



INDEX

Numerics

4GE SSM

- connector types [7-2, 8-2](#)
- fiber [7-2, 8-2](#)
- SFP [7-2, 8-2](#)
- support [1-2](#)

802.1Q trunk [7-3, 8-5](#)

A

AAA

- about [14-1](#)
- accounting [23-15](#)
- authentication
 - CLI access [16-20](#)
 - network access [23-1](#)
 - proxy limit [23-9](#)
- authorization
 - command [16-23](#)
 - downloadable access lists [23-10](#)
 - network access [23-9](#)
- local database support [14-8](#)
- performance [23-1](#)
- server
 - adding [14-9, 14-10](#)
 - types [14-3](#)
- support summary [14-3](#)
- web clients [23-5](#)

AAA server group, add (group-policy) [35-6](#)

ABR

- definition of [11-2](#)

Access Control Server [34-25](#)

Access Group panel [12-2](#)

- description [12-2](#)
- fields [12-2](#)

access lists

- downloadable [23-11](#)
- implicit deny [20-2](#)
- inbound [20-2](#)
- IP address guidelines with NAT [20-4](#)
- NAT addresses [20-4](#)
- overview [20-1](#)

Accounting tab, tunnel group [35-67](#)

ACE

- add/edit/paste [35-16](#)
- Extended ACL tab [35-15](#)

ACL

- enabling IPSEC authenticated inbound sessions to bypass ACLs [35-80, 38-29](#)
- extended [35-15](#)
- for Clientless SSL VPN [35-41](#)
- standard [35-14](#)

ACL Manager

- Add/Edit/Paste ACE [35-16](#)
- dialog box [35-14](#)

Active/Active failover

- about [15-2](#)
- command replication [15-2](#)
- configuration synchronization [15-2](#)

Active/Standby failover [15-2](#)

ActiveX

- object filtering, benefits of [26-6](#)

Adaptive Security Algorithm [2-19](#)

Add/Edit Access Group dialog box [12-3](#)

- description [12-3](#)

- fields [12-3](#)
- Add/Edit Filtering Entry dialog box [11-9](#)
 - description [11-9](#)
 - fields [11-9](#)
- Add/Edit IGMP Join Group dialog box [12-4](#)
 - description [12-4](#)
 - fields [12-4](#)
- Add/Edit IGMP Static Group dialog box [12-7](#)
 - description [12-7](#)
 - fields [12-7](#)
- Add/Edit Multicast Group dialog box [12-18](#)
 - description [12-18](#)
 - fields [12-18](#)
- Add/Edit Multicast Route dialog box
 - description [12-8](#)
 - fields [12-8](#)
- Add/Edit OSPF Area dialog box [11-5](#)
 - description [11-5](#)
 - fields [11-6](#)
- Add/Edit OSPF Neighbor Entry dialog box [11-17](#)
 - description [11-17](#)
 - fields [11-18](#)
 - Restrictions [11-17](#)
- Add/Edit Periodic Time Range dialog box [19-16](#)
- Add/Edit Redistribution dialog box [11-16](#)
 - description [11-16](#)
 - fields [11-16](#)
- Add/Edit Rendezvous Point dialog box [12-16](#)
 - description [12-16](#)
 - fields [12-17](#)
 - restrictions [12-17](#)
- Add/Edit Route Summarization dialog box [11-8](#)
 - about [11-8](#)
 - fields [11-8](#)
- Add/Edit Summary Address dialog box
 - description [11-19](#)
 - fields [11-19](#)
- Add/Edit Time Range dialog box [19-15](#)
- Add/Edit Virtual Link dialog box [11-20](#)
 - description [11-20](#)
 - fields [11-20](#)
- address assignment, client [35-67](#)
- Address Pool panel, VPN wizard [32-10](#)
- address pools, tunnel group [35-67](#)
- Address Translation Exemption panel, VPN wizard [32-11](#)
- admin context
 - overview [10-1](#)
- administrative access
 - using ICMP for [16-7](#)
- Advanced DHCP Options dialog box [13-7](#)
 - description [13-7](#)
 - fields [13-7](#)
- Advanced OSPF Interface Properties dialog box [11-14](#)
 - description [11-14](#)
 - fields [11-14](#)
- Advanced OSPF Virtual Link Properties dialog box [11-21](#)
 - description [11-21](#)
 - fields [11-21](#)
- Advanced tab, tunnel group [35-68](#)
- AIP SSM
 - about [28-1](#)
 - configuration [28-4](#)
 - sending traffic to [28-6](#)
 - support [1-2](#)
- alternate address, ICMP message [16-8](#)
- anti-replay window size [25-7, 34-11](#)
- APN, GTP application inspection [24-88](#)
- APPE command, denied request [24-82](#)
- application access
 - and e-mail proxy [37-7](#)
 - and Web Access [37-7](#)
 - configuring client applications [37-6](#)
 - enabling cookies on browser [37-6](#)
 - privileges [37-6](#)
 - quitting properly [37-6](#)
 - setting up on client [37-6](#)
 - using e-mail [37-7](#)
 - with IMAP client [37-7](#)

