INDEX

A

AAA
accounting 8-17
authentication
network access 8-2
proxy limit 8-11
authorization
downloadable access lists 8-13
network access 8-12
performance 8-1
web clients 8-8
access lists
downloadable 8-14
global access rules 7-2
implicit deny 7-3
inbound 7-3
outbound 7-3
overview 7-1
phone proxy 17-7
access rules
turn off expansion 7-12
AIP
See IPS module
AIP SSC
loading an image 30-26, 31-20, 31-22, 32-28
AIP SSM
about 31-1
loading an image 30-26, 31-20, 31-22, 32-28
anti-replay window size 23-10
APN, GTP application inspection 14-10
APPE command, denied request 11-24
application firewall 11-32
application inspection
about 10-1
applying 10-7
configuring 10-7
inspection class map 2-3
inspection policy map 2-3
special actions 2-1
ASA CX module
about 30-1
ASA feature compatibility 30-5
authentication proxy
about 30-5
port 30-18
troubleshooting 30-32
basic settings 30-16
cabling 30-9
configuration 30-8
failover 30-7
licensing 30-6
management access 30-4
management defaults 30-8
management IP address 30-14
monitoring 30-27
password reset 30-23
PRSM 30-5
reload 30-24
security policy 30-17
sending traffic to shutdown 30-19
traffic flow 30-2
VPN 30-5
asymmetric routing
TCP state bypass 22-4
attacks

DNS HINFO request 28-10
DNS request for all records 28-10
DNS zone transfer 28-10
DNS zone transfer from high port 28-10
fragmented ICMP traffic 28-9
IP fragment 28-7
IP impossible packet 28-7
large ICMP traffic 28-9
ping of death 28-9
proxied RPC request 28-10
statd buffer overflow 28-11
TCP FIN only flags 28-10
TCP NULL flags 28-9
TCP SYN+FIN flags 28-9
UDP bomb 28-10
UDP chargen DoS 28-10
UDP snork 28-10

classifying traffic 26-10
configuring 26-7
databases 26-2
default settings 26-6
DNS Reverse Lookup Cache
  information about 26-4
  using with dynamic database 26-9
DNS snooping 26-9
dropping traffic 26-11
graylist 26-11
dynamic database
  enabling use of 26-8
  files 26-3
  information about 26-2
  searching 26-13
  updates 26-8
feature history 26-16
graylist
  description 26-2
  dropping traffic 26-11
guidelines and limitations 26-6
information about 26-1
licensing 26-6
monitoring 26-14
static database
  adding entries 26-9
  information about 26-3
syslog messages 26-14
task flow 26-7
threat level
  dropping traffic 26-11
whitelist
  adding entries 26-9
  description 26-2
working overview 26-5
bypassing firewall checks 22-3

B

basic threat detection
  See threat detection

Botnet Traffic Filter
  actions 26-2
  address categories 26-2
  blacklist
    adding entries 26-9
    description 26-2
    blocking traffic manually 26-12
C

