
Symbols

/bits subnet masks D-3

?

command string C-4

help C-4

Numerics

4GE SSM

connector types 4-1

fiber 4-3

SFP 4-3

A

A 25-7

AAA

accounting 16-12

addressing, configuring 27-2

authentication

CLI access 33-5

network access 16-1

privileged EXEC mode 33-6

authorization

command 33-7

downloadable access lists 16-7

network access 16-6

local database support 10-11

overview 10-1

performance 16-1

server

adding 10-14

types 10-3

support summary 10-3

with web clients 16-4

abbreviating commands C-3

access hours

username attribute 26-54

access list

use in classifying QoS traffic 21-4

access lists

ACE logging, configuring 13-18

comments 13-16

deny flows, managing 13-20

downloadable 16-8

EtherType, adding 13-7

extended, adding 13-6

extended, overview 13-5

implicit deny 13-3

inbound 15-1

interface, applying 15-4

IP address guidelines 13-3

logging 13-18

logging activity 13-18

NAT addresses 13-3

NAT guidelines 13-3

object grouping 13-9

object groups 13-16

outbound 15-1

overview 13-1

remarks 13-16

scheduling activation 13-16

standard, adding 13-9

types 13-2

accessing the VPN Concentrator using SSL 30-3

accessing the VPN Concentrator using TKS1 30-3

ACEs

logging 13-18

ACL

group policy WebVPN filter 26-45

WebVPN username connections 26-63

ACL filter

username attribute 26-55

ACLs

IPSec 24-20

Active Directory procedures E-19–E-23

Active/Active failover

- about 11-9
 - actions 11-12
 - avoiding duplicate MAC addresses 11-10, 11-31
 - command replication 11-11
 - configuration synchronization 11-10
 - configuring
 - asymmetric routing support 11-31
 - cable-based failover 11-23
 - failover criteria 11-30
 - failover group preemption 11-29
 - HTTP replication 11-29
 - interface monitoring 11-30
 - interface poll times 11-30
 - LAN-based failover 11-25
 - prerequisites 11-23
 - unit poll times 11-30
 - virtual MAC addresses 11-30
 - device initialization 11-10
 - primary status 11-10
 - secondary status 11-10
 - triggers 11-11
- Active/Standby failover
- about 11-6
 - actions 11-8
 - command replication 11-7
 - configuration synchronization 11-6
 - configuring
 - cable-based 11-16
 - failover criteria 11-22
 - HTTP replication 11-21
 - interface monitoring 11-21
 - interface poll times 11-22
 - LAN-based 11-18
 - prerequisites 11-16
 - unit poll times 11-22
 - virtual MAC addresses 11-22
 - device initialization 11-6
 - primary unit 11-6
 - secondary unit 11-6
 - triggers 11-8
- address
- pool, configuring 28-4
 - range, subnets D-4
- admin context
- changing 5-5
 - overview 1-6, 3-1
- administrative distance
- about 8-2
- Advanced Encryption Standard (AES) 24-3
- AIP SSM
- checking status 19-1, 19-13
 - configuration 19-2
 - initial setup 19-4
 - loading an image 19-14
 - overview 19-1
 - sending traffic to 19-2
- alternate address, ICMP message D-15
- application access
- and e-mail proxy 30-50
 - and hosts file errors 30-18
 - and Web Access 30-50
 - configuring client applications 30-49
 - enabling cookies on browser 30-49
 - group policy WebVPN attribute 26-47
 - privileges 30-49
 - quitting properly 30-19, 30-49
 - re-enabling 30-19
 - setting up on client 30-49
 - username WebVPN attribute 26-64
 - using e-mail 30-50
 - with IMAP client 30-50
- Application Access Panel, WebVPN 30-33
- application inspection
- applying 22-5
 - configuring 22-1, ??–22-51
 - security level requirements 6-1
- Application Profile Customization Framework 30-29
- ARP

- inspection
 - enabling 23-2
 - overview 23-1
 - static entry 23-2
 - test, failover 11-15
- ARP inspection
 - configuring 23-1
 - overview 23-1
 - static ARP entry, adding 23-2
- ARP spoofing 23-2
- ASA 1-4
- ASDM software
 - installing 34-3
- ASR 11-31
 - See* asymmetric routing support
- asymmetric routing support 11-31
- attributes
 - LDAP E-5
 - policy E-2
 - RADIUS E-26
 - username 26-53
- attribute-value pairs (AVP) 26-19
- authenticating
 - WebVPN users with digital certificates 30-15
- authentication
 - FTP 16-2
 - HTTP 16-2
 - network access 16-1
 - overview 10-2
 - Telnet 16-2
 - web clients 16-4
- authentication restrictions, WebVPN 30-4
- authorization
 - network access 16-6
 - overview 10-2
- Auto-MDI/MDIX 4-1
- auto-signon
 - group policy WebVPN attribute 26-44
 - username WebVPN attribute 26-65

- Auto-Update
 - configuring 34-9-??

