



Numerics

802.1q encapsulation for VLAN groups [5-24](#)

A

AAA authentication

 configuring [4-23](#)

AAA RADIUS

 functionality [4-30](#)

 limitations [4-30](#)

accessing

 IPS software [18-2](#)

 service account [4-28, C-5](#)

access-list command [4-6](#)

access list misconfiguration [C-22](#)

access lists

 changing [4-7](#)

 configuring [4-7](#)

account locking

 configuring [4-34](#)

 security [4-34](#)

account unlocking configuring [4-35](#)

ACLs

 described [14-3](#)

 Post-Block [14-22, 14-23](#)

 Pre-Block [14-22, 14-23](#)

adding

 denied attackers [8-36](#)

 event action overrides [8-18](#)

 external product interfaces [11-5](#)

 global parameters [6-11](#)

 hosts to the SSH known hosts list [4-46, 4-47](#)

 login banners [4-9](#)

 signature variables [7-10](#)

 target value ratings [8-16](#)

 trusted hosts [4-52](#)

 users [4-18, 4-19, 4-31, 4-32](#)

 virtual sensors [6-6, 6-8](#)

Address Resolution Protocol. See ARP.

administrative tasks notes and caveats [17-2](#)

administrator role privileges [1-3](#)

aggregation

 alert frequency [8-34](#)

 operating modes [8-34](#)

AIC engine

 AIC FTP [B-11](#)

 AIC FTP engine parameters (table) [B-13](#)

 AIC HTTP [B-11](#)

 AIC HTTP engine parameters (table) [B-12](#)

 described [B-11](#)

 features [B-11](#)

 signature categories [7-23](#)

AIC policy enforcement

 default configuration [7-23, B-11](#)

 described [7-23, B-11](#)

 sensor oversubscription [7-23, B-11](#)

Alarm Channel

 described [8-3, A-26](#)

 risk rating [10-6](#)

alert and log actions (list) [8-5](#)

alert-frequency command [7-12](#)

alert frequency modes [B-7](#)

alert-severity command [7-14](#)

alert severity configuring [7-14](#)

allow-sensor-block command [14-8](#)

- alternate TCP reset interface
 - configuration restrictions [5-7](#)
 - designating [5-4](#)
 - restrictions [5-2](#)
- Analysis Engine
 - described [6-1](#)
 - error messages [C-19](#)
 - IDM exits [C-50](#)
 - sensing interfaces [5-3](#)
 - verify it is running [C-15](#)
 - virtual sensors [6-1](#)
- anomaly detection [9-1](#)
 - asymmetric traffic [9-1, 9-2](#)
 - caution [9-1, 9-2](#)
 - configuration sequence [9-5](#)
 - default anomaly detection configuration [9-4](#)
 - default configuration (example) [9-4](#)
 - described [9-2](#)
 - detect mode [9-4](#)
 - enabling [9-8](#)
 - event actions [9-6, B-70](#)
 - inactive mode [9-4](#)
 - learning accept mode [9-3](#)
 - learning process [9-3](#)
 - limiting false positives [9-37](#)
 - protocols [9-3](#)
 - signatures (table) [9-6, B-71](#)
 - signatures described [9-6](#)
 - worms
 - attacks [9-37](#)
 - described [9-3](#)
 - zones [9-4](#)
- anomaly detection disabling [9-48, C-14](#)
- anomaly-detection load command [9-41](#)
- anomaly detection operational settings
 - configuring [9-11, 9-38](#)
 - described [9-10](#)
- anomaly detection policies
 - copying [9-9](#)
 - creating [9-9](#)
 - deleting [9-9](#)
 - displaying [9-9](#)
 - editing [9-9](#)
 - lists [17-23](#)
- anomaly-detection save command [9-41](#)
- anomaly detection statistics
 - clearing [9-47](#)
 - displaying [9-47](#)
- Anomaly Detection zones
 - illegal [9-20](#)
 - internal [9-12](#)
- appliances
 - GRUB menu [17-3, C-8](#)
 - initializing [3-8](#)
 - logging in [2-2](#)
 - password recovery [17-3, C-8](#)
 - resetting [17-40](#)
 - setting system clock [4-38, 17-21](#)
 - terminal servers
 - described [2-3, 19-15](#)
 - setting up [2-3, 19-15](#)
 - upgrading recovery partition [19-7](#)
- Application Inspection and Control. See AIC.
- application partition
 - described [A-4](#)
 - image recovery [19-14](#)
- application-policy command [7-23](#)
- application policy configuring [7-24](#)
- application policy enforcement described [7-23, B-11](#)
- applications in XML format [A-4](#)
- applying
 - software updates [C-47](#)
 - threat profiles [7-6](#)
- ARC
 - ACLs [14-22, A-14](#)
 - authentication [A-15](#)
 - blocking
 - connection-based [A-17](#)

- response [A-13](#)
- unconditional blocking [A-17](#)
- blocking application [14-2](#)
- blocking not occurring for signature [C-37](#)
- Catalyst switches
 - VACL commands [A-19](#)
 - VACLs [A-16, A-19](#)
 - VLANs [A-16](#)
- checking status [14-4, 14-5](#)
- described [A-4](#)
- design [14-2](#)
- device access issues [C-35](#)
- enabling SSH [C-37](#)
- 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 [14-1](#)
- functions [14-2, A-12](#)
- illustration [A-13](#)
- inactive state [C-33](#)
- interfaces [A-14](#)
- maintaining states [A-16](#)
- master blocking sensors [A-14](#)
- maximum blocks [14-2](#)
- misconfigured master blocking sensor [C-38](#)
- nac.shun.txt file [A-16](#)
- NAT addressing [A-15](#)
- number of blocks [A-15](#)
- postblock ACL [A-16](#)
- preblock ACL [A-16](#)
- prerequisites [14-6](#)
- rate limiting [14-4](#)
- responsibilities [A-13](#)
- single point of control [A-15](#)
- SSH [A-14](#)
- supported devices [14-6, A-15](#)
- Telnet [A-14](#)
- troubleshooting [C-31](#)
- VACLs [A-14](#)
- verifying device interfaces [C-36](#)
- verifying status [C-32](#)
- ARP
 - Layer 2 signatures [B-14](#)
 - protocol [B-14](#)
- ARP spoof tools
 - dsniff [B-14](#)
 - ettercap [B-14](#)
- assigning interfaces to virtual sensors [6-4](#)
- assigning policies to virtual sensors [6-4](#)
- asymmetric mode
 - described [6-3](#)
 - normalization [6-3](#)
- asymmetric traffic
 - anomaly detection [9-1, 9-2](#)
 - caution [9-1, 9-2](#)
- asymmetric traffic and disabling anomaly detection [9-48, C-14](#)
- Atomic ARP engine
 - described [B-14](#)
 - parameters (table) [B-14](#)
- Atomic IP Advanced engine
 - described [B-15](#)
 - parameters (table) [B-17](#)
 - restrictions [B-16](#)
- Atomic IP engine
 - described [B-25](#)
 - parameters (table) [B-25](#)
- Atomic IPv6 engine
 - described [B-28](#)
- Neighborhood Discovery protocol [B-29](#)
- signatures [B-29](#)

attack relevance rating
 calculating risk rating [8-14](#)
 described [8-14, 8-27](#)

Attack Response Controller

described [A-4](#)
 formerly known as Network Access Controller [A-4](#)
 See ARC

attack severity rating
 calculating risk rating [8-14](#)
 described [8-14](#)

attempt limit

RADIUS [C-16](#)

attemptLimit command [4-34](#)

audit mode

described [10-9](#)
 testing global correlation [10-9](#)

authenticated NTP [4-2, 4-36, 4-44, C-11](#)

authentication

local [4-20](#)
 RADIUS [4-20](#)

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

user roles [A-30](#)

authorized keys

defining [4-49](#)
 RSA authentication [4-48](#)

automatic setup [3-3](#)

automatic update

DNS servers [4-11](#)
 immediate [19-11](#)
 proxy server [4-11](#)

automatic upgrade

information required [19-8](#)
 troubleshooting [C-47](#)

autoupdatenow command [19-11](#)

auto-upgrade-option command [19-8](#)

B

backing up

configuration [16-24, C-2](#)
 current configuration [16-23, C-4](#)

BackOrifice. See BO.

BackOrifice 2000. See BO2K.

backup-config command [16-20](#)

banner login command [17-14](#)

basic setup [3-5](#)

block connection command [14-33](#)

block-enable command [14-9](#)

block hosts command [14-31](#)

blocking

addresses never to block [14-19](#)
 block time [14-13](#)
 connection [14-33](#)
 described [14-2](#)
 disabling [14-10](#)
 hosts [14-31](#)
 list of blocked hosts [14-33](#)
 managing firewalls [14-27](#)
 managing routers [14-23](#)
 managing switches [14-26](#)
 master blocking sensor [14-28](#)
 maximum entries [14-11](#)
 necessary information [14-3](#)
 notes and caveats [14-1](#)
 prerequisites [14-6](#)
 properties [14-7](#)
 sensor block itself [14-8](#)
 show statistics [14-33](#)
 supported devices [14-6](#)