- application firewall [24-95](#)
- application inspection
 - about [24-2](#)
 - applying [24-4](#)
 - configuring [24-4](#)
 - described [24-60](#)
 - enabling for different protocols [24-29](#)
 - security level requirements [7-4, 8-8](#)
- Apply button [1-13](#)
- Area/Networks tab [11-5](#)
 - description [11-5](#)
 - fields [11-5](#)
- area border router [11-2](#)
- ARP inspection
 - configuring [30-1](#)
- ARP spoofing [30-2](#)
- ARP table
 - monitoring [41-1](#)
 - static entry [30-3](#)
- ASA (Adaptive Security Algorithm) [2-19](#)
- ASA 5505
 - Base license [9-2](#)
 - client
 - Xauth [35-85](#)
 - MAC addresses [9-4](#)
 - maximum VLANs [9-2](#)
 - power over Ethernet [9-4](#)
 - Security Plus license [9-2](#)
 - SPAN [9-4](#)
- ASBR
 - definition of [11-2](#)
- ASDM
 - version [1-18](#)
- attacks
 - DNS HINFO request [27-16](#)
 - DNS request for all records [27-16](#)
 - DNS zone transfer [27-16](#)
 - DNS zone transfer from high port [27-16](#)
 - fragmented ICMP traffic [27-15](#)
 - IP fragment [27-13](#)
 - IP impossible packet [27-13](#)
 - large ICMP traffic [27-15](#)
 - ping of death [27-15](#)
 - proxied RPC request [27-16](#)
 - statd buffer overflow [27-17](#)
 - TCP FIN only flags [27-16](#)
 - TCP NULL flags [27-15](#)
 - TCP SYN+FIN flags [27-15](#)
 - UDP bomb [27-16](#)
 - UDP chargen DoS [27-16](#)
 - UDP snork [27-16](#)
- attributes
 - RADIUS [C-15](#)
- Attributes Pushed to Client panel, VPN wizard [32-11](#)
- attribute-value pairs
 - TACACS+ [C-23](#)
- authenticating a certificate [33-1](#)
- authentication
 - about [14-2](#)
 - CLI access [16-20](#)
 - FTP [23-3](#)
 - HTTP [23-2](#)
 - network access [23-1](#)
 - Telnet [23-2](#)
 - web clients [23-5](#)
- Authentication tab [11-10](#)
 - description [11-10](#)
 - fields [11-10](#)
- Authentication tab, tunnel group [35-65](#)
- authorization
 - about [14-2](#)
 - command [16-23](#)
 - downloadable access lists [23-10](#)
 - network access [23-9](#)
- Authorization tab, tunnel group [35-65](#)
- Auto-MDI/MDIX [7-2, 8-2](#)

B

backed up configurations

restoring [3-29](#)

backing up configurations [3-26](#)

bandwidth [1-19](#)

banner, view/configure [35-25](#)

Basic tab

IPSec LAN-to-LAN, General tab [35-71](#)

basic threat detection

See threat detection

bridging

MAC address table

learning, disabling [30-6](#)

overview [30-4](#)

static entry [30-6](#)

management IP address [6-1](#)

Browse ICMP [35-19](#)

Browse Other [35-21](#)

Browse Source or Destination Address [35-18](#)

Browse Source or Destination Port [35-18](#)

Browse Time Range [35-11](#)

building blocks [19-1](#)

bypass mode [1-24](#)

C

CA certificate [33-1](#)

CA Certificates [33-1](#)

call agents

MGCP application inspection [24-109, 24-110](#)

Cancel button [1-13](#)

capturing packets [B-12](#)

CDUP command, denied request [24-82](#)

certificate

CA [33-1](#)

code-signer [33-18](#)

Identity [33-11](#)

Local CA [33-20](#)

certificate authentication [33-1](#)

certificate enrollment [33-3, 33-12](#)

Cisco-AV-Pair LDAP attributes [C-12](#)

Cisco Client Parameters tab [35-26](#)

Cisco IP Phones, application inspection [24-23](#)

classes

See resource management

Client Access Rule, add or edit [35-23](#)

Client Address Assignment [35-67](#)

Client Authentication panel, VPN wizard [32-8](#)

Client Configuration tab [35-24](#)

Client Firewall tab [35-29](#)

Clientless SSL VPN

client application requirements [37-2](#)

client requirements [37-2](#)

for file management [37-5](#)

for network browsing [37-5](#)

for web browsing [37-4](#)

start-up [37-3](#)

enable cookies for [37-6](#)

end user set-up [37-1](#)

printing and [37-3](#)

remote requirements

for port forwarding [37-6](#)

for using applications [37-6](#)

remote system configuration and end-user requirements [37-3](#)

security tips [37-2](#)

supported applications [37-2](#)

supported browsers [37-3](#)

supported types of Internet connections [37-3](#)

URL [37-3](#)

username and password required [37-3](#)

usernames and passwords [37-1](#)

use suggestions [37-1](#)

client parameters, configuring [35-24](#)

Client Update, edit , Windows and VPN 3002 clients [35-3](#)

Client Update window, Windows and VPN 3002 clients [35-1](#)

- code-signer certificate [33-18](#)
- command authorization
 - about [16-23](#)
 - configuring [16-23](#)
 - multiple contexts [16-24](#)
- configuration
 - context files [10-2](#)
 - factory default [4-1](#)
- configurations, backing up [3-26](#)
- Configure IGMP Parameters dialog box [12-5](#)
 - description [12-5](#)
 - fields [12-5](#)
- configuring
 - CSC activation [29-10](#)
 - CSC email [29-22](#)
 - CSC file transfer [29-24](#)
 - CSC IP address [29-11](#)
 - CSC license [29-10](#)
 - CSC management access [29-12](#)
 - CSC notifications [29-11](#)
 - CSC password [29-13](#)
 - CSC Setup Wizard [29-15](#), [29-19](#)
 - CSC Setup Wizard Activation Codes Configuration [29-15](#)
 - CSC Setup Wizard Host Configuration [29-17](#)
 - CSC Setup Wizard IP Configuration [29-16](#)
 - CSC Setup Wizard Management Access Configuration [29-17](#)
 - CSC Setup Wizard Password Configuration [29-18](#)
 - CSC Setup Wizard Summary [29-20](#)
 - CSC Setup Wizard Traffic Selection for CSC Scan [29-18](#)
 - CSC updates [29-25](#)
 - CSC Web [29-21](#)
- connections per second [1-19](#)
- context mode
 - viewing [1-18](#)
- contexts
 - See security contexts
- conversion error, ICMP message [16-8](#)
- CPU usage [1-19](#)
- crash dump [B-12](#)
- CRL
 - cache refresh time [33-10](#)
 - enforce next update [33-10](#)
- CSC [29-15](#)
- CSC activation
 - configuring [29-10](#)
- CSC CPU
 - monitoring [47-4](#)
- CSC email
 - configuring [29-22](#)
- CSC file transfer
 - configuring [29-24](#)
- CSC File Transfer panel
 - fields [29-24](#)
- CSC IP address
 - configuring [29-11](#)
- CSC license
 - configuring [29-10](#)
- CSC management access
 - configuring [29-12](#)
- CSC memory
 - monitoring [47-5](#)
- CSC notifications
 - configuring [29-11](#)
- CSC password
 - configuring [29-13](#)
- CSC security events
 - monitoring [47-2](#)
- CSC Setup Wizard [29-15](#)
 - activation codes configuratrion [29-15](#)
 - Host configuratrion [29-17](#)
 - IP configuratrion [29-16](#)
 - management access configuratrion [29-17](#)
 - password configuratrion [29-18](#)
 - specifying traffic for CSC Scanning [29-19](#)
 - summary [29-20](#)
 - traffic selection for CSC Scan [29-18](#)