B

- backup device
 - load balancing 25-5
- backup server attributes, group policy 26-35
- Baltimore Technologies
 - CA server support 32-4
- Bandwidth Limiting Traffic stream (BLT) 21-6
- banner message, group policy 26-28
- basic settings 7-1
- BGP 13-6
- bits subnet masks D-3
- BPDUs
 - ACL, EtherType 13-8
- bridge
 - entry timeout 23-3
 - table
 - See* MAC address table
- broadcast Ping test 11-15

C

- CA
 - CRs. and 32-2
 - public key cryptography 32-1
 - revoked certificates 32-2
 - server support 32-4
 - supported servers 32-4
- CA certificate validation, not done in WebVPN 30-2
- caching 30-27
- capturing packets 36-10
- cascading ACLs 24-15
- certificate authentication
 - e-mail proxy 30-26
- certificate enrollment protocol 32-7

- certificate group matching
 - configuring 24-9
 - rule and policy, creating 24-10
- Certificate Revocation Lists
 - See CRLs
- certification authority
 - See CA
- changing between contexts 5-6
- Cisco 32-4
- Cisco IP Phones
 - application inspection 22-44
 - with DHCP 8-27
- Cisco LDAP attributes E-5
- Cisco-AV-Pair LDAP attributes E-14
- Class A, B, and C addresses D-2
- classification policy, traffic 21-2
- classifying traffic for QoS 21-4
- CLI
 - abbreviating commands C-3
 - adding comments C-5
 - command line editing C-3
 - command output paging C-5
 - displaying C-5
 - help C-4
 - paging C-5
 - syntax formatting C-3
- client
 - VPN 3002 hardware, forcing client update 25-3
 - Windows, client update notification 25-3
- client access rules, group policy 26-38
- client firewall, group policy 26-36
- client update, performing 25-3
- cluster
 - load balancing configurations 25-7
 - mixed scenarios 25-8
- cluster IP address, load balancing 25-6
- cluster, virtual 25-5
- command authorization
 - configuring 33-7
 - overview 33-7
- command prompts C-2
- comments
 - access lists 13-16
 - configuration C-5
- configuration
 - clearing 2-4
 - comments C-5
 - context files 3-2
 - saving 2-3
 - text file 2-5
 - URL for a context 5-3
 - viewing 2-4
- configuration mode
 - accessing 2-2
 - prompt C-2
- connect time, maximum, username attribute 26-55
- connection
 - blocking 20-6
- connection limits
 - configuring 20-4
- content transformation, WebVPN 30-28
- contexts
 - resource usage 5-10
 - See security contexts
- conversion error, ICMP message D-16
- cookies, enabling for WebVPN 30-5
- crash dump 36-10
- crypto map
 - ACLs 24-20
 - applying to interfaces 24-20, 29-7
 - clearing configurations 24-28
 - creating an entry to use the dynamic crypto map 28-7
 - definition 24-12
 - dynamic 24-25
 - dynamic, creating 28-6
 - entries 24-12
 - examples 24-21
 - policy 24-13

- crypto show commands 24-27
 - CSC SSM
 - checking status 19-1, 19-13
 - failover 19-7
 - getting started 19-7
 - loading an image 19-14
 - overview 19-5
 - sending traffic to 19-11
 - what to scan 19-9
 - CSD support A-8
 - customization
 - group policy WebVPN attribute 26-42
 - username WebVPN attribute 26-62
 - customizing login windows for WebVPN users 26-18
 - cut-through proxy 16-1
-
- D**
- data flow
 - routed firewall 12-3
 - transparent firewall 12-12
 - debug messages 36-10
 - default
 - DefaultL2Lgroup 26-1
 - DefaultRAGroup 26-1
 - queue 21-2
 - tunnel group 24-11
 - default domain name, group policy 26-31
 - default group policy 26-1, 26-19
 - default LAN-to-LAN tunnel group 26-10
 - default remote access tunnel group, configuring 26-5
 - default routes
 - configuring 8-3
 - defining equal cost routes 8-3
 - overview 8-3
 - default tunnel group 26-2
 - delay-sensitive traffic, priority 21-6
 - deny flows, logging 13-20
 - deny in a crypto map 24-15
 - deny-message
 - group policy WebVPN attribute 26-42
 - username WebVPN attribute 26-62
 - DES
 - IKE policy keywords (table) 24-3
 - DfltGrpPolicy 26-20
 - DHCP
 - addressing, configuring 27-3
 - relay 8-28
 - server
 - Cisco IP Phones 8-27
 - configuring 8-24
 - overview 8-24
 - transparent firewall 13-6
 - Diffie-Hellman
 - Group 5 24-4
 - groups supported 24-4
 - digital certificates
 - authenticating WebVPN users 30-15
 - SSL 30-4
 - WebVPN authentication restrictions 30-4
 - directory hierarchy search E-4
 - disabling content rewrite 30-28
 - DMZ, definition 1-1
 - DNS
 - NAT effect on 14-14
 - DNS inspection
 - managing 22-10
 - overview 22-10
 - rewrite, configuring 22-12
 - rewrite, overview 22-11
 - DNS server, configuring 26-23
 - DNS, configuring for WebVPN 30-15
 - domain attributes, group policy 26-31
 - domain name 7-2
 - dotted decimal subnet masks D-3
 - downloadable access lists
 - configuring 16-8
 - converting netmask expressions 16-11