- types [14-3](#)
 - user profiles [14-20](#)
 - blocking not occurring for signature [C-37](#)
 - block network command [14-32](#)
 - BO
 - described [B-73](#)
 - Trojans [B-73](#)
 - BO2K
 - described [B-73](#)
 - Trojans [B-73](#)
 - BST
 - described [C-1](#)
 - URL [C-1](#)
 - Bug Search Tool. See BST.
 - bypass mode
 - configuring [5-39](#)
 - described [5-39](#)
 - bypass-option command [5-39](#)
-
- ## C
- calculating risk rating
 - attack relevance rating [8-14](#)
 - attack severity rating [8-14](#)
 - promiscuous delta [8-14](#)
 - signature fidelity rating [8-13](#)
 - target value rating [8-14](#)
 - watch list rating [8-14](#)
 - cannot access sensor [C-20](#)
 - capture packet files
 - notes and caveats [13-1](#)
 - capturing live traffic [13-5](#)
 - caution for clearing databases [17-6](#)
 - CDP mode
 - configuring [5-42](#)
 - described [5-42](#)
 - interfaces [5-42](#)
 - certificates (IDM) [4-51](#)
 - changing
 - access lists [4-7](#)
 - CLI inactivity timeout [4-14](#)
 - FTP timeout [4-8](#)
 - host IP address [4-4](#)
 - hostname [4-3](#)
 - passwords [4-30](#)
 - privilege [4-31](#)
 - web server settings [4-16](#)
 - cidDump obtaining information [C-81](#)
 - CIDEE
 - defined [A-34](#)
 - example [A-34](#)
 - IPS extensions [A-34](#)
 - protocol [A-34](#)
 - supported IPS events [A-34](#)
 - cisco
 - default password [2-2](#)
 - default username [2-2](#)
 - Cisco.com
 - accessing software [18-2](#)
 - downloading software [18-1](#)
 - software downloads [18-1](#)
 - Cisco Bug Search Tool
 - described [C-1](#)
 - Cisco Discovery Protocol. See CDP.
 - Cisco IOS rate limiting [14-4](#)
 - cisco-security-agents-mc-settings command [11-4](#)
 - Cisco Security Intelligence Operations
 - described [18-7](#)
 - URL [18-7](#)
 - Cisco Services for IPS
 - service contract [4-55](#)
 - supported products [4-55](#)
 - clear database command [17-6](#)
 - clear denied-attackers command [8-37, 17-21](#)
 - clear events command [4-36, 8-42, 17-19, C-12, C-81](#)
 - clearing
 - anomaly detection statistics [9-47](#)
 - denied attackers statistics [8-37, 17-21](#)

- events [8-42, 17-19, C-81](#)
- global correlation statistics [10-14](#)
- OS IDs [8-32](#)
- sensor databases [17-6](#)
- statistics [17-24, C-62](#)
- clearing databases caution [17-6](#)
- clear line command [17-15](#)
- clear os-identification command [8-32](#)
- CLI
 - command line editing [1-6](#)
 - command modes [1-7](#)
 - default keywords [1-10](#)
 - described [A-4, A-30](#)
 - error messages [D-1](#)
 - generic commands [1-10](#)
 - password recovery [17-5, C-10](#)
 - regular expression syntax [1-8](#)
- CLI behavior [1-5](#)
 - case sensitivity [1-6](#)
 - display options [1-6](#)
 - help [1-5](#)
 - prompts [1-5](#)
 - recall [1-5](#)
 - tab completion [1-5](#)
- client manifest described [A-28](#)
- CLI guide introduction [1-1](#)
- CLI inactivity timeout
 - configuring [4-14](#)
 - described [4-14](#)
- cli-inactivity-timeout command [4-14](#)
- CLI session termination [17-15](#)
- clock set command [4-38, 17-20](#)
- CollaborationApp described [A-4, A-28](#)
- command and control interface
 - described [5-3](#)
 - list [5-3](#)
- command line editing (table) [1-6](#)
- command modes [1-7](#)
 - anomaly detection configuration [1-7](#)
 - event action rules configuration [1-7](#)
 - EXEC [1-7](#)
 - global configuration [1-7](#)
 - privileged EXEC [1-7](#)
 - service mode configuration [1-7](#)
 - signature definition configuration [1-7](#)
- commands [15-4](#)
 - access-list [4-6](#)
 - alert-frequency [7-12](#)
 - alert-severity [7-14](#)
 - allow-sensor-block [14-8](#)
 - anomaly-detection load [9-41](#)
 - anomaly-detection save [9-41](#)
 - application-policy [7-23](#)
 - attemptLimit [4-34](#)
 - autoupdatenow [19-11](#)
 - auto-upgrade-option [19-8](#)
 - backup-config [16-20](#)
 - banner login [17-14](#)
 - block connection [14-33](#)
 - block-enable [14-9](#)
 - block hosts [14-31](#)
 - block network [14-32](#)
 - bypass-option [5-39](#)
 - cisco-security-agents-mc-settings [11-4](#)
 - clear database [17-6](#)
 - clear denied-attackers [8-37, 17-21](#)
 - clear events [4-36, 8-42, 17-19, C-12, C-81](#)
 - clear line [17-15](#)
 - clear os-identification [8-32](#)
 - cli-inactivity-timeout [4-14](#)
 - clock set [4-38, 17-20](#)
 - copy ad-knowledge-base [9-42](#)
 - copy anomaly-detection [9-8](#)
 - copy backup-config [16-21, C-3](#)
 - copy current-config [16-21, C-3](#)
 - copy event-action-rules [8-8](#)
 - copy iplog [12-7](#)
 - copy license-key [4-55](#)

- copy packet-file [13-6](#)
- copy signature-definition [7-2](#)
- current-config [16-20](#)
- default service anomaly-detection [9-9](#)
- default service event-action-rules [8-8](#)
- default service signature-definition [7-2](#)
- deny attacker [8-36](#)
- downgrade [19-12](#)
- enable-acl-logging [14-14](#)
- enable-detail-traps [15-4](#)
- enable-nvram-write [14-15](#)
- erase [16-24](#)
- erase ad-knowledge-base [9-42](#)
- erase license-key [4-57](#)
- erase packet-file [13-7](#)
- event-action [7-20](#)
- event-action-rules-configurations [17-23](#)
- event-counter [7-15](#)
- external-zone [9-28](#)
- filters [8-22](#)
- fragment-reassembly [7-35](#)
- ftp-timeout [4-8](#)
- global-block-timeout [8-34, 14-13](#)
- global-deny-timeout [8-34](#)
- global-filters-status [8-34](#)
- global-metaevent-status [8-34](#)
- global-overrides-status [8-34](#)
- global-parameters [6-11](#)
- global-summarization [8-35](#)
- health-monitor [10-8](#)
- host-ip [4-4](#)
- host-name [4-3](#)
- ignore [9-10](#)
- illegal-zone [9-20](#)
- inline-interfaces [5-14](#)
- interface-notifications [5-40](#)
- internal-zone [9-12](#)
- ip-log [7-44](#)
- iplog [12-3](#)
- ip-log-bytes [12-2](#)
- ip-log-packets [12-2](#)
- iplog-status [12-5](#)
- ip-log-time [12-2](#)
- ipv6-target-value [8-15](#)
- learning-accept-mode [9-38](#)
- list anomaly-detection-configurations [9-9, 17-23](#)
- list event-action-rules-configurations [8-8](#)
- list signature-definition-configurations [7-2](#)
- log-all-block-events-and-errors [14-16](#)
- login-banner-text [4-9](#)
- max-block-entries [14-11](#)
- max-denied-attackers [8-35](#)
- max-interfaces [14-17](#)
- more [16-20](#)
- more current-config [16-1](#)
- never-block-hosts [14-19](#)
- never-block-networks [14-19](#)
- no iplog [12-6](#)
- no ipv6-target-value [8-15](#)
- no service anomaly-detection [9-9](#)
- no service event-action-rules [8-8](#)
- no service signature-definition [7-2](#)
- no target-value [8-15](#)
- no variables [8-11](#)
- os-identifications [8-28](#)
- other [9-18, 9-26, 9-34](#)
- overrides [8-18](#)
- packet capture [13-4](#)
- packet-display [13-2](#)
- password [4-18, 4-30](#)
- permit-packet-logging [4-26](#)
- physical-interfaces [5-8, 5-19, 5-25](#)
- ping [17-39](#)
- privilege [4-18, 4-31](#)
- rename ad-knowledge-base [9-42](#)
- reset [17-40](#)
- service anomaly-detection [9-8](#)
- service event-action-rules [8-8](#)

- service signature-definition 7-2
- setup 3-1, 3-5, 3-8
- show ad-knowledge-base diff 9-44, 9-45
- show ad-knowledge-base files 9-40, 9-41
- show clock 4-37, 17-20
- show configuration 16-1
- show events 8-39, 17-16, C-78
- show health 10-9, 17-13, C-53
- show history 17-41
- show inspection-load 17-7
- show interfaces 5-43
- show interfaces-history 5-45, C-75
- show inventory 17-41
- show lacp 5-35
- show os-identification 8-32
- show settings 16-3, 16-18, 17-5, 17-43, C-10
- show statistics 14-33, 17-24, C-62
- show statistics anomaly-detection 9-47
- show statistics denied-attackers 8-37, 17-21
- show statistics virtual-sensor 17-24, C-19, C-62
- show tech-support 17-35, C-54
- show users 4-32
- show version 17-36, C-59
- sig-fidelity-rating 7-17, 7-19
- signature-definition-configurations 17-23
- snmp-agent-port 15-2
- snmp-agent-protocol 15-2
- ssh authorized-key 4-48
- ssh-generate-key 4-50
- ssh host-key 4-46, 4-47
- sshv1-fallback 4-13
- status 7-18
- stream-reassembly 7-43
- subinterface-type 5-19, 5-25
- summertime-option non-recurring 4-40
- summertime-option recurring 4-38
- target-value 8-15
- tcp 9-13, 9-21, 9-29
- telnet-option 4-5
- terminal 17-16
- threat-profile 7-5
- time-zone-settings 4-42
- tls generate-key 4-53
- tls trusted-host 4-52
- trace 17-42
- trap-community-name 15-4
- trap-destinations 15-4
- udp 9-15, 9-24, 9-32
- unlock user username 4-35
- upgrade 19-4, 19-7
- username 4-18
- user-profile 14-20
- variables 7-10, 8-11
- virtual-sensor name 6-4
- worm-timeout 9-10
- comparing KBs 9-44
- configuration files
 - backing up 16-24, C-2
 - merging 16-24, C-2
- configuration restrictions
 - alternate TCP reset interface 5-7
 - inline interface pairs 5-7
 - inline VLAN pairs 5-7
 - interfaces 5-6
 - physical interfaces 5-6
 - VLAN groups 5-7
- configured OS mapping (example) 8-28
- configuring
 - AAA authentication 4-23
 - access lists 4-7
 - account locking 4-34
 - account unlocking 4-35
 - ACL logging 14-14
 - alert frequency parameters 7-13
 - alert severity 7-14
 - anomaly detection operational settings 9-11, 9-38
 - application policy 7-24, 7-32
 - automatic IP logging 12-3