call agents
  MGCP application inspection  12-15, 12-16
CDUP command, denied request  11-24
certificate
  Cisco Unified Mobility  19-4
  Cisco Unified Presence  20-4
Cisco IP Communicator  17-10
Cisco IP Phones, application inspection  12-32
Cisco UMA. See Cisco Unified Mobility.
Cisco Unified Mobility
  architecture  19-2
  ASA role  15-2, 15-3, 16-2
  certificate  19-4
  functionality  19-1
  NAT and PAT requirements  19-3, 19-4
  trust relationship  19-4
Cisco Unified Presence
  ASA role  15-2, 15-3, 16-2
  configuring the TLS Proxy  20-8
  NAT and PAT requirements  20-2
  trust relationship  20-4
Cisco UP. See CiscoUnified Presence.
classmap
  inspection  2-3
configuring
  CSC activation  32-11
  CSC email  32-21
  CSC file transfer  32-22
  CSC IP address  32-11
  CSC license  32-11
  CSC management access  32-13
  CSC notifications  32-12
  CSC password  32-13
  CSC Setup Wizard  32-15, 32-18
  CSC Setup Wizard Activation Codes Configuration  32-15
  CSC Setup Wizard Host Configuration  32-16
  CSC Setup Wizard IP Configuration  32-16
  CSC Setup Wizard Management Access Configuration  32-17
  CSC Setup Wizard Password Configuration  32-17
  CSC Setup Wizard Summary  32-19
  CSC Setup Wizard Traffic Selection for CSC Scan  32-17
  CSC updates  32-23
  CSC Web  32-20
connection limits
  configuring  22-1
context modes  32-6
CSC activation
  configuring  32-11
CSC CPU
  monitoring  32-27
CSC email
  configuring  32-21
CSC file transfer
  configuring  32-22
CSC IP address
  configuring  32-11
CSC license
  configuring  32-11
CSC management access
  configuring  32-13
CSC memory
  monitoring  32-27
CSC notifications
  configuring  32-12
CSC password
  configuring  32-13
CSC security events
  monitoring  32-25
CSC Setup Wizard
  activation codes configuration  32-15
  Host configuration  32-15
  IP configuration  32-16
  management access configuration  32-17
password configuration 32-17
specifying traffic for CSC Scanning 32-18
summary 32-19
traffic selection for CSC Scan 32-17
CSC software updates
monitoring 32-26
CSC SSM
about 32-1
loading an image 30-26, 31-20, 31-22, 32-28
what to scan 32-3
CSC SSM feature history 32-31
CSC SSM GUI
configuring 32-20
CSC threats
monitoring 32-24
CSC updates
configuring 32-23
CSC Web
configuring 32-20
cut-through proxy
AAA performance 8-1
CX module
about 30-1
ASA feature compatibility 30-5
authentication proxy
about 30-5
port 30-18
troubleshooting 30-32
basic settings 30-16
cabling 30-9
configuration 30-8
failover 30-7
licensing 30-6
management access 30-4
management defaults 30-8
management IP address 30-14
monitoring 30-27
password reset 30-23
PRSM 30-5
reload 30-24
security policy 30-17
sending traffic to 30-19
shutdown 30-25
traffic flow 30-2
VPN 30-5

D

default policy 1-7
DHCP
transparent firewall 7-6
DiffServ preservation 23-5
DNS
inspection
about 11-2
managing 11-1
NAT effect on 3-30
NAT effect on (8.2 and earlier) 6-14
DNS HINFO request attack 28-10
DNS request for all records attack 28-10
DNS zone transfer attack 28-10
DNS zone transfer from high port attack 28-10
downloadable access lists
configuring 8-14
converting netmask expressions 8-17
DSCP preservation 23-5
dynamic NAT
about 3-8
configuring (8.2 and earlier) 6-17
network object NAT 4-4
twice NAT 5-4
dynamic PAT
network object NAT 4-9
See also NAT
twice NAT 5-12
**E**

EIGRP  7-6
EtherType access list
  compatibility with extended access lists 7-2
  implicit deny  7-3

**F**

failover
  guidelines 32-6
Fibre Channel interfaces
  default settings 7-7
filtering
  rules 29-6
  servers supported  29-2
  URLs 29-1, 29-2
fragmented ICMP traffic attack 28-9
Fragment panel 28-2
fragment size 28-2
FTP
  application inspection
    viewing 11-21, 11-22, 11-33, 11-46, 11-54, 11-55, 12-7, 12-8, 12-15, 12-18, 12-26, 12-34, 12-35, 14-2, 14-12
  filtering option 29-10
FTP inspection
  about 11-17
  configuring 11-17

**G**

gateways
  MGCP application inspection  12-16
GTP
  application inspection
    viewing 14-6
GTP inspection
  about 14-5
  configuring 14-4

**H**

H.323 inspection
  about 12-3
  configuring 12-2
  limitations 12-4
HELP command, denied request 11-24
hierarchical policy, traffic shaping and priority queueing 23-11
HTTP
  application inspection
    viewing 11-32
  filtering 29-1
    configuring 29-9
HTTP(S)
  filtering 29-2
HTTP inspection
  about 11-26
  configuring 11-26