DSA keys
 generating 32-5
 dual IP stack
 configuring 9-7
 duplex, configuring 4-1
 dynamic crypto map 24-25
 creating 28-6
 See also crypto map
 dynamic NAT
 See NAT

E
 echo reply, ICMP message D-15
 ECMP 8-2
 editing command lines C-3
 EIGRP 13-6
 e-mail
 closing the Outlook connection 30-27
 configuring for WebVPN 30-25
 proxies, WebVPN 30-25
 WebVPN, configuring 30-25
 e-mail proxy
 and WebVPN 30-50
 certificate authentication 30-26
 enable
 accessing 2-2
 end-user interface, WebVPN, defining 30-32
 Entrust
 CA server support 32-4
 ESP security protocol 24-2
 established command
 security level requirements 6-2
 Ethernet
 Auto-MDI/MDIX 4-1
 duplex 4-1
 speed 4-1
 EtherType
 assigned numbers 13-8

external group policy, configuring 26-21

F

failover
 Active/Active, configuring 11-23
 Active/Active, *See* Active/Active failover
 Active/Standby, configuring 11-16
 Active/Standby, *See* Active/Standby failover
 configuration file
 terminal messages 11-7
 configuring 11-16
 contexts 11-6
 controlling 11-42
 debug messages 11-44
 disabling 11-43
 displaying commands 11-41
 encrypting failover communication 11-32
 Ethernet failover cable 11-3
 examples
 Active/Active LAN-based failover 11-48
 Active/Standby cable-based failover 11-45
 Active/Standby LAN-based failover 11-46
 failover link 11-3
 forcing 11-42
 health monitoring 11-14
 interface health 11-15
 interface monitoring 11-15
 interface tests 11-15
 licenses 11-2
 link communications 11-3
 MAC addresses 11-6
 monitoring 11-14, 11-42
 network tests 11-15
 overview 11-1
 primary unit 11-6
 restoring a failed group 11-43
 restoring a failed unit 11-43
 secondary unit 11-6

- serial cable 11-4
- SNMP syslog traps 11-44
- software versions 11-2
- state link 11-4
- Stateful Failover, *See* Stateful Failover
- system messages 11-44
- system requirements 11-2
- testing 11-42
- type selection 11-13
- understanding 11-1
- unit health 11-14
- verifying the configuration 11-33
- fast path 1-4
- fiber interfaces 4-3
- filter (ACL)
 - group policy WebVPN attribute 26-45
 - username WebVPN attribute 26-63
- filtering
 - ActiveX 17-1
 - overview 17-1
 - security level requirements 6-1
 - servers supported 17-4
 - show command output C-4
 - URLs 17-4
- firewall mode
 - configuring 2-2
 - overview 12-1
- firewall policy, group policy 26-36
- FO (failover) license 11-2
- FO_AA license 11-2
- fragment size
 - configuring 20-6
- fragmentation policy, IPSec 24-8
- FTP inspection
 - configuring 22-18
 - overview 22-18
- functions
 - username WebVPN attribute 26-59
 - WebVPN group policy attribute 26-41

G

- general attributes, tunnel group 26-2
- general parameters, tunnel group 26-2
- general tunnel-group connection parameters 26-2
- generating
 - DSA keys 32-5
 - RSA keys 32-5
- global addresses
 - recommendations 14-13
 - specifying 14-24
- global e-mail proxy attributes 30-25
- global IPSec SA lifetimes, changing 24-22
- group policy
 - attributes 26-23
 - backup server attributes 26-35
 - client access rules 26-38
 - configuring 26-21
 - default domain name for tunneled packets 26-31
 - definition 26-1, 26-19
 - domain attributes 26-31
 - external, configuring 26-21
 - firewall policy 26-36
 - hardware client user idle timeout 26-33
 - internal, configuring 26-22
 - IP phone bypass 26-33
 - IPSec over UDP attributes 26-28
 - LEAP Bypass 26-34
 - network extension mode 26-34
 - security attributes 26-26
 - split tunneling attributes 26-29
 - split-tunneling domains 26-31
 - user authentication 26-32
 - VPN attributes 26-24
 - VPN hardware client attributes 26-32
 - webvpn attributes 26-40
 - WINS and DNS servers 26-23
- group policy WebVPN attributes
 - application access 26-47

- auto-signon 26-44
- customization 26-42
- deny-message 26-42
- filter 26-45
- home page 26-44
- html-content filter 26-43
- keep-alive-ignore 26-48
- port forward 26-47
- port-forward-name 26-47
- sso-server 26-48
- svc 26-48
- url-list 26-45
- group policy, default 26-19
- group policy, secure unit authentication 26-32
- group-lock
 - username attribute 26-57
- GTP inspection
 - configuring 22-21
 - overview 22-21

H

- H.225
 - timeouts 22-28
- H.245
 - troubleshooting 22-29
- H.323
 - troubleshooting 22-29, 22-30
- H.323 inspection
 - configuring 22-27
 - limitations 22-28
 - overview 22-27
- hairpinning 24-20
- hardware client
 - group policy attributes 26-32
- help, command line C-4
- HMAC hashing method 24-3
- homepage
 - group policy WebVPN attribute 26-44