- automatic upgrades [19-9](#)
- blocking
 - firewalls [14-27](#)
 - routers [14-23](#)
 - switches [14-26](#)
 - time [14-13](#)
- bypass mode [5-39](#)
- CDP mode [5-42](#)
- cli-inactivity-timeout [4-14](#)
- connection blocking [14-33](#)
- CSA MC IPS interfaces [11-4](#)
- DNS servers [4-11](#)
- event action filters [8-23](#)
- event actions [7-21](#)
- event counter [7-16](#)
- external zone [9-29](#)
- ftp-timeout [4-8](#)
- global correlation [10-10, 10-12](#)
- health statistics [17-10](#)
- host blocks [14-31](#)
- host IP address [4-4](#)
- hostname [4-3](#)
- hosts never to block [14-19](#)
- illegal zone [9-20](#)
- inline interface pairs [5-14](#)
- inline VLAN groups [5-26](#)
- inline VLAN pairs [5-20](#)
- internal zone [9-12](#)
- IP fragment reassembly [7-36](#)
- IP fragment reassembly parameters [7-35, 7-42](#)
- IP logging [7-44](#)
- LACP [5-34](#)
- logging all blocking events and errors [14-16](#)
- logical devices [14-20](#)
- login-banner-text [4-9](#)
- manual IP logging [12-4](#)
- master blocking sensor [14-29](#)
- maximum block entries [14-12](#)
- maximum blocking interfaces [14-18](#)
- maximum denied attackers [8-35](#)
- Meta Event Generator [8-35](#)
- network blocks [14-32](#)
- networks never to block [14-19](#)
- NTP servers [4-43](#)
- NVRAM write [14-15](#)
- OS maps [8-30](#)
- other protocols
 - external zone [9-35](#)
 - illegal zone [9-26](#)
 - internal zone [9-18](#)
- packet command restrictions [4-27](#)
- password policy [4-33](#)
- passwords [4-30](#)
- physical interfaces [5-10](#)
- privilege [4-31](#)
- proxy servers [4-11](#)
- sensor sequence [1-1](#)
- sensor to block itself [14-8](#)
- sensor to use NTP [4-44](#)
- signature fidelity rating [7-17, 7-19](#)
- sshv1-fallback [4-13](#)
- status [7-18](#)
- summarizer [8-35](#)
- summertime
 - non-recurring [4-40](#)
 - recurring [4-38](#)
- TCP
 - external zone [9-30](#)
 - illegal zone [9-22](#)
 - internal zone [9-13](#)
- TCP stream reassembly [7-43](#)
- telnet-option [4-5](#)
- threat profiles [7-6](#)
- time zone settings [4-42](#)
- traffic flow notifications [5-40](#)
- UDP
 - external zone [9-32](#)
 - illegal zone [9-24](#)

- internal zone [9-16](#)
 - upgrades [19-5](#)
 - user profiles [14-20](#)
 - web server settings [4-15](#)
 - configuring interfaces
 - notes and caveats [5-1](#)
 - sequence [5-8](#)
 - control transactions
 - characteristics [A-9](#)
 - request types [A-9](#)
 - copy ad-knowledge-base command [9-42](#)
 - copy anomaly-detection command [9-8](#)
 - copy backup-config command [16-21, C-3](#)
 - copy command syntax [9-42](#)
 - copy current-config command [16-21, C-3](#)
 - copy event-action-rules command [8-8](#)
 - copying
 - anomaly detection policies [9-9](#)
 - event action rules policies [8-8](#)
 - IP log files [12-7](#)
 - KBs [9-42, 9-43](#)
 - packet files [13-7](#)
 - signature definition policies [7-2](#)
 - copy iplog command [12-7](#)
 - copy license-key command [4-55](#)
 - copy packet-file command [13-6](#)
 - copy signature-definition command [7-2](#)
 - correcting time on the sensor [4-36, C-12](#)
 - creating
 - anomaly detection policies [9-9](#)
 - Atomic IP Advanced signatures [7-56](#)
 - banner logins [17-14](#)
 - custom signatures [7-45](#)
 - event action rules policies [8-8](#)
 - event action variables [8-12](#)
 - global parameters [6-11](#)
 - Meta signatures [7-54](#)
 - OS maps [8-30](#)
 - Post-Block VACLs [14-26](#)
 - Pre-Block VACLs [14-26](#)
 - service HTTP signatures [7-50](#)
 - signature definition policies [7-2](#)
 - string TCP signatures [7-47](#)
 - string TCP XL signatures [7-57, 7-61](#)
 - user profiles [14-20](#)
 - virtual sensors [6-6, 6-8](#)
 - creating the service account [4-29, C-5](#)
 - cryptographic account
 - Encryption Software Export Distribution Authorization from [18-2](#)
 - obtaining [18-2](#)
 - CSA MC
 - configuring IPS interfaces [11-4](#)
 - host posture events [11-2, 11-4](#)
 - quarantined IP address events [11-2](#)
 - supported IPS interfaces [11-4](#)
 - CtlTransSource
 - described [A-4, A-11](#)
 - illustration [A-12](#)
 - Ctrl-N [1-5](#)
 - Ctrl-P [1-5](#)
 - current-config command [16-20](#)
 - current configuration back up [16-24, C-2](#)
 - custom signatures
 - AIC MIME-type [7-32](#)
 - Atomic IP Advanced signature [7-56](#)
 - configuration sequence [7-45](#)
 - described [7-4](#)
 - Meta signature [7-54](#)
 - service HTTP example [7-50](#)
 - String TCP [7-47](#)
 - String TCP XL [7-57, 7-61](#)
-
- ## D
- data nodes [B-68](#)
 - data structures (examples) [A-8](#)

- DDoS
 - protocols [B-72](#)
 - Stacheldraht [B-72](#)
 - TFN [B-72](#)
- debug logging enable [C-40](#)
- default blocking time [14-13](#)
- default keywords [1-10](#)
- defaults
 - password [2-2](#)
 - username [2-2](#)
 - virtual sensor vs0 [6-2](#)
- default service anomaly-detection command [9-9](#)
- default service event-action-rules command [8-8](#)
- default service signature-definition command [7-2](#)
- defining authorized keys [4-49](#)
- defining signatures [7-1](#)
- deleting
 - anomaly detection policies [9-9](#)
 - denied attackers list [8-37, 17-21](#)
 - event action rules policies [8-8](#)
 - event action variables [8-12](#)
 - inline interface pairs [5-17](#)
 - inline VLAN pairs [5-23](#)
 - OS maps [8-31](#)
 - signature definition policies [7-2](#)
 - signature variables [7-10](#)
 - target value ratings [8-16](#)
 - VLAN groups [5-29](#)
- Denial of Service. See DoS.
- denied attackers add [8-36](#)
- deny actions (list) [8-5](#)
- deny attacker command [8-36](#)
- deny-packet-inline described [8-7](#)
- detect mode (anomaly detection) [9-4](#)
- device access issues [C-35](#)
- diagnosing network connectivity [17-39](#)
- disabling
 - anomaly detection [9-48, C-14](#)
 - blocking [14-10](#)
 - global correlation [10-14](#)
 - password recovery [17-5, C-10](#)
 - signatures [7-18](#)
 - SSHv1 fallback [4-13](#)
 - Telnet [4-5](#)
- disaster recovery [C-6](#)
- displaying
 - anomaly detection policies [9-9](#)
 - anomaly detection policy lists [17-23](#)
 - anomaly detection statistics [9-47](#)
 - contents of logical file [16-20](#)
 - current configuration [16-1](#)
 - current submode configuration [16-3](#)
 - event action rules policies [8-8](#)
 - event actions rules lists [17-23](#)
 - events [8-40, 17-17, C-79](#)
 - global correlation statistics [10-14](#)
 - health status [17-13, C-53](#)
 - inspection load [17-7](#)
 - interface statistics [5-37, 5-43](#)
 - interface traffic history [5-46, C-76](#)
 - IP log contents [12-5](#)
 - KB files [9-40](#)
 - KB thresholds [9-46](#)
 - LACP information [5-37](#)
 - live traffic [13-3](#)
 - OS IDs [8-32](#)
 - password recovery setting [17-5, C-10](#)
 - PEP information [17-41](#)
 - policy lists [17-23](#)
 - signature definition lists [17-23](#)
 - statistics [17-24, C-62](#)
 - submode settings [17-43](#)
 - system clock [4-37, 17-20](#)
 - tech support information [17-36, C-55](#)
 - threat profiles [7-6](#)
 - version [17-37, C-59](#)
- Distributed Denial of Service. See DDoS.

