



INDEX

Symbols

- /bits subnet masks [B-3](#)
- ?
 - command string [A-4](#)
 - help [A-4](#)

A

AAA

- about [33-1](#)
 - accounting [35-18](#)
 - authentication
 - CLI access [34-18](#)
 - network access [35-2](#)
 - privileged EXEC mode [34-19](#)
 - authorization
 - command [34-21](#)
 - downloadable access lists [35-14](#)
 - network access [35-11](#)
 - local database support [33-7](#)
 - performance [35-1](#)
 - server [52-4](#)
 - adding [33-11](#)
 - types [33-1](#)
 - support summary [33-3](#)
 - web clients [35-6](#)
- abbreviating commands [A-3](#)
- ABR
 - definition of [22-2](#)
- Access Group pane
 - description [24-7](#)
- access lists

- about [13-1](#)
- ACE logging, configuring [18-1](#)
- deny flows, managing [18-5](#)
- downloadable [35-14](#)
- global access rules [32-2](#)
- implicit deny [13-3, 32-3](#)
- inbound [32-3](#)
- IP address guidelines [13-3](#)
- IPv6
 - about [17-1](#)
 - configuring [17-4](#)
 - default settings [17-3](#)
 - logging [18-1](#)
 - NAT guidelines [13-3](#)
 - object groups [12-2](#)
 - outbound [32-3](#)
 - remarks [14-5](#)
 - scheduling activation [12-16](#)
 - types [13-1](#)
- ACEs
 - See* access lists
- activation key
 - entering [4-10](#)
 - location [4-9](#)
 - obtaining [4-9](#)
- Active/Active failover
 - about [51-1](#)
 - actions [51-5](#)
 - command replication [51-3](#)
 - configuration synchronization [51-3](#)
 - configuring
 - asymmetric routing support [51-18](#)
 - failover criteria [51-16](#)

- failover group preemption [51-12](#)
- HTTP replication [51-14](#)
- interface monitoring [51-14](#)
- virtual MAC addresses [51-16](#)
- device initialization [51-3](#)
- duplicate MAC addresses, avoiding [51-2, 51-17](#)
- optional settings
 - about [51-6](#)
 - configuring [51-12](#)
- primary status [51-2](#)
- secondary status [51-2](#)
- triggers [51-4](#)
- Active/Standby failover
 - about [50-1](#)
 - actions [50-4](#)
 - command replication [50-3](#)
 - configuration synchronization [50-2](#)
 - device initialization [50-2](#)
 - primary unit [50-2](#)
 - secondary unit [50-2](#)
 - triggers [50-4](#)
- Active Directory procedures [C-16 to ??](#)
- ActiveX filtering [36-2](#)
- Adaptive Security Algorithm [1-10](#)
- Add/Edit Access Group dialog box
 - description [24-7](#)
- Add/Edit IGMP Join Group dialog box
 - description [24-6](#)
- Add/Edit OSPF Neighbor Entry dialog box [22-12](#)
- admin context
 - about [6-2](#)
 - changing [6-23](#)
- administrative access
 - using ICMP for [34-11](#)
- administrative distance [20-3, 20-5](#)
- AIP SSM
 - port-forwarding
 - enabling [7-4, 8-6](#)
- alternate address, ICMP message [B-15](#)
- analyzing syslog messages [52-2](#)
- application inspection
 - about [39-1](#)
 - applying [39-6](#)
 - configuring [39-6](#)
 - inspection class map [31-6](#)
 - inspection policy map [31-2](#)
 - security level requirements [7-2, 8-2](#)
 - special actions [31-1](#)
- area border router [22-2](#)
- ARP
 - NAT [27-22](#)
- ARP inspection
 - about [5-10](#)
 - enabling [5-12](#)
 - static entry [5-11](#)
- ARP spoofing [5-10](#)
- ARP test, failover [49-17](#)
- ASA (Adaptive Security Algorithm) [1-10](#)
- ASBR
 - definition of [22-2](#)
- ASDM software
 - allowing access [34-6](#)
 - installing [56-2](#)
- ASR [51-18](#)
- asymmetric routing
 - TCP state bypass [44-4](#)
- asymmetric routing support [51-18](#)
- attacks
 - DNS request for all records [48-10](#)
 - DNS zone transfer [48-10](#)
 - DNS zone transfer from high port [48-10](#)
 - fragmented ICMP traffic [48-6, 48-9](#)
 - IP fragment [48-4, 48-7](#)
 - IP impossible packet [48-4, 48-7](#)
 - large ICMP traffic [48-6, 48-9](#)
 - ping of death [48-6, 48-9](#)
 - proxied RPC request [48-10](#)
 - statd buffer overflow [48-11](#)

- TCP NULL flags [48-6, 48-9](#)
- TCP SYN+FIN flags [48-6, 48-9](#)
- attributes
 - RADIUS [C-27](#)
- attribute-value pairs
 - TACACS+ [C-38](#)
- authentication
 - about [33-2](#)
 - CLI access [34-18](#)
 - FTP [35-3](#)
 - HTTP [35-3](#)
 - network access [35-2](#)
 - privileged EXEC mode [34-19](#)
 - Telnet [35-3](#)
 - web clients [35-6](#)
- authorization
 - about [33-2](#)
 - command [34-21](#)
 - downloadable access lists [35-14](#)
 - network access [35-11](#)
- autostate messaging [2-10](#)
- Auto-Update, configuring [56-16](#)