- username WebVPN attribute 26-61
- hostname
 - configuring 7-2
- hosts file
 - errors 30-18
 - WebVPN 30-18
- hosts file, reconfiguring 30-19
- hosts, subnet masks for D-3
- HSRP 12-9
- html-content-filter
 - group policy WebVPN attribute 26-43
 - username WebVPN attribute 26-61
- HTTP
 - authentication 33-5
 - filtering 17-4
- HTTP inspection
 - configuring 22-30
 - overview 22-30
- HTTP/HTTPS Web VPN proxy, setting 30-5
- HTTPS
 - for WebVPN sessions 30-3
- hub-and-spoke 24-20

I

- ICMP
 - testing connectivity 36-1
 - type numbers D-15
- ID method for ISAKMP peers, determining 24-6
- idle timeout
 - hardware client user, group policy 26-33
 - username attribute 26-55
- IKE
 - benefits 24-3
 - creating policies 24-4
 - See also ISAKMP
- IKE keepalive setting
 - tunnel group 26-3
- ILS

- application inspection 22-34
- IM 22-42
- inbound access lists 15-1
- information
 - reply, ICMP message D-16
 - request, ICMP message D-16
- inheritance
 - tunnel group 26-1
 - username attribute 26-54
- inside, definition 1-1
- inspection engines
 - overview 22-2
 - See application inspection
- Instant Messaging
 - See IM
- interfaces
 - configuring for remote access 28-2
 - configuring IPv6 on 9-2
 - duplex 4-1
 - enabled status 4-1, 4-2, 6-2
 - enabling 4-1, 4-2
 - failover monitoring 11-15
 - fiber 4-3
 - global addresses 14-24
 - IDs 4-2
 - naming 6-3
 - SFP 4-3
 - shared 3-6
 - speed 4-1
 - subinterfaces 4-3
 - viewing monitored interface status 11-41
- internal group policy, configuring 26-22
- Internet Security Association and Key Management Protocol
 - See ISAKMP
- intrusion prevention configuration 19-2
- IP addresses
 - classes D-2
 - configuring an assignment method 27-1
 - configuring for VPNs 27-1
 - configuring local IP address pools 27-2
 - management, transparent firewall 7-5
 - overlapping between contexts 3-4
 - private D-2
 - subnet mask D-4
- IP phone bypass, group policy 26-33
- IP spoofing
 - preventing 20-5
- IPS configuration 19-2
- IPSec
 - ACLs 24-20
 - basic configuration with static crypto maps 24-23
 - Cisco VPN Client 24-2
 - configuring 24-1, 24-11
 - crypto map entries 24-12
 - fragmentation policy 24-8
 - LAN-to-LAN configurations 24-2
 - over NAT-T, enabling 24-7
 - over TCP, enabling 24-8
 - overview 24-2
 - remote access configurations 24-2
 - SA lifetimes, changing 24-22
 - setting maximum active VPN sessions 25-3
 - tunnel 24-11
 - viewing configuration 24-27
- IPSec over UDP, group policy, configuring attributes 26-28
- IPSec parameters, tunnel group 26-3
- IPSec remote-access tunnel group 26-6
- IPv6
 - access lists 9-4
 - commands 9-1
 - configuring alongside IPv4 9-7
 - default route 9-4
 - dual IP stack 9-7
 - enabling 9-2
 - static routes 9-4
 - verifying 9-5

IPv6 addresses

- anycast D-9
- command support for 9-1
- format D-5
- multicast D-8
- prefixes D-10
- required D-10
- types of D-6
- unicast D-6

ISAKMP

- configuring 24-1, 24-2
- determining an ID method for peers 24-6
- disabling in aggressive mode 24-6
- enabling on the outside interface 24-6, 28-3
- overview 24-3
- policies, configuring 24-5
- See also IKE

ISAKMP keepalive setting

- tunnel group 26-3

J

Java applets

- filtering 17-2

K

keep-alive-ignore

- group policy WebVPN attribute 26-48
- username WebVPN attribute 26-65

Kerberos

- configuring 10-14
- support 10-7

L

LAN-to-LAN tunnel group, configuring 26-10

latency 21-1, 21-8

reducing 21-9

Layer 2

- forwarding table
 - See MAC address table

Layer 2 firewall

- See transparent firewall

LDAP

- AAA support 10-8
- application inspection 22-34
- attribute mapping 10-10
- Cisco attributes E-5
- Cisco-AV-pair E-14
- configuring 10-14
- configuring a AAA server E-2–E-18
- directory overview E-3
- directory search E-4
- example configuration procedures E-19–E-23
- hierarchy example E-3
- permissions policy E-2
- SASL 10-8
- schema example E-15
- schema loading E-18
- schema planning E-3–E-5
- server configuration overview E-3
- server type 10-9
- user authentication 10-8
- user authorization 10-9
- user permissions E-18

