INDEX

Symbols

(number sign) 10-4

* (wildcard) 2-6, 4-5, 10-3

A

AAA

- accounting 3-13
- authentication 3-6
- authorization 3-11
- configuring 3-4

aaa accounting command 3-13

aaa authentication command 3-6

aaa authorization command 3-11

accounting, configuring 3-13

action command 6-18

action flow 10-6

activation

- activation-extent command 8-11, 8-12
- activation-interface command 8-12

activation sensitivity 8-12

add-service command 6-9

admin privilege level 2-2, 3-7

always-accept 6-19

always-ignore 6-19

anomaly

- detected 10-2
- flow 10-3

anomaly detection engine memory usage 11-24, 11-26

arp command 11-26

attack report

- copying 10-7
- detected anomalies 10-2
- exporting 10-6, 10-7, 12-5
- exporting automatically 10-6
- history 11-23
- layout 10-1
- notify 10-4
- statistics 10-2
- timing 10-1
- viewing 10-4

attack type

- detected attack 10-5

authentication, configuring 3-6

authorization

- disabling zone command completion 3-13, 4-6

authorization, configuring 3-9

auth packet types 6-11

automatic detect mode 1-5

automatic protection mode 8-3

automatic protect mode 8-3, 9-1

B

banner

- configuring login 3-32

Berkeley Packet filter 5-7

BGP 8-8

burn flash 12-9

bypass filter

- command 5-10
- configuring 5-10
- definition 1-4, 5-1
- deleting 5-12
- displaying 5-11

C

capture, packets 11-12
caution, symbol overview 1-xiii
CFE 12-9
clear counters command 2-10, 11-4
clear log command 11-9
CLI
  changing prompt 3-28
  command shortcuts 2-6
  error messages 2-5
  getting help 2-6
  issuing commands 2-3
  TAB completion 2-6
  using 2-1
command completion 3-13
command line interface
  See CLI 2-1
command shortcuts 2-6
config privilege level 2-2, 3-7
configuration
  file
    copying 12-2
    exporting 12-3
    importing 12-4
    viewing 11-1
  importing 12-4
  saving router 8-10, 8-13
configuration, accessing command mode 3-12
configuration mode 2-2
configure command 2-7
constructing policies 7-4
copy command
  packet-dump 11-15
copy commands
  ftp running-config 12-4
  log 11-6, 11-8
  new-version 12-8
  reports 10-7
  running-config 4-15, 12-3
  zone log 11-8
copy-from-this 4-5
copy guard-running-config command 4-14, 4-17
copy login-banner command 3-33
copy-policies command 7-16
copy wbm-logo command 3-34
counters
  clearing 2-10, 11-4
  history 11-3
counters, viewing 11-3
cpu utilization 11-24

D

date command 3-23, 3-24
DDoS
  nonspoofed attacks 1-3
  overview 1-2
  spoofed attacks 1-2
  zombies 1-3
deactivate command 8-5
deactivating commands
  commands, deactivating 2-5
default-gateway command 2-10
description command 4-6
detect
  automatic mode 1-5
  interactive mode 1-5
detect command 8-4
detected
  anomalies 10-2
  flow 10-6
detected attack 10-5
DETECTOR_DEFAULT 4-2
DETECTOR_WORM 4-2
Detector configuration
  resetting 12-12
diff command 7-13, 7-14

disable command 6-6
disabling
automatic export 12-6
disk usage 11-23
DNS
detected anomalies 10-2
TCP policy templates 6-2
tcp protocol flow 10-5
dst-ip-by-ip activation form 8-4
dst-ip-by-ip activation method 8-7
dst-ip-by-name activation method 8-4
dst traffic characteristics 6-11
Dynamic filter
command 8-14
displaying 8-11
timeout 8-8
dynamic filter
1000 and more 5-13
command 5-15
definition 1-4
deleting 5-15
displaying 5-13
displaying events 11-7
overview 5-2, 5-12
preventing production of 5-16
sorting 5-13
worm 6-21
dynamic filters 9-1
dynamic privilege level 2-2, 3-7

E

enable
command 3-10, 6-6
password command 3-10
enabling services 3-2
entire-zone activation method 8-3
even log
deactivating 11-6
event log
activating 11-6
event monitor command 11-6
export
disabling automatic 12-6
export command 12-5
packet-dump 11-14
reports 10-7
exporting
configuration file 12-3
log file 11-8
reports automatically 10-6
exporting GUARD configuration 4-14, 4-17
export sync-config command 4-16
extracting signatures 11-18