B

- Baltimore Technologies, CA server support [38-4](#)
- basic threat detection
 - See* threat detection
- bits subnet masks [B-3](#)
- Botnet Traffic Filter
 - actions [46-2](#)
 - address categories [46-2](#)
 - blacklist
 - adding entries [46-9](#)
 - description [46-2](#)
 - blocking traffic manually [46-15](#)
 - classifying traffic [46-12](#)
 - configuring [46-6](#)
 - databases [46-2](#)
 - default settings [46-6](#)
 - DNS Reverse Lookup Cache
 - information about [46-4](#)
 - maximum entries [46-4](#)
 - using with dynamic database [46-10](#)
 - DNS snooping [46-10](#)
 - dropping traffic [46-13](#)
 - graylist [46-13](#)
 - dynamic database
 - enabling use of [46-7](#)
 - files [46-3](#)
 - information about [46-2](#)
 - searching [46-16](#)
 - updates [46-7](#)
 - examples [46-19](#)
 - feature history [46-22](#)
 - graylist
 - description [46-2](#)
 - dropping traffic [46-13](#)
 - guidelines and limitations [46-6](#)
 - information about [46-1](#)
 - licensing [46-6](#)
 - monitoring [46-17](#)
 - static database
 - adding entries [46-9](#)
 - information about [46-3](#)
 - syslog messages [46-17](#)
 - task flow [46-7](#)
 - threat level
 - dropping traffic [46-13](#)
 - whitelist
 - adding entries [46-9](#)
 - description [46-2](#)
 - working overview [46-5](#)
- BPDUs
 - forwarding on the switch [2-10](#)
- bridge
 - entry timeout [5-15](#)
 - table, *See* MAC address table

- broadcast Ping test [49-17](#)
 - building blocks [12-1](#)
 - bypassing firewall checks [44-3](#)
 - bypassing the firewall, in the switch [2-7](#)
-
- C**
- CA
 - CRs and [38-2](#)
 - public key cryptography [38-2](#)
 - revoked certificates [38-2](#)
 - supported servers [38-4](#)
 - capturing packets [57-14](#)
 - CA server
 - Digicert [38-4](#)
 - Geotrust [38-4](#)
 - Godaddy [38-4](#)
 - iPlanet [38-4](#)
 - Netscape [38-4](#)
 - RSA Keon [38-4](#)
 - Thawte [38-4](#)
 - Catalyst 6500
 - See* switch
 - certificate
 - enrollment protocol [38-11](#)
 - Certificate Revocation Lists
 - See* CRLs
 - change query interval [24-8](#)
 - change query response time [24-8](#)
 - change query timeout value [24-8](#)
 - changing between contexts [6-22](#)
 - changing the severity level [52-18](#)
 - Cisco 7600
 - See* switch
 - Cisco-AV-Pair LDAP attributes [C-13](#)
 - Cisco IOS CS CA
 - server support [38-4](#)
 - Cisco IP Phones
 - DHCP [10-6](#)
 - Cisco IP Phones, application inspection [41-25](#)
 - Class A, B, and C addresses [B-1](#)
 - class-default class map [30-9](#)
 - classes, logging
 - filtering messages by [52-16](#)
 - message class variables [52-4](#)
 - types [52-4](#)
 - classes, resource
 - See* resource management
 - class map
 - inspection [31-6](#)
 - Layer 3/4
 - management traffic [30-14](#)
 - match commands [30-12, 30-15](#)
 - through traffic [30-12](#)
 - regular expression [12-15](#)
 - CLI
 - abbreviating commands [A-3](#)
 - adding comments [A-5](#)
 - command line editing [A-3](#)
 - command output paging [A-5](#)
 - displaying [A-5](#)
 - help [A-4](#)
 - paging [A-5](#)
 - syntax formatting [A-3](#)
 - command authorization
 - about [34-14](#)
 - configuring [34-21](#)
 - multiple contexts [34-15](#)
 - command prompts [A-2](#)
 - comments
 - configuration [A-5](#)
 - configuration
 - clearing [3-15](#)
 - comments [A-5](#)
 - saving [3-12](#)
 - switch [2-1](#)
 - text file [3-15](#)
 - URL for a context [6-20](#)

- viewing [3-14](#)
 - configuration examples
 - logging [52-20](#)
 - configuration examples for SNMP [54-27](#)
 - configuration mode
 - accessing [3-3](#)
 - prompt [A-2](#)
 - connection blocking [48-2](#)
 - connection limits
 - configuring [44-1](#)
 - per context [6-16](#)
 - console port logging [52-11](#)
 - context mode [25-2](#)
 - context modes [20-2, 21-3, 22-3, 23-3, 24-3](#)
 - contexts
 - See* security contexts
 - conversion error, ICMP message [B-15](#)
 - copying files using copy smb
 - command [56-8](#)
 - Coredump [57-14](#)
 - crash dump [57-14](#)
 - creating a custom event list [52-13](#)
 - custom messages list
 - logging output destination [52-4](#)
 - cut-through proxy
 - AAA performance [35-1](#)
-
- D**
- data flow
 - routed firewall [5-17](#)
 - transparent firewall [5-23](#)
 - date and time in messages [52-18](#)
 - DDNS [11-2](#)
 - debug messages [57-13](#)
 - default
 - class [6-9](#)
 - routes, defining equal cost routes [20-4](#)
 - default policy [30-7](#)
 - default routes
 - about [20-4](#)
 - configuring [20-4](#)
 - delay sending flow-create events
 - flow-create events
 - delay sending [53-9](#)
 - deleting files from Flash [56-2](#)
 - deny flows, logging [18-5](#)
 - device ID, including in messages [52-17](#)
 - device ID in messages [52-17](#)
 - DHCP
 - Cisco IP Phones [10-6](#)
 - options [10-4](#)
 - relay [10-7](#)
 - server [10-3](#)
 - transparent firewall [32-5](#)
 - DHCP Relay panel [11-6](#)
 - DHCP services [9-3](#)
 - DiffServ preservation [45-2](#)
 - directory hierarchy search [C-3](#)
 - disabling messages [52-18](#)
 - disabling messages, specific message IDs [52-18](#)
 - DMZ, definition [1-7](#)
 - DNS
 - dynamic [11-2](#)
 - inspection
 - about [40-2](#)
 - managing [40-1](#)
 - rewrite, about [40-2](#)
 - rewrite, configuring [40-3](#)
 - NAT effect on [27-24](#)
 - server, configuring [9-8](#)
 - DNS request for all records attack [48-10](#)
 - DNS zone transfer attack [48-10](#)
 - DNS zone transfer from high port attack [48-10](#)
 - domain name [9-3](#)
 - dotted decimal subnet masks [B-3](#)
 - downloadable access lists
 - configuring [35-14](#)