- CSC software updates
 - monitoring [47-4](#)
 - CSC SSM
 - getting started [29-4](#)
 - overview [29-2](#)
 - support [1-2](#)
 - what to scan [29-6](#)
 - CSC threats
 - monitoring [47-1](#)
 - CSC updates
 - configuring [29-25](#)
 - CSC Web
 - configuring [29-21](#)
 - CTIQBE
 - application inspection, enabling [24-29](#)
 - cut-through proxy [23-1](#)
-
- D**
- data flow
 - routed firewall [18-1](#)
 - transparent firewall [18-11](#)
 - debug messages [B-12](#)
 - default class [10-12](#)
 - default configuration [4-1](#)
 - default policy [22-2](#)
 - default routes
 - defining equal cost routes [11-41](#)
 - definition of [11-41](#)
 - for tunneled traffic [11-41](#)
 - default tunnel gateway [35-4](#)
 - destination address, browse [35-18](#)
 - destination port, browse [35-18](#)
 - device ID, including in messages [17-6](#)
 - Device Pass-Through [35-86](#)
 - DHCP
 - configuring [13-4](#)
 - interface IP address [9-8](#)
 - monitoring
 - interface lease [41-2](#)
 - IP addresses [41-2](#)
 - server [41-2](#)
 - statistics [41-3](#)
 - services [13-1](#)
 - statistics [41-3](#)
 - transparent firewall [20-6](#)
 - DHCP relay
 - overview [13-1](#)
 - DHCP Relay - Add/Edit DHCP Server dialog box [13-3](#)
 - description [13-3](#)
 - fields [13-3](#)
 - restrictions [13-3](#)
 - DHCP Relay panel [13-1](#)
 - description [13-1](#)
 - fields [13-2](#)
 - prerequisites [13-2](#)
 - restrictions [13-1](#)
 - DHCP Server panel [13-4](#)
 - description [13-4](#)
 - fields [13-4](#)
 - DHCP services [13-1](#)
 - DiffServ preservation [25-5](#)
 - digital certificates [33-1](#)
 - directory hierarchy search [C-4](#)
 - disabling content rewrite [38-13](#)
 - DMZ, definition [2-16](#)
 - DNS
 - application inspection, enabling [24-29](#)
 - inspection
 - about [24-6](#)
 - managing [24-6](#)
 - rewrite, about [24-7](#)
 - NAT effect on [21-13](#)
 - DNS client [13-9](#)
 - DNS HINFO request attack [27-16](#)
 - DNS request for all records attack [27-16](#)
 - DNS zone transfer attack [27-16](#)
 - DNS zone transfer from high port attack [27-16](#)

- downloadable access lists
 - configuring [23-11](#)
 - converting netmask expressions [23-15](#)
- DSCP preservation [25-5](#)
- duplex
 - interface [9-13](#)
- duplex, configuring [7-2, 8-2](#)
- dynamic NAT
 - See* NAT

E

- Easy VPN
 - client
 - Xauth [35-85](#)
 - Easy VPN, advanced properties [35-86](#)
 - Easy VPN client [35-84](#)
 - Easy VPN Remote [35-84](#)
- ECMP [11-40](#)
- Edit DHCP Relay Agent Settings dialog box [13-3](#)
 - description [13-3](#)
 - fields [13-3](#)
 - prerequisites [13-3](#)
 - restrictions [13-3](#)
- Edit DHCP Server dialog box [13-6](#)
 - description [13-6](#)
 - fields [13-6](#)
- Edit OSPF Interface Authentication dialog box [11-11](#)
 - description [11-11](#)
 - fields [11-11](#)
- Edit OSPF Interface Properties dialog box [11-13](#)
 - fields [11-13](#)
- Edit OSPF Process Advanced Properties dialog box [11-3](#)
 - description [11-3](#)
 - fields [11-3](#)
- Edit PIM Protocol dialog box [12-12](#)
 - description [12-12](#)
 - fields [12-12](#)
- EIGRP [20-6](#)

- e-mail proxy
 - and Clientless SSL VPN [37-7](#)
- Enable IPsec authenticated inbound sessions [35-80, 38-29](#)
- enrolling
 - certificate [33-3, 33-12](#)
- ESMTP
 - application inspection, enabling [24-29](#)
- established command, security level requirements [7-5, 8-9](#)
- Ethernet
 - Auto-MDI/MDIX [7-2, 8-2](#)
 - duplex [7-2, 8-2](#)
 - jumbo frame support
 - multiple mode [8-7](#)
 - single mode [7-8](#)
 - MTU [7-8, 8-10, 9-10](#)
 - speed [7-2, 8-2](#)
- EtherType access list
 - compatibility with extended access lists [20-2](#)
 - implicit deny [20-2](#)
- extended ACL [35-15](#)
- external filtering server [26-5](#)
- External Group Policy, add or edit [35-5](#)

F

- factory default configuration [4-1](#)
- failover
 - about virtual MAC addresses [15-21](#)
 - criteria [15-20, 15-28](#)
 - defining standby IP addresses [15-18, 15-19](#)
 - defining virtual MAC addresses [15-22](#)
 - enable [15-26](#)
 - enabling Active/Standby [15-15](#)
 - enabling LAN-based [15-15](#)
 - enabling LAN-based failover [15-26](#)
 - enabling Stateful Failover [15-16](#)
 - graphs [46-4](#)
 - in multiple context mode [15-26](#)
 - interface

