

# Blue Coat® Systems ProxySG™

## *Command Line Interface Reference*

*Version SGOG 4.1.3*



## Contact Information

Blue Coat Systems Inc.  
420 North Mary Ave  
Sunnyvale, CA 94085-4121

<http://www.bluecoat.com/support/index.html>

[bcs.info@bluecoat.com](mailto:bcs.info@bluecoat.com)  
[support@bluecoat.com](mailto:support@bluecoat.com)  
<http://www.bluecoat.com>

Copyright© 1999-2005 Blue Coat Systems, Inc. All rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of Blue Coat Systems, Inc. All right, title and interest in and to the Software and documentation are and shall remain the exclusive property of Blue Coat Systems, Inc. and its licensors. ProxySG™, ProxyAV™, CacheOS™, SGOS™, Spyware Interceptor™, Scope™ are trademarks of Blue Coat Systems, Inc. and CacheFlow®, Blue Coat®, Accelerating The Internet®, WinProxy®, AccessNow®, Ositis®, Powering Internet Management®, and The Ultimate Internet Sharing Solution® are registered trademarks of Blue Coat Systems, Inc. All other trademarks contained in this document and in the Software are the property of their respective owners.

BLUE COAT SYSTEMS, INC. DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL BLUE COAT SYSTEMS, INC., ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF BLUE COAT SYSTEMS, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Document Number: 231-02779

Document Revision: SGOS 4.1.3—11/11/05

# Contents

## Contact Information

## Chapter 1: Introduction

Audience for this Document.....	7
Organization of this Document.....	7
Related Blue Coat Documentation.....	7
Document Conventions.....	8
SSH and Script Considerations .....	8
Standard and Privileged Modes.....	8
Accessing Quick Command Line Help .....	8

## Chapter 2: Standard and Privileged Mode Commands

Standard Mode Commands.....	11
> display .....	11
> enable .....	12
> exit.....	12
> help .....	12
> ping .....	13
> show .....	13
> traceroute.....	21
Privileged Mode Commands.....	22
# acquire-utc.....	22
# bridge.....	23
# cancel-upload.....	23
# clear-arp.....	23
# clear-cache .....	24
# clear-statistics.....	24
# configure.....	25
# disable.....	25
# disk.....	25
# display .....	26
# exit.....	26
# help.....	27
# hide-advanced .....	27
# inline .....	27
# kill.....	31
# licensing.....	31
# load.....	32
# pcap .....	34
# ping .....	37
# policy.....	37
# purge-dns-cache.....	37
# restart .....	38
# restore-sgos3-config.....	38
# restore-defaults.....	39
# reveal-advanced .....	40
# show .....	40
# temporary-route.....	53
# test .....	53

# traceroute .....	54
# upload .....	55

### Chapter 3: Privileged Mode Configure Commands

Configure Commands .....	57
#(config) accelerated-pac .....	59
#(config) access-log .....	60
#(config access-log) edit log <i>log_name</i> .....	63
#(config access-log) edit format <i>format_name</i> .....	68
#(config) archive-configuration .....	69
#(config) attack-detection .....	70
#(config) bandwidth-gain .....	75
#(config) bandwidth-management .....	75
#(config bandwidth-management) edit <i>class_name</i> .....	76
#(config) banner .....	78
#(config) bridge .....	78
#(config bridge) edit <i>bridge_name</i> .....	79
#(config) bypass-list .....	82
#(config) caching .....	83
#(config caching) ftp .....	85
#(config) clock .....	86
#(config) content .....	87
#(config) content-filter .....	88
#(config content-filter) bluecoat .....	92
#(config content-filter) i-filter .....	94
#(config content-filter) intersafe .....	96
#(config content-filter) local .....	98
#(config content-filter) optenet .....	100
#(config content-filter) proventia .....	102
#(config content-filter) smartfilter .....	104
#(config content-filter) surfcontrol .....	106
#(config content-filter) websense .....	108
#(config content-filter) webwasher .....	111
#(config) diagnostics .....	113
#(config diagnostics) service-info .....	114
#(config diagnostics) snapshot <i>snapshot_name</i> .....	116
#(config) dns .....	118
#(config) dynamic-bypass .....	119
#(config) event-log .....	120
#(config) exceptions .....	122
#(config exceptions) edit [user-defined.] <i>exception_id</i> .....	124
#(config) exit .....	125
#(config) external-services .....	125
#(config external-services) edit <i>icap_service_name</i> .....	127
#(config external-services) edit <i>service_group_name</i> .....	128
#(config external-services) edit <i>websense_service_name</i> .....	130
#(config) failover .....	132
#(config failover) edit <i>group_address</i> .....	132
#(config) forwarding .....	134
#(config forwarding) edit <i>group_alias</i> .....	138
#(config forwarding) edit <i>host_alias</i> .....	139
#(config) front-panel .....	142
#(config) ftp .....	143

---

#(config) health-check .....	144
#(config health-check) edit entry_name .....	146
#(config) hide-advanced .....	148
#(config) hostname .....	148
#(config) http .....	148
#(config) icp .....	152
#(config) identd .....	152
#(config) im .....	153
#(config) inline .....	154
#(config) installed-systems .....	154
#(config) interface .....	155
#(config) ip-default-gateway .....	157
#(config) license-key .....	158
#(config) line-vty .....	158
#(config) load .....	159
#(config) netbios .....	159
#(config) no .....	160
#(config) ntp .....	161
#(config) policy .....	162
#(config) profile .....	164
#(config) restart .....	164
#(config) return-to-sender .....	165
#(config) reveal-advanced .....	166
#(config) rip .....	166
#(config) security .....	167
#(config) security certificate edit-realm <i>realm_name</i> .....	175
#(config) security coreid edit-realm <i>realm_name</i> .....	177
#(config) security ldap edit-realm <i>realm_name</i> .....	180
#(config) security local edit-realm <i>realm_name</i> .....	185
#(config) security local-user-list edit <i>local_user_list</i> .....	186
#(config) security ntlm edit-realm <i>realm_name</i> .....	189
#(config) security policy-substitution edit-realm <i>realm_name</i> .....	190
#(config) security radius edit-realm <i>realm_name</i> .....	192
#