C-98](#)
- event variables
 - adding [8-35, 11-29](#)
 - configuring [8-35, 11-29](#)
 - deleting [8-35, 11-29](#)
 - described [8-33, 11-28](#)
 - editing [8-35, 11-29](#)
 - example [8-34, 11-29](#)
- Event Variables tab
 - configuring [8-35, 11-29](#)
 - field descriptions [8-34, 11-29](#)
- Event Viewer pane
 - displaying events [20-3](#)

- field descriptions [20-3](#)
- event views
 - creating [21-4](#)
 - using [21-4](#)
- evError [A-9](#)
- evLogTransaction [A-9](#)
- evShunRqst [A-9](#)
- evStatus [A-9](#)
- example custom signatures
 - Atomic IP Advanced [9-33, 10-14](#)
 - Meta [9-30](#)
 - Service HTTP [10-17](#)
 - String TCP [10-22](#)
 - String TCP XL [9-35](#)
- examples
 - AIC engine signature [9-52](#)
 - ASA failover configuration [C-59, C-70](#)
 - Atomic IP Advanced engine signature [9-33, 10-14](#)
 - automatic update [19-24](#)
 - configured OS maps [8-30, 11-24](#)
 - default anomaly detection configuration [12-4](#)
 - email notification (IME) [1-12](#)
 - email notifications (IME) [1-14](#)
 - IP Fragment Reassembly signature [9-56](#)
 - IPv6 attacker address [8-21, 11-16](#)
 - IPV6 victim address [8-21, 11-16](#)
 - KB histogram [12-13, 20-8](#)
 - Meta engine signature [9-30](#)
 - Service HTTP engine signature [10-17](#)
 - SPAN configuration for IPv6 support [7-12](#)
 - String TCP engine signature [10-22](#)
 - String TCP XL engine signature [9-35, 9-38](#)
 - System Configuration Dialog [24-2](#)
 - TCP Stream Reassembly signature [9-64](#)
- external product interfaces
 - adding [18-7](#)
 - described [18-1](#)
 - issues [18-3, C-22](#)
 - troubleshooting [18-10, C-22](#)

- trusted hosts [18-4](#)
- External Product Interfaces pane
 - described [18-4](#)
 - field descriptions [18-5](#)
- external zone
 - configuring [12-32](#)
 - protocols [12-29](#)
- External Zone tab
 - described [12-29](#)
 - tabs [12-29](#)
 - user roles [12-29](#)

F

- failover
 - TCP support [7-22](#)
- fallback
 - TCP support [7-22](#)
- false positives described [9-2](#)
- Fields tab described [21-2](#)
- files
 - Cisco IPS (list) [25-1](#)
- Filtered Events vs All Events Reports described [1-15, 22-2](#)
- filtering described [21-2](#)
- Filter pane field descriptions [21-3](#)
- filters
 - configuring [3-16, 21-6](#)
 - creating reports [22-3](#)
- Fixed engine described [B-28](#)
- Fixed ICMP engine parameters (table) [B-29](#)
- Fixed TCP engine parameters (table) [B-29](#)
- Fixed UDP engine parameters (table) [B-30](#)
- Flood engine described [B-31](#)
- Flood Host engine parameters (table) [B-31](#)
- Flood Net engine parameters (table) [B-32](#)
- flow states clearing [20-23](#)
- FTP servers
 - automatic updates [19-20](#)
 - signature updates [19-25, 19-26](#)

FTP servers and software updates [19-21, 26-3](#)

G

gadgets

- adding [3-1](#)
- Attacks Over Time [3-13](#)
- deleting [3-1](#)
- Global Correlation Health [3-7](#)
- Global Correlation Reports [3-6](#)
- Interface Status [3-5](#)
- Licensing [3-5](#)
- Memory & Load [3-10](#)
- Network Security [3-8](#)
- RSS Feed [3-11](#)
- Sensor Health [3-3](#)
- Sensor Information [3-2](#)
- Top Applications [3-9](#)
- Top Attackers [3-11](#)
- Top Signatures [3-13](#)
- Top Victims [3-12](#)

General dialog box

- configuring [1-8](#)
- described [1-8](#)
- field descriptions [1-8](#)
- user roles [1-8](#)

general settings

- configuring [8-40, 11-34](#)
- described [8-39, 11-33](#)

General tab

- configuring [8-40, 11-34](#)
- described [8-39, 11-33, 12-16, 12-23](#)
- described (IME) [21-2](#)
- enabling zones [12-16, 12-23](#)
- field descriptions [8-39, 11-34, 12-16, 12-23](#)
- user roles [8-39, 11-33](#)

generating diagnostics reports [20-25](#)

global correlation [22-2](#)

- described [1-2, 13-1, 13-2](#)

disabling [13-12](#)

disabling about [13-12](#)

DNS server [13-6](#)

error messages [A-29](#)

features [13-5](#)

goals [13-5](#)

health metrics [13-7](#)

health status [13-7](#)

HTTP proxy server [13-6](#)

license [6-3, 13-6, 13-8, 24-1, 24-5](#)

no IPv6 support [8-22, 8-27, 8-35, 13-6](#)

Produce Alert [9-3, 9-16, 11-8](#)

requirements [13-6](#)

risk rating [13-5](#)

troubleshooting [13-11, C-21](#)

update client (illustration) [13-8](#)

global correlation connection status

- displaying [2-5](#)

- starting [2-5](#)

- stopping [2-5](#)

Global Correlation Health gadget

- configuring [3-8](#)

- described [3-7](#)

Global Correlation Reports described [22-2](#)

Global Correlation Reports gadget

- configuring [3-6](#)

- described [3-6](#)

Global Correlation Update

- client described [A-28](#)

- server described [A-28](#)

Group By tab described [21-2](#)

grouping events [21-2](#)

GRUB menu password recovery [19-5, C-8](#)

H

H.225.0 protocol [B-43](#)

H.323 protocol [B-43](#)

- health connection status
 - displaying [2-5](#)
 - starting [2-5](#)
 - stopping [2-5](#)
 - health status
 - global correlation [13-7](#)
 - metrics [3-4](#)
 - sensor [3-3](#)
 - health status display [C-76](#)
 - host blocks
 - adding [16-4](#)
 - deleting [16-4](#)
 - managing [16-4](#)
 - Host Blocks pane
 - configuring [16-4](#)
 - described [16-3](#)
 - field descriptions [16-3](#)
 - user roles [16-3](#)
 - host posture events
 - CSA MC [18-3](#)
 - described [18-2](#)
 - HTTP/HTTPS servers supported [19-21, 26-3](#)
 - HTTP advanced decoding
 - described [8-4](#)
 - platform support [8-5](#)
 - restrictions [8-4](#)
 - HTTP deobfuscation
 - ASCII normalization [10-16, B-45](#)
 - described [10-16, B-45](#)
 - hw-module module slot_number password-reset command [19-8, C-12](#)
 - 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-56](#)
 - certificates [14-11](#)
 - Custom Signature Wizard supported signature engines [10-2](#)
 - TLS [14-11](#)
 - will not load [C-55](#)
 - illegal zone
 - configuring [12-25](#)
 - Illegal Zone tab
 - described [12-22](#)
 - user roles [12-22](#)
 - IME
 - color rules [21-2](#)
 - Color Rules tab [21-2](#)
 - configuring
 - automatic reporting [1-16](#)
 - email notification [1-13](#)
 - filters [3-16, 21-6](#)
 - RSS feeds [4-2](#)
 - views [3-16, 21-6](#)
 - cryptographic features [1-2](#)
 - dashboards
 - adding [3-1](#)
 - deleting [3-1](#)
 - Demo mode [1-4](#)
 - described [1-1](#)
 - devices
 - adding [2-4](#)
 - deleting [2-4](#)
-
- IDAPI
 - communications [A-4, A-32](#)
 - described [A-4](#)
 - functions [A-32](#)
 - illustration [A-32](#)