**I**

ICMP
  testing connectivity 24-1
identity NAT
  about 3-12
  configuring (8.2 and earlier) 6-17
  network object NAT 4-15
  twice NAT 5-24
ILS inspection 13-1
IM 12-22
inbound access lists 7-3
inspection engines
  See application inspection
Instant Messaging inspection 12-22
interfaces
  default settings 7-7, 32-6
IP audit
  enabling 28-5
signatures 28-6
IP fragment attack 28-7
IP fragment database, displaying 28-2
IP fragment database, editing 28-3
IP impossible packet attack 28-7
IP overlapping fragments attack 28-8
IP phone
  phone proxy provisioning 17-11
IP phones
  addressing requirements for phone proxy 17-9
  supported for phone proxy 17-3, 18-3
IPS
  IP audit 28-5
IPSec
  anti-replay window 23-10
IPSec rules
  anti-replay window size 23-10
IPS module
  about 31-1
  configuration 31-7
  operating modes 31-3
  sending traffic to 31-18
  traffic flow 31-2
  virtual sensors 31-17
IP spoofing, preventing 28-1
IP teardrop attack 28-8
licenses
  Cisco Unified Communications Proxy features 15-4, 18-4, 19-6, 20-7, 21-8
licensing requirements
  CSC SSM 32-5
LLQ
  See low-latency queue
login
  FTP 8-4
low-latency queue
  applying 23-2, 23-3