- converting netmask expressions [35-18](#)
- DSCP preservation [45-2](#)
- dual IP stack, configuring [7-2](#)
- dual-ISP support [20-6](#)
- Dynamic DNS [11-2](#)
- dynamic NAT
 - about [27-8](#)
 - network object NAT [28-4](#)
 - twice NAT [29-4](#)
- dynamic PAT
 - network object NAT [28-6](#)
 - See also* NAT
 - twice NAT [29-8](#)

E

- echo reply, ICMP message [B-15](#)
- ECMP [20-3](#)
- editing command lines [A-3](#)
- EIGRP [32-5](#)
 - DUAL algorithm [25-2](#)
 - hello interval [25-13](#)
 - hello packets [25-1](#)
 - hold time [25-2, 25-13](#)
 - neighbor discovery [25-1](#)
 - stub routing [25-3](#)
 - stuck-in-active [25-2](#)
- enabling logging [52-6](#)
- enabling secure logging [52-16](#)
- Enterprises [10-6](#)
- Entrust, CA server support [38-4](#)
- established command, security level requirements [7-2, 8-2](#)
- Ethernet
 - MTU [7-8, 8-9](#)
- EtherType access list
 - compatibility with extended access lists [32-2](#)
 - implicit deny [32-3](#)
- evaluation license [4-4](#)
- exporting NetFlow records [53-5](#)

- extended ACLs
 - configuring
 - for management traffic [14-2](#)

F

- facility, syslog [52-9](#)
- failover
 - about [49-1](#)
 - Active/Active, *See* Active/Active failover
 - Active/Standby, *See* Active/Standby failover
 - configuration file
 - terminal messages, Active/Active [51-3](#)
 - terminal messages, Active/Standby [50-2](#)
 - contexts [50-2](#)
 - debug messages [49-19](#)
 - disabling [50-17, 51-24](#)
 - Ethernet failover cable [49-3](#)
 - failover link [49-2](#)
 - forcing [50-16, 51-24](#)
 - guidelines [54-16](#)
 - health monitoring [49-16](#)
 - interface health [49-17](#)
 - interface monitoring [49-17](#)
 - interface tests [49-17](#)
 - link communications [49-2](#)
 - MAC addresses
 - about [50-2](#)
 - automatically assigning [6-12](#)
 - module placement
 - inter-chassis [49-10](#)
 - intra-chassis [49-10](#)
 - monitoring, health [49-16](#)
 - network tests [49-17](#)
 - primary unit [50-2](#)
 - restoring a failed group [50-17, 51-24](#)
 - restoring a failed unit [50-17, 51-24](#)
 - secondary unit [50-2](#)
 - SNMP syslog traps [49-19](#)

- Stateful Failover, *See* Stateful Failover
- state link [49-3](#)
- switch configuration [2-9](#)
- system log messages [49-18](#)
- system requirements [49-2](#)
- testing [50-17, 51-24](#)
- trunk [2-10](#)
- type selection [49-7](#)
- unit health [49-17](#)

fast path [1-11](#)

Fibre Channel interfaces

- default settings [15-2, 16-2, 32-7](#)

filtering

- ActiveX [36-2](#)
- FTP [36-14](#)
- Java applet [36-4](#)
- Java applets [36-4](#)
- security level requirements [7-2, 8-2](#)
- servers supported [36-6](#)
- show command output [A-4](#)
- URLs [36-1, 36-7](#)

filtering messages [52-4](#)

firewall mode

- about [5-1](#)
- configuring [5-1](#)

Flash memory

- removing files [56-2](#)

flash memory available for logs [52-15](#)

flow-export actions [53-4](#)

format of messages [52-3](#)

fragmented ICMP traffic attack [48-6, 48-9](#)

fragment protection [1-8](#)

fragment size [48-2](#)

FTP inspection

- about [40-11](#)
- configuring [40-11](#)

G

- generating RSA keys [38-9](#)
- groups
 - SNMP [54-15](#)
- GTP inspection
 - about [43-3](#)
 - configuring [43-3](#)

H

- H.225 timeouts [41-9](#)
- H.245 troubleshooting [41-10](#)
- H.323
 - transparent firewall guidelines [5-4](#)
- H.323 inspection
 - about [41-4](#)
 - configuring [41-3](#)
 - limitations [41-5](#)
 - troubleshooting [41-10](#)
- help, command line [A-4](#)
- high availability
 - about [49-1](#)
- host
 - SNMP [54-15](#)
- hostname
 - configuring [9-2](#)
 - in banners [9-2](#)
 - multiple context mode [9-2](#)
- hosts, subnet masks for [B-3](#)
- HSRP [5-3](#)
- HTTP
 - filtering [36-1](#)
- HTTP(S)
 - authentication [34-18](#)
 - filtering [36-7](#)
- HTTP inspection
 - about [40-16](#)
 - configuring [40-16](#)

HTTPS/Telnet/SSH

allowing network or host access to ASDM [34-1](#)

ICMP

rules for access to ASDM [34-11](#)

testing connectivity [57-1](#)

type numbers [B-15](#)

identity NAT

about [27-11](#)

network object NAT [28-12](#)

twice NAT [29-18](#)

ILS inspection [42-1](#)IM [41-19](#)implementing SNMP [54-15](#)inbound access lists [32-3](#)information reply, ICMP message [B-15](#)information request, ICMP message [B-15](#)inside, definition [1-7](#)inspection_default class-map [30-8](#)

inspection engines

See application inspection

installation

module verification [2-3](#)