- editing [2-4](#)
- email notification example [1-14](#)
- EPS [1-3](#)
- event connection status
 - displaying [2-5](#)
 - starting [2-5](#)
 - stopping [2-5](#)
- Event Monitoring pane [21-1](#)
- Fields tab [21-2](#)
- filtering [21-2](#)
- gadgets
 - adding [3-1](#)
 - deleting [3-1](#)
- General tab [21-2](#)
- global correlation connection status
 - displaying [2-5](#)
 - starting [2-5](#)
 - stopping [2-5](#)
- Group By tab [21-2](#)
- grouping events [21-2](#)
- health connection status
 - displaying [2-5](#)
 - starting [2-5](#)
 - stopping [2-5](#)
- installation notes and caveats [1-5](#)
- installing [1-5](#)
- known host key retrieval [14-6, 14-7, 14-8, 14-9](#)
- menu features [1-3](#)
- MySQL database [1-5](#)
- password recovery [19-11, C-14](#)
- password requirements [1-6](#)
- reports
 - configuring [22-3](#)
 - described [22-1](#)
 - generating [22-3](#)
- report types [22-1](#)
- using event views [21-4](#)
- video help [1-3](#)
- working with
 - top attacker IP addresses [3-14](#)
 - top signatures [3-15](#)
 - top victim IP addresses [3-14](#)
- IME Home pane
 - described [1-3](#)
 - EPS [1-3](#)
 - features [1-3](#)
- IME time synchronization problems [C-58](#)
- Imported OS pane
 - clearing [20-18](#)
 - described [20-18](#)
 - field descriptions [20-18](#)
- imported OS values
 - clearing [20-18](#)
 - deleting [20-18](#)
- inactive mode (anomaly detection) [12-4](#)
- initializing
 - appliances [24-7](#)
 - ASA 5500-X IPS SSP [24-13](#)
 - ASA 5585-X IPS SSP [24-17](#)
 - sensors [6-1, 24-1, 24-4](#)
 - verifying [24-21](#)
- inline interface pair mode
 - configuration restrictions [7-8](#)
 - described [7-12](#)
 - illustration [7-13](#)
- Inline Interface Pair window
 - described [5-10](#)
 - Startup Wizard [5-10](#)
- inline mode
 - interface cards [7-3](#)
 - normalization [8-4](#)
 - pairing interfaces [7-3](#)
- inline TCP session tracking modes described [8-4](#)
- inline VLAN pair mode
 - configuration restrictions [7-8](#)
 - configuring [5-11](#)
 - described [7-13](#)

- illustration [7-14](#)
 - supported sensors [7-13](#)
- Inline VLAN Pairs window
 - described [5-10](#)
 - field descriptions [5-11](#)
 - Startup Wizard [5-10](#)
- Inspection/Reputation pane
 - configuring [13-9](#)
 - described [13-8](#)
 - field descriptions [13-9](#)
- Inspection Load Statistics pane
 - configuring [20-5](#)
 - described [20-4](#)
 - field descriptions [20-4](#)
 - user roles [20-4](#)
- installer major version [25-5](#)
- installer minor version [25-5](#)
- installing
 - IME [1-5](#)
 - sensor license [19-14](#)
 - system image
 - ASA 5500-X IPS SSP [26-22](#)
 - ASA 5585-X IPS SSP [26-24](#)
 - IPS 4345 [26-17](#)
 - IPS 4360 [26-17](#)
 - IPS 4510 [26-20](#)
 - IPS 4520 [26-20](#)
 - IPS 4520-XL [26-20](#)
- IntelliShield
 - alerts [9-12](#)
 - MySDN [9-11](#)
- InterfaceApp described [A-4](#)
- interface pairs
 - configuring [7-25](#)
 - described [7-24](#)
- Interface Pairs pane
 - configuring [7-25](#)
 - described [7-24](#)
 - field descriptions [7-25](#)
- user roles [7-24](#)
- interfaces
 - alternate TCP reset [7-2](#)
 - command and control [7-2](#)
 - configuration restrictions [7-8](#)
 - configuring [7-19](#)
 - described [5-8, 7-1](#)
 - disabling [7-19](#)
 - editing [7-20](#)
 - enabling [7-19](#)
 - logical [5-8](#)
 - physical [5-8](#)
 - port numbers [7-1](#)
 - sensing [7-2, 7-3](#)
 - slot numbers [7-1](#)
 - support (table) [7-4](#)
 - TCP reset [7-6](#)
- Interface Selection window
 - described [5-10](#)
 - Startup Wizard [5-10](#)
- Interfaces pane
 - configuring [7-19](#)
 - described [7-18](#)
 - field descriptions [7-18](#)
 - user roles [7-17](#)
- Interface Statistics pane
 - configuring [20-6](#)
 - described [20-5](#)
 - field descriptions [20-6](#)
- Interface Status gadget
 - configuring [3-6](#)
 - described [3-5](#)
- Interface Summary window
 - described [5-8](#)
 - field descriptions [5-9](#)
- internal zone configuring [12-19](#)
- Internal Zone tab
 - described [12-15](#)
 - user roles [12-15](#)

- IP fragmentation described [B-35](#)
- IP fragment reassembly
 - configuring [9-55](#)
 - described [9-53](#)
 - mode [9-55](#)
 - parameters (table) [9-54](#)
 - signatures [9-56](#)
 - signatures (example) [9-56](#)
 - signatures (table) [9-54](#)
- IP logging
 - described [9-65, 16-10](#)
 - event actions [16-11](#)
 - system performance [16-10, 16-11](#)
- IP Logging pane
 - configuring [16-12](#)
 - described [16-11](#)
 - field descriptions [16-11](#)
 - user roles [16-10](#)
- IP Logging Variables pane
 - described [19-18](#)
 - field description [19-18](#)
 - user roles [19-18](#)
- IP logs
 - circular buffer [16-10](#)
 - states [16-10](#)
 - TCPDUMP [16-10](#)
 - viewing [16-12](#)
 - WireShark [16-10](#)
- IPS 4345
 - installing system image [26-17](#)
 - password recovery [19-5, C-8, C-9](#)
 - reimaging [26-17](#)
- IPS 4360
 - installing system image [26-17](#)
 - password recovery [19-5, C-8, C-9](#)
 - reimaging [26-17](#)
- IPS 4510
 - installing system image [26-20](#)
 - LACP grouping [7-15](#)
 - password recovery [19-5, C-8, C-9](#)
 - reimaging [26-20](#)
 - SwitchApp [A-29](#)
- IPS 4520
 - installing system image [26-20](#)
 - LACP grouping [7-15](#)
 - password recovery [19-5, C-8, C-9](#)
 - reimaging [26-20](#)
 - SwitchApp [A-29](#)
- IPS 4520-XL
 - installing system image [26-20](#)
 - LACP grouping [7-15](#)
 - password recovery [19-5, C-8, C-9](#)
 - reimaging [26-20](#)
 - SwitchApp [A-29](#)
- IPS appliances
 - Deny Connection Inline [9-5, 9-18, 11-10](#)
 - Deny Packet Inline [9-5, 9-18, 11-10](#)
 - Reset TCP Connection [9-5, 9-18, 11-10](#)
 - TCP reset packets [9-5, 9-18, 11-10](#)
- IPS applications
 - summary [A-35](#)
 - table [A-35](#)
 - XML format [A-4](#)
- IPS clock synchronization [C-16](#)
- 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 Manager Express described [1-1](#)
- IPS modules unsupported features [5-2](#)