- system [8-2](#)
- key [15-15, 15-26](#)
- make active [46-4](#)
- make standby [46-4](#)
- monitoring [46-1](#)
- monitoring interfaces [15-19](#)
- redundant interfaces [7-2, 8-4](#)
- reload standby [46-4](#)
- reset [46-4, 46-8](#)
- stateful [15-3](#)
- Stateful Failover [15-27](#)
- stateless [15-3](#)
- status [46-1](#)

failover groups

- about [15-29](#)
- adding [15-30](#)
- editing [15-30](#)
- monitoring [46-9](#)
- reset [46-10](#)

fast path [2-19](#)

fiber interfaces [7-2, 8-2](#)

filtering

- benefits of [26-5](#)
- rules [26-7](#)
- security level requirements [7-5, 8-8](#)
- servers supported [26-1](#)
- URLs [26-1](#)

Filtering panel [11-8](#)

- benefits [11-8](#)
- description [11-8](#)
- fields [11-9](#)
- restrictions [11-8](#)

firewall, client, configuring settings [35-29](#)

firewall mode

- configuring [4-4](#)
- overview [18-1](#)
- viewing [1-18](#)

firewall server, Zone Labs [35-82](#)

fragmentation policy, IPsec [34-2](#)

fragmented ICMP traffic attack [27-15](#)

fragment protection [2-17](#)

FTP

application inspection

enabling [24-29](#)

viewing [22-16, 24-62, 24-64, 24-71, 24-72, 24-79, 24-80, 24-89, 24-90, 24-96, 24-103, 24-106, 24-109, 24-113, 24-115, 24-116, 24-120](#)

filtering option [26-9](#)

FTP inspection

about [24-8](#)

configuring [24-8](#)

G

gateway, default tunnel gateway [35-4](#)

gateways

MGCP application inspection [24-111](#)

General Client Parameters tab [35-24](#)

global addresses

recommendations [21-13](#)

Group Policy window

add or edit, General tab [35-6, 35-11](#)

introduction [35-4](#)

IPSec tab, add or edit [35-22](#)

GTP

application inspection

enabling [24-29](#)

viewing [24-84](#)

GTP inspection

configuring [24-10](#)

H

H.323

transparent firewall guidelines [18-8](#)

H.323 inspection

about [24-12](#)

configuring [24-11](#)

- limitations [24-13](#)
 - H225
 - application inspection, enabling [24-29](#)
 - H323 RAS
 - application inspection, enabling [24-29](#)
 - Hardware Client tab [35-31](#)
 - Help button [1-13](#)
 - HELP command, denied request [24-82](#)
 - Help menu [1-10](#)
 - hierarchical policy, traffic shaping and priority queueing [25-8](#)
 - history metrics [6-6](#)
 - HSRP [18-8](#)
 - HTTP
 - application inspection
 - enabling [24-29](#)
 - viewing [24-95](#)
 - filtering [26-1](#)
 - benefits of [26-6](#)
 - configuring [26-8](#)
 - HTTP inspection
 - configuring [24-13](#)
 - HTTPS
 - filtering option [26-9](#)
 - HTTPS/Telnet/SSH
 - allowing network or host access to ASDM [16-1](#)
-
- ICMP
 - add group [35-20](#)
 - application inspection, enabling [24-30](#)
 - browse [35-19](#)
 - rules for access to ADSM [16-7](#)
 - testing connectivity [B-1](#)
 - ICMP Error
 - application inspection, enabling [24-30](#)
 - ICMP Group [35-20](#)
 - ICMP unreachable message limits [16-9](#)
 - Identity Certificates [33-11](#)
 - IDM version [1-24](#)
 - IGMP
 - access groups [12-2](#)
 - configuring interface parameters [12-5](#)
 - group membership [12-3](#)
 - interface parameters [12-5](#)
 - static group assignment [12-6](#)
 - IGMP panel
 - IGMP
 - overview [12-2](#)
 - IKE Policy panel, VPN wizard [32-4](#)
 - IKE tunnels, amount [1-19](#)
 - ILS
 - application inspection, enabling [24-30](#)
 - ILS inspection [24-14](#)
 - IM [24-21](#)
 - inbound access lists [20-2](#)
 - information reply, ICMP message [16-8](#)
 - information request, ICMP message [16-8](#)
 - inside, definition [2-16](#)
 - inspection engines
 - See* application inspection
 - Instant Messaging inspection [24-21](#)
 - interface
 - duplex [9-13](#)
 - failover link
 - system [8-2](#)
 - IP address
 - DHCP [9-8](#)
 - management only [9-8](#)
 - MTU [7-8, 8-10, 9-10](#)
 - name [9-8](#)
 - security level [9-8](#)
 - status [1-19](#)
 - subinterface, adding [7-5, 8-6](#)
 - throughput [1-19](#)
 - Interface panel [11-10](#)
 - interfaces

- ASA 5505
 - MAC addresses [9-4](#)
 - maximum VLANs [9-2](#)
- duplex [7-2, 8-2](#)
- enabled status [8-2](#)
- fiber [7-2, 8-2](#)
- jumbo frame support
 - multiple mode [8-7](#)
 - single mode [7-8](#)
- monitoring [41-5](#)
- redundant [8-3](#)
- SFP [7-2, 8-2](#)
- speed [7-2, 8-2](#)
- subinterfaces [8-5](#)
- intrusion prevention configuration [28-4](#)
- IP address [6-1](#)
 - configuration [9-8](#)
 - configuring [9-6](#)
 - interface
 - DHCP [9-8](#)
 - management, transparent firewall [6-1](#)
- IP audit
 - enabling [27-11](#)
 - monitoring [44-14](#)
 - signatures [27-12](#)
 - statistics
 - IP audit
 - signature matches [44-14](#)
- IP fragment attack [27-13](#)
- IP fragment database, defaults [27-19](#)
- IP fragment database, editing [27-20](#)
- IP impossible packet attack [27-13](#)
- IP overlapping fragments attack [27-14](#)
- IPS
 - IP audit [27-11](#)
- IPS configuration [28-4](#)
- IPSec
 - anti-replay window [25-7](#)
- IPsec