DNS servers

- configuring [4-11](#)

DoS tools

- Stacheldraht [B-72](#)

- stick [B-7](#)

- TFN [B-72](#)

- downgrade command [19-12](#)

- downgrading sensors [19-12](#)

- downloading Cisco software [18-1](#)

- duplicate IP addresses [C-23](#)

E

editing

- anomaly detection policies [9-9](#)

- event action rules policies [8-8](#)

- event action variables [8-12](#)

- signature definition policies [7-2](#)

- signature variables [7-10](#)

- target value ratings [8-16](#)

efficacy

- described [10-5](#)

- measurements [10-5](#)

- enable-acl-logging command [14-14](#)

- enable-detail-traps command [15-4](#)

- enable-nvram-write command [14-15](#)

enabling

- anomaly detection [9-8](#)

- signatures [7-18](#)

- SSHv1 fallback [4-13](#)

- Telnet [4-5](#)

- enabling debug logging [C-40](#)

Encryption Software Export Distribution Authorization form

- cryptographic account [18-2](#)

- described [18-2](#)

engines

- AIC [7-22, B-11](#)

- AIC FTP [B-11](#)

- AIC HTTP [B-11](#)

- Atomic ARP [B-14](#)

- Atomic IP [B-25](#)

- Atomic IP Advanced [B-15](#)

- Atomic IPv6 [B-28](#)

- Fixed [B-29](#)

- Fixed ICMP [B-29](#)

- Fixed TCP [B-29](#)

- Fixed UDP [B-29](#)

- Flood [B-32](#)

- Flood Host [B-32](#)

- Flood Net [B-32](#)

- Master [B-4](#)

- Meta [7-52, B-33](#)

- Multi String [B-35](#)

- Normalizer [B-36](#)

- Service [B-39](#)

- Service DNS [B-39](#)

- Service FTP [B-40](#)

- Service Generic [B-41](#)

- Service H225 [B-43](#)

- Service HTTP [7-49, B-45](#)

- Service IDENT [B-47](#)

- Service MSRPC [B-48](#)

- Service MSSQL [B-50](#)

- Service NTP [B-51](#)

- Service P2P [B-52](#)

- Service RPC [B-52](#)

- Service SMB Advanced [B-54](#)

- Service SNMP [B-56](#)

- Service SSH [B-57](#)

- Service TNS [B-58](#)

- State [B-59](#)

- String [7-46, B-61](#)

- String ICMP [7-46, B-61](#)

- String TCP [7-46, B-61](#)

- String UDP [7-46, B-61](#)

- Sweep [B-67](#)

- Sweep Other TCP [B-69](#)

- Traffic Anomaly [B-70](#)
- Traffic ICMP [B-72](#)
- Trojan [B-73](#)
- erase ad-knowledge-base command [9-42](#)
- erase command [16-24](#)
- erase license-key command [4-57](#)
- erase packet-file command [13-7](#)
- erasing
 - current configuration [16-24](#)
 - KBs [9-42, 9-43](#)
 - packet files [13-7](#)
- error messages
 - described [D-1](#)
 - validation [D-6](#)
- evAlert [A-9](#)
- event-action command [7-20](#)
- event action filters
 - described [8-21](#)
 - using variables [8-21](#)
- event action overrides
 - described [8-17](#)
 - risk rating range [8-17](#)
- event action rules
 - described [8-2](#)
 - functions [8-2](#)
 - notes and caveats [8-1](#)
 - task list [8-8](#)
- event action rules lists display [17-23](#)
- event action rules policies
 - copying [8-8](#)
 - creating [8-8](#)
 - deleting [8-8](#)
 - displaying [8-8](#)
 - editing [8-8](#)
- event actions
 - risk ratings [8-14](#)
 - threat ratings [8-14](#)
- event actions configure [7-21](#)
- event-counter command [7-15](#)
- event counter configure [7-16](#)
- events
 - clearing [8-42, 17-19, C-81](#)
 - displaying [8-40, 17-17, C-79](#)
 - host posture [11-2](#)
 - quarantined IP address [11-2](#)
- Event Store
 - clearing [8-42, 17-19, C-81](#)
 - clearing events [4-36, C-12](#)
 - data structures [A-8](#)
 - described [A-4](#)
 - examples [A-8](#)
 - no alerts [C-27](#)
 - responsibilities [A-7](#)
 - time stamp [4-36, C-12](#)
 - timestamp [A-7](#)
- event types [C-77](#)
- event variables
 - described [8-10](#)
 - example [8-11](#)
- evError [A-9](#)
- evLogTransaction [A-9](#)
- evShunRqst [A-9](#)
- evStatus [A-9](#)
- examples
 - default anomaly detection configuration [9-4](#)
 - KB histogram [9-37](#)
 - password [4-19](#)
 - password policy [4-33](#)
 - privilege [4-19](#)
 - SPAN configuration for IPv6 support [5-13](#)
 - System Configuration Dialog [3-3](#)
 - username [4-19](#)
- external product interfaces
 - adding [11-5](#)
 - described [11-1](#)
 - issues [11-3, C-17](#)
 - notes and caveats [11-1](#)
 - troubleshooting [11-8, C-18](#)

external zone

- configuring [9-29](#)
- configuring other protocols [9-35](#)
- configuring TCP [9-30](#)
- configuring UDP [9-32](#)
- described [9-28](#)

external-zone command [9-28](#)

F

failover

- TCP support [5-33](#)

fallback

- TCP support [5-33](#)

false positives described [7-4](#)

files

- Cisco IPS (list) [18-1](#)

filtering

- more command [16-17](#)
- submode configuration [16-18](#)

filters command [8-22](#)

Fixed engine described [B-29](#)

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

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

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

Flood engine described [B-32](#)

Flood Host engine parameters (table) [B-32](#)

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

fragment-reassembly command [7-35](#)

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

FTP timeout

- configuring [4-8](#)
- described [4-8](#)

ftp-timeout command [4-8](#)

G

generating

- SSH server host key [4-50](#)
- TLS certificate [4-53](#)

generic commands [1-10](#)

global-block-timeout command [8-34, 14-13](#)

global correlation [10-1](#)

described [3-2, 10-2](#)

disabling about [10-13](#)

DNS server [10-7](#)

DNS servers [4-11](#)

error messages [A-29](#)

features [10-6](#)

goals [10-6](#)

health metrics [10-8](#)

health status [10-8](#)

HTTP proxy server [10-7](#)

license [3-1, 3-6, 10-1, 10-7, 10-9](#)

no IPv6 support [8-1, 8-10, 8-11, 8-15, 8-21, 10-2, 10-7](#)

notes and caveats [10-1](#)

options [10-10, 10-11, 10-13](#)

Produce Alert [8-5](#)

proxy servers [4-11](#)

requirements [10-7](#)

risk rating [10-6](#)

troubleshooting [10-13, C-16](#)

update client (illustration) [10-9](#)

Global Correlation Update

client described [A-28](#)

server described [A-28](#)

global-deny-timeout command [8-34](#)

global-filters-status command [8-34](#)

global-metaevent-status command [8-34](#)

global-overrides-status command [8-34](#)

global parameters

adding [6-11](#)

creating [6-11](#)

maximum open IP logs [6-11](#)

- options [6-11](#)
- global-parameters command [6-11](#)
- global-summarization command [8-35](#)
- GRUB menu password recovery [17-3, C-8](#)

H

- H.225.0 protocol [B-43](#)
- H.323 protocol [B-43](#)
- health-monitor command [10-8](#)
- health statistics configuration [17-10](#)
- health status
 - display [17-13, C-53](#)
 - global correlation [10-8](#)
- help
 - question mark [1-5](#)
 - using [1-5](#)
- host blocks configure [14-31](#)
- host IP address
 - changing [4-4](#)
 - configuring [4-4](#)
- host-ip command [4-4](#)
- hostname
 - changing [4-3](#)
 - configuring [4-3](#)
- host-name command [4-3](#)
- host posture events
 - CSA MC [11-4](#)
 - described [11-2](#)
- HTTP/HTTPS servers supported [19-3](#)
- HTTP advanced decoding
 - described [6-4](#)
 - platform support [6-4](#)
 - restrictions [6-4](#)
- HTTP deobfuscation
 - ASCII normalization [7-49, B-45](#)
 - described [7-49, B-45](#)

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-50](#)
 - certificates [4-51](#)
 - TLS [4-51](#)
 - will not load [C-49](#)
- ignore command [9-10](#)
- illegal zone
 - configuring [9-20](#)
 - configuring other protocols [9-26](#)
 - configuring TCP [9-22](#)
 - configuring UDP [9-24](#)
 - described [9-20](#)
 - protocols [9-20](#)
- illegal-zone command [9-20](#)
- IME time synchronization problems [C-52](#)
- inactive mode (anomaly detection) [9-4](#)
- initializing
 - appliances [3-8](#)
 - sensors [3-1, 3-5](#)
 - user roles [3-1, 3-2](#)
 - verifying [3-13](#)
- initializing the sensor (notes and caveats) [3-1](#)