- IPS Policies pane
 - described [8-8](#)
 - Event Action Rules [8-8](#)
 - field descriptions [8-9](#)
 - IPS port channel
 - illustration [7-15](#)
 - IPS software
 - application list [A-4](#)
 - available files [25-1](#)
 - configuring device parameters [A-5](#)
 - directory structure [A-34](#)
 - Linux OS [A-1](#)
 - obtaining [25-1](#)
 - retrieving data [A-5](#)
 - security features [A-5](#)
 - tuning signatures [A-5](#)
 - updating [A-5](#)
 - user interaction [A-5](#)
 - versioning scheme [25-3](#)
 - IPS software file names
 - major updates (illustration) [25-4](#)
 - minor updates (illustration) [25-4](#)
 - patch releases (illustration) [25-4](#)
 - service packs (illustration) [25-4](#)
 - IPv4
 - address format [8-33, 11-28](#)
 - event variables [8-33, 11-28](#)
 - IPv4 Add Target Value Rating dialog box
 - field descriptions [11-20](#)
 - user roles [11-19](#)
 - IPv4 Edit Target Value Rating dialog box
 - field descriptions [11-20](#)
 - user roles [11-19](#)
 - IPv4 target value ratings
 - adding [8-25, 11-20](#)
 - deleting [8-25, 11-20](#)
 - editing [8-25, 11-20](#)
 - IPv4 Target Value Rating tab
 - configuring [8-25, 11-20](#)
 - field descriptions [8-25, 11-20](#)
 - IPv6
 - address format [8-34, 11-28](#)
 - described [B-28](#)
 - event variables [8-34, 11-28](#)
 - SPAN ports [7-11](#)
 - switches [7-11](#)
 - IPv6 Add Target Value Rating dialog box
 - field descriptions [11-22](#)
 - user roles [11-21](#)
 - IPv6 Edit Target Value Rating dialog box
 - field descriptions [11-22](#)
 - user roles [11-21](#)
 - IPv6 target value ratings
 - adding [8-27, 11-22](#)
 - configuring [8-27, 11-22](#)
 - deleting [8-27, 11-22](#)
 - editing [8-27, 11-22](#)
 - IPv6 Target Value Rating tab
 - configuring [8-27, 11-22](#)
 - field descriptions [8-26, 11-21](#)
-
- ## K
- KBs
 - comparing [20-12](#)
 - default filename [12-12](#)
 - deleting [20-14](#)
 - described [12-3](#)
 - downloading [20-15](#)
 - histogram [12-12, 20-7](#)
 - initial baseline [12-3](#)
 - learning accept mode [12-12](#)
 - loading [20-13](#)
 - monitoring [20-10](#)
 - renaming [20-15](#)
 - saving [20-14](#)
 - scanner threshold [12-12, 20-7](#)
 - tree structure [12-12, 20-7](#)

uploading [20-16](#)

Knowledge Base. See KB.

Known Host RSA1 Keys pane

- configuring [14-9](#)
- described [14-8](#)
- field descriptions [14-9](#)

Known Host RSA Keys pane

- configuring [14-7](#)
- described [14-6](#)
- field descriptions [14-7](#)

L

LACP

- enabling [7-23](#)
- link states [7-22](#)
- restrictions [7-22](#)

LACP Internals pane

- described [20-20](#)
- output [20-21](#)

LACP Neighbor pane

- described [20-19](#)
- field descriptions [20-19](#)

LACP pane

- described [7-21](#)
- field descriptions [7-23](#)

Learned OS pane

- clearing [20-17](#)
- described [20-17](#)
- field descriptions [20-17](#)

learned OS values

- clearing [20-17](#)
- deleting [20-17](#)

learning accept mode

- anomaly detection [12-3](#)
- configuring [12-14](#)

Learning Accept Mode tab

- described [12-12](#)
- field descriptions [12-14](#)

- user roles [12-12](#)

license key

- obtaining [19-12](#)
- trial [19-12](#)
- uninstalling [19-15](#)
- viewing status of [19-12](#)

licensing

- described [19-12](#)
- IPS device serial number [19-12](#)

Licensing gadget

- configuring [3-5](#)
- described [3-5](#)

Licensing pane

- configuring [19-14](#)
- described [19-12](#)
- field descriptions [19-13](#)
- user roles [19-12](#)

limitations for concurrent CLI sessions [23-1](#)

Link Aggregation Control Protocol Data Unit. See LACPDU.

Link Aggregation Control Protocol. See LACP.

listings UNIX-style [19-21](#)

loading KBs [20-13](#)

local authentication configuring [6-23](#)

Logger

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

logging in

- appliances [23-2](#)
- ASA 5500-X IPS SSP [23-4](#)
- ASA 5585-X IPS SSP [23-5](#)
- sensors
 - SSH [23-6](#)
 - Telnet [23-6](#)
- service role [23-2](#)
- terminal servers [23-3, 26-16](#)
- user role [23-1](#)

LOKI

described [B-72](#)protocol [B-71](#)loose connections on sensors [C-23](#)

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 [25-3](#)Manage Filter Rules dialog box field descriptions [3-18](#)

managing

host blocks [16-4](#)network blocks [16-7](#)rate limiting [16-9](#)

manifests

client [A-28](#)server [A-28](#)manually updating sensor [19-25, 19-26](#)

master blocking sensor

described [15-24](#)not set up properly [C-43](#)verifying configuration [C-43](#)

Master Blocking Sensor pane

configuring [15-25](#)described [15-24](#)field descriptions [15-25](#)

Master engine

alert frequency [B-7](#)alert frequency parameters (table) [B-7](#)described [B-4](#)event actions [B-8](#)general parameters (table) [B-4](#)universal parameters [B-4](#)

master engine parameters

obsoletes [B-6](#)promiscuous delta [B-6](#)vulnerable OSES [B-6](#)

Memory & Load gadget

configuring [3-11](#)described [3-10](#)merging configuration files [C-2](#)

Meta engine

described [9-29, B-32](#)parameters (table) [B-33](#)Signature Event Action Processor [9-29, B-32](#)Meta Event Generator described [8-39, 11-33](#)metrics for sensor health [19-16](#)MIBs supported [17-10, C-18](#)minor updates described [25-3](#)

Miscellaneous tab

application policy parameters [9-42](#)

configuring

application policy [9-52](#)IP fragment reassembly mode [9-55](#)IP logging [9-65](#)TCP stream reassembly mode [9-63](#)described [9-42](#)field descriptions [9-43](#)IP fragment reassembly options [9-42](#)IP logging options [9-43](#)TCP stream reassembly [9-42](#)user roles [9-42](#)

modes

anomaly detection detect [12-4](#)anomaly detection learning accept [12-3](#)asymmetric [8-4](#)bypass [7-31](#)inactive (anomaly detection) [12-4](#)inline interface pair [7-12](#)inline TCP tracking [8-4](#)inline VLAN pair [7-13](#)Normalizer [8-4](#)

- promiscuous [7-10](#)
 - VLAN groups [7-14](#)
 - monitoring
 - displaying statistics [20-6](#)
 - events [20-3](#)
 - inspection load statistics [20-4, 20-5](#)
 - KBs [20-10](#)
 - moving
 - event action filters [8-22, 11-17](#)
 - OS maps [8-32, 11-27](#)
 - Multi String engine
 - described [B-34](#)
 - parameters (table) [B-34](#)
 - Regex [B-34](#)
 - MySDN
 - described [9-12](#)
 - IntelliShield [9-12](#)
 - MySQL database
 - coexisting with IME [1-5](#)
 - installing IME [1-5](#)
-
- ## N
- NAS-ID
 - described [6-23](#)
 - RADIUS authentication [6-23](#)
 - Neighborhood Discovery
 - options [B-28](#)
 - types [B-28](#)
 - network blocks
 - adding [16-7](#)
 - deleting [16-7](#)
 - managing [16-7](#)
 - Network Blocks pane
 - configuring [16-7](#)
 - described [16-6](#)
 - field descriptions [16-6](#)
 - user roles [16-6](#)
 - Network pane
 - configuring [6-3](#)
 - described [6-2](#)
 - field descriptions [6-2](#)
 - TLS/SSL [6-4](#)
 - user roles [6-2](#)
 - network participation
 - data gathered [13-3](#)
 - data use (table) [1-2, 13-2](#)
 - described [13-3](#)
 - health metrics [13-7](#)
 - modes [13-4](#)
 - requirements [13-3](#)
 - SensorBase Network [13-4](#)
 - statistics [13-4](#)
 - network participation data
 - improving signature fidelity [13-4](#)
 - understanding sensor deployment [13-4](#)
 - Network Participation pane
 - configuring [13-11](#)
 - described [13-10](#)
 - field descriptions [13-10](#)
 - Network Security gadget
 - configuring [3-9](#)
 - described [3-8](#)
 - never block
 - hosts [15-7](#)
 - networks [15-7](#)
 - normalization described [8-4](#)
 - Normalizer engine
 - ASA 5500-X IPS SSP [B-36, C-67, C-74](#)
 - ASA 5585-X IPS SSP [B-36, C-67, C-74](#)
 - described [B-35](#)
 - IPv6 fragments [B-36](#)
 - modify packets inline [8-3](#)
 - parameters (table) [B-37](#)
 - 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](#)