F

facility 11-6
file server
configuring 12-1
file-server
command 4-16, 12-2
configuring 12-2
deleting 12-2
displaying 12-2, 12-6
displaying sync-config 4-16, 12-6
file server, displaying sync-config 12-6
filters
bypass 1-4, 5-10
dynamic 1-4, 5-2, 5-12
flex-content 1-4, 5-2
overview 5-1
fixed-threshold 6-15
flash-burn command 12-9
flex-content filter
configuring 5-3
definition 1-4, 5-1
displaying 5-8

filtering criteria 5-2
renumbering 5-3
fragments 10-5
detected anomalies 10-2
policy template 6-2

G

generating signatures 11-18
global mode 2-2
global traffic characteristics 6-11
Guard
configuration mode 2-3
exporting configuration 12-5
GUARD_DEFAULT 4-3
GUARD_LINK 4-3
GUARD_TCP_NO_PROXY 4-3
GUARD_ zone template
policy templates included with zone templates 6-3
guard-conf command 4-10
GUARD configuration, exporting 4-14, 4-17
GUARD configuration, importing 4-15
Guard-protection activation methods 8-3, 8-10

H

histogram command 6-20
history command 11-23
host, logging 11-7
host keys
deleting 3-20, 3-21
hostname
changing 3-28
command 3-28
HTTP
detected anomalies 10-2
policy template 6-2
hybrid 10-5

I

idle session, configuring timeout 3-35
idle session, displaying timeout 3-36
importing
configuration 12-4
importing GUARD configuration 4-15
in-band
configuring interface 2-8
in packet types 6-11
install new-version command 12-8
interactive
operation mode 9-3
policy status 6-19
interactive detect mode 1-5
interactive protection mode 8-3
interactive protect mode 8-3, 9-1
interactive-status command 6-19
interface
activating 2-8, 2-9
clearing counters 2-10
command 2-8
configuration mode 2-2
configuring 2-8
configuring IP address 2-9
out-of-band 2-8
ip address
modifying, zone 4-8
IP address command
excluding 4-7
ip address command
deleting 4-8
interface 2-9
zone 4-7
ip route command 2-10
IP scan 10-5
detected anomalies 10-2
policy template 6-2
IP threshold configuration 6-17

K

key command
- add 3-21, 3-25
- generate 3-22, 3-27
- remove 3-26

key publish command 3-22

L

learning
- command 7-5, 7-7
- constructing policies 7-4
- overview 7-1
- policy-construction command 7-4
- synchronizing results 7-3
- terminating process 7-5, 7-7
- threshold-tuning command 7-6
- tuning thresholds 7-6

learning accept command 7-5, 7-6
learning parameters, displaying 7-8
learning-params
- deactivating periodic action 7-7
- deactivating periodic-action command 7-5
- periodic-action command 4-12, 7-5, 7-7, 7-8
- threshold-multiplier command 6-15
- threshold-selection command 7-6, 7-9
- threshold-tuned command 4-8, 7-10

learning-params command 4-11, 4-16
learning-params fixed-threshold command 6-15
LINK templates 7-4
log file
- clearing 11-9
- exporting 11-6, 11-8
- history 11-23
- viewing 11-8

logging, viewing configuration 11-7
logging command 11-6
login banner
- configuring 3-32, 3-33
- deleting 3-34
- importing 3-33

login-banner command 3-33
logo, adding WBM 3-34
logo, deleting WBM 3-35

M

management
- MDM 2-12
- overview 2-11
- SSH 2-13
- WBM 2-11

max-services command 6-5
MDM
- activating 2-12

memory consumption 11-23
memory usage, anomaly detection engine 11-24, 11-26
min-threshold command 6-6
monitoring
- network traffic 11-14, 11-15

MP
- upgrading 12-8

mtu command 2-9

N

netstat command 11-28
network server
- configuring 12-1, 12-2
- deleting 12-2
- displaying 12-2, 12-6
- displaying sync-config 4-16, 12-6

network server, displaying sync-config 12-6
new version
- installing 12-8
- upgrading 12-8

no learning command 7-5, 7-7
non_estb_conns packet type 6-11
nonspoofed attacks 1-3
no proxy policy templates 6-4
note, symbol overview 1-xiii
notify 10-4
notify policy action 6-18
ns policy templates 6-4
NTP 3-24
  enable service 3-24
  permit 3-25
  server 3-25

O

other protocols
  detected anomalies 10-2
  policy template 6-3
out_pkts packet types 6-11
out-of-band
  configuring interface 2-8
out-of-band interface 2-8