- Cisco VPN Client [34-8](#)
- fragmentation policy [34-2](#)
- IPSec rules
 - anti-replay window size [25-7, 34-11](#)
- IPSec tab
 - internal group policy [35-22](#)
 - IPSec LAN-to-LAN [35-73](#)
 - tunnel group [35-68](#)
- IPSec tunnels, amount [1-19](#)
- IP teardrop attack [27-14](#)

J

- Java
 - applet filtering
 - benefits of [26-6](#)
- Java console [3-13](#)
- Join Group panel [12-3](#)
 - description [12-3](#)
 - fields [12-4](#)
- jumbo frame support
 - multiple mode [8-7](#)
 - single mode [7-8](#)

K

- Kerberos
 - configuring [14-9](#)
 - support [14-5](#)
- key pairs [33-13](#)

L

- large ICMP traffic attack [27-15](#)
- latency
 - about [25-1](#)
 - configuring [25-2, 25-3](#)
 - reducing [25-5](#)
- Layer 2 firewall

- See* transparent firewall
- Layer 3/4
 - matching multiple policy maps [22-5](#)
- LDAP
 - application inspection [24-14](#)
 - attribute mapping [14-22](#)
 - Cisco-AV-pair [C-12](#)
 - configuring [14-9](#)
 - configuring a AAA server [C-3 to ??](#)
 - directory search [C-4](#)
 - hierarchy example [C-4](#)
 - SASL [14-6](#)
 - server type [14-7](#)
 - user authorization [14-7](#)
- LLQ
 - See* low-latency queue
- Local CA [33-20](#)
- Local CA User Database [33-28](#)
- Local Hosts and Networks panel, VPN wizard [32-5](#)
- local user database
 - support [14-8](#)
- lockout recovery [16-32, B-6](#)
- logging
 - viewing last 10 messages [1-17](#)
- login
 - FTP [23-3](#)
- low-latency queue
 - applying [25-2, 25-3](#)
- LSA
 - about Type 1 [43-1](#)
 - about Type 2 [43-2](#)
 - about Type 3 [43-3](#)
 - about Type 4 [43-3](#)
 - about Type 5 [43-4](#)
 - about Type 7 [43-4](#)
-
- M**
- MAC address
 - redundant interfaces [7-3, 8-4](#)
- MAC addresses
 - ASA 5505 [9-4](#)
- MAC address table [30-4](#)
 - about [18-11](#)
 - built-in-switch [30-5](#)
 - learning, disabling [30-6](#)
 - monitoring [41-4](#)
 - overview [30-4](#)
 - static entry [30-6](#)
- management traffic [9-8](#)
- man-in-the-middle attack [30-2](#)
- mask reply, ICMP message [16-8](#)
- mask request, ICMP message [16-8](#)
- maximum sessions, IPSec [35-81](#)
- memory usage [1-19](#)
- menus [1-7](#)
- MGCP
 - application inspection
 - configuring [24-111](#)
 - enabling [24-30](#)
 - viewing [24-109](#)
- MGCP inspection
 - configuring [24-15](#)
- Microsoft client parameters, configuring [35-24](#)
- mobile redirection, ICMP message [16-8](#)
- mode
 - bypass in IPS [1-24](#)
 - context [10-9](#)
 - firewall [4-4](#)
- model [1-18](#)
- Modular Policy Framework
 - See* MPF
- monitoring
 - ARP table [41-1](#)
 - CSC CPU [47-4](#)
 - CSC memory [47-5](#)
 - CSC security events [47-2](#)
 - CSC software updates [47-4](#)

- CSC threats [47-1](#)
 - DHCP
 - interface lease [41-2](#)
 - IP addresses [41-2](#)
 - server [41-2](#)
 - statistics [41-3](#)
 - failover [46-1, 46-6](#)
 - failover groups [46-9](#)
 - history metrics [6-6](#)
 - interfaces [41-5](#)
 - MAC address table [41-4](#)
 - routes [43-8](#)
 - monitoring interfaces [15-19](#)
 - monitoring switch traffic, ASA 5505 [9-4](#)
 - MPF
 - about [22-1](#)
 - default policy [22-2](#)
 - feature directionality [22-3](#)
 - features [22-1](#)
 - flows [22-5](#)
 - matching multiple policy maps [22-5](#)
 - See also* class map
 - See also* policy map
 - MPLS
 - LDP [20-7](#)
 - router-id [20-7](#)
 - TDP [20-7](#)
 - MRoute panel [12-11](#)
 - description [12-7](#)
 - fields [12-7](#)
 - MTU [7-8, 8-10, 9-10](#)
 - Multicast panel
 - description [12-1](#)
 - fields [12-1](#)
 - Multicast Route panel [12-11](#)
 - multicast traffic [18-8](#)
 - multiple mode, enabling [10-9](#)
-
- N**
 - N2H2 filtering server [26-5](#)
 - name resolution [13-9](#)
 - NAT
 - about [21-1](#)
 - application inspection [24-60](#)
 - bypassing NAT
 - about [21-10](#)
 - DNS [21-13](#)
 - dynamic NAT
 - about [21-6](#)
 - configuring [21-22](#)
 - implementation [21-16](#)
 - exemption from NAT
 - about [21-10](#)
 - identity NAT
 - about [21-10](#)
 - order of statements [21-13](#)
 - PAT
 - about [21-8](#)
 - configuring [21-22](#)
 - implementation [21-16](#)
 - policy NAT
 - about [21-10](#)
 - RPC not supported with [24-26](#)
 - same security level [21-12](#)
 - security level requirements [7-5, 8-8](#)
 - static NAT
 - about [21-8](#)
 - configuring [21-26](#)
 - static PAT
 - about [21-9](#)
 - transparent mode [21-3](#)
 - types [21-6](#)
 - NETBIOS
 - application inspection, enabling [24-30](#)
 - NetBIOS server
 - tab [35-48](#)