- inline interface pair mode
 - configuration restrictions [5-7](#)
 - described [5-13](#)
 - illustration [5-14](#)
- inline interface pairs
 - configuring [5-14](#)
 - deleting [5-17](#)
- inline-interfaces command [5-14](#)
- inline mode
 - interface cards [5-3](#)
 - normalization [6-3](#)
 - pairing interfaces [5-3](#)
- inline TCP session tracking modes described [6-3](#)
- inline VLAN groups
 - configuring [5-26](#)
 - deleting [5-29](#)
- inline VLAN pair mode
 - configuration restrictions [5-7](#)
 - described [5-18](#)
 - illustration [5-18](#)
 - supported sensors [5-18](#)
- inline VLAN pairs
 - configuring [5-20](#)
 - deleting [5-23](#)
- inspection load
 - description [17-7](#)
 - displaying [17-7](#)
- installer major version [18-5](#)
- installer minor version [18-5](#)
- installing
 - license key [4-56](#)
 - system image
 - IPS 4345 [19-16](#)
 - IPS 4360 [19-16](#)
 - IPS 4510 [19-20](#)
 - IPS 4520 [19-20](#)
- InterfaceApp described [A-4](#)
- interface configuration sequence [5-8](#)
- interface-notifications command [5-40](#)
- interfaces
 - alternate TCP reset [5-2](#)
 - command and control [5-2, 5-3](#)
 - configuration restrictions [5-6](#)
 - described [5-2](#)
 - displaying live traffic [13-3](#)
 - port numbers [5-2](#)
 - sensing [5-2, 5-3](#)
 - slot numbers [5-2](#)
 - support (table) [5-5](#)
 - TCP reset [5-4](#)
- interface statistics displaying [5-37, 5-43](#)
- interface traffic history displaying [5-46, C-76](#)
- internal zone
 - configuring [9-12](#)
 - configuring other protocols [9-18](#)
 - configuring TCP [9-13](#)
 - configuring UDP [9-16](#)
 - described [9-12](#)
 - protocols [9-12](#)
- internal-zone command [9-12](#)
- introducing the CLI guide [1-1](#)
- IP fragmentation described [B-36](#)
- IP fragment reassembly
 - described [7-33](#)
 - parameters (table) [7-33](#)
 - signatures (table) [7-33](#)
- ip-log-bytes command [12-2](#)
- ip-log command [7-44](#)
- iplog command [12-3](#)
- IP log contents
 - displaying [12-5](#)
 - viewing [12-5](#)
- IP log files copying [12-7](#)
- IP logging
 - automatic [12-2](#)
 - configuring [12-2](#)
 - copying files [12-7](#)
 - described [7-44, 12-2](#)

- manual [12-4](#)
 - notes and caveats [12-1](#)
- ip-log-packets command [12-2](#)
- ip logs
 - TCPDUMP [12-2](#)
 - Wireshark [12-2](#)
- iplog-status command [12-5](#)
- ip-log-time command [12-2](#)
- IP packet trace [17-42](#)
- IPS 4345
 - installing system image [19-16](#)
 - password recovery [17-3, C-8, C-9](#)
 - reimaging [19-16](#)
- IPS 4360
 - installing system image [19-16](#)
 - password recovery [17-3, C-8, C-9](#)
 - reimaging [19-16](#)
- IPS 4510
 - installing system image [19-20](#)
 - LACP grouping [5-30](#)
 - password recovery [17-3, C-8, C-9](#)
 - reimaging [19-20](#)
 - SwitchApp [A-29](#)
- IPS 4520
 - installing system image [19-20](#)
 - LACP grouping [5-30](#)
 - password recovery [17-3, C-8, C-9](#)
 - reimaging [19-20](#)
 - SwitchApp [A-29](#)
- IPS applications
 - summary [A-35](#)
 - table [A-35](#)
 - XML format [A-4](#)
- 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 port channel
 - illustration [5-31](#)
- IPS software
 - application list [A-4](#)
 - available files [18-1](#)
 - configuring device parameters [A-5](#)
 - directory structure [A-34](#)
 - Linux OS [A-1](#)
 - obtaining [18-1](#)
 - retrieving data [A-5](#)
 - security features [A-5](#)
 - tuning signatures [A-5](#)
 - updating [A-5](#)
 - user interaction [A-5](#)
 - versioning scheme [18-2](#)
- IPS software file names
 - major updates (illustration) [18-4](#)
 - minor updates (illustration) [18-4](#)
 - patch releases (illustration) [18-4](#)
 - service packs (illustration) [18-4](#)
- IPv4
 - address format [8-10](#)
 - event variables [8-10](#)
- IPv6
 - address format [8-11](#)
 - described [B-28](#)
 - event variables [8-11](#)
 - SPAN ports [5-13](#)
 - switches [5-13](#)
- ipv6-target-value command [8-15](#)

K

KB files

displaying [9-40](#)

KBs

comparing [9-44](#)

copying [9-42, 9-43](#)

described [9-3](#)

erasing [9-42, 9-43](#)

histogram [9-36](#)

initial baseline [9-3](#)

manually loading [9-41](#)

manually saving [9-41](#)

renaming [9-42, 9-43](#)

scanner threshold [9-36](#)

tree structure [9-36](#)

KB thresholds display [9-46](#)

keywords

default [1-10](#)

no [1-10](#)

Knowledge Base. See KB.

L

LACP

configuring [5-34](#)

displaying information [5-37](#)

link states [5-33](#)

restrictions [5-32](#)

learning accept mode

anomaly detection [9-3](#)

learning-accept-mode command [9-38](#)

license key

installing [4-56](#)

obtaining [4-54](#)

trial [4-54](#)

uninstalling [4-57](#)

viewing status of [4-54](#)

licensing

described [4-54](#)

IPS device serial number [4-54](#)

Licensing pane

described [4-54](#)

Link Aggregation Control Protocol Data Unit. See LACPDU.

Link Aggregation Control Protocol. See LACP.

list anomaly-detection-configurations command [9-9, 17-23](#)

list event-action-rules-configurations command [8-8, 17-23](#)

list of blocked hosts [14-33](#)

list signature-definition-configurations command [7-2, 17-23](#)

loading KBs [9-41](#)

log-all-block-events-and-errors command [14-16](#)

Logger

described [A-4, A-19](#)

functions [A-19](#)

syslog messages [A-19](#)

logging in

appliances [2-2](#)

notes and caveats [2-1](#)

sensors

SSH [2-4](#)

Telnet [2-4](#)

service role [2-2](#)

terminal servers [2-3, 19-15](#)

user role [2-1](#)

login banners

adding [4-9](#)

login-banner-text

command [4-9](#)

configuring [4-9](#)

LOKI

described [B-72](#)

protocol [B-72](#)

loose connections on sensors [C-18](#)

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 [18-3](#)

managing

- firewalls [14-27](#)
- routers [14-23](#)
- switches [14-26](#)

manifests

- client [A-28](#)
- server [A-28](#)

manual blocking [14-31, 14-33](#)

manual block to bogus host [C-37](#)

manually loading

- KBs [9-41](#)

manually saving

- KBs [9-41](#)

master blocking sensor

- described [14-28](#)
- not set up properly [C-38](#)
- verifying configuration [C-38](#)

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](#)

max-block-entries command [14-11](#)

max-denied-attackers command [8-35](#)

maximum open IP logs [6-11](#)

max-interfaces command [14-17](#)

merging configuration files [16-24, C-2](#)

Meta engine

- described [7-52, B-33](#)
- parameters (table) [B-34](#)
- Signature Event Action Processor [7-52, B-33](#)

MIBs supported [15-6, C-14](#)

minor updates described [18-3](#)

modes

- anomaly detection detect [9-4](#)
- anomaly detection learning accept [9-3](#)
- asymmetric [6-3](#)
- bypass [5-39](#)
- inactive (anomaly detection) [9-4](#)
- inline interface pair [5-13](#)
- inline TCP tracking [6-3](#)
- inline VLAN pair [5-18](#)
- Normalizer [6-3](#)
- promiscuous [5-12](#)
- VLAN groups [5-23](#)

modifying

- terminal properties [17-16](#)

monitoring

- viewer privileges [1-4](#)

more command [16-20](#)

- filtering [16-17](#)

more current-config command [16-1](#)

moving

- OS maps [8-30](#)

Multi String engine

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

N

Neighborhood Discovery

- options [B-29](#)

- types [B-29](#)
 - network blocks
 - configuring [14-32](#)
 - network connectivity diagnosis [17-39](#)
 - network participation
 - data gathered [10-4](#)
 - data use (table) [3-2, 10-3](#)
 - described [10-4](#)
 - health metrics [10-8](#)
 - modes [10-5](#)
 - requirements [10-4](#)
 - SensorBase Network [10-5](#)
 - statistics [10-5](#)
 - network participation data
 - improving signature fidelity [10-5](#)
 - understanding sensor deployment [10-5](#)
 - never-block-hosts command [14-19](#)
 - never-block-networks command [14-19](#)
 - no iplog command [12-6](#)
 - no ipv6-target-value command [8-15](#)
 - normalization described [6-3](#)
 - Normalizer engine
 - described [B-36](#)
 - IPv6 fragments [B-37](#)
 - modify packets inline [6-3](#)
 - parameters (table) [B-37](#)
 - no service anomaly-detection command [9-9](#)
 - no service event-action-rules command [8-8](#)
 - no service signature-definition command [7-2](#)
 - no target-value command [8-15](#)
 - notes and caveats [7-1, 9-1, 10-1](#)
 - administrative tasks [17-2](#)
 - anomaly detection [9-1](#)
 - blocking [14-1](#)
 - capture packet files [13-1](#)
 - configuring interfaces [5-1](#)
 - event action rules [8-1](#)
 - external product interfaces [11-1](#)
 - initializing the sensor [3-1](#)
 - IP logging [12-1](#)
 - logging in [2-1](#)
 - setting up the sensor [4-1](#)
 - SNMP [15-1](#)
 - virtual sensors [6-1](#)
 - NotificationApp
 - alert information [A-9](#)
 - described [A-4](#)
 - functions [A-9](#)
 - SNMP gets [A-9](#)
 - SNMP traps [A-9](#)
 - statistics [A-11](#)
 - system health information [A-10](#)
 - no variables command [8-11](#)
 - NTP
 - authenticated [4-2, 4-36, 4-44, C-11](#)
 - configuring servers [4-43](#)
 - described [4-36, C-11](#)
 - incorrect configuration [C-12](#)
 - sensor time source [4-43, 4-44](#)
 - time synchronization [4-36, C-11](#)
 - unauthenticated [4-2, 4-36, 4-44, C-11](#)
-
- O**
- obsoletes field described [B-6](#)
 - obtaining
 - command history [17-41](#)
 - cryptographic account [18-2](#)
 - IPS software [18-1](#)
 - license key [4-54](#)
 - list of blocked hosts and connections [14-33](#)
 - used commands list [17-41](#)
 - operator role privileges [1-4](#)
 - options
 - global correlation [10-10, 10-11, 10-13](#)
 - os-identifications command [8-28](#)
 - OS IDs
 - clearing [8-32](#)