Instant Messaging inspection [41-19](#)

interface

MTU [7-8, 8-9](#)

interfaces

default settings [15-2, 16-2, 32-7](#)

failover monitoring [49-17](#)

IP address [7-5](#)

MAC addresses

automatically assigning [6-21](#)

manually assigning to interfaces [7-8, 8-9](#)

mapped name [6-19](#)

naming, physical and subinterface [7-5, 8-7](#)

turning off [7-14, 8-13](#)

turning on [7-14, 8-13](#)

IOS

upgrading [2-1](#)

IP addresses

classes [B-1](#)

interface [7-5](#)

management, transparent firewall [8-5](#)

private [B-2](#)

subnet mask [B-4](#)

IP fragment attack [48-4, 48-7](#)IP impossible packet attack [48-4, 48-7](#)IP overlapping fragments attack [48-5](#)IP spoofing, preventing [48-1](#)IP teardrop attack [48-5](#)

IPv6

commands [19-10](#)

configuring alongside IPv4 [7-2](#)

default route [20-5](#)

dual IP stack [7-2](#)

duplicate address detection [7-9, 8-10](#)

neighbor discovery [26-1](#)

router advertisement messages [26-3](#)

static neighbors [26-4](#)

static routes [20-5](#)

IPv6 addresses

anycast [B-9](#)

command support for [19-10](#)

format [B-5](#)

multicast [B-8](#)

prefixes [B-10](#)

required [B-10](#)

types of [B-6](#)

unicast [B-6](#)

IPv6 prefixes [26-11](#)IPX [2-7](#)

J

Java applet filtering [36-4](#)Java applets, filtering [36-2](#)

Join Group pane
 description [24-6](#)
 jumbo frames [7-7, 8-8](#)

K

Kerberos
 configuring [33-11](#)
 support [33-6](#)

L

large ICMP traffic attack [48-6, 48-9](#)
 latency
 about [45-1](#)
 Layer 2 firewall
 See transparent firewall
 Layer 2 forwarding table
 See MAC address table
 Layer 3/4
 matching multiple policy maps [30-5](#)
 LDAP
 application inspection [42-1](#)
 attribute mapping [33-16, 33-17](#)
 Cisco-AV-pair [C-13](#)
 configuring [33-11](#)
 configuring a AAA server [C-2 to ??](#)
 directory search [C-3](#)
 example configuration procedures [C-16 to ??](#)
 hierarchy example [C-3](#)
 SASL [33-6](#)
 user authentication [33-6](#)
 licenses
 activation key
 entering [4-10](#)
 location [4-9](#)
 obtaining [4-9](#)
 ASA 5580 [4-2](#)

 default [4-3](#)
 evaluation [4-4](#)
 failover [4-8](#)
 guidelines [4-8](#)
 managing [4-1](#)
 preinstalled [4-3](#)
 Product Authorization Key [4-9](#)
 temporary [4-4](#)
 viewing current [4-11](#)
 VPN Flex [4-4](#)

licensing requirements
 logging [52-5](#)
 licensing requirements for SNMP [54-16](#)
 link up/down test [49-17](#)
 local user database
 adding a user [33-19](#)
 configuring [33-19](#)
 logging in [34-19](#)
 support [33-7](#)
 lockout recovery [34-30](#)
 logging
 access lists [18-1](#)
 classes
 filtering messages by [52-4](#)
 types [52-4, 52-16](#)
 device-id, including in system log messages [52-17](#)
 e-mail
 source address [52-10](#)
 EMBLEM format [52-14](#)
 facility option [52-9](#)
 filtering
 by message class [52-16](#)
 by message list [52-4](#)
 by severity level [52-1](#)
 logging queue, configuring [52-15](#)
 output destinations [52-8](#)
 console port [52-8, 52-10, 52-11](#)
 internal buffer [52-1, 52-6](#)
 Telnet or SSH session [52-6](#)

- queue
 - changing the size of [52-15](#)
 - configuring [52-15](#)
 - viewing queue statistics [52-19](#)
- severity level, changing [52-19](#)
- timestamp, including [52-18](#)
- logging feature history [52-20](#)
- logging queue
 - configuring [52-15](#)
- login
 - banner, configuring [34-7](#)
 - FTP [35-3](#)
 - local user [34-19](#)
 - password [9-1](#)
 - session [3-3](#)
 - SSH [3-3, 34-5](#)
 - Telnet [3-3, 9-1](#)
- loops, avoiding [2-10](#)

M

- MAC addresses
 - automatically assigning [6-21](#)
 - failover [50-2](#)
 - manually assigning to interfaces [7-8, 8-9](#)
 - security context classification [6-3](#)
- MAC address table
 - about [5-23](#)
 - built-in-switch [5-14](#)
 - entry timeout [5-15](#)
 - MAC learning, disabling [5-16](#)
 - resource management [6-16](#)
 - static entry [5-15](#)
- MAC learning, disabling [5-16](#)
- management interfaces
 - default settings [15-2, 16-2, 32-7](#)
- management IP address, transparent firewall [8-5](#)
- man-in-the-middle attack [5-10](#)
- mapped addresses
 - guidelines [27-21](#)
- mapped interface name [6-19](#)
- mask
 - reply, ICMP message [B-15](#)
 - request, ICMP message [B-15](#)
- Master Passphrase [9-3](#)
- match commands
 - inspection class map [31-4](#)
 - Layer 3/4 class map [30-12, 30-15](#)
- message filtering [52-4](#)
- message list
 - filtering by [52-4](#)
- message-of-the-day banner [34-8](#)
- messages, logging
 - classes
 - about [52-4](#)
 - list of [52-4](#)
 - component descriptions [52-3](#)
 - filtering by message list [52-4](#)
 - format of [52-3](#)
 - message list, creating [52-13](#)
 - severity levels [52-3](#)
- messages classes [52-4](#)
- messages in EMBLEM format [52-14](#)
- metacharacters, regular expression [12-13](#)
- MGCP inspection
 - about [41-11](#)
 - configuring [41-11](#)
- mgmt0 interfaces
 - default settings [15-2, 16-2, 32-7](#)
- MIBs [54-3](#)
- MIBs for SNMP [54-28](#)
- Microsoft Windows CA, supported [38-4](#)
- mobile redirection, ICMP message [B-15](#)
- mode
 - context [6-14](#)
 - firewall [5-1](#)
- modular policy framework
 - configuring flow-export actions for NetFlow [53-5](#)