LEAP Bypass, group policy 26-34

licenses

- FO 11-2
- FO_AA 11-2
- managing 34-1
- UR 11-2

link up/down test 11-15

LLQ

- See low-latency queue

load balancing

- cluster configurations 25-7

- concepts 25-5
 - eligible clients 25-7
 - eligible platforms 25-7
 - implementing 25-6
 - mixed cluster scenarios 25-8
 - platforms 25-7
 - prerequisites 25-6
 - local user database
 - adding a user 10-13
 - configuring 10-13
 - logging in 33-6
 - support 10-11
 - lockout
 - recovery 33-15
 - logging
 - access lists 13-18
 - login
 - FTP 16-2
 - local user 33-6
 - login banner
 - configuring 33-16
 - login windows, customizing for WebVPN users 26-18
 - logins, simultaneous, username attribute 26-54
 - low-latency queue 21-2
 - applying 21-8
-
- M**
- MAC address table 23-3
 - entry timeout 23-3
 - MAC learning, disabling 23-4
 - overview 12-12
 - static entry 23-3
 - MAC addresses, failover 11-6
 - MAC learning, disabling 23-4
 - management IP address, transparent firewall 7-5
 - man-in-the-middle attack 23-2
 - MAPI, configuring 30-26
 - mapped interface name 5-2
 - mask
 - reply, ICMP message D-16
 - request, ICMP message D-16
 - matching
 - command criteria for QoS 21-5
 - matching, certificate group 24-9
 - maximum active IPsec VPN sessions, setting 25-3
 - maximum connect time,username attribute 26-55
 - maximum object size to ignore username WebVPN attribute 26-65
 - maximum sessions
 - IPsec 25-11
 - MD5
 - IKE policy keywords (table) 24-3
 - message-of-the-day banner 33-16
 - MGCP inspection
 - configuring 22-35
 - overview 22-36
 - MIBs 35-1
 - Microsoft Windows 2000 CA
 - supported 32-4
 - mixed cluster scenarios, load balancing 25-8
 - mobile redirection, ICMP message D-16
 - mode
 - context 3-10
 - monitoring
 - failover 11-14
 - OSPF 8-15
 - SNMP 35-1
 - More prompt C-5
 - MPLS
 - LDP 13-8
 - router-id 13-8
 - TDP 13-8
 - multicast traffic 12-9
 - multiple context mode 5-1
 - multiple mode, enabling 3-10

N

N2H2 filtering server

supported 17-4

URL for website 17-4

naming an interface 6-3

NAT

bypassing NAT

configuration 14-29

overview 14-9

DNS 14-14

dynamic NAT

configuring 14-22

implementation 14-16

overview 14-5

examples 14-32

exemption from NAT

configuration 14-31

overview 14-9

identity NAT

configuration 14-29

overview 14-9

NAT ID 14-16

order of statements 14-13

overlapping addresses 14-33

overview 14-1, 14-2

PAT

configuring 14-22

implementation 14-16

overview 14-6

policy NAT

overview 14-9

port redirection 14-34

RPC not supported with 22-49

same security level 14-12

security level requirements 6-2

static identify, configuring 14-30

static NAT

configuring 14-25

overview 14-7

static PAT

configuring 14-26

overview 14-7

transparent firewall 12-11

types 14-5

NAT-T

enabling IPSec over NAT-T 24-7

using 24-7

Netscape CMS

CA server support 32-4

Network Activity test 11-15

Network Address Translation

See NAT

network extension mode, group policy 26-34

networks, overlapping 14-33

NT server

configuring 10-14

support 10-7

NTLM support 10-7

O

object groups

nesting 13-13

removing 13-15

open ports D-14

OSPF

area authentication 8-10

area MD5 authentication 8-10

area parameters 8-10

authentication key 8-8

cost 8-8

dead interval 8-8

default route 8-13

displaying update packet pacing 8-14

enabling 8-5

hello interval 8-8

interface parameters 8-8

- link-state advertisement 8-4
- logging neighbor states 8-14
- MD5 authentication 8-8
- monitoring 8-15
- NSSA 8-11
- overview 8-4
- packet pacing 8-14
- processes 8-4
- redistributing routes 8-5
- route calculation timers 8-13
- route map 8-6
- route summarization 8-12
- stub area 8-10
 - summary route cost 8-10
- outbound access lists 15-1
- Outlook connection, closing 30-27
- Outlook Exchange proxy, configuring 30-26
- Outlook Web Access (OWA) and WebVPN 30-50
- outside, definition 1-1

P

- packet
 - capture 36-10
 - classifier 3-3
 - flow, transparent firewall 12-12
- packet flow
 - routed firewall 12-3
- paging screen displays C-5
- parameter problem, ICMP message D-15
- password
 - username, setting 26-52
 - WebVPN 30-44
- passwords
 - changing 7-1
 - recovery 36-6
- password-storage, username attribute 26-57
- PAT
 - static 14-26

- PAT (Port Address Translation)
 - limitations 22-41
 - See also NAT
- PDA support for WebVPN 30-24
- peers
 - alerting before disconnecting 24-9
 - ISAKMP, determining ID method 24-6
- performance, optimizing for WebVPN 30-27
- permit in a crypto map 24-15
- ping
 - See ICMP
- PKI protocol 32-7
- policing
 - flow within a tunnel 21-4
 - QoS 21-2
 - strict 21-6
 - verifying the configuration 21-13
- policy NAT
 - dynamic, configuring 14-23
 - overview 14-9
 - static PAT, configuring 14-27
 - static, configuring 14-25
- policy, QoS 21-1
- policy-map
 - defining for QoS 21-5
 - use in QoS 21-7
- pools
 - address
 - global NAT 14-24
- pools, address
 - DHCP 8-25
- Port Forwarding
 - configuring client applications 30-49
- port forwarding
 - automatic applet download 30-17
- port-forward
 - group policy WebVPN attribute 26-47
 - username WebVPN attribute 26-64
- port-forward-name