- displaying [8-32](#)
- OS information sources [8-27](#)
- OS maps
 - creating [8-30](#)
 - deleting [8-31](#)
 - moving [8-30](#)
- other actions (list) [8-6](#)
- other command [9-18, 9-26, 9-34](#)
- output
 - clearing current line [1-6](#)
 - displaying [1-6](#)
- overrides command [8-18](#)

P

- P2P networks described [B-52](#)
- packet capture command [13-4](#)
- packet command restrictions
 - configuring [4-27](#)
- packet display command [13-2](#)
- packet files
 - viewing
 - TCPDUMP [13-7](#)
 - Wireshark [13-7](#)
- partitions
 - application [A-4](#)
 - recovery [A-4](#)
- passive OS fingerprinting
 - components [8-27](#)
 - configuring [8-28](#)
 - described [8-26](#)
 - enabled (default) [8-28](#)
- password command [4-18, 4-30](#)
- password policy
 - caution [4-32](#)
 - configuring [4-33](#)
- password recovery
 - appliances [17-3, C-8](#)
 - CLI [17-5, C-10](#)
 - described [17-2, C-7](#)
 - disabling [17-5, C-10](#)
 - displaying setting [17-5, C-10](#)
 - GRUB menu [17-3, C-8](#)
 - IPS 4345 [17-3, C-8, C-9](#)
 - IPS 4360 [17-3, C-8, C-9](#)
 - IPS 4510 [17-3, C-8, C-9](#)
 - IPS 4520 [17-3, C-8, C-9](#)
 - platforms [17-2, C-7](#)
 - ROMMON [17-3, C-9](#)
 - troubleshooting [17-6, C-11](#)
 - verifying [17-5, C-10](#)
- passwords [4-30](#)
 - changing [4-30](#)
 - configuring [4-30](#)
 - policy [4-32](#)
- patch releases described [18-3](#)
- peacetime learning (anomaly detection) [9-3](#)
- Peer-to-Peer. See P2P.
- PEP information
 - PID [17-41](#)
 - SN [17-41](#)
 - VID [17-41](#)
- permit-packet-logging command [4-26](#)
- physical connectivity issues [C-26](#)
- physical interfaces
 - configuration restrictions [5-6](#)
 - configuring [5-10](#)
- physical-interfaces command [5-8, 5-19, 5-25](#)
- ping command [17-39](#)
- policies
 - passwords [4-32](#)
- policy lists
 - displaying [17-23](#)
- port channel configuration
 - illustration [5-31](#)
 - switch [5-31](#)
- Post-Block ACLs [14-22, 14-23](#)
- Pre-Block ACLs [14-22, 14-23](#)

prerequisites for blocking [14-6](#)

privilege

changing [4-31](#)

configuring [4-31](#)

privilege command [4-18, 4-31](#)

privilege levels

administrator [1-3](#)

operators [1-3](#)

service [1-3](#)

viewers [1-3](#)

promiscuous delta

calculating risk rating [8-14](#)

described [7-12, 8-14, B-6](#)

promiscuous mode

atomic attacks [5-12](#)

configuring [5-12](#)

described [5-12](#)

illustration [5-12](#)

packet flow [5-12](#)

SPAN ports [5-13](#)

TCP reset interfaces [5-4](#)

VACL capture [5-13](#)

prompts

default input [1-5](#)

protocols

ARP [B-14](#)

CDP [5-42](#)

CIDEE [A-34](#)

DCE [B-48](#)

DDoS [B-72](#)

H.323 [B-43](#)

H225.0 [B-43](#)

HTTP [4-15](#)

ICMPv6 [B-15](#)

IDAPI [A-32](#)

IDCONF [A-33](#)

IDIOM [A-32](#)

IPv6 [B-28](#)

LOKI [B-72](#)

MSSQL [B-50](#)

Neighborhood Discovery [B-29](#)

Q.931 [B-43](#)

RPC [B-48](#)

SDEE [A-33](#)

proxy servers

configuring [4-11](#)

Q

Q.931 protocol

described [B-43](#)

SETUP messages [B-43](#)

quarantined IP address events described [11-2](#)

R

RADIUS

attempt limit [C-16](#)

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

RADIUS authentication

described [4-20](#)

service account [4-29](#)

shared secret [4-24, 4-25](#)

rate limiting

ACLs [14-5](#)

described [14-4](#)

routers [14-4](#)

service policies [14-5](#)

supported signatures [14-4](#)

raw expression syntax

described [B-64](#)

expert mode [B-64](#)

Raw Regex

described [7-58, 7-61, B-64](#)

expert mode [7-58, 7-61, B-64](#)

recall

help and tab completion [1-5](#)

- using [1-5](#)
 - recover command [19-13](#)
 - recovering the application partition image [19-14](#)
 - recovery partition
 - described [A-4](#)
 - upgrade [19-7](#)
 - Regex
 - described [1-8](#)
 - Multi String engine [B-35](#)
 - standardized [B-1](#)
 - Regular Expression. See also [Regex](#).
 - regular expression syntax
 - described [1-8](#)
 - raw Regex [7-58, 7-61, B-64](#)
 - signatures [B-9](#)
 - table [1-8](#)
 - reimaging
 - described [19-2](#)
 - IPS 4345 [19-16](#)
 - IPS 4360 [19-16](#)
 - IPS 4510 [19-20](#)
 - IPS 4520 [19-20](#)
 - sensors [19-2, 19-13](#)
 - removing
 - last applied
 - service pack [19-12](#)
 - signature update [19-12](#)
 - threat profiles [7-6](#)
 - users [4-19](#)
 - rename ad-knowledge-base command [9-42](#)
 - renaming
 - KBs [9-42, 9-43](#)
 - reputation
 - described [10-3](#)
 - illustration [10-4](#)
 - servers [10-3](#)
 - reset command [17-40](#)
 - reset not occurring for a signature [C-45](#)
 - resetting appliances [17-40](#)
 - restoring the current configuration [16-23, C-4](#)
 - retiring signatures [7-18](#)
 - risk rating
 - Alarm Channel [10-6](#)
 - calculating [8-13](#)
 - described [8-27](#)
 - global correlation [10-6](#)
 - reputation score [10-6](#)
 - ROMMON
 - described [19-15](#)
 - IPS 4345 [17-3, 19-16, C-9](#)
 - IPS 4360 [17-3, 19-16, C-9](#)
 - IPS 4510 [17-3, 19-20, C-9](#)
 - IPS 4520 [17-3, 19-20, C-9](#)
 - password recovery [17-3, C-9](#)
 - remote sensors [19-15](#)
 - serial console port [19-15](#)
 - TFTP [19-15](#)
 - round-trip time. See [RTT](#).
 - RPC portmapper [B-52](#)
 - RSA authentication
 - authorized keys [4-48](#)
 - RTT
 - described [19-15](#)
 - TFTP limitation [19-15](#)
-
- ## S
- saving
 - KBs [9-41](#)
 - scheduling automatic upgrades [19-9](#)
 - SDEE
 - described [A-33](#)
 - HTTP [A-33](#)
 - protocol [A-33](#)
 - server requests [A-34](#)
 - searching
 - submode configuration [16-18](#)

- security
 - account locking [4-34](#)
 - information on Cisco Security Intelligence Operations [18-7](#)
 - SSH [4-46](#)
- security policies described [7-2, 8-2, 9-2](#)
- 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](#)
 - TCP normalization [A-24](#)
- SensorBase Network
 - described [3-2, 10-2](#)
 - network participation [10-5](#)
 - participation [3-2, 10-2](#)
 - servers [3-2, 10-2](#)
- sensor databases
 - clearing [17-6](#)
- Sensor Key pane
 - described [4-50](#)
- sensors
 - access problems [C-20](#)
 - application partition image [19-14](#)
 - asymmetric traffic and disabling anomaly detection [9-48, C-14](#)
 - command and control interfaces (list) [5-3](#)
 - configuration sequence [1-1](#)
 - configuring to use NTP [4-44](#)
 - corrupted SensorApp configuration [C-30](#)
 - disaster recovery [C-6](#)
 - downgrading [19-12](#)
 - incorrect NTP configuration [C-12](#)
 - initializing [3-1, 3-5](#)
 - interface support [5-5](#)
 - IP address conflicts [C-23](#)
 - logging in
 - SSH [2-4](#)
 - Telnet [2-4](#)
 - loose connections [C-18](#)
 - managing
 - firewalls [14-27](#)
 - routers [14-23](#)
 - switches [14-26](#)
 - misconfigured access lists [C-22](#)
 - no alerts [C-27, C-51](#)
 - not seeing packets [C-29](#)
 - NTP time source [4-44](#)
 - NTP time synchronization [4-36, C-11](#)
 - partitions [A-4](#)
 - physical connectivity [C-26](#)
 - preventive maintenance [C-2](#)
 - reimaging [19-2](#)
 - sensing process not running [C-24](#)
 - setup command [3-1, 3-5, 3-8](#)
 - time sources [4-36, C-11](#)
 - troubleshooting software upgrades [C-48](#)
 - upgrading [19-5](#)
 - using NTP time source [4-43](#)
- server manifest described [A-28](#)
- service account
 - accessing [4-28, C-5](#)
 - cautions [4-2, 4-28, C-5](#)
 - creating [4-29, C-5](#)
 - described [4-28, A-31, C-5](#)
 - RADIUS authentication [4-29](#)