- monitoring
 - failover [49-16](#)
 - OSPF [22-16](#)
 - resource management [6-27](#)
 - SNMP [54-1](#)
 - monitoring logging [52-19](#)
 - monitoring NSEL [53-10](#)
 - More prompt [A-5](#)
 - MPF
 - default policy [30-7](#)
 - examples [30-18](#)
 - feature directionality [30-3](#)
 - features [30-2](#)
 - flows [30-5](#)
 - matching multiple policy maps [30-5](#)
 - service policy, applying [30-17](#)
 - See also* class map
 - See also* policy map
 - MPLS
 - LDP [32-6](#)
 - router-id [32-6](#)
 - TDP [32-6](#)
 - MRoute pane
 - description [24-4](#)
 - MSFC
 - overview [1-5](#)
 - SVIs [2-7](#)
 - MTU [7-8, 8-9](#)
 - multicast traffic [5-3](#)
 - multiple context mode
 - logging [52-2](#)
 - See* security contexts
 - multiple SVIs [2-6](#)
-
- N**
- naming an interface
 - other models [7-5, 8-7](#)
 - NAT
 - about [27-1](#)
 - bidirectional initiation [27-2](#)
 - disabling proxy ARP for global addresses [19-11](#)
 - DNS [27-24](#)
 - dynamic
 - about [27-8](#)
 - dynamic NAT
 - network object NAT [28-4](#)
 - twice NAT [29-4](#)
 - dynamic PAT
 - about [27-10](#)
 - network object NAT [28-6](#)
 - twice NAT [29-8](#)
 - identity
 - about [27-11](#)
 - identity NAT
 - network object NAT [28-12](#)
 - twice NAT [29-18](#)
 - implementation [27-16](#)
 - interfaces [27-21](#)
 - mapped address guidelines [27-21](#)
 - network object
 - comparison with twice NAT [27-16](#)
 - network object NAT
 - about [27-17](#)
 - configuring [28-1](#)
 - dynamic NAT [28-4](#)
 - dynamic PAT [28-6](#)
 - examples [28-15](#)
 - guidelines [28-2](#)
 - identity NAT [28-12](#)
 - monitoring [28-14](#)
 - prerequisites [28-2](#)
 - static NAT [28-9](#)
 - no proxy ARP [28-13, 29-17](#)
 - routed mode [27-13](#)
 - route lookup [28-13, 29-22](#)
 - RPC not supported with [42-4](#)
 - rule order [27-20](#)

- static
 - about [27-3](#)
 - few-to-many mapping [27-7](#)
 - many-to-few mapping [27-6, 27-7](#)
 - one-to-many [27-6](#)
 - static NAT
 - network object NAT [28-9](#)
 - twice NAT [29-13](#)
 - static with port translation
 - about [27-4](#)
 - terminology [27-2](#)
 - transparent mode [27-13](#)
 - twice NAT
 - about [27-17](#)
 - comparison with network object NAT [27-16](#)
 - configuring [29-1](#)
 - dynamic NAT [29-4](#)
 - dynamic PAT [29-8](#)
 - examples [29-22](#)
 - guidelines [29-2](#)
 - identity NAT [29-18](#)
 - monitoring [29-22](#)
 - prerequisites [29-2](#)
 - static NAT [29-13](#)
 - types [27-3](#)
 - VPN [27-14](#)
 - VPN client rules [27-20](#)
 - neighbor reachable time [26-3](#)
 - neighbor solicitation messages [26-2](#)
 - neighbor advertisement messages [26-2](#)
 - NetFlow
 - overview [53-1](#)
 - NetFlow collector
 - configuring [53-5](#)
 - NetFlow event
 - matching to configured collectors [53-5](#)
 - NetFlow event logging
 - disabling [53-9](#)
 - Network Activity test [49-17](#)
 - network object NAT
 - about [27-17](#)
 - comparison with twice NAT [27-16](#)
 - configuring [28-1](#)
 - dynamic NAT [28-4](#)
 - dynamic PAT [28-6](#)
 - examples [28-15](#)
 - guidelines [28-2](#)
 - identity NAT [28-12](#)
 - monitoring [28-14](#)
 - prerequisites [28-2](#)
 - static NAT [28-9](#)
 - No Payload Encryption [4-7](#)
 - no proxy ARP [29-17](#)
 - NSEL and syslog messages
 - redundant messages [53-2](#)
 - NSEL configuration examples [53-12](#)
 - NSEL feature history [53-14](#)
 - NSEL licensing requirements [53-3](#)
 - NSEL runtime counters
 - clearing [53-10](#)
 - NTLM support [33-6](#)
 - NT server
 - configuring [33-11](#)
 - support [33-6](#)
-
- O**
- object groups
 - about [12-1](#)
 - configuring [12-6](#)
 - removing [12-11](#)
 - object NAT
 - See* network object NAT
 - open ports [B-14](#)
 - OSPF
 - area authentication [22-11](#)
 - area MD5 authentication [22-11](#)
 - area parameters [22-10](#)