Notifications dialog box

- configuring [1-13](#)
- field descriptions [1-12](#)

NTP

- authenticated [6-11, 6-14, C-15](#)
- configuring servers [6-13](#)
- described [6-11, C-15](#)
- incorrect configuration [6-11, C-16](#)
- sensor time source [6-13, 6-14](#)
- time synchronization [6-11, C-15](#)
- unauthenticated [6-11, 6-14, C-15](#)
- verifying configuration [6-12](#)

O

Obfuscated Traffic/Attacks reports described [22-2](#)

obsoletes field described [B-6](#)

obtaining

- cryptographic account [25-2](#)
- IPS software [25-1](#)
- license key [19-12](#)
- sensor license [19-14](#)

one-way TCP reset described [8-39, 11-33](#)

Operation Settings tab

- described [12-11](#)
- field descriptions [12-11](#)
- user roles [12-11](#)

OS Identifications tab

- described [8-30, 11-23](#)
- field descriptions [8-31, 11-25](#)

OS information sources [8-29, 11-24](#)

OS maps

- adding [8-32, 11-27](#)

- configuring [8-32, 11-27](#)
- deleting [8-32, 11-27](#)
- editing [8-32, 11-27](#)
- moving [8-32, 11-27](#)

other actions (list) [9-4, 9-17, 11-9](#)

Other Protocols tab

- described [12-18, 12-25, 12-31](#)
- enabling other protocols [12-18](#)
- external zone [12-31](#)
- field descriptions [12-18, 12-31](#)
- illegal zone [12-25](#)

P

P2P networks described [B-52](#)

Packet Logging pane

- described [19-3](#)
- field descriptions [19-3](#)

partitions

- application [A-4](#)
- recovery [A-4](#)

passive OS fingerprinting

- components [8-29, 11-24](#)
- configuring [8-30, 11-25](#)
- described [8-29, 11-24](#)
- enabled (default) [8-30, 11-25](#)

password policy caution [19-2, 19-3](#)

password recovery

- appliances [19-5, C-8](#)
- ASA 5500-X IPS SSP [19-6, C-10](#)
- ASA 5585-X IPS SSP [19-8, C-12](#)
- CLI [19-10, C-14](#)
- described [19-4, C-8](#)
- disabling [19-10, C-14](#)
- displaying setting [19-11, C-14](#)
- GRUB menu [19-5, C-8](#)
- IME [19-11, C-14](#)
- IPS 4345 [19-5, C-8, C-9](#)
- IPS 4360 [19-5, C-8, C-9](#)

IPS 4510 [19-5, C-8, C-9](#)
 IPS 4520 [19-5, C-8, C-9](#)
 IPS 4520-XL [19-5, C-8, C-9](#)
 platforms [19-4, C-8](#)
 ROMMON [19-5, C-9](#)
 troubleshooting [19-11, C-15](#)
 verifying [19-11, C-14](#)
 password requirements configuring [19-2](#)
 Passwords pane
 configuring [19-2](#)
 described [19-1](#)
 field descriptions [19-2](#)
 patch releases described [25-3](#)
 peacetime learning (anomaly detection) [12-3](#)
 Peer-to-Peer. See P2P.
 physical connectivity issues [C-31](#)
 physical interfaces configuration restrictions [7-8](#)
 ping device tool (IME) [1-3, 2-6, 3-15, 3-16, 21-6](#)
 platforms concurrent CLI sessions [23-1](#)
 port channel configuration
 illustration [7-15](#)
 switch [7-15](#)
 Post-Block ACLs [15-17, 15-18](#)
 Pre-Block ACLs [15-17, 15-18](#)
 prerequisites for blocking [15-5](#)
 promiscuous delta
 calculating risk rating [8-6, 11-3](#)
 described [8-6, 11-3](#)
 promiscuous delta described [B-6](#)
 promiscuous mode
 atomic attacks [7-10](#)
 described [7-10](#)
 illustration [7-11](#)
 packet flow [7-10](#)
 SPAN ports [7-11](#)
 TCP reset interfaces [7-7](#)
 VACL capture [7-11](#)
 protocols
 ARP [B-13](#)

CDP [7-33](#)
 CIDEE [A-34](#)
 DCE [10-11, B-48](#)
 DDoS [B-72](#)
 H.323 [B-43](#)
 H225.0 [B-43](#)
 ICMPv6 [B-14](#)
 IDAPI [A-32](#)
 IDCONF [A-33](#)
 IDIOM [A-32](#)
 IPv6 [B-28](#)
 LOKI [B-71](#)
 MSSQL [B-50](#)
 Neighborhood Discovery [B-28](#)
 Q.931 [B-43](#)
 RPC [10-11, B-48](#)
 SDEE [A-33](#)
 Signature Wizard [10-10](#)

Q

Q.931 protocol
 described [B-43](#)
 SETUP messages [B-43](#)
 quarantined IP address events described [18-2](#)

R

RADIUS
 attempt limit [C-21](#)
 multiple cisco av-pairs [6-21, 6-24](#)
 RADIUS authentication
 configuring [6-23](#)
 described [6-19](#)
 NAS-ID [6-23](#)
 service account [6-19](#)
 shared secret [6-24](#)

- rate limiting
 - ACLs [15-5](#)
 - configuring [16-9](#)
 - described [15-4](#)
 - managing [16-9](#)
 - percentages [16-8](#)
 - routers [15-4](#)
 - service policies [15-5](#)
 - supported signatures [15-4](#)
- rate limiting devices
 - adding [15-15](#)
 - deleting [15-15](#)
 - editing [15-15](#)
- rate limits
 - adding [16-9](#)
 - deleting [16-9](#)
- Rate Limits pane
 - configuring [16-9](#)
 - described [16-7](#)
 - field descriptions [16-8](#)
- raw expression syntax
 - described [B-63](#)
 - expert mode [B-63](#)
- Raw Regex
 - described [9-36, 9-39, B-63](#)
 - expert mode [9-36, 9-39, B-63](#)
- rebooting the sensor [19-28](#)
- Reboot Sensor pane
 - configuring [19-28](#)
 - described [19-28](#)
 - user roles [19-28](#)
- receiving RSS feeds (IME) [4-1](#)
- recover command [26-14](#)
- recovering the application partition image [26-14](#)
- recovery partition
 - described [A-4](#)
- recovery partition upgrade [26-7](#)
- Regex
 - Multi String engine [B-34](#)
 - standardized [9-6, B-1](#)
- Regular Expression. See also Regex.
- regular expression syntax
 - raw Regex [9-36, 9-39, B-63](#)
 - signatures [B-9](#)
- reimaging
 - ASA 5500-X IPS SSP [26-22](#)
 - described [26-3](#)
 - IPS 4345 [26-17](#)
 - IPS 4360 [26-17](#)
 - IPS 4510 [26-20](#)
 - IPS 4520 [26-20](#)
 - IPS 4520-XL [26-20](#)
 - sensors [26-3, 26-14](#)
- removing
 - last applied
 - service pack [26-12](#)
 - signature update [26-12](#)
 - threat profiles [9-19](#)
- Rename Knowledge Base dialog box field descriptions [20-14](#)
- renaming KBs [20-15](#)
- reports
 - configuring [22-3](#)
 - customizing [22-3](#)
 - described [22-1](#)
 - generating [22-3](#)
 - using filters [22-3](#)
- Reports dialog box
 - configuring [1-16](#)
 - field descriptions [1-15](#)
- report types [22-2](#)
 - attacks over time [1-15, 22-2](#)
 - demo [22-1](#)
 - filtered events vs all events [1-15, 22-2](#)
 - obfuscated traffic/attacks [22-2](#)
 - top attackers [1-15, 22-1](#)
 - top signatures [1-15, 22-2](#)
 - top victim [1-15, 22-2](#)