- group policy WebVPN attribute 26-47
- username WebVPN attribute 26-64

ports

- open on device D-14
- redirection, NAT 14-34

primary unit, failover

- overview 11-6

priority queue

- configuration for an interface, viewing 21-13
- configuring 21-8
- for delay-sensitive traffic 21-6
- sizing 21-8

private networks D-2

privilege level, username, setting 26-53

privileged mode

- accessing 2-2
- prompt C-2

prompts

- command C-2
- more C-5

protocol numbers and literal values D-11

proxy

- See e-mail proxy

proxy bypass 30-29

proxy servers

- SIP and 22-42

public key cryptography 32-1

Q

QoS

- (definition) 21-1
- action 21-3
- classifying traffic 21-4
- concepts 21-2
- defining a policy map 21-5
- match command criteria 21-5
- overview 21-1
- policies 21-1

- policing 21-2

- policy, configuring 21-3

- statistics 21-14

- traffic class 21-3

- viewing statistics 21-14

Quality of Service, See QoS

question mark

- command string C-4
- help C-4

queue

- latency, reducing 21-9
- limit 21-8
- priority, configuring 21-6, 21-8

R

RADIUS

- attribute policy E-2
- attributes E-26
- Cisco AV pair E-14
- configuring a AAA server E-26
- configuring a server 10-14
- downloadable access lists 16-8
- network access authentication 16-3
- network access authorization 16-7
- permissions policy E-2
- support 10-4

RAS

- H.323 troubleshooting 22-30

- rate limiting 21-6

- RealPlayer 22-40

- reboot, waiting until active sessions end 24-8

- redirect, ICMP message D-15

- redundancy, in site-to-site VPNs, using crypto maps 24-27

Registration Authority

- description 32-2

reloading

- context 5-7

- remarks 13-16

- remote access
 - configuration summary 28-1
 - IPSec tunnel group, configuring 26-6
 - restricting 26-57
 - tunnel group, configuring default 26-5
 - user
 - adding 28-4
 - VPN, configuring 28-1
 - resource usage 5-10
 - resource types 5-10
 - revoked certificates 32-2
 - rewrite, disabling 30-28
 - RIP
 - default route updates 8-16
 - enabling 8-16
 - overview 8-16
 - passive 8-16
 - routed mode
 - setting 2-2
 - router
 - advertisement, ICMP message D-15
 - solicitation, ICMP message D-15
 - routes
 - about default 8-3
 - about static 8-1
 - configuring default routes 8-3
 - configuring IPv6 default 9-4
 - configuring IPv6 static 9-4
 - configuring static routes 8-2
 - routing
 - OSPF 8-16
 - other protocols 13-5
 - RIP 8-17
 - RS-232 cable
 - See failover 11-4
 - RSA
 - KEON
 - CA server support 32-4
 - keys
 - generating 32-5, 33-2
 - signatures
 - IKE authentication method 32-2
 - RTSP inspection
 - configuring 22-40
 - overview 22-40
-
- S**
- same security level communication
 - NAT 14-12
 - SAs
 - lifetimes 24-22
 - SCCP (Skinny) inspection
 - configuration 22-44
 - configuring 22-44
 - overview 22-44
 - SDI
 - configuring 10-14
 - support 10-6
 - secondary device, virtual cluster 25-5
 - secondary unit, failover 11-6
 - secure unit authentication, group policy 26-32
 - security
 - WebVPN 30-2, 30-5
 - security appliance
 - connecting to 2-1
 - reloading 36-6
 - security association
 - clearing 24-27
 - See also SAs
 - security attributes, group policy 26-26
 - security context
 - cascading 3-9
 - managing 5-1
 - monitoring 5-8
 - security contexts
 - adding 5-2
 - admin context

- changing 5-5
- overview 1-6, 3-1
- changing between 5-6
- classifier 3-3
- configuration
 - files 3-2
 - URL, changing 5-6
 - URL, setting 5-3
- logging in 3-10
- mapped interface name 5-2
- multiple mode, enabling 3-10
- nesting or cascading 3-9
- overview 3-1
- prompt C-2
- reloading 5-7
- removing 5-5
- unsupported features 3-2
- VLAN allocation 5-2
- security level
 - overview 6-1
- serial cable
 - See failover
- session management path 1-4
- SHA
 - IKE policy keywords (table) 24-3
- shared interfaces 3-6
- shared VLANs 3-6
- show command, filtering output C-4
- simultaneous logins
 - username attribute 26-54
- single mode
 - backing up configuration 3-10
 - configuration 3-10
 - enabling 3-10
 - restoring 3-11
- single sign-on
 - See SSO
- single-signon
 - group policy WebVPN attribute 26-48
 - username WebVPN attribute 26-66
- SIP
 - troubleshooting 22-44
- SIP inspection
 - configuring 22-42
 - instant messaging 22-42
 - overview 22-42
 - timeouts 22-43
- site-to-site VPNs, redundancy 24-27
- sizing the priority queue 21-8
- SMTP inspection
 - configuring 22-46
- SNMP
 - MIBs 35-1
 - overview 35-1
 - traps 35-2
- source quench, ICMP message D-15
- speed, configuring 4-1
- split tunneling
 - group policy 26-29
 - group policy, domains 26-31
- SSH
 - authentication 33-5
 - concurrent connections 33-2
 - login 33-3
 - RSA key 33-2
 - username 33-3
- SSL
 - certificate 30-4
 - used to access the VPN Concentrator 30-3
- SSL VPN Client
 - benefits 31-1
 - compression 31-7
 - DPD 31-6
 - enabling 31-3
 - address assignment 31-3
 - groups and users 31-4
 - permanent installation 31-5
 - tunnel group 31-4