- authentication key [22-9](#)
 - authentication support [22-2](#)
 - cost [22-9](#)
 - dead interval [22-9](#)
 - defining a static neighbor [22-12](#)
 - interaction with NAT [22-2](#)
 - interface parameters [22-8](#)
 - link-state advertisement [22-2](#)
 - logging neighbor states [22-13](#)
 - LSAs [22-2](#)
 - MD5 authentication [22-9](#)
 - monitoring [22-16](#)
 - NSSA [22-11](#)
 - packet pacing [22-16](#)
 - processes [22-2](#)
 - redistributing routes [22-4](#)
 - route calculation timers [22-13](#)
 - route summarization [22-7](#)
 - outbound access lists [32-3](#)
 - output destination [52-5](#)
 - output destinations [52-1, 52-6](#)
 - e-mail address [52-1, 52-6](#)
 - SNMP management station [52-1, 52-6](#)
 - Telnet or SSH session [52-1, 52-6](#)
 - outside, definition [1-7](#)
 - oversubscribing resources [6-8](#)
-
- P**
- packet
 - capture [57-14](#)
 - classifier [6-3](#)
 - packet flow
 - routed firewall [5-17](#)
 - transparent firewall [5-23](#)
 - packet trace, enabling [57-7](#)
 - paging screen displays [A-5](#)
 - parameter problem, ICMP message [B-15](#)
 - password
 - resetting on SSM hardware module [57-11](#)
 - passwords
 - changing [9-2](#)
 - recovery [57-8](#)
 - security appliance [9-1](#)
 - PAT
 - See* dynamic PAT
 - ping
 - See* ICMP
 - ping of death attack [48-6, 48-9](#)
 - PKI protocol [38-11](#)
 - policy, QoS [45-1](#)
 - policy map
 - inspection [31-2](#)
 - Layer 3/4
 - about [30-1](#)
 - feature directionality [30-3](#)
 - flows [30-5](#)
 - pools, address
 - DHCP [10-3](#)
 - port-forwarding
 - enabling [7-4, 8-6](#)
 - ports
 - open on device [B-14](#)
 - TCP and UDP [B-11](#)
 - port translation
 - about [27-4](#)
 - primary unit, failover [50-2](#)
 - private networks [B-2](#)
 - privileged EXEC mode
 - accessing [3-3](#)
 - privileged mode
 - prompt [A-2](#)
 - Product Authorization Key [4-9](#)
 - prompts
 - command [A-2](#)
 - more [A-5](#)
 - protocol numbers and literal values [B-11](#)
 - Protocol pane (PIM)

- description [24-10](#)
- proxied RPC request attack [48-10](#)
- proxy ARP
 - NAT
 - proxy ARP [27-22](#)
 - proxy ARP, disabling [19-11](#)
- proxy servers
 - SIP and [41-19](#)
- public key cryptography [38-2](#)

Q

QoS

- about [45-1, 45-2](#)
- DiffServ preservation [45-2](#)
- DSCP preservation [45-2](#)
- policies [45-1](#)
- statistics [45-6](#)
- token bucket [45-2](#)
- viewing statistics [45-6](#)

Quality of Service

See QoS

question mark

- command string [A-4](#)
- help [A-4](#)

queue, logging

- changing the size of [52-15](#)
- viewing statistics [52-19](#)

R

RADIUS

- attributes [C-27](#)
- Cisco AV pair [C-13](#)
- configuring a AAA server [C-27](#)
- configuring a server [33-11](#)
- downloadable access lists [35-14](#)
- network access authentication [35-4](#)

- network access authorization [35-14](#)
- support [33-3](#)

- rapid link failure detection [2-10](#)

- RAS, H.323 troubleshooting [41-10](#)

- rate limit [52-19](#)

- rate limiting [45-2](#)

- RealPlayer [41-15](#)

- redirect, ICMP message [B-15](#)

- Registration Authority description [38-2](#)

- regular expression [12-12](#)

reloading

- context [6-25](#)

- security appliance [57-8](#)

Request Filter pane

- description [24-11](#)

- resetting the services module [2-11](#)

- resetting the SSM hardware module password [57-11](#)

resource management

- about [6-8](#)

- assigning a context [6-20](#)

- class [6-15](#)

- configuring [6-8](#)

- default class [6-9](#)

- monitoring [6-27](#)

- oversubscribing [6-8](#)

- resource types [6-16](#)

- unlimited [6-9](#)

- resource usage [6-30](#)

- revoked certificates [38-2](#)

- RFCs for SNMP [54-28](#)

RIP

- authentication [23-2](#)

- definition of [23-1](#)

- enabling [23-4](#)

- support for [23-2](#)

RIP panel

- limitations [23-3](#)

- RIP Version 2 Notes [23-3](#)

routed mode

- about [5-1](#)
 - NAT [27-13](#)
 - setting [5-1](#)
 - route map
 - definition [21-1](#)
 - route maps
 - defining [21-4](#)
 - uses [21-1](#)
 - router
 - advertisement, ICMP message [B-15](#)
 - solicitation, ICMP message [B-15](#)
 - router advertisement messages [26-3](#)
 - router advertisement transmission interval [26-8](#)
 - router lifetime value [26-8](#)
 - routes
 - about default [20-4](#)
 - configuring default routes [20-4](#)
 - configuring IPv6 default [20-5](#)
 - configuring IPv6 static [20-5](#)
 - configuring static routes [20-3](#)
 - routing
 - other protocols [32-5](#)
 - RSA
 - keys, generating [34-4, 38-9](#)
 - RTSP inspection
 - about [41-15](#)
 - configuring [41-15](#)
 - rules
 - ICMP [34-10](#)
 - running configuration
 - copying [56-8](#)
 - saving [3-12](#)
 - configuration [41-25](#)
 - configuring [41-25](#)
 - SDI
 - configuring [33-11](#)
 - support [33-5](#)
 - secondary unit, failover [50-2](#)
 - security appliance
 - CLI [A-1](#)
 - managing licenses [4-1](#)
 - managing the configuration [3-11](#)
 - reloading [57-8](#)
 - upgrading software [56-2](#)
 - viewing files in Flash memory [56-1](#)
 - security contexts
 - about [6-1](#)
 - adding [6-17](#)
 - admin context
 - about [6-2](#)
 - changing [6-23](#)
 - assigning to a resource class [6-20](#)
 - cascading [6-6](#)
 - changing between [6-22](#)
 - classifier [6-3](#)
 - command authorization [34-15](#)
 - configuration
 - URL, changing [6-23](#)
 - URL, setting [6-20](#)
 - logging in [6-7](#)
 - MAC addresses
 - automatically assigning [6-21](#)
 - classifying using [6-3](#)
 - managing [6-1, 6-22](#)
 - mapped interface name [6-19](#)
 - monitoring [6-26](#)
 - MSFC compatibility [1-7](#)
 - multiple mode, enabling [6-14](#)
 - nesting or cascading [6-7](#)
 - prompt [A-2](#)
 - reloading [6-25](#)
-
- S**
- same security level communication
 - enabling [7-12, 8-13](#)
 - SCCP (Skinny) inspection
 - about [41-25](#)