L
large ICMP traffic attack 28-9
latency
  about 23-1
  configuring 23-2, 23-3
  reducing 23-8
Layer 3/4
  matching multiple policy maps 1-5
LCS Federation Scenario 20-2
LDAP
  application inspection 13-1
management interfaces
  default settings 7-7
mapped addresses
  guidelines 3-21
  guidelines (8.2 and earlier) 6-14
media termination address, criteria 17-6
MGCP
  application inspection
    configuring 12-16
    viewing 12-14
MGCP inspection
  about 12-12
  configuring 12-12
mgmt0 interfaces
  default settings 7-7
Microsoft Access Proxy 20-1
MMP inspection 19-1
monitoring
  CSC CPU 32-27
  CSC memory 32-27
  CSC security events 32-25
  CSC software updates 32-26
  CSC SSM 32-24
  CSC threats 32-24
MPF
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>default policy</td>
<td>1-7</td>
</tr>
<tr>
<td>feature directionality</td>
<td>1-3</td>
</tr>
<tr>
<td>features</td>
<td>1-1</td>
</tr>
<tr>
<td>flows</td>
<td>1-5</td>
</tr>
<tr>
<td>matching multiple policy maps</td>
<td>1-5</td>
</tr>
<tr>
<td>See also class map</td>
<td></td>
</tr>
<tr>
<td>See also policy map</td>
<td></td>
</tr>
<tr>
<td><strong>MPLS</strong></td>
<td></td>
</tr>
<tr>
<td>LDP</td>
<td>7-7</td>
</tr>
<tr>
<td>router-id</td>
<td>7-7</td>
</tr>
<tr>
<td>TDP</td>
<td>7-7</td>
</tr>
<tr>
<td>multi-session PAT</td>
<td>4-19</td>
</tr>
<tr>
<td><strong>N</strong></td>
<td></td>
</tr>
<tr>
<td><strong>NAT</strong></td>
<td></td>
</tr>
<tr>
<td>about</td>
<td>3-1, 6-1</td>
</tr>
<tr>
<td>about (8.2 and earlier)</td>
<td>6-1</td>
</tr>
<tr>
<td>bidirectional initiation</td>
<td>3-2</td>
</tr>
<tr>
<td>bypassing NAT (8.2 and earlier)</td>
<td>6-10</td>
</tr>
<tr>
<td>DNS</td>
<td>3-30</td>
</tr>
<tr>
<td>DNS (8.2 and earlier)</td>
<td>6-14</td>
</tr>
<tr>
<td>dynamic</td>
<td></td>
</tr>
<tr>
<td>about</td>
<td>3-8</td>
</tr>
<tr>
<td>dynamic NAT</td>
<td></td>
</tr>
<tr>
<td>about (8.2 and earlier)</td>
<td>6-6</td>
</tr>
<tr>
<td>configuring (8.2 and earlier)</td>
<td>6-23</td>
</tr>
<tr>
<td>implementation (8.2 and earlier)</td>
<td>6-17</td>
</tr>
<tr>
<td>network object NAT</td>
<td>4-4</td>
</tr>
<tr>
<td>twice NAT</td>
<td>5-4</td>
</tr>
<tr>
<td>dynamic PAT</td>
<td></td>
</tr>
<tr>
<td>about</td>
<td>3-10</td>
</tr>
<tr>
<td>network object NAT</td>
<td>4-9</td>
</tr>
<tr>
<td>twice NAT</td>
<td>5-12</td>
</tr>
<tr>
<td>exemption (8.2 and earlier)</td>
<td>6-11</td>
</tr>
<tr>
<td>identity</td>
<td></td>
</tr>
<tr>
<td>about</td>
<td>3-12</td>
</tr>
<tr>
<td>identity NAT</td>
<td></td>
</tr>
<tr>
<td>about (8.2 and earlier)</td>
<td>6-10</td>
</tr>
<tr>
<td>network object NAT</td>
<td>4-15</td>
</tr>
<tr>
<td>twice NAT</td>
<td>5-24</td>
</tr>
<tr>
<td>implementation</td>
<td>3-24</td>
</tr>
<tr>
<td>interfaces</td>
<td>3-21</td>
</tr>
<tr>
<td>mapped address guidelines</td>
<td>3-21</td>
</tr>
<tr>
<td>network object</td>
<td></td>
</tr>
<tr>
<td>comparison with twice NAT</td>
<td>3-15</td>
</tr>
<tr>
<td>network object NAT</td>
<td></td>
</tr>
<tr>
<td>about</td>
<td>3-16</td>
</tr>
<tr>
<td>configuring</td>
<td>4-1</td>
</tr>
<tr>
<td>dynamic NAT</td>
<td>4-4</td>
</tr>
<tr>
<td>dynamic PAT</td>
<td>4-9</td>
</tr>
<tr>
<td>examples</td>
<td>4-21</td>
</tr>
<tr>
<td>guidelines</td>
<td>4-2</td>
</tr>
<tr>
<td>identity NAT</td>
<td>4-15</td>
</tr>
<tr>
<td>monitoring</td>
<td>4-20</td>
</tr>
<tr>
<td>prerequisites</td>
<td>4-2</td>
</tr>
<tr>
<td>static NAT</td>
<td>4-12</td>
</tr>
<tr>
<td>no proxy ARP</td>
<td>4-18</td>
</tr>
<tr>
<td>object</td>
<td></td>
</tr>
<tr>
<td>extended PAT</td>
<td>4-4</td>
</tr>
<tr>
<td>flat range for PAT</td>
<td>4-4</td>
</tr>
<tr>
<td><strong>PAT</strong></td>
<td></td>
</tr>
<tr>
<td>about (8.2 and earlier)</td>
<td>6-8</td>
</tr>
<tr>
<td>configuring (8.2 and earlier)</td>
<td>6-23</td>
</tr>
<tr>
<td>implementation (8.2 and earlier)</td>
<td>6-17</td>
</tr>
<tr>
<td>policy NAT, about (8.2 and earlier)</td>
<td>6-11</td>
</tr>
<tr>
<td>routed mode</td>
<td>3-13</td>
</tr>
<tr>
<td>route lookup</td>
<td>4-18, 5-29</td>
</tr>
<tr>
<td>RPC not supported with</td>
<td>13-3</td>
</tr>
<tr>
<td>rule order</td>
<td>3-20</td>
</tr>
<tr>
<td>rule order (8.2 and earlier)</td>
<td>6-14</td>
</tr>
<tr>
<td>same security level (8.2 and earlier)</td>
<td>6-13</td>
</tr>
<tr>
<td>static</td>
<td></td>
</tr>
<tr>
<td>about</td>
<td>3-3</td>
</tr>
<tr>
<td>few-to-many mapping</td>
<td>3-7</td>
</tr>
<tr>
<td>many-to-few mapping</td>
<td>3-6, 3-7</td>
</tr>
<tr>
<td>one-to-many</td>
<td>3-6</td>
</tr>
<tr>
<td>static NAT</td>
<td></td>
</tr>
</tbody>
</table>
about (8.2 and earlier) 6-9
configuring (8.2 and earlier) 6-27
network object NAT 4-12
twice NAT 5-18