P

packet-dump
  auto-capture command 11-11
  automatic
    activating 11-10
    deactivating 11-11
  displaying settings 11-12
  exporting 11-14, 11-15, 12-5
  signatures 11-19
packet-dump command 11-12
packets, capturing 11-12
password
  changing 3-7
  enabling 3-10
  encrypted 3-7
  resetting 12-10
pending 9-1
pending dynamic filters 9-1, 9-2
  displaying 9-3, 9-5
periodic action
  accepting policies automatically 7-5, 7-7
  deactivating 7-5, 7-7
permit
  command 2-12, 2-13, 3-3
permit ssh command 3-21
ping command 11-31
pkts packet type 6-11
policy
  action 6-12, 6-18
  activating 6-13
  adding services 6-9
  backing up current 6-25, 7-17
  command 6-12
  configuration mode 2-3
  constructing 1-4, 7-2, 7-4
  copying parameters 7-16
  copy-policies 7-16
  deleting services 6-9
  disabling 6-13
  displaying 8-11
  inactivating 6-13
  learning-params, fixed-threshold command 6-15
  marking as tuned 4-8, 7-10
  marking threshold as fixed 6-15
  multiplying thresholds 6-16
  navigating path 6-12
  packet types 6-10
  show statistics 6-23
  state 6-13
  threshold 6-12, 6-14
  threshold-list command 6-17
  timeout 6-12, 6-17
  timeout, configuring 8-11

traffic characteristics 6-11
tuning thresholds 1-4, 7-2, 7-6
using wildcards 6-12, 6-22, 6-24
viewing statistics 7-8
policy set-timeout command 6-18, 8-11
policy template
command 6-4, 6-6
configuration command level 6-4
configuration mode 2-3
displaying list 6-4
Guard policy templates for synchronization 6-3
max-services 6-5
min-threshold 6-6
overview 6-2
parameters 6-4
state 6-6
worm_tcp 6-4
policy-template add-service command 6-9
policy-template remove service command 6-9
policy-type activation method 8-4
port scan 10-5
detected anomalies 10-2
policy template 6-3
poweroff command 12-7
privilege levels 2-2
assigning passwords 3-10
moving between 3-10
protect
activation methods 8-3, 8-10
automatic mode 8-3, 9-1
deactivating 8-5
interactive mode 8-3, 9-1
protect command 8-5
protection-end-timer 8-7, 8-14
protection-end-timer command 8-12
protect-ip-state command 8-3, 8-10
protect learning command 7-6
protect-packet command 8-12
protocol traffic characteristics 6-11
proxy
no proxy policy templates 6-4
public-key
displaying 3-27

R

rates
history 11-3
rates, viewing 11-3
reactivate-zones 12-7
reboot command 12-7
rebooting
parameters 12-7
recommendations 9-1
accepting 9-6
activating 9-3, 9-5
change decision 6-19
command 9-6
deactivating 9-3, 9-7
dynamic filters 9-1
ignoring 9-6
overview 9-1
viewing 9-4
viewing pending-filters 9-3, 9-5
redistribute detector command 8-10
reload command 12-6
remote-activate policy action 6-18
remote Guard
activating 5-14
commands
activation-extent 8-11, 8-12
activation-interface 8-12
protection-end-timer 8-12
protect-packet 8-12
terminating protection 8-7, 8-14
remote-guard command 8-7, 8-8
remote Guard list
displaying 8-8

remote Guards
activating 8-5
BGP, activating 8-8
default list 8-7
list 8-8
list activation order 8-8
remove service command 6-9
renumbering flex-content filters 5-3
report
See attack report 10-1
reports
details 10-4
exporting 12-5
reqs packet type 6-11
router
command 8-10, 8-13
configuration mode 8-10, 8-13
configuring adjacent 8-11
enabling service 8-10
router configuration mode 2-3
routes, redistributing 8-10
routing table
manipulation 2-10
viewing 2-11
running-config
copy 4-15, 12-3, 12-4
show 11-1

S

saving configuration, router 8-10, 8-13
scanners traffic characteristics 6-12
service
adding 6-9
command 2-11, 2-13, 3-2
copy 7-16
deleting 6-9
MDM 2-13
permissions 3-3
snmp-trap 3-28
wbm 2-11
services
enabling 3-2
session, configuring timeout 3-35
session, displaying idle timeout 3-36
session timeout, disabling 3-36
session-timeout command 3-35
set-action 6-18
show commands
counters 11-3
cpu 11-24
diagnostic-info 11-21
disk-usage 11-23
dynamic-filters 5-13, 5-15
file-servers 12-2, 12-6
flex-content-filter 5-8
host-keys 3-21, 3-23
learning parameters 7-8
learning-params 6-15
log 11-8
log export-ip 11-7
logging 11-7
login-banner 3-33
memory 11-24
packet-dump 11-12
packet-dump signatures 11-19
policies 6-22
policies statistics 6-23, 7-8
public-key 3-23, 3-27
rates 11-3
recommendations 9-4
recommendations pending-filters 9-3, 9-5
remote-guards 8-8
reports details 10-4
running-config 11-1
show 11-3
sorting dynamic-filters 5-13
sync-config 4-16