- installing 31-2
 - images 31-2
 - order 31-2
 - keepalive messages 31-6
 - logging out sessions 31-8
 - viewing sessions 31-8
 - SSL VPN Client (SVC)
 - group policy WebVPN attribute 26-48
 - username WebVPN attribute 26-66
 - SSL/TLS encryption protocols
 - configuring 30-4
 - WebVPN 30-4
 - SSM
 - checking status 19-1, 19-13
 - configuration
 - AIP SSM 19-2
 - CSC SSM 19-7
 - loading an image 19-14
 - See also AIP SSM
 - See also CSC SSM
 - SSO with WebVPN 30-5–30-14
 - configuring HTTP Basic and NTLM authentication 30-6
 - configuring HTTP form protocol 30-9
 - configuring SiteMinder 30-7
 - sso-server
 - group policy WebVPN attribute 26-48
 - username WebVPN attribute 26-66
 - startup configuration 3-2
 - state information 11-13
 - state link 11-4
 - Stateful Failover
 - overview 11-13
 - state information 11-13
 - state link 11-4
 - statistics 11-36, 11-40
 - stateful inspection 1-4
 - static ARP entry 23-2
 - static bridge entry 23-3
 - static NAT
 - See NAT
 - static PAT
 - See NAT
 - static routes
 - configuring 8-2
 - overview 8-1
 - statistics
 - QoS 21-14
 - viewing QoS 21-14
 - stealth firewall
 - See transparent firewall
 - stub multicast routing
 - See SMR
 - subcommand mode prompt C-2
 - subinterfaces
 - adding 4-3
 - subnet masks
 - /bits D-3
 - address range D-4
 - determining D-3
 - dotted decimal D-3
 - number of hosts D-3
 - overview D-2
 - Sun Microsystems Java™ Runtime Environment (JRE) and WebVPN 30-49
 - Sun RPC inspection
 - configuring 22-48
 - overview 22-49
 - svc
 - group policy WebVPN attribute 26-48
 - username WebVPN attribute 26-66
 - syntax formatting C-3
 - system configuration
 - network settings 3-2
 - overview 1-6, 3-1
-
- T**
- TACACS+

- configuring a server 10-14
- network access authorization 16-6
- support 10-5
- TACACS+ command authorization
 - configuring 33-11
- tail drop 21-8
- TCP
 - ports and literal values D-11
 - sequence number randomization
 - disabling
- TCP normalization
 - configuring 20-1
- Telnet
 - authentication 33-5
 - concurrent connections 33-1
- testing configuration 36-1
- time exceeded, ICMP message D-15
- time ranges
 - access lists 13-16
- timestamp
 - reply, ICMP message D-16
 - request, ICMP message D-16
- TLS1
 - used to access the VPN Concentrator 30-3
- toolbar, floating, WebVPN 30-34
- traffic
 - classifying for QoS 21-4
- traffic class, QoS 21-3
- traffic flow
 - routed firewall 12-3
 - transparent firewall 12-12
- traffic policing
 - verifying the configuration 21-13
- Transform 24-12
- transform set
 - creating 28-4
 - definition 24-12
- transmit queue ring limit 21-8
- transparent firewall
 - ARP inspection
 - enabling 23-2
 - overview 23-1
 - static entry 23-2
 - data flow 12-12
 - DHCP packets, allowing 13-6
 - guidelines 12-10
 - HSRP 12-9
 - MAC address timeout 23-3
 - MAC learning, disabling 23-4
 - management IP address 7-5
 - multicast traffic 12-9
 - NAT 12-11
 - overview 12-9
 - packet handling 13-5
 - static bridge entry 23-3
 - VRRP 12-9
- transparent mode
 - guidelines 12-10
 - overview 12-8
 - unsupported features 12-11
- traps, SNMP 35-2
- troubleshooting
 - H.323 22-29
 - H.323 RAS 22-30
 - SIP 22-44
- trustpoint 32-3
- tunnel
 - IPSec 24-11
 - security appliance as a tunnel endpoint 24-1
- tunnel group
 - configuring 26-5
 - default 24-11, 26-1, 26-2
 - default LAN-to-LAN, configuring 26-10
 - default, remote access, configuring 26-5
 - definition 26-1, 26-2
 - general parameters 26-2
 - inheritance 26-1
 - IPSec parameters 26-3