- removing [6-22](#)
- resource management [6-8](#)
- resource usage [6-30](#)
- saving all configurations [3-13](#)
- unsupported features [6-13](#)
- VLAN allocation [6-19](#)
- security level
 - about [7-1](#)
 - interface [7-6, 8-7](#)
- security models for SNMP [54-15](#)
- sending messages to an e-mail address [52-10](#)
- sending messages to an SNMP server [52-12](#)
- sending messages to ASDM [52-11](#)
- sending messages to a specified output destination [52-16](#)
- sending messages to a syslog server [52-8](#)
- sending messages to a Telnet or SSH session [52-12](#)
- sending messages to the console port [52-11](#)
- sending messages to the internal log buffer [52-9](#)
- service policy
 - applying [30-17](#)
 - default [30-17](#)
 - interface [30-18](#)
- session management path [1-10](#)
- severity levels, of system log messages
 - changing [52-1](#)
 - filtering by [52-1](#)
 - list of [52-3](#)
- severity levels, of system messages
 - definition [52-3](#)
- show command, filtering output [A-4](#)
- single mode
 - backing up configuration [6-15](#)
 - configuration [6-14](#)
 - enabling [6-14](#)
 - restoring [6-15](#)
- SIP inspection
 - about [41-19](#)
 - configuring [41-19](#)
 - instant messaging [41-19](#)
 - timeouts [41-24](#)
 - troubleshooting [41-24](#)
- Smart Call Home monitoring [55-19](#)
- SMTP inspection [40-31](#)
- SNMP
 - about [54-1](#)
 - failover [54-16](#)
 - management station [52-1, 52-6](#)
 - prerequisites [54-16](#)
- SNMP configuration [54-17](#)
- SNMP groups [54-15](#)
- SNMP hosts [54-15](#)
- SNMP monitoring [54-25, 54-26](#)
- SNMP terminology [54-2](#)
- SNMP traps [54-3](#)
- SNMP users [54-15](#)
- SNMP Version 3 [54-14, 54-22](#)
- SNMP Versions 1 and 2c [54-21](#)
- source quench, ICMP message [B-15](#)
- SPAN session [2-2](#)
- SSH
 - authentication [34-18](#)
 - concurrent connections [34-2](#)
 - login [34-5](#)
 - password [9-1](#)
 - RSA key [34-4](#)
 - username [34-5](#)
- startup configuration
 - copying [56-8](#)
 - saving [3-12](#)
- statd buffer overflow attack [48-11](#)
- Stateful Failover
 - about [49-8](#)
 - state information [49-9](#)
 - state link [49-3](#)
- stateful inspection [1-10](#)
 - bypassing [44-3](#)
- state information [49-9](#)
- state link [49-3](#)

- static ARP entry [5-11](#)
- static bridge entry [5-15](#)
- Static Group pane
 - description [24-6](#)
- static NAT
 - about [27-3](#)
 - few-to-many mapping [27-7](#)
 - many-to-few mapping [27-6, 27-7](#)
 - network object NAT [28-9](#)
 - twice NAT [29-13](#)
- static NAT with port translation
 - about [27-4](#)
- static routes
 - configuring [20-3](#)
- statistics, QoS [45-6](#)
- stealth firewall
 - See* transparent firewall
- stuck-in-active [25-2](#)
- subcommand mode prompt [A-2](#)
- subnet masks
 - /bits [B-3](#)
 - about [B-2](#)
 - address range [B-4](#)
 - determining [B-3](#)
 - dotted decimal [B-3](#)
 - number of hosts [B-3](#)
- Sun RPC inspection
 - about [42-3](#)
 - configuring [42-3](#)
- SVIs
 - configuring [2-8](#)
 - multiple [2-6](#)
 - overview [2-6](#)
- switch
 - assigning VLANs to module [2-4](#)
 - autostate messaging [2-10](#)
 - BPDU forwarding [2-10](#)
 - configuration [2-1](#)
 - failover compatibility with transparent firewall [2-10](#)
 - failover configuration [2-9](#)
 - trunk for failover [2-10](#)
 - verifying module installation [2-3](#)
- switched virtual interfaces
 - See* SVIs
- switch MAC address table [5-14](#)
- SYN attacks, monitoring [6-31](#)
- SYN cookies [6-31](#)
- syntax formatting [A-3](#)
- syslogd server program [52-5](#)
- syslog messages
 - analyzing [52-2](#)
- syslog messaging for SNMP [54-26](#)
- syslog server
 - designating more than one as output destination [52-5](#)
 - EMBLEM format
 - configuring [52-14](#)
 - enabling [52-8, 52-14](#)
- system configuration [6-2](#)
- system log messages
 - classes [52-4](#)
 - classes of [52-4](#)
 - configuring in groups
 - by message list [52-4](#)
 - by severity level [52-1](#)
 - device ID, including [52-17](#)
 - disabling logging of [52-1](#)
 - filtering by message class [52-4](#)
 - managing in groups
 - by message class [52-16](#)
 - output destinations [52-1, 52-6](#)
 - syslog message server [52-6](#)
 - Telnet or SSH session [52-6](#)
 - severity levels
 - about [52-3](#)
 - changing the severity level of a message [52-1](#)
 - timestamp, including [52-18](#)