sync-config file-servers 4-16, 12-6
templates 4-5
zone policies 6-22
show privilege level 2-2, 3-7
show public-key command 3-27
shutdown command 2-9
signature
generating 11-18
snapshot
backing up policies 6-25, 7-17
command 7-12
comparing 7-13
deleting 7-15
displaying 7-15
saving 7-12, 7-13
snapshot command 7-12
snapshots
save periodically 7-8
SNMP
configuring trap generator 3-28
traps description 3-29
snmp commands
community 3-32
trap-dest 3-28
specific IP threshold 6-17
speed command 2-9
spoofed attacks 1-2
src traffic characteristics 6-12
SSH
configuring 2-13
deleting keys 3-26
generating key 3-22, 3-27
host key 3-23
service 2-13
viewing public key 3-23
ssh key, publishing 3-22
state command 6-13
static route
adding 2-10
syn_by_fin packet type 6-11
sync command 4-12, 4-13
synchronization
exporting configuration 12-5
syns packet type 6-11
syslog
configuring export parameters 11-6
configuring server 11-7
message format 11-6
system log
message format 11-6

T

TACACS+
authentication
key generate command 3-19
key publish command 3-22
clearing statistics 3-17
configuring search 3-16
configuring server 3-14
server connection timeout 3-16
server encryption key 3-15
server IP address 3-15
viewing statistics 3-17
tacacs-server commands
clear statistics 3-17
first-hit 3-14
host 3-14, 3-15
key 3-14, 3-15, 3-16
show statistics 3-17
timeout 3-14, 3-16
TCP
detected anomalies 10-2, 10-5
no proxy policy templates 6-4
policy templates 6-3
templates
LINK 7-4
viewing policies 4-5

zone 4-2
thresh-mult 6-16
threshold
command 6-14
configuring IP threshold 6-17
configuring list 6-17
configuring specific IP 6-17
marking as tuned 4-8, 7-10
multiplying before accepting 6-15
selection 7-12
setting as fixed 6-14
tuning 1-4, 7-2
worm 6-20
threshold-list command 6-17
threshold selection 7-6
threshold tuning
save results periodically 7-8
time, configuring 3-23
timeout command 6-17, 8-11
timeout session, configuring 3-35
timeout session, disabling 3-36
timesaver, symbol overview 1-xiii
timezone 3-24
tip, symbol overview 1-xiii
traceroute command 11-30
traffic
monitoring 11-14, 11-15
trap 11-6
trap-dest 3-28
tuning policy thresholds 7-6

U

UDP
detected anomalies 10-3
policy templates 6-3
unauth_pkts packet type 6-11
unauthenticated TCP detected anomalies 10-3
upgrading 12-8
MP 12-8
user
detected anomalies 10-3
user filter
command 5-3
username
encrypted password 3-7
username command 3-7
users
adding 3-7
adding new 3-7
assigning privilege levels 3-6
deleting 3-8
privilege levels 2-2, 3-9
system users
admin 2-7
riverhead 2-7
username command 3-7

W

WBM
activating 2-11
WBM logo
adding 3-34
deleting 3-35
worm
dynamic filter 6-21
identifying attack 6-21
overview 6-19
policy 6-11, 6-12
policy templates 6-3, 6-20
thresholds 6-20
worm_tcp policy template 6-4

X

XML schema 10-6 to 10-9, 11-14, 12-6

Z

zombies 1-3
zone
anomaly detection 8-1
clearing counters 11-4
command 4-4, 4-5, 9-3
command completion 3-13, 4-6
comparing 7-14
configuration mode 2-3, 4-6
copying 4-5
creating 4-4
defining IP address 4-7
deleting 4-5
deleting IP address 4-8
duplicating 4-5
excluding IP address 4-7
exporting configuration 4-16
IP address 4-7
learning 7-1
LINK templates 7-4
modifying IP address 4-8
operation mode 4-5
reconfiguring 4-6
synchronize configuration 4-8
synchronizing automatically 4-11
synchronizing offline 4-14
templates 4-2
viewing configuration 4-7
viewing policies 6-22
viewing status 11-2
zone policy
marking as tuned 4-8, 7-10
zone synchronization 7-3