- NetFlow event
 - matching to configured collectors [17-19](#)
 - Network Admission Control
 - uses, requirements, and limitations [34-24](#)
 - New Authentication Server Group panel, VPN wizard [32-9](#)
 - NTLM support [14-5](#)
 - NT server
 - configuring [14-9](#)
 - support [14-5](#)
- ## O
-
- Options menu [1-8](#)
 - OSPF
 - about [11-1](#)
 - adding an LSA filter [11-9](#)
 - authentication settings [11-10](#)
 - authentication support [11-1](#)
 - configuring authentication [11-11](#)
 - defining a static neighbor [11-17](#)
 - defining interface properties [11-13](#)
 - interaction with NAT [11-2](#)
 - interface properties [11-10, 11-12](#)
 - LSA filtering [11-8](#)
 - LSAs [11-2](#)
 - LSA types [43-1](#)
 - monitoring LSAs [43-1](#)
 - neighbor states [43-5](#)
 - route redistribution [11-14](#)
 - static neighbor [11-17](#)
 - summary address [11-18](#)
 - virtual links [11-19](#)
 - OSPF area
 - defining [11-5](#)
 - OSPF Neighbors panel [43-5](#)
 - description [43-5](#)
 - fields [43-5](#)
 - OSPF parameters
 - dead interval [11-14](#)
 - hello interval [11-14](#)
 - retransmit interval [11-14](#)
 - transmit delay [11-14](#)
 - OSPF route summarization
 - about [11-7](#)
 - defining [11-8](#)
 - outbound access lists [20-2](#)
 - Outlook Web Access (OWA) and Clientless SSL VPN [37-7](#)
 - outside, definition [2-16](#)
 - oversubscribing resources [10-11](#)
- ## P
-
- packet
 - capture [B-12](#)
 - classifier [10-2](#)
 - packet flow
 - routed firewall [18-1](#)
 - transparent firewall [18-11](#)
 - packet trace, enabling [3-7](#)
 - parameter problem, ICMP message [16-8](#)
 - password
 - Clientless SSL VPN [37-1](#)
 - passwords
 - recovery [B-7](#)
 - PAT
 - See also* NAT
 - PDP context, GTP application inspection [24-86](#)
 - PIM
 - interface parameters [12-12](#)
 - overview [12-11](#)
 - register message filter [12-18](#)
 - rendezvous points [12-16](#)
 - shortest path tree settings [12-20](#)
 - ping
 - See* ICMP
 - ping of death attack [27-15](#)

platform model [1-18](#)

PoE [9-4](#)

policy, QoS [25-1](#)

policy map

- Layer 3/4
 - feature directionality [22-3](#)
 - flows [22-5](#)

policy NAT

- about [21-10](#)

Port Forwarding

- configuring client applications [37-6](#)

port forwarding entry [38-19](#)

posture validation

- uses, requirements, and limitations [34-24](#)

Posture Validation Exception, add/edit [34-26](#)

power over Ethernet [9-4](#)

PPP tab, tunnel-group [35-71](#)

PPTP

- application inspection, enabling [24-30](#)

priority queueing

- hierarchical policy with traffic shaping [25-8](#)
- IPSec anti-replay window size [25-7, 34-11](#)

Process Instances tab [11-3](#)

- description [11-3](#)
- fields [11-3](#)

Properties tab [11-12](#)

- description [11-12](#)
- fields [11-12](#)

Protocol Group, add [35-21](#)

Protocol panel (IGMP) [12-5](#)

- description [12-5](#)
- fields [12-5](#)

Protocol panel (PIM) [12-12](#)

- description [12-12](#)
- fields [12-12](#)

proxied RPC request attack [27-16](#)

proxy ARP, disabling [11-46](#)

proxy bypass [38-23](#)

proxy servers

SIP and [24-21](#)

Q

QoS

about [25-1, 25-3](#)

DiffServ preservation [25-5](#)

DSCP preservation [25-5](#)

feature interaction [25-4](#)

policies [25-1](#)

priority queueing

- hierarchical policy with traffic shaping [25-8](#)
- IPSec anti-replay window [25-7](#)
- IPSec anti-replay window size [25-7, 34-11](#)

token bucket [25-2](#)

traffic shaping

- overview [25-4](#)

Quality of Service

See QoS

queue, QoS

latency, reducing [25-5](#)

limit [25-2, 25-3](#)

R

RADIUS

attributes [C-15](#)

Cisco AV pair [C-12](#)

configuring a AAA server [C-15](#)

configuring a server [14-9](#)

downloadable access lists [23-11](#)

network access authentication [23-4](#)

network access authorization [23-10](#)

support [14-4](#)

RAM, amount

memory, amount

- RAM [1-18](#)

rate limiting [25-3](#)

RealPlayer [24-20](#)