T

TACACS+

- command authorization, configuring [34-28](#)
- configuring a server [33-11](#)
- network access authorization [35-11](#)
- support [33-5](#)

TCP

- connection limits per context [6-16](#)
- ports and literal values [B-11](#)
- sequence number randomization
 - disabling using Modular Policy Framework [44-12](#)

TCP Intercept

- enabling using Modular Policy Framework [44-12](#)
- monitoring [6-31](#)

TCP normalization [44-3](#)TCP NULL flags attack [48-6, 48-9](#)

TCP state bypass

- AAA [44-5](#)
- configuring [44-10](#)
- failover [44-5](#)
- firewall mode [44-5](#)
- inspection [44-5](#)
- multiple context mode [44-5](#)
- NAT [44-5](#)
- SSMs and SSCs [44-5](#)
- TCP Intercept [44-5](#)
- TCP normalization [44-5](#)
- unsupported features [44-5](#)

TCP SYN+FIN flags attack [48-6, 48-9](#)

Telnet

- allowing management access [34-1](#)
- authentication [34-18](#)
- concurrent connections [34-2](#)
- login [34-4](#)
- password [9-1](#)

template timeout intervals

- configuring for flow-export actions [53-7](#)

temporary license [4-4](#)testing configuration [57-1](#)

threat detection

basic

- drop types [47-2](#)
- enabling [47-4](#)
- overview [47-2](#)
- rate intervals [47-2](#)
- rate intervals, setting [47-4](#)
- statistics, viewing [47-5](#)
- system performance [47-3](#)

scanning

- attackers, viewing [47-18](#)
- default limits, changing [47-17](#)
- enabling [47-17](#)
- host database [47-15](#)
- overview [47-15](#)
- shunned hosts, releasing [47-18](#)
- shunned hosts, viewing [47-17](#)
- shunning attackers [47-17](#)
- system performance [47-15](#)
- targets, viewing [47-18](#)

scanning statistics

- enabling [47-7](#)
- system performance [47-6](#)
- viewing [47-9](#)

time exceeded, ICMP message [B-15](#)time ranges, access lists [12-16](#)timestamp, including in system log messages [52-18](#)timestamp reply, ICMP message [B-15](#)timestamp request, ICMP message [B-15](#)token bucket [45-2](#)

traffic flow

- routed firewall [5-17](#)
- transparent firewall [5-23](#)

transparent firewall

about [5-2](#)

ARP inspection

- about [5-10](#)

- enabling [5-12](#)
 - static entry [5-11](#)
- data flow [5-23](#)
- DHCP packets, allowing [32-5](#)
- guidelines [5-7](#)
- H.323 guidelines [5-4](#)
- HSRP [5-3](#)
- MAC address timeout [5-15](#)
- MAC learning, disabling [5-16](#)
- management IP address [8-5](#)
- multicast traffic [5-3](#)
- packet handling [32-5](#)
- static bridge entry [5-15](#)
- unsupported features [5-7](#)
- VRRP [5-3](#)
- transparent mode
 - NAT [27-13](#)
- troubleshooting
 - H.323 [41-9](#)
 - H.323 RAS [41-10](#)
 - SIP [41-24](#)
- troubleshooting SNMP [54-23](#)
- Trusted Flow Acceleration
 - modes [5-6, 5-11, 5-14, 14-1, 32-7, 51-7](#)
- trustpoint [38-3](#)
- twice NAT
 - about [27-17](#)
 - comparison with network object NAT [27-16](#)
 - configuring [29-1](#)
 - dynamic NAT [29-4](#)
 - dynamic PAT [29-8](#)
 - examples [29-22](#)
 - guidelines [29-2](#)
 - identity NAT [29-18](#)
 - monitoring [29-22](#)
 - prerequisites [29-2](#)
 - static NAT [29-13](#)

U

- UDP
 - connection limits per context [6-16](#)
 - connection state information [1-11](#)
 - ports and literal values [B-11](#)
- unprivileged mode
 - accessing [3-3](#)
- unreachable, ICMP message [B-15](#)
- unreachable messages
 - required for MTU discovery [34-10](#)
- upgrading
 - IOS [2-1](#)
- URLs
 - context configuration, changing [6-23](#)
 - context configuration, setting [6-20](#)
 - filtering [36-1](#)
 - filtering, about [36-7](#)
 - filtering, configuration [36-11](#)
- user EXEC mode
 - prompt [A-2](#)
- username
 - adding [33-19](#)
 - encrypted [33-21](#)
 - password [33-21](#)
- users
 - SNMP [54-15](#)

V

- VeriSign, configuring CAs example [38-4](#)
- viewing QoS statistics [45-6](#)
- viewing RMS [56-19](#)
- virtual firewalls
 - See* security contexts
- virtual HTTP [35-3](#)
- virtual reassembly [1-8](#)
- VLANs
 - allocating to a context [6-19](#)

assigning to FWSM [2-4](#)
interfaces [2-4](#)
mapped interface name [6-19](#)

VoIP

proxy servers [41-19](#)
troubleshooting [41-9](#)

VPN

address range, subnets [B-4](#)

VPN client

NAT rules [27-20](#)

VPN flex license [4-4](#)

VRRP [5-3](#)

W

WCCP [37-1](#)

web caching [37-1](#)

web clients, secure authentication [35-6](#)