static PAT
about (8.2 and earlier) 6-9
static with port translation
about 3-4
terminology 3-2
transparent mode 3-13
transparent mode (8.2 and earlier) 6-3
twice
extended PAT 5-4
flat range for PAT 5-4
twice NAT
about 3-16
comparison with network object NAT 3-15
configuring 5-1
dynamic NAT 5-4
dynamic PAT 5-12
examples 5-30
guidelines 5-2
identity NAT 5-24
monitoring 5-29
prerequisites 5-2
static NAT 5-18
types 3-3
types (8.2 and earlier) 6-6
VPN 3-24
VPN client rules 3-20

network object NAT
about 3-16
comparison with twice NAT 3-15
configuring 4-1
dynamic NAT 4-4
dynamic PAT 4-9
examples 4-21
guidelines 4-2
identity NAT 4-15

monitoring 4-20
prerequisites 4-2
static NAT 4-12

O

object NAT
See network object NAT
outbound access lists 7-3

P

packet trace, enabling 24-7
PAT
per-session and multi-session 4-19
See dynamic PAT
PAT pool 4-7, 5-9
round robin 4-7, 5-9
PDP context, GTP application inspection 14-8
per-session PAT 4-19
phone proxy
access lists 17-7
ASA role 15-3
Cisco IP Communicator 17-10
Cisco UCM supported versions 17-3, 18-3
IP phone addressing 17-9
IP phone provisioning 17-11
IP phones supported 17-3, 18-3
Linksys routers, configuring 17-21
NAT and PAT requirements 17-8
ports 17-7
rate limiting 17-10
TLS Proxy on ASA, described 15-3
ping
See ICMP
using 24-3
ping of death attack 28-9
policy, QoS 23-1
Index

policy map
  inspection 2-3
Layer 3/4
  about 1-1
  feature directionality 1-3
  flows 1-5
policy NAT, about (8.2 and earlier) 6-11
ports
  phone proxy 17-7
port translation
  about 3-4
prerequisites for use
  CSC SSM 32-5
presence_proxy_remotecert 16-15
priority queueing
  hierarchical policy with traffic shaping 23-11
  IPSec anti-replay window size 23-10
proxied RPC request attack 28-10
proxy servers
  SIP and 12-21
PRSM 30-5

Quality of Service
  See QoS
queue, QoS
  latency, reducing 23-8
  limit 23-2, 23-3

R

RADIUS
  downloadable access lists 8-14
  network access authentication 8-6
  network access authorization 8-13
rate limiting 23-3
rate limiting, phone proxy 17-10
RealPlayer 12-17
reset
  inbound connections 28-3
  outside connections 28-3
RNFR command, denied request 11-24
RNTO command, denied request 11-24
routed mode
  NAT 3-13
diffServ preservation 23-5
DSCP preservation 23-5
feature interaction 23-4
policies 23-1
priority queueing
  hierarchical policy with traffic shaping 23-11
  IPSec anti-replay window size 23-10
statistics 23-11
token bucket 23-2
traffic shaping
  overview 23-4
  viewing statistics 23-11, 23-12

Cisco ASA Series Firewall ASDM Configuration Guide
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
</table>