- TAC [A-31](#)
- troubleshooting [A-31](#)
- service anomaly-detection command [9-8](#)
- Service DNS engine
 - described [B-39](#)
 - parameters (table) [B-39](#)
- Service engine
 - described [B-39](#)
 - Layer 5 traffic [B-39](#)
- service event-action-rules command [8-8](#)
- 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
 - described [7-49, B-45](#)
 - parameters (table) [B-46](#)
- service HTTP engine
 - signature [7-50](#)
- Service IDENT engine
 - described [B-47](#)
 - parameters (table) [B-48](#)
- Service MSRPC engine
 - DCS/RPC protocol [B-48](#)
 - described [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 [18-3](#)
- service role
 - described [1-4, 2-2, A-30](#)
 - privileges [1-4](#)
- Service RPC engine
 - described [B-52](#)
 - parameters (table) [B-52](#)
 - RPC portmapper [B-52](#)
- service signature-definition command [7-2](#)
- 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-58](#)
 - parameters (table) [B-58](#)
- setting
 - system clock [4-38, 17-21](#)
- setting up
 - notes and caveats [4-1](#)
 - terminal servers [2-3, 19-15](#)
- setup
 - automatic [3-3](#)
 - command [3-1, 3-5, 3-8](#)
 - simplified mode [3-3](#)
- setup command
 - user roles [3-1, 3-2](#)
- shared secret
 - described [4-24, 4-25](#)

- RADIUS authentication [4-24, 4-25](#)
- show ad-knowledge-base diff command [9-44, 9-45](#)
- show ad-knowledge-base files command [9-40, 9-41](#)
- show clock command [4-37, 17-20](#)
- show configuration command [16-1](#)
- show events command [8-39, 17-16, C-77, C-78](#)
- show health command [10-9, 17-13, C-53](#)
- show history command [17-41](#)
- showing user information [4-32](#)
- show inspection-load command [17-7](#)
- show interfaces command [5-43, C-73](#)
- show interfaces-history command [5-45, C-75](#)
- show inventory command [17-41](#)
- show lacp command [5-35](#)
- show os-identification command [8-32](#)
- show settings command [7-8, 16-3, 16-18, 17-5, 17-43, C-10](#)
- show statistics anomaly-detection command [9-47](#)
- show statistics command [14-33, 17-24, C-61, C-62](#)
- show statistics denied-attackers command [8-37, 17-21](#)
- show statistics virtual-sensor command [17-24, C-19, C-62](#)
- show tech-support command [17-35, C-54](#)
- show users command [4-32](#)
- show version command [7-8, 17-36, C-58, C-59](#)
- sig-fidelity-rating command [7-17, 7-19](#)
- signature definition lists
 - displaying [17-23](#)
- signature definition policies
 - copying [7-2](#)
 - creating [7-2](#)
 - deleting [7-2](#)
 - editing [7-2](#)
- signature engines
 - AIC [7-22, B-11](#)
 - Atomic [B-14](#)
 - Atomic ARP [B-14](#)
 - Atomic IP [B-25](#)
 - Atomic IP Advanced [B-15](#)
 - Atomic IPv6 [B-28](#)
 - described [B-1](#)
- Fixed [B-29](#)
- Flood [B-32](#)
- Flood Host [B-32](#)
- Flood Net [B-33](#)
- list [B-2](#)
- Master [B-4](#)
- Meta [7-52, B-33](#)
- Multi String [B-35](#)
- Normalizer [B-36](#)
- Regex
 - patterns [B-10](#)
 - syntax [B-9](#)
- Service [B-39](#)
- Service DNS [B-39](#)
- Service FTP [B-40](#)
- Service Generic [B-41](#)
- Service H225 [B-43](#)
- Service HTTP [7-49, B-45](#)
- Service IDENT [B-47](#)
- Service MSRPC [B-48](#)
- Service MSSQL [B-50](#)
- Service NTP [B-51](#)
- Service P2P [B-52](#)
- Service RPC [B-52](#)
- Service SMB Advanced [B-54](#)
- Service SNMP [B-56](#)
- Service SSH engine [B-57](#)
- Service TNS [B-58](#)
- State [B-59](#)
- String [7-46, B-61](#)
- Sweep [B-67](#)
- Sweep Other TCP [B-69](#)
- Traffic Anomaly [B-70](#)
- Traffic ICMP [B-72](#)
- Trojan [B-73](#)
- signature engine update files described [18-4](#)
- Signature Event Action Filter
 - described [8-3, A-26](#)
 - parameters [8-3, A-26](#)

- Signature Event Action Handler described [8-4, A-26](#)
- Signature Event Action Override described [8-3, A-26](#)
- Signature Event Action Processor
 - Alarm Channel [8-3, A-26](#)
 - components [8-3, A-26](#)
 - described [8-3, A-23, A-26](#)
- signature fidelity rating
 - calculating risk rating [8-13](#)
 - configuring [7-17, 7-19](#)
 - described [8-13](#)
- signatures
 - custom [7-4](#)
 - default [7-4](#)
 - described [7-3](#)
 - false positives [7-4](#)
 - general parameters [7-11](#)
 - rate limits [14-4](#)
 - service HTTP [7-50](#)
 - string TCP [7-47](#)
 - string TCP XL [7-57, 7-61](#)
 - subsignatures [7-4](#)
 - TCP reset [C-45](#)
 - threat profile tuned [7-8](#)
 - tuned [7-4](#)
- Signatures window described [7-4](#)
- signature threat profiles
 - platform support [7-4](#)
- signature update
 - files [18-4](#)
- signature variables
 - adding [7-10](#)
 - deleting [7-10](#)
 - described [7-9](#)
 - editing [7-10](#)
- SNMP
 - configuring
 - agent parameters [15-3](#)
 - traps [15-5](#)
 - described [15-1](#)
 - general parameters [15-2](#)
 - Get [15-1](#)
 - GetNext [15-1](#)
 - notes and caveats [15-1](#)
 - Set [15-1](#)
 - supported MIBs [15-6, C-14](#)
 - Trap [15-1](#)
- snmp-agent-port command [15-2](#)
- snmp-agent-protocol command [15-2](#)
- SNMP traps
 - described [15-2](#)
- software architecture
 - ARC (illustration) [A-13](#)
 - IDAPI (illustration) [A-32](#)
- software downloads Cisco.com [18-1](#)
- software file names
 - recovery (illustration) [18-5](#)
 - signature/virus updates (illustration) [18-4](#)
 - signature engine updates (illustration) [18-5](#)
 - system image (illustration) [18-5](#)
- software release examples
 - platform identifiers [18-6](#)
 - platform-independent [18-6](#)
- software updates
 - supported FTP servers [19-3](#)
 - supported HTTP/HTTPS servers [19-3](#)
- SPAN port issues [C-26](#)
- specifying
 - worm timeout [9-11](#)
 - worm timeout [9-38](#)
- SSH
 - adding hosts [4-47](#)
 - described [4-46](#)
 - security [4-46](#)
- ssh authorized-key command [4-48](#)
- ssh generate-key command [4-50](#)
- ssh host-key command [4-46, 4-47](#)
- SSH known hosts list
 - adding hosts [4-46](#)

- SSH Server
 - private keys [A-21](#)
 - public keys [A-21](#)
- SSH server host key
 - generating [4-50](#)
- SSHv1 fallback
 - disabling [4-13](#)
 - enabling [4-13](#)
- sshv1-fallback
 - command [4-13](#)
 - configuring [4-13](#)
- standards
 - CIDEE [A-34](#)
 - IDCONF [A-33](#)
 - IDIOM [A-32](#)
 - SDEE [A-33](#)
- Startup Wizard
 - Signatures window described [7-4](#)
- State engine
 - Cisco Login [B-59](#)
 - described [B-59](#)
 - LPR Format String [B-59](#)
 - parameters (table) [B-60](#)
 - SMTP [B-59](#)
- statistic display [17-24, C-62](#)
- status command [7-18](#)
- stopping
 - IP logging [12-6](#)
- stream-reassembly command [7-43](#)
- String engine described [7-46, B-61](#)
- String ICMP engine parameters (table) [B-62](#)
- String TCP engine
 - parameters [7-46](#)
 - parameters (table) [B-62](#)
 - signature (example) [7-47](#)
- String TCP XL signature
 - example [7-57, 7-61](#)
- String UDP engine parameters (table) [B-63](#)
- String XL engine
 - description [B-64](#)
 - hardware support [6-11, B-3, B-64](#)
 - parameters (table) [B-64](#)
 - unsupported parameters [B-67](#)
- subinterface 0 described [5-24](#)
- subinterface-type command [5-19, 5-25](#)
- submode configuration
 - filtering output [16-18](#)
 - searching output [16-18](#)
- submode settings display [17-43](#)
- subsignatures described [7-4](#)
- summarization
 - described [8-33](#)
 - fire-all [8-34](#)
 - fire-once [8-34](#)
 - global-summarization [8-34](#)
 - Meta engine [8-34](#)
 - summary [8-34](#)
- summertime
 - configuring
 - non-recurring [4-40](#)
 - recurring [4-38](#)
- summertime-option non-recurring command [4-40](#)
- summertime-option recurring command [4-38](#)
- supported
 - FTP servers [19-3](#)
 - HTTP/HTTPS servers [19-3](#)
 - IPS interfaces for CSA MC [11-4](#)
- supported sensors
 - signature threat profiles [7-4](#)
- Sweep engine [B-68](#)
 - described [B-67](#)
 - parameters (table) [B-68](#)
- Sweep Other TCP engine
 - described [B-69](#)
 - parameters (table) [B-70](#)
- SwitchApp
 - described [A-29](#)