- recurring time range, add or edit [35-13](#)
 - redirect, ICMP message [16-8](#)
 - Redistribution panel [11-14](#)
 - description [11-14](#)
 - fields [11-15](#)
 - redundant interfaces
 - configuring [8-5](#)
 - failover [7-2, 8-4](#)
 - MAC address [7-3, 8-4](#)
 - reloading
 - security appliance [B-6](#)
 - Remote Access Client panel, VPN wizard [32-6](#)
 - Remote Site Peer panel, VPN wizard [32-3](#)
 - Rendezvous Points panel [12-16](#)
 - description [12-16](#)
 - fields [12-16](#)
 - Request Filter panel [12-18](#)
 - description [12-18](#)
 - fields [12-18](#)
 - reset
 - inbound connections [27-21](#)
 - outside connections [27-21](#)
 - Reset button [1-13](#)
 - resource management
 - configuring [10-10](#)
 - default class [10-12](#)
 - oversubscribing [10-11](#)
 - overview [10-11](#)
 - unlimited [10-11](#)
 - restoring backups [3-29](#)
 - rewrite, disabling [38-13](#)
 - RIP
 - authentication [11-22](#)
 - definition of [11-22](#)
 - support for [11-22](#)
 - RIP panel [11-22](#)
 - fields [11-23](#)
 - limitations [11-22](#)
 - RIP Version 2 Notes [11-22](#)
 - RNFR command, denied request [24-82](#)
 - RNTO command, denied request [24-82](#)
 - routed mode
 - about [18-1](#)
 - setting [4-4](#)
 - router advertisement, ICMP message [16-8](#)
 - router solicitation, ICMP message [16-8](#)
 - Routes panel [43-8](#)
 - description [43-8](#)
 - fields [43-8, 47-4](#)
 - Route Summarization tab [11-7](#)
 - about [11-7](#)
 - fields [11-7](#)
 - Route Tree panel [12-20](#)
 - description [12-20](#)
 - fields [12-20](#)
 - routing
 - other protocols [20-6](#)
 - RPC
 - application inspection, enabling [24-30](#)
 - RSH
 - application inspection, enabling [24-30](#)
 - RTSP
 - application inspection, enabling [24-30](#)
 - RTSP inspection
 - about [24-20](#)
 - configuring [24-19](#)
 - rules
 - filtering [26-5](#)
 - ICMP [16-7](#)
- ## S
-
- same security level communication
 - NAT [21-12](#)
 - SCCP (Skinny) inspection
 - about [24-23](#)
 - configuration [24-23](#)
 - configuring [24-22](#)

- SDI
 - configuring [14-9](#)
 - support [14-5](#)
- Secure Computing SmartFilter filtering server
 - supported [26-1](#)
 - URL for website [26-1](#)
- Secure Copy
 - configure server [16-5](#)
- security appliance
 - reloading [B-6](#)
- security contexts
 - admin context
 - overview [10-1](#)
 - cascading [10-7](#)
 - classifier [10-2](#)
 - command authorization [16-24](#)
 - configuration
 - files [10-2](#)
 - logging in [10-8](#)
 - multiple mode, enabling [10-9](#)
 - nesting or cascading [10-8](#)
 - overview [10-1](#)
 - resource management [10-11](#)
 - unsupported features [10-2](#)
- security level
 - configuration [9-8](#)
- segment size
 - maximum and minimum [27-21](#)
- Server and URL List
 - add/edit [35-33](#)
- Server or URL
 - dialog box [35-34](#)
- session management path [2-19](#)
- Setup panel [11-2](#)
 - about [11-2](#)
- shun
 - duration [27-4](#)
- signatures
 - attack and informational [27-12](#)
- single mode
 - backing up configuration [10-9](#)
 - configuration [10-10](#)
 - enabling [10-9](#)
 - restoring [10-10](#)
- SIP
 - application inspection, enabling [24-30](#)
- SIP inspection
 - about [24-21](#)
 - configuring [24-21](#)
 - instant messaging [24-21](#)
- SITE command, denied request [24-82](#)
- Skinny
 - application inspection, enabling [24-30](#)
- SMTP inspection [24-24](#)
- SNMP
 - application inspection
 - enabling [24-30](#)
 - viewing [24-126](#)
 - traps [16-11](#)
- software
 - version [1-18, 1-24](#)
- source address, browse [35-18](#)
- source port, browse [35-18](#)
- source quench, ICMP message [16-8](#)
- SPAN [9-4](#)
- specifying traffic for CSC scanning [29-19](#)
- speed, configuring [7-2, 8-2](#)
- spoofing, preventing [27-20](#)
- SQLNET
 - application inspection, enabling [24-30](#)
- SSM
 - configuration
 - AIP SSM [28-4](#)
 - CSC SSM [29-4](#)
- Standard Access List Rule, add/edit [35-28](#)
- Standard ACL tab [35-14](#)
- startup configuration [10-2](#)
- statd buffer overflow attack [27-17](#)

- stateful application inspection [24-60](#)
 - Stateful Failover [15-3](#)
 - enabling [15-16](#)
 - Logical Updates Statistics [46-7, 46-9](#)
 - settings [15-27](#)
 - stateful failover
 - interface
 - system [8-2](#)
 - stateful inspection [2-19](#)
 - stateless failover [15-3](#)
 - Static Group panel [12-6](#)
 - description [12-6](#)
 - fields [12-6](#)
 - static NAT
 - See* NAT
 - Static Neighbor panel [11-17](#)
 - description [11-17](#)
 - fields [11-17](#)
 - static PAT
 - See* PAT
 - static routes
 - about [11-40](#)
 - floating [11-40](#)
 - status bar [1-12](#)
 - stealth firewall
 - See* transparent firewall
 - STOU command, denied request [24-82](#)
 - subinterface
 - adding [7-5, 8-6](#)
 - subinterfaces, adding [8-5](#)
 - subordinate certificate [33-1](#)
 - Summary Address panel [11-18](#)
 - description [11-18](#)
 - fields [11-18](#)
 - Summary panel, VPN wizard [32-6](#)
 - Sun Microsystems Java™ Runtime Environment (JRE) and Clientless SSL VPN [37-6](#)
 - Sun Microsystems Java™ Runtime Environment (JRE) and WebVPN [38-20](#)
 - Sun RPC inspection
 - about [24-26](#)
 - configuring [24-26](#)
 - switch MAC address table [30-5](#)
 - switch ports
 - default configuration [9-4](#)
 - SPAN [9-4](#)
 - system
 - interface
 - failover link [8-2](#)
 - system configuration
 - network settings [10-2](#)
 - overview [10-1](#)
 - system messages
 - device ID, including [17-6](#)
 - viewing last 10 [1-17](#)
-
- T**
- TACACS+
 - command authorization, configuring [16-27](#)
 - configuring a server [14-9](#)
 - network access authorization [23-9](#)
 - support [14-4](#)
 - tail drop [25-3](#)
 - TCP
 - application inspection [24-60](#)
 - maximum segment size [27-21](#)
 - TIME_WAIT state [27-21](#)
 - TCP FIN only flags attack [27-16](#)
 - TCP Intercept
 - statistics [27-5](#)
 - TCP NULL flags attack [27-15](#)
 - TCP Service Group, add [35-19](#)
 - TCP SYN+FIN flags attack [27-15](#)
 - testing configuration [B-1](#)
 - TFTP
 - application inspection, enabling [24-30](#)
 - threat detection