- user-defined [22-1](#)
- reputation
 - described [13-2](#)
 - illustration [13-3](#)
 - servers [13-3](#)
- requirements passwords (IME) [1-6](#)
- Reset Network Security Health pane
 - described [20-23](#)
 - field descriptions [20-23](#)
 - resetting data [20-24](#)
 - user roles [20-23](#)
- reset not occurring for a signature [C-50](#)
- resetting
 - hit counts for denied attackers [16-2](#)
 - network security health data [20-24](#)
 - passwords
 - ASDM [19-8, 19-10, C-11, C-13](#)
 - hw-module command [19-8, C-12](#)
 - sw-module command [19-7, C-10](#)
- resetting the password
 - ASA 5500-X IPS SSP [19-7, C-10](#)
 - ASA 5585-X IPS SSP [19-9, C-12](#)
- Restore Default Interface dialog box field descriptions [5-9](#)
- Restore Defaults pane
 - configuring [19-28](#)
 - described [19-28](#)
 - user roles [19-28](#)
- restoring
 - defaults [19-28](#)
- restoring the current configuration [C-5](#)
- retiring signatures [9-21](#)
- risk categories
 - adding [8-37, 11-32](#)
 - configuring [8-37, 11-32](#)
 - deleting [8-37, 11-32](#)
 - editing [8-37, 11-32](#)
- Risk Category tab
 - configuring [8-37, 11-32](#)
 - described [8-36, 11-31](#)
 - field descriptions [8-37, 11-31](#)
- risk rating
 - Alarm Channel [13-5](#)
 - calculating [8-5, 11-2](#)
 - described [8-29, 11-24](#)
 - global correlation [13-5](#)
 - reputation score [13-5](#)
- ROMMON
 - ASA 5585-X IPS SSP [26-26](#)
 - described [26-15](#)
 - IPS 4345 [19-5, 26-17, C-9](#)
 - IPS 4360 [19-5, 26-17, C-9](#)
 - IPS 4510 [19-5, 26-20, C-9](#)
 - IPS 4520 [19-5, 26-20, C-9](#)
 - IPS 4520-XL [19-5, 26-20, C-9](#)
 - password recovery [19-5, C-9](#)
 - remote sensors [26-15](#)
 - serial console port [26-15](#)
 - TFTP [26-16](#)
- round-trip time. See [RTT](#).
- Router Blocking Device Interfaces pane
 - configuring [15-20](#)
 - described [15-17](#)
 - field descriptions [15-19](#)
- RPC portmapper [10-19, B-52](#)
- RSS Feed gadgets
 - configuring [3-11](#)
 - described [3-11](#)
- RSS feeds
 - channels [4-1](#)
 - configuring [4-2](#)
 - described [4-1](#)
 - formats [4-1](#)
 - receiving [4-1](#)
- RTT
 - described [26-16](#)
 - TFTP limitation [26-16](#)

S

Save Knowledge Base dialog box

described [20-13](#)

field descriptions [20-13](#)

saving KBs [20-14](#)

scheduling automatic upgrades [26-10](#)

SDEE

described [A-33](#)

HTTP [19-19, A-33](#)

protocol [A-33](#)

server requests [19-19, A-34](#)

SDEE Subscriptions pane

field descriptions [19-19](#)

security

account locking [6-25](#)

information on Cisco Security Intelligence Operations [25-7](#)

information on MySDN [9-12](#)

SSH [14-1](#)

security policies described [8-1, 9-1, 11-1, 12-1](#)

sensing interface

ASA 5500-X IPS SSP [8-15](#)

sensing interfaces

Analysis Engine [7-3](#)

described [7-3](#)

interface cards [7-3](#)

modes [7-3](#)

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 [19-22](#)

TCP normalization [A-24](#)

SensorBase Network

described [1-2, 13-1, 13-2](#)

network participation [13-4](#)

participation [1-2, 13-2](#)

servers [1-2, 13-2](#)

sensor health

critical settings [19-16](#)

metrics [19-16](#)

Sensor Health gadget

configuring [3-4](#)

described [3-3](#)

metrics [3-4](#)

status [3-4](#)

Sensor Health pane

described [19-16](#)

field descriptions [19-17](#)

user roles [19-16](#)

Sensor Information gadget

configuring [3-3](#)

described [3-2](#)

Sensor Key pane

button functions [14-11](#)

described [14-10](#)

field descriptions [14-11](#)

sensor SSH host key

displaying [14-11](#)

generating [14-11](#)

user roles [14-10](#)

sensor license

installing [19-14](#)

obtaining [19-14](#)

sensors

access problems [C-25](#)

application partition image [26-14](#)

asymmetric traffic and disabling anomaly detection [12-35, C-19](#)

- blocking self [15-8](#)
 - command and control interfaces (list) [7-2](#)
 - configuring to use NTP [6-14](#)
 - corrupted SensorApp configuration [C-35](#)
 - diagnostics reports [20-25](#)
 - disaster recovery [C-6](#)
 - downgrading [26-12](#)
 - incorrect NTP configuration [6-11, C-16](#)
 - initializing [6-1, 24-1, 24-4](#)
 - interface support [7-4](#)
 - IP address conflicts [C-27](#)
 - logging in
 - SSH [23-6](#)
 - Telnet [23-6](#)
 - loose connections [C-23](#)
 - misconfigured access lists [C-27](#)
 - no alerts [C-32, C-57](#)
 - not seeing packets [C-34](#)
 - NTP time source [6-14](#)
 - NTP time synchronization [6-11, C-15](#)
 - partitions [A-4](#)
 - physical connectivity [C-31](#)
 - preventive maintenance [C-2](#)
 - rebooting [19-28](#)
 - reimaging [26-3](#)
 - restoring defaults [19-28](#)
 - sensing process not running [C-29](#)
 - setup command [6-1, 24-1, 24-4, 24-7](#)
 - shutting down [19-29](#)
 - statistics [20-26](#)
 - system information [20-27](#)
 - time sources [6-11, C-15](#)
 - troubleshooting software upgrades [C-54](#)
 - updating [19-26](#)
 - upgrading [26-5](#)
 - using NTP time source [6-13](#)
- Sensor Setup window
- described [5-2, 5-4](#)
 - Startup Wizard [5-2, 5-4](#)
- Server Certificate pane
- button functions [14-16](#)
 - certificate
 - displaying [14-16](#)
 - generating [14-16](#)
 - described [14-16](#)
 - field descriptions [14-16](#)
 - user roles [14-16](#)
- server manifest described [A-28](#)
- service account
- accessing [6-18, C-5](#)
 - cautions [6-18, C-5](#)
 - creating [C-6](#)
 - described [6-18, A-31, C-5](#)
 - RADIUS authentication [6-19](#)
 - TAC [A-31](#)
 - troubleshooting [A-31](#)
- Service Activity pane
- described [19-18](#)
 - field descriptions [19-18](#)
- Service DNS engine
- described [B-39](#)
 - parameters (table) [B-39](#)
- Service engine
- described [B-38](#)
 - Layer 5 traffic [B-38](#)
- Service FTP engine
- described [B-40](#)
 - parameters (table) [B-41](#)
 - PASV port spoof [B-40](#)
- Service Generic engine
- described [B-41](#)
 - no custom signatures [B-41](#)
 - parameters (table) [B-42](#)
- Service H225 engine
- ASN.1PER validation [B-43](#)
 - described [B-43](#)
 - features [B-43](#)
 - parameters (table) [B-44](#)