- switches
 - TCP reset interfaces [5-4](#)
 - syntax
 - case sensitivity [1-6](#)
 - system architecture
 - directory structure [A-34](#)
 - supported platforms [A-1](#)
 - system clock
 - displaying [4-37, 17-20](#)
 - setting [4-38, 17-21](#)
 - system components IDAPI [A-32](#)
 - System Configuration Dialog
 - described [3-3](#)
 - example [3-3](#)
 - system design (illustration) [A-2, A-3](#)
 - system images
 - installing
 - IPS 4345 [19-16](#)
 - IPS 4360 [19-16](#)
 - IPS 4510 [19-20](#)
 - IPS 4520 [19-20](#)
-
- T**
- tab completion
 - using [1-5](#)
 - TAC
 - PEP information [17-41](#)
 - service account [4-28, A-31, C-5](#)
 - show tech-support command [17-35, C-54](#)
 - troubleshooting [A-31](#)
 - target-value command [8-15](#)
 - IPv4 [8-15](#)
 - IPv6 [8-15](#)
 - target value rating
 - calculating risk rating [8-14](#)
 - described [8-14, 8-15](#)
 - tasks
 - configuring the sensor [1-1](#)
 - tcp command [9-13, 9-21, 9-29](#)
 - TCPDUMP
 - copy packet-file command [13-6](#)
 - expression syntax [13-2](#)
 - ip logs [12-2](#)
 - packet capture command [13-5](#)
 - packet display command [13-2](#)
 - TCP fragmentation described [B-37](#)
 - TCP reset interfaces
 - conditions [5-4](#)
 - described [5-4](#)
 - list [5-4](#)
 - promiscuous mode [5-4](#)
 - switches [5-4](#)
 - TCP resets
 - not occurring [C-45](#)
 - TCP stream reassembly
 - described [7-36](#)
 - parameters (table) [7-37, 7-42](#)
 - signatures (table) [7-37, 7-42](#)
 - tech support information display [17-36, C-55](#)
 - Telnet
 - disabling [4-5](#)
 - enabling [4-5](#)
 - telnet-option
 - command [4-5](#)
 - configuring [4-5](#)
 - terminal
 - command [17-16](#)
 - modifying length [17-16](#)
 - terminal server setup [2-3, 19-15](#)
 - terminating
 - CLI sessions [17-15](#)
 - TFN2K
 - described [B-72](#)
 - Trojans [B-73](#)
 - TFTP servers
 - recommended
 - UNIX [19-15](#)

- Windows [19-15](#)
- RTT [19-15](#)
- threat-profile command [7-5](#)
- threat profiles
 - applying [7-6](#)
 - displaying [7-6](#)
 - removing [7-6](#)
- threat rating
 - described [8-14](#)
 - risk rating [8-14](#)
- time
 - correction on the sensor [4-36, C-12](#)
 - sensors [4-36, C-11](#)
- time zone settings
 - configuring [4-42](#)
- time-zone-settings command [4-42](#)
- TLS
 - handshaking [4-51](#)
 - IDM [4-51](#)
 - web server [4-51](#)
- TLS certificates
 - generating [4-53](#)
- tls generate-key command [4-53](#)
- tls trusted-host command [4-52](#)
- trace command [17-42](#)
- tracing IP packet route [17-42](#)
- Traffic Anomaly engine
 - described [B-70](#)
 - protocols [B-70](#)
 - signatures [B-70](#)
- traffic flow notifications
 - configuring [5-40](#)
 - described [5-40](#)
- Traffic ICMP engine
 - DDoS [B-72](#)
 - described [B-72](#)
 - LOKI [B-72](#)
 - parameters (table) [B-73](#)
 - TFN2K [B-72](#)
- trap-community-name [15-4](#)
- trap-destinations command [15-4](#)
- trial license key [4-54](#)
- Tribe Flood Network. See TFN.
- Tribe Flood Network 2000. See TFN2K.
- Trojan engine
 - BO2K [B-73](#)
 - described [B-73](#)
 - TFN2K [B-73](#)
- Trojans
 - BO [B-73](#)
 - BO2K [B-73](#)
 - LOKI [B-72](#)
 - TFN2K [B-73](#)
- troubleshooting [C-1](#)
 - Analysis Engine busy [C-50](#)
 - applying software updates [C-47](#)
 - ARC
 - blocking not occurring for signature [C-37](#)
 - device access issues [C-35](#)
 - enabling SSH [C-37](#)
 - inactive state [C-33](#)
 - misconfigured master blocking sensor [C-38](#)
 - verifying device interfaces [C-36](#)
 - automatic updates [C-47](#)
 - cannot access sensor [C-20](#)
 - cidDump [C-81](#)
 - cidLog messages to syslog [C-44](#)
 - communication [C-20](#)
 - corrupted SensorApp configuration [C-30](#)
 - debug logger zone names (table) [C-44](#)
 - debug logging [C-40](#)
 - disaster recovery [C-6](#)
 - duplicate sensor IP addresses [C-23](#)
 - enabling debug logging [C-40](#)
 - external product interfaces [11-8, C-18](#)
 - gathering information [C-52](#)
 - global correlation [10-13, C-16](#)

- IDM
 - cannot access sensor [C-50](#)
 - will not load [C-49](#)
 - IME time synchronization [C-52](#)
 - manual block to bogus host [C-37](#)
 - misconfigured access list [C-22](#)
 - no alerts [C-27, C-51](#)
 - NTP [C-45](#)
 - password recovery [17-6, C-11](#)
 - physical connectivity issues [C-26](#)
 - preventive maintenance [C-2](#)
 - RADIUS
 - attempt limit [C-16](#)
 - reset not occurring for a signature [C-45](#)
 - sensing process not running [C-24](#)
 - sensor events [C-77](#)
 - sensor loose connections [C-18](#)
 - sensor not seeing packets [C-29](#)
 - sensor software upgrade [C-48](#)
 - service account [4-28, C-5](#)
 - show events command [C-77](#)
 - show interfaces command [C-73](#)
 - show statistics command [C-61](#)
 - show tech-support command [C-53, C-54, C-55](#)
 - show version command [C-58](#)
 - software upgrades [C-47](#)
 - SPAN
 - port issue [C-26](#)
 - verifying Analysis Engine is running [C-15](#)
 - verifying ARC status [C-32](#)
 - trusted hosts add [4-52](#)
 - tuned signatures described [7-4](#)
-
- U**
- udp command [9-15, 9-24, 9-32](#)
 - unassigned VLAN groups described [5-24](#)
 - unauthenticated NTP [4-2, 4-36, 4-44, C-11](#)
 - uninstalling
 - license key [4-57](#)
 - unlocking accounts [4-35](#)
 - unlock user username command [4-35](#)
 - updating the sensor immediately [19-11](#)
 - upgrade command [19-4, 19-7](#)
 - upgrade notes and caveats
 - upgrading IPS software [19-1](#)
 - upgrading
 - application partition [19-13](#)
 - recovery partition [19-7](#)
 - sensors [19-5](#)
 - upgrading IPS software
 - upgrade notes and caveats [19-1](#)
 - URLs for Cisco Security Intelligence Operations [18-7](#)
 - username command [4-18](#)
 - user-profile command [14-20](#)
 - user profiles [14-20](#)
 - user roles
 - administrator [1-3](#)
 - authentication [4-20](#)
 - operator [1-3](#)
 - service [1-3](#)
 - viewer [1-3](#)
 - users
 - adding [4-18, 4-19](#)
 - removing [4-18, 4-19](#)
 - using
 - debug logging [C-40](#)
 - TCP reset interfaces [5-4](#)
-
- V**
- VACLs
 - described [14-3](#)
 - Post-Block [14-26](#)
 - Pre-Block [14-26](#)
 - validation error messages described [D-6](#)
 - variables command [7-10, 8-11](#)
 - IPv4 [8-11](#)

IPv6 [8-11](#)

verifying

- password recovery [17-5, C-10](#)
- sensor initialization [3-13](#)
- sensor setup [3-13](#)

version display [17-37, C-59](#)

viewer role privileges [1-4](#)

viewing

- IP log contents [12-5](#)
- license key status [4-54](#)
- threat profile tuned signatures [7-8](#)
- user information [4-32](#)

virtualization

- advantages [6-2, C-13](#)
- restrictions [6-2, C-13](#)
- supported sensors [6-3, C-13](#)
- traffic capture requirements [6-3, C-13](#)

virtual-sensor name command [6-4](#)

virtual sensors

- adding [6-6, 6-8](#)
- assigning interfaces [6-4](#)
- assigning policies [6-4](#)
- creating [6-6, 6-8](#)
- default virtual sensor [6-2](#)
- described [6-2](#)
- displaying KB files [9-40](#)
- notes and caveats [6-1](#)
- options [6-4](#)

VLAN groups

- 802.1q encapsulation [5-24](#)
- configuration restrictions [5-7](#)
- deploying [5-24](#)
- switches [5-24](#)

VLAN groups mode

- described [5-23](#)

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

W

watch list rating

- calculating risk rating [8-14](#)
- described [8-14](#)

web server

- described [A-4, A-22](#)
- HTTP 1.0 and 1.1 support [A-22](#)
- HTTP protocol [4-15](#)
- port (default) [4-1, 4-15](#)
- private keys [A-21](#)
- public keys [A-21](#)
- SDEE support [A-22](#)
- TLS [4-51](#)

web server settings

- changing [4-16](#)
- configuring [4-15](#)

Wireshark

- copy packet-file command [13-6](#)
- ip logs [12-2](#)

worms

- Blaster [9-2](#)
- Code Red [9-2](#)
- histograms [9-37](#)
- Nimble [9-2](#)
- protocols [9-3](#)
- Sasser [9-2](#)
- scanners [9-3](#)
- Slammer [9-2](#)
- SQL Slammer [9-2](#)

worm-timeout command [9-10](#)

worm timeout specify [9-11, 9-38](#)

Z

zones

- external [9-4](#)
- illegal [9-4](#)
- internal [9-4](#)