- LAN-to-LAN, configuring 26-10
- remote access
 - configuring 28-5
- remote-access, configuring 26-6
- tunnel-group
 - general attributes 26-2
 - webvpn attributes 26-4
- tunnel-group ISAKMP/IKE keepalive settings 26-3
- tunneling
 - overview 24-1
- tx-ring-limit 21-8

U

- UDP
 - connection state information 1-4
 - ports and literal values D-11
- unprivileged mode
 - prompt C-2
- unreachable, ICMP message D-15
- UR (unrestricted) license 11-2
- URL
 - context configuration, changing 5-6
 - context configuration, setting 5-3
- url-list
 - group policy WebVPN attribute 26-45
 - username WebVPN attribute 26-63
- URLs
 - filtering 17-4
 - filtering, configuration 17-6
- user
 - configuring specific 26-52
 - definition 26-1
 - remote access
 - adding 28-4
- user access, restricting 26-57
- user authentication, group policy 26-32
- username
 - WebVPN 30-44
 - attributes
 - access hours 26-54
 - configuring 26-51, 26-53
 - group-lock 26-57
 - inheritance 26-54
 - password, setting 26-52
 - password-storage 26-57
 - privilege level, setting 26-53
 - simultaneous logins 26-54
 - vpn-filter 26-55
 - vpn-framed-ip-address 26-56
 - vpn-idle timeout 26-55
 - vpn-session-timeout 26-55
 - vpn-tunnel-protocol 26-56
 - configuration, viewing 26-51
 - WebVPN attributes
 - auto-signon 26-65
 - customization 26-62
 - deny message 26-62
 - filter (ACL) 26-63
 - functions 26-59
 - homepage 26-61
 - html-content-filter 26-61
 - keep-alive ignore 26-65
 - port-forward 26-64
 - port-forward-name 26-64
 - sso-server 26-66
 - svc 26-66
 - url-list 26-63
 - WebVPN mode 26-58
- U-turn 24-20

V

- verifying the traffic-policing configuration 21-13
- VeriSign
 - configuring CAs, example 32-4
- viewing
 - RMS 34-11

- viewing QoS statistics 21-14
 - virtual cluster 25-5
 - IP address 25-6
 - master 25-5
 - virtual firewalls
 - See security contexts
 - VLANs 4-3
 - allocating to a context 5-2
 - mapped interface name 5-2
 - shared 3-6
 - VoIP
 - proxy servers 22-42
 - troubleshooting 22-29
 - VPN
 - Client, IPSec attributes 24-2
 - parameters, general, setting 25-1
 - setting maximum number of IPSec sessions 25-3
 - VPN attributes, group policy 26-24
 - VPN hardware client, group policy attributes 26-32
 - vpn load balancing, *see* load balancing 25-5
 - vpn-filter username attribute 26-55
 - vpn-framed-ip-address username attribute 26-56
 - vpn-idle-timeout username attribute 26-55
 - vpn-session-timeout username attribute 26-55
 - vpn-tunnel-protocol username attribute 26-56
 - VRRP 12-9
-
- W**
- web browsing with WebVPN 30-47
 - web clients
 - secure authentication 16-4
 - web e-Mail (Outlook Web Access)
 - Outlook Web Access 30-27
 - WebVPN
 - assigning users to group policies 30-16
 - authenticating with digital certificates 30-15
 - CA certificate validation not done 30-2
 - client application requirements 30-45
 - client requirements 30-45
 - for file management 30-48
 - for network browsing 30-48
 - for port forwarding 30-49
 - for using applications 30-49
 - for web browsing 30-47
 - start-up 30-46
 - configuring
 - DNS globally 30-15
 - e-mail 30-25
 - configuring for specific users 26-58
 - cookies 30-5
 - defining the end-user interface 30-32
 - definition 30-1
 - digital certificate authentication restrictions 30-4
 - e-mail 30-25
 - e-mail proxies 30-25
 - enable cookies for 30-49
 - end user set-up 30-31
 - establishing a session 30-3
 - floating toolbar 30-34
 - group policy attributes, configuring 30-17
 - hosts file 30-18
 - hosts files, reconfiguring 30-19
 - HTTP/HTTPS proxy, setting 30-5
 - printing and 30-46
 - remote system configuration and end-user requirements 30-46
 - security precautions 30-2, 30-5
 - security tips 30-44
 - setting HTTP/HTTPS proxy 30-4
 - SSL/TLS encryption protocols 30-4
 - supported applications 30-45
 - supported browsers 30-46
 - supported types of Internet connections 30-46
 - troubleshooting 30-18
 - unsupported features 30-3
 - URL 30-46
 - use of HTTPS 30-3

- use suggestions 30-31, 30-45
- username and password required 30-46
- usernames and passwords 30-44
- webvpn attributes
 - group policy 26-40
 - tunnel-group 26-4
- WebVPN group policy attributes
 - functions 26-41
- WebVPN tunnel-group connection parameters 26-4
- WebVPN, Application Access Panel 30-33
- welcome message, group policy 26-28
- WINS server, configuring 26-23