- TPKT validation [B-43](#)
- Service HTTP engine
 - custom signature [10-17](#)
 - described [10-16, B-45](#)
 - example signature [10-17](#)
 - parameters (table) [B-46](#)
- Service IDENT engine
 - described [B-47](#)
 - parameters (table) [B-48](#)
- Service MSRPC engine
 - DCS/RPC protocol [10-11, B-48](#)
 - described [10-11, B-48](#)
 - parameters (table) [B-49](#)
- Service MSSQL engine
 - described [B-50](#)
 - MSSQL protocol [B-50](#)
 - parameters (table) [B-51](#)
- Service NTP engine
 - described [B-51](#)
 - parameters (table) [B-51](#)
- Service P2P engine described [B-52](#)
- service packs described [25-3](#)
- service role [6-18, 23-2, A-30](#)
- Service RPC engine
 - described [10-19, B-52](#)
 - parameters (table) [B-52](#)
 - RPC portmapper [10-19, B-52](#)
- Service SMB Advanced engine
 - described [B-54](#)
 - parameters (table) [B-54](#)
- Service SNMP engine
 - described [B-56](#)
 - parameters (table) [B-56](#)
- Service SSH engine
 - described [B-57](#)
 - parameters (table) [B-57](#)
- Service TNS engine
 - described [B-57](#)
 - parameters (table) [B-58](#)
- session command
 - ASA 5500-X IPS SSP [23-4](#)
 - ASA 5585-X IPS SSP [23-5](#)
- sessioning in
 - ASA 5500-X IPS SSP [23-4](#)
 - ASA 5585-X IPS SSP [23-5](#)
- setting
 - current KB [20-13](#)
 - system clock [6-16](#)
- setting up
 - IME email notification [1-11](#)
 - terminal servers [23-3, 26-16](#)
- setup
 - automatic [24-2](#)
 - command [6-1, 24-1, 24-4, 24-7, 24-13, 24-17](#)
 - simplified mode [24-2](#)
- shared secret
 - described [6-24](#)
 - RADIUS authentication [6-24](#)
- show events command [C-99](#)
- show health command [C-76](#)
- show interfaces command [C-97](#)
- show module 1 details command [C-60, C-71](#)
- show settings command [19-11, C-14](#)
- show statistics command [C-85](#)
- show statistics virtual-sensor command [C-24, C-85](#)
- show tech-support command [C-77](#)
- show version command [C-82](#)
- Shut Down Sensor pane
 - configuring [19-29](#)
 - described [19-29](#)
 - user roles [19-29](#)
- shutting down the sensor [19-29](#)
- sig0 pane
 - column heads [9-11](#)
 - configuration buttons [9-11](#)
 - default [9-11](#)
 - described [9-11](#)
 - field descriptions [9-13](#)

- signatures
 - assigning actions [9-25](#)
 - cloning [9-23](#)
 - tuning [9-24](#)
- tabs [9-11](#)
- signature definition policies
 - adding [9-10](#)
 - cloning [9-10](#)
 - default policy [9-9](#)
 - deleting [9-10](#)
 - sig0 [9-9](#)
- Signature Definitions pane
 - described [9-9](#)
 - field descriptions [9-9](#)
- signature engines
 - AIC [B-10](#)
 - Atomic [B-13](#)
 - Atomic ARP [B-13](#)
 - Atomic IP [10-13, B-24](#)
 - Atomic IP Advanced [B-14](#)
 - Atomic IPv6 [B-27](#)
 - creating custom signatures [10-1](#)
 - described [9-6, B-1](#)
 - Fixed [B-28](#)
 - Flood [B-31](#)
 - Flood Host [B-31](#)
 - Flood Net [B-32](#)
 - list [9-6, B-2](#)
 - Master [B-4](#)
 - Meta [9-29, B-32](#)
 - Multi String [B-34](#)
 - Normalizer [B-35](#)
 - Regex
 - patterns [B-10](#)
 - syntax [B-9](#)
 - Service [B-38](#)
 - Service DNS [B-39](#)
 - Service FTP [B-40](#)
 - Service Generic [B-41](#)
 - Service H225 [B-43](#)
 - Service HTTP [10-16, B-45](#)
 - Service IDENT [B-47](#)
 - Service MSRPC [10-11, B-48](#)
 - Service MSSQL [B-50](#)
 - Service NTP [B-51](#)
 - Service P2P [B-52](#)
 - Service RPC [10-19, B-52](#)
 - Service SMB Advanced [B-54](#)
 - Service SNMP [B-56](#)
 - Service SSH engine [B-57](#)
 - Service TNS [B-57](#)
 - State [10-20, B-59](#)
 - String [10-21, 10-24, B-61](#)
 - supported by IDM [10-2](#)
 - Sweep [10-24, B-66](#)
 - Sweep Other TCP [B-68](#)
 - Traffic Anomaly [B-69](#)
 - Traffic ICMP [B-71](#)
 - Trojan [B-72](#)
- Signature Event Action Filter
 - described [11-6, A-26](#)
 - parameters [11-6, A-26](#)
- Signature Event Action Handler described [11-6, A-26](#)
- Signature Event Action Override described [11-6, A-26](#)
- Signature Event Action Processor
 - Alarm Channel [11-6, A-26](#)
 - components [11-6, A-26](#)
 - described [11-6, A-23, A-26](#)
- signature fidelity rating
 - calculating risk rating [8-5, 11-3](#)
 - described [8-5, 11-2](#)
- signatures
 - adding [9-21](#)
 - alert frequency [9-27](#)
 - assigning actions [9-25](#)
 - cloning [9-23](#)
 - custom [9-2](#)
 - default [9-2](#)

- described [9-1](#)
- disabling [9-21](#)
- editing [9-24](#)
- enabling [9-21](#)
- false positives [9-2](#)
- rate limits [15-4](#)
- retiring [9-21](#)
- String TCP XL [9-38](#)
- subsignatures [9-2](#)
- TCP reset [C-50](#)
- tuned [9-2](#)
- tuning [9-24](#)
- Signatures window
 - field descriptions [5-16](#)
 - user roles [5-15](#)
- Signatures window described [5-15](#)
- signature threat profiles
 - applying [5-17](#)
 - platform support [5-15](#)
- signature update
 - files [25-4](#)
- signature updates
 - bypass mode [19-22](#)
 - FTP server [19-25, 19-26](#)
 - installation time [19-21](#)
 - SensorApp [19-22](#)
- signature variables
 - adding [9-41](#)
 - configuring [9-41](#)
 - deleting [9-41](#)
 - described [9-40](#)
 - editing [9-41](#)
- Signature Variables tab
 - configuring [9-41](#)
 - field descriptions [9-40](#)
- Signature Wizard
 - protocols [10-10](#)
 - signature identification [10-11](#)
- SNMP
 - configuring [17-3](#)
 - described [17-1](#)
 - General Configuration pane
 - field descriptions [17-2](#)
 - user roles [17-2](#)
 - Get [17-1](#)
 - GetNext [17-1](#)
 - Set [17-1](#)
 - supported MIBs [17-10, C-18](#)
 - Trap [17-1](#)
 - Traps Configuration pane
 - field descriptions [17-7](#)
 - user roles [17-7](#)
 - SNMP General Configuration pane
 - configuring [17-3](#)
 - described [17-2](#)
 - SNMP traps
 - configuring [17-8](#)
 - described [17-1](#)
 - SNMPv3 protocol
 - described [17-4](#)
 - SNMPv3 users
 - configuring [17-6](#)
 - SNMPv3 Users pane
 - configuring [17-6](#)
 - described [17-4](#)
 - field descriptions [17-4](#)
- software architecture
 - ARC (illustration) [A-13](#)
 - IDAPI (illustration) [A-32](#)
- software downloads Cisco.com [25-5](#)
- software file names
 - recovery (illustration) [25-5](#)
 - signature/virus updates (illustration) [25-4](#)
 - system image (illustration) [25-5](#)
- software release examples
 - platform identifiers [25-6](#)
 - platform-independent [25-5](#)