- basic
 - drop types [27-2](#)
 - enabling [27-2](#)
 - overview [27-2](#)
 - rate intervals [27-2](#)
 - system performance [27-2](#)
- scanning
 - default limits, changing [27-4](#)
 - enabling [27-3](#)
 - host database [27-3](#)
 - overview [27-3](#)
 - shunning attackers [27-4](#)
 - system performance [27-4](#)
- scanning statistics
 - enabling [27-4](#)
 - system performance [1-20, 27-5](#)
- shun
 - duration [27-4](#)
- TIME_WAIT state [27-21](#)
- time exceeded, ICMP message [16-8](#)
- time range
 - add or edit [35-12](#)
 - browse [35-11](#)
 - recurring [35-13](#)
- timestamp reply, ICMP message [16-8](#)
- timestamp request, ICMP message [16-8](#)
- token bucket [25-2](#)
- Tools menu [1-9](#)
- traceroute, enabling [1-9, 3-11](#)
- traffic flow
 - routed firewall [18-1](#)
 - transparent firewall [18-11](#)
- traffic shaping
 - overview [25-4](#)
- traffic usage [1-19](#)
- transmit queue ring limit [25-2, 25-3](#)
- transparent firewall
 - about [18-7](#)
 - data flow [18-11](#)
 - DHCP packets, allowing [20-6](#)
 - guidelines [18-9](#)
 - H.323 guidelines [18-8](#)
 - HSRP [18-8](#)
 - MAC address table
 - learning, disabling [30-6](#)
 - overview [30-4](#)
 - static entry [30-6](#)
 - Management 0/0 IP address [7-6, 8-9](#)
 - management IP address [6-1](#)
 - multicast traffic [18-8](#)
 - packet handling [20-6](#)
 - unsupported features [18-10](#)
 - VRRP [18-8](#)
- transparent mode
 - NAT [21-3](#)
- traps, SNMP [16-11](#)
- trunk, 802.1Q [7-3, 8-5](#)
- Tunneled Management [35-86](#)
- tunnel gateway, default [35-4](#)
- tx-ring-limit [25-2, 25-3](#)
- Type 1 panel [43-1](#)
 - description [43-1](#)
 - fields [43-2](#)
- Type 2 panel [43-2](#)
 - description [43-2](#)
 - fields [43-2](#)
- Type 3 panel [43-3](#)
 - description [43-3](#)
 - fields [43-3](#)
- Type 4 panel [43-3](#)
 - description [43-3](#)
 - fields [43-3](#)
- Type 5 panel [43-4](#)
 - description [43-4](#)
 - fields [43-4](#)
- Type 7 panel [43-4](#)
 - description [43-4](#)
 - fields [43-5](#)

U

UDP

- application inspection [24-60](#)
- bomb attack [27-16](#)
- chargen DoS attack [27-16](#)
- connection state information [2-20](#)
- snork attack [27-16](#)

Unicast Reverse Path Forwarding [27-20](#)

unreachable messages

- ICMP type [16-8](#)
- required for MTU discovery [16-7](#)

uptime [1-18](#)

URL

- filtering
 - benefits of [26-6](#)
 - configuring [26-8](#)

URLs

- filtering [26-1](#)
- filtering, configuration [26-4](#)

User Accounts panel, VPN wizard [32-10](#)

username

- Clientless SSL VPN [37-1](#)
- Xauth for Easy VPN client [35-85](#)

V

version

- ASDM [1-18](#)
- IPS software [1-24](#)
- platform software [1-18](#)

View/Config Banner [35-25](#)

virtual firewalls

- See security contexts
- See security contexts

virtual HTTP [23-3](#)

Virtual Link panel [11-19](#)

- description [11-19](#)
- fields [11-19](#)

virtual MAC address

- defining for Active/Active failover [15-31](#)

virtual MAC addresses

- about [15-21, 15-32](#)
- defaults for Active/Active failover [15-31](#)
- defining [15-22](#)
- defining for Active/Standby failover [15-33](#)

virtual private network

- overview [32-2](#)

virtual reassembly [2-17](#)

VLANs [7-3, 8-5](#)

- 802.1Q trunk [7-3, 8-5](#)
- ASA 5505
 - MAC addresses [9-4](#)
 - maximum [9-2](#)
- subinterfaces [7-3, 8-5](#)

VoIP

- proxy servers [24-21](#)

VPN

- overview [32-1, 32-2](#)
- system options [35-80](#)

VPN Client, IPsec attributes [34-8](#)

VPN Tunnel Type panel, VPN wizard [32-2](#)

VPN wizard [32-1](#)

- Address Pool panel [32-10](#)
- Address Translation Exemption panel [32-11](#)
- Attributes Pushed to Client panel [32-11](#)
- Client Authentication panel [32-8](#)
- IKE Policy panel [32-4](#)
- Remote Access Client panel [32-6](#)
- Remote Site Peer panel [32-3](#)
- Summary panel [32-6](#)
- User Accounts panel [32-10](#)
- VPN Tunnel Type panel [32-2](#)

VPNwizard

- Local Hosts and Networks panel [32-5](#)
- New Authentication Server Group panel [32-9](#)

VRRP [18-8](#)

W

web browsing with Clientless SSL VPN [37-4](#)

web clients, secure authentication [23-5](#)

Websense filtering server [26-1, 26-5](#)

WebVPN

 use suggestions [37-2](#)

Window menu [1-10](#)

Wizards menu [1-10](#)

X

Xauth, Easy VPN client [35-85](#)

XDMCP

 application inspection, enabling [24-30](#)

Z

Zone Labs Integrity Server [35-82](#)