- **maximum and minimum** 28-4
- **shun**
  - duration 27-10
- **signatures**
  - attack and informational 28-6
- **SIP inspection**
  - about 12-21
  - configuring 12-20
  - instant messaging 12-22
- **SITE command, denied request** 11-24
- **SMTP inspection** 11-52
- **SNMP**
  - application inspection
    - viewing 14-14
- **specifying traffic for CSC scanning** 32-18
- **SSCs**
  - management access 31-4
  - management defaults 31-6
  - management interface 31-14
  - password reset 31-23, 32-29
  - reload 31-24, 32-30
  - reset 31-24, 32-30
  - routing 31-10
  - sessioning to 31-13
  - shutdown 31-22, 32-30
- **SSMs**
  - loading an image 30-26, 31-20, 31-22, 32-28
  - management access 31-4
  - management defaults 31-6
  - password reset 31-23, 32-29
  - reload 31-24, 32-30
  - reset 31-24, 32-30
  - routing 31-10
  - sessioning to 31-13
  - shutdown 31-22, 32-30
- **Startup Wizard**
  - licensing requirements 16-3
  - statd buffer overflow attack 28-11
  - stateful inspection

- **bypassing** 22-3
- **static NAT**
  - about 3-3
  - few-to-many mapping 3-7
  - many-to-few mapping 3-6, 3-7
  - network object NAT 4-12
  - twice NAT 5-18
- **static NAT with port translation**
  - about 3-4
- **static PAT**
  - See PAT 23-11
- **statistics, QoS** 23-11
- **STOU command, denied request** 11-24
- **Sun RPC inspection**
  - about 13-3
  - configuring 13-3

### T

- **TACACS+**
  - network access authorization 8-12
- **tail drop** 23-3
- **TCP**
  - maximum segment size 28-4
  - TIME_WAIT state 28-4
  - TCP FIN only flags attack 28-10
  - TCP Intercept
    - statistics 27-6
  - TCP normalization 22-3
  - TCP NULL flags attack 28-9
  - TCP state bypass
    - AAA 22-5
    - configuring 22-8
    - failover 22-5
    - firewall mode 22-5
    - inspection 22-5
    - multiple context mode 22-5
    - NAT 22-5
    - SSMs and SSCs 22-5
TCP Intercept 22-5
TCP normalization 22-5
unsupported features 22-5
TCP SYN+FIN flags attack 28-9
testing configuration 24-1
threat detection
  basic
    drop types 27-2
    enabling 27-4
    overview 27-2
    rate intervals 27-2
    statistics, viewing 27-4
    system performance 27-2
scanning
  enabling 27-10
  host database 27-9
  overview 27-8
  shunning attackers 27-10
  system performance 27-9
scanning statistics
  enabling 27-6
  system performance 27-5
  viewing 27-7
shun
  duration 27-10
TIME_WAIT state 28-4
TLS Proxy
  applications supported by ASA 15-3
  Cisco Unified Presence architecture 20-1
  configuring for Cisco Unified Presence 20-8
  licenses 15-4, 18-4, 19-6, 20-7, 21-8
token bucket 23-2
traceroute, enabling 24-6
traffic shaping
  overview 23-4
  transmit queue ring limit 23-2, 23-3
transparent firewall
  DHCP packets, allowing 7-6
  packet handling 7-5
transparent mode
  NAT 3-13
  NAT (8.2 and earlier) 6-3
Trusted Flow Acceleration
  modes 7-7
trust relationship
  Cisco Unified Mobility 19-4
  Cisco Unified Presence 20-4
twice NAT
  about 3-16
  comparison with network object NAT 3-15
  configuring 5-1
dynamic NAT 5-4
dynamic PAT 5-12
dynamic examples 5-30
guidelines 5-2
identity NAT 5-24
monitoring 5-29
prerequisites 5-2
static NAT 5-18
tx-ring-limit 23-2, 23-3

U

UDP
  bomb attack 28-10
  chargen DoS attack 28-10
  snork attack 28-10
URL
  filtering
  configuring 29-9
URLs
  filtering 29-1
  filtering, about 29-2

V

viewing QoS statistics 23-11, 23-12
virtual HTTP 8-3
virtual sensors 31-17
VoIP
  proxy servers 12-21
VPN client
  NAT rules 3-20

W

web clients, secure authentication 8-8
Websense filtering server 29-3