- software updates
 - supported FTP servers [19-21, 26-3](#)
 - supported HTTP/HTTPS servers [19-21, 26-3](#)
- SPAN port issues [C-31](#)
- specialized [22-2](#)
- Specialized Reports described [22-2](#)
- SSH
 - described [14-1](#)
 - security [14-1](#)
- SSH Server
 - private keys [A-21](#)
 - public keys [A-21](#)
- standards
 - CIDEE [A-34](#)
 - IDCONF [A-33](#)
 - IDIOM [A-32](#)
 - SDEE [19-19, A-33](#)
- Startup Wizard
 - access lists [5-3](#)
 - adding ACLs [5-6](#)
 - adding virtual sensors [5-14](#)
 - Add Virtual Sensor dialog box [5-13](#)
 - Auto Update configuring [5-18](#)
 - described [5-1](#)
 - Inline Interface Pair window
 - described [5-10](#)
 - field descriptions [5-10](#)
 - Inline VLAN Pairs window configuring [5-11](#)
 - Interface Selection window [5-10](#)
 - Interface Summary window [5-8](#)
 - Sensor Setup window
 - configuring [5-5](#)
 - described [5-2, 5-4](#)
 - field descriptions [5-2](#)
 - Signatures window described [5-15](#)
 - Traffic Inspection Mode window [5-9](#)
 - Virtual Sensors window
 - described [5-12](#)
 - field descriptions [5-13](#)
 - VLAN groups unsupported [5-1, 5-8](#)
- State engine
 - Cisco Login [10-20, B-59](#)
 - described [10-20, B-59](#)
 - LPR Format String [10-20, B-59](#)
 - parameters (table) [B-59](#)
 - SMTP [10-20, B-59](#)
- statistic display [C-86](#)
- Statistics pane
 - button functions [20-26](#)
 - categories [20-25](#)
 - described [20-25](#)
 - using [20-26](#)
- statistics viewing [20-26](#)
- String engine described [10-21, 10-24, B-61](#)
- String ICMP engine parameters (table) [B-61](#)
- String TCP engine
 - custom signature [10-22](#)
 - example signature [10-22](#)
 - parameters (table) [B-61](#)
- String TCP XL signature (example) [9-35, 9-38](#)
- String UDP engine parameters (table) [B-62](#)
- String XL engine
 - description [B-63](#)
 - hardware support [9-8, 10-3, B-3, B-63](#)
 - parameters (table) [B-64](#)
 - unsupported parameters [B-66](#)
- subinterface 0 described [7-14](#)
- subsignatures described [9-2](#)
- summarization
 - described [8-7, 11-5](#)
 - Fire All [8-7, 11-5](#)
 - Fire Once [8-8, 11-5](#)
 - Global Summarization [8-7, 11-5](#)
 - Meta engine [8-7, 11-5](#)
 - Summary [8-7, 11-5](#)
- Summarizer described [8-39, 11-33](#)
- Summary pane
 - described [7-17](#)

- field descriptions [7-17](#)
- supported
 - FTP servers [19-21, 26-3](#)
 - HTTP/HTTPS servers [19-21, 26-3](#)
 - IPS interfaces for CSA MC [18-3](#)
- supported sensors
 - signature threat profiles [5-15](#)
- Sweep engine [10-25, B-67](#)
 - described [10-24, B-66](#)
 - parameters (table) [B-67](#)
- Sweep Other TCP engine
 - described [B-68](#)
 - parameters (table) [B-69](#)
- SwitchApp
 - described [A-29](#)
- switches
 - TCP reset interfaces [7-7](#)
- sw-module module slot_number password-reset command [19-7, C-10](#)
- system architecture
 - directory structure [A-34](#)
 - supported platforms [A-1](#)
- system clock setting [6-16](#)
- system components IDAPI [A-32](#)
- System Configuration Dialog
 - described [24-2](#)
 - example [24-2](#)
- system design (illustration) [A-2, A-3](#)
- system images
 - installing
 - ASA 5500-X IPS SSP [26-22](#)
 - IPS 4345 [26-17](#)
 - IPS 4360 [26-17](#)
 - IPS 4510 [26-20](#)
 - IPS 4520 [26-20](#)
 - IPS 4520-XL [26-20](#)
- System Information pane
 - described [20-26](#)
 - using [20-27](#)

- system information viewing [20-27](#)

T

TAC

- contact information [20-26](#)
- service account [6-18, A-31, C-5](#)
- show tech-support command [C-77](#)
- troubleshooting [A-31](#)

target value rating

- calculating risk rating [8-6, 11-3](#)
- described [8-6, 8-25, 8-26, 11-3, 11-20, 11-21](#)

TCP fragmentation described [B-36](#)

TCP Protocol tab

- described [12-16, 12-23, 12-29](#)
- enabling TCP [12-16](#)
- external zone [12-29](#)
- field descriptions [12-16, 12-23, 12-29](#)
- illegal zone [12-23](#)

TCP reset interfaces

- conditions [7-7](#)
- described [7-6](#)
- list [7-7](#)
- promiscuous mode [7-7](#)
- switches [7-7](#)

TCP resets

- not occurring [C-50](#)

TCP stream reassembly

- described [9-56](#)
- parameters (table) [9-57](#)
- signatures (table) [9-57](#)

TCP stream reassembly mode [9-63](#)

tech support information display [C-78](#)

terminal server setup [23-3, 26-16](#)

TFN2K

- described [B-71](#)
- Trojans [B-72](#)

TFTP servers

- maximum file size limitation [26-16](#)

- RTT [26-16](#)
- Threat Category tab
 - described [8-38, 11-32](#)
 - field descriptions [8-38, 11-33](#)
- threat profiles
 - applying [9-19](#)
 - changing [9-19](#)
 - removing [9-19](#)
- threat rating
 - described [8-6, 11-4](#)
 - risk rating [8-6, 11-4](#)
- Thresholds for KB Name window
 - described [20-10](#)
 - field descriptions [20-10](#)
 - filtering information [20-10](#)
- time
 - correction on the sensor [6-12, C-17](#)
 - sensors [6-11, C-15](#)
 - synchronizing IPS clocks [C-16](#)
- Time pane
 - configuring [6-9](#)
 - described [6-7](#)
 - field descriptions [6-8](#)
 - user roles [6-7](#)
- time sources
 - appliances [6-11, C-15](#)
 - ASA 5500-X IPS SSP [5-12, 6-11, C-15](#)
 - ASA 5585-X IPS SSP [5-12, 6-11, C-15](#)
- TLS
 - described [6-4](#)
 - handshaking [14-12](#)
 - IDM [14-11](#)
 - web server [14-11](#)
- Top Applications gadget
 - configuring [3-9](#)
 - described [3-9](#)
- Top Attacker Reports described [1-15, 22-1](#)
- Top Attackers gadgets
 - configuring [3-12](#)
 - described [3-11](#)
- Top Signature Reports described [1-15, 22-2](#)
- Top Signatures gadgets
 - configuring [3-13](#)
 - described [3-13](#)
- Top Victim Reports described [1-15, 22-2](#)
- Top Victims gadgets
 - configuring [3-12](#)
 - described [3-12](#)
- traceroute device tool (IME) [1-3, 2-6, 3-15, 3-16, 21-6](#)
- Traffic Anomaly engine
 - described [B-69](#)
 - protocols [B-69](#)
 - signatures [B-69](#)
- traffic flow notifications
 - configuring [7-32](#)
 - described [7-32](#)
- Traffic Flow Notifications pane
 - configuring [7-32](#)
 - field descriptions [7-32](#)
 - user roles [7-32](#)
- Traffic ICMP engine
 - DDoS [B-71](#)
 - described [B-71](#)
 - LOKI [B-71](#)
 - parameters (table) [B-72](#)
 - TFN2K [B-71](#)
- Traffic Inspection Mode window described [5-9](#)
- Traps Configuration pane
 - configuring [17-8](#)
 - described [17-7](#)
- trial license key [19-12](#)
- Tribe Flood Network. See TFN.
- Tribe Flood Network 2000. See TFN2K.
- Trojan engine
 - BO2K [B-72](#)
 - described [B-72](#)
 - TFN2K [B-72](#)

- Trojans
 - BO [B-72](#)
 - BO2K [B-72](#)
 - LOKI [B-72](#)
 - TFN2K [B-72](#)
- troubleshooting
 - Analysis Engine busy [C-56](#)
 - applying software updates [C-53](#)
 - ARC
 - blocking not occurring for signature [C-42](#)
 - device access issues [C-40](#)
 - enabling SSH [C-42](#)
 - inactive state [C-38](#)
 - misconfigured master blocking sensor [C-43](#)
 - verifying device interfaces [C-41](#)
 - ASA 5500-X IPS SSP
 - commands [C-60](#)
 - failover scenarios [C-59](#)
 - ASA 5585-X IPS SSP
 - commands [C-71](#)
 - failover scenarios [C-70](#)
 - traffic flow stopped [C-71](#)
 - automatic updates [C-53](#)
 - cannot access sensor [C-25](#)
 - cidDump [C-103](#)
 - cidLog messages to syslog [C-49](#)
 - communication [C-24](#)
 - corrupted SensorApp configuration [C-35](#)
 - debug logger zone names (table) [C-49](#)
 - debug logging [C-45](#)
 - disaster recovery [C-6](#)
 - duplicate sensor IP addresses [C-27](#)
 - enabling debug logging [C-45](#)
 - external product interfaces [18-10, C-22](#)
 - gathering information [C-76](#)
 - global correlation [13-11, C-21](#)
 - IDM
 - cannot access sensor [C-56](#)
 - will not load [C-55](#)
 - IME time synchronization [C-58](#)
 - IPS clock time drift [6-11, C-16](#)
 - misconfigured access list [C-27](#)
 - no alerts [C-32, C-57](#)
 - password recovery [19-11, C-15](#)
 - physical connectivity issues [C-31](#)
 - preventive maintenance [C-2](#)
 - RADIUS
 - attempt limit [C-21](#)
 - reset not occurring for a signature [C-50](#)
 - sensing process not running [C-29](#)
 - sensor events [C-98](#)
 - sensor loose connections [C-23](#)
 - sensor not seeing packets [C-34](#)
 - sensor software upgrade [C-54](#)
 - service account [6-18, C-5](#)
 - show events command [C-98](#)
 - show interfaces command [C-97](#)
 - show tech-support command [C-77, C-79](#)
 - show version command [C-82](#)
 - software upgrades [C-52](#)
 - SPAN
 - port issue [C-31](#)
 - upgrading [C-52](#)
 - verifying Analysis Engine is running [C-20](#)
 - verifying ARC status [C-37](#)
- Trusted Hosts pane
 - configuring [14-13](#)
 - described [14-13](#)
 - field descriptions [14-13](#)
- Trusted Root Certificates pane
 - configuring [14-15](#)
 - described [14-14](#)
 - field descriptions [14-15](#)
- tuned signatures described [9-2](#)
- tuning
 - AIC signatures [9-52](#)
 - IP fragment reassembly signatures [9-56](#)
 - signatures [9-24](#)

TCP fragment reassembly signatures [9-64](#)

U

UDP Protocol tab

described [12-17, 12-24, 12-30](#)

enabling UDP [12-17](#)

external zone [12-30](#)

field descriptions [12-17, 12-31](#)

illegal zone [12-24](#)

unassigned VLAN groups described [7-14](#)

unauthenticated NTP [6-11, 6-14, C-15](#)

uninstalling

license key [19-15](#)

UNIX-style directory listings [19-21](#)

unlocking accounts [6-26](#)

unlock user username command [6-26](#)

Update Sensor pane

configuring [19-26](#)

described [19-25](#)

field descriptions [19-26](#)

user roles [19-25](#)

updating

sensors [19-26](#)

sensors immediately [26-12](#)

trusted root certificates [14-15](#)

upgrade command [26-4, 26-7](#)

upgrade notes and caveats

upgrading IPS software [26-1](#)

upgrading

application partition [26-14](#)

latest version [C-52](#)

recovery partition [26-7](#)

sensors [26-5](#)

upgrading IPS software

upgrade notes and caveats [26-1](#)

uploading KBs

FTP [20-16](#)

SCP [20-16](#)

Upload Knowledge Base to Sensor dialog box

described [20-16](#)

field descriptions [20-16](#)

URLs for Cisco Security Intelligence Operations [25-7](#)

user-defined reports described [22-1](#)

user roles authentication [6-19](#)

users

configuring [6-23](#)

using

debug logging [C-45](#)

TCP reset interfaces [7-7](#)

V

VACLs

described [15-3](#)

Post-Block [15-21](#)

Pre-Block [15-21](#)

verifying

NTP configuration [6-12](#)

password recovery [19-11, C-14](#)

sensor initialization [24-21](#)

sensor setup [24-21](#)

version display [C-82](#)

video help described [1-3](#)

viewing

denied attacker hit counts [16-2](#)

denied attackers list [16-2](#)

IP logs [16-12](#)

license key status [19-12](#)

statistics [20-26](#)

system information [20-27](#)

virtualization

advantages [8-3, C-17](#)

restrictions [8-3, C-17](#)

supported sensors [8-3, C-18](#)

traffic capture requirements [8-3, C-17](#)

virtual-sensor name command [8-16](#)

virtual sensors

- adding [5-14, 8-12](#)
- adding (ASA 5500-X IPS SSP) [8-16](#)
- adding (ASA 5585-X IPS SSP) [8-16](#)
- ASA 5500-X IPS SSP [8-18](#)
- ASA 5585-X IPS SSP [8-18](#)
- creating (ASA 5500-X IPS SSP) [8-16](#)
- creating (ASA 5585-X IPS SSP) [8-16](#)
- default virtual sensor [8-2, 8-8](#)
- deleting [8-12](#)
- described [8-2, 8-8](#)
- editing [8-12](#)
- options [8-16](#)

Virtual Sensors window

- described [5-12](#)

VLAN groups

- 802.1q encapsulation [7-14](#)
- configuration restrictions [7-9](#)
- configuring [7-30](#)
- deploying [7-29](#)
- switches [7-29](#)
- VLAN IDs [7-28](#)

VLAN groups mode

- described [7-14](#)

VLAN Groups pane

- configuring [7-30](#)
- described [7-28](#)
- field descriptions [7-29](#)
- user roles [7-28](#)

VLAN Pairs pane

- configuring [7-27](#)
- described [7-26](#)
- field descriptions [7-27](#)
- user roles [7-26](#)

vulnerable OSES field described [B-6](#)

W

watch list rating

- calculating risk rating [8-6, 11-3](#)
- described [8-6, 11-3](#)

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 [14-11](#)

whois device tool (IME) [1-3, 2-6, 3-15, 3-16, 21-6](#)

worms

- Blaster [12-2](#)
- Code Red [12-2](#)
- histograms [12-13, 20-8](#)
- Nimda [12-2](#)
- protocols [12-3](#)
- Sasser [12-2](#)
- scanners [12-3](#)
- Slammer [12-2](#)
- SQL Slammer [12-2](#)

Z

zones

- external [12-5](#)
- illegal [12-5](#)
- internal [12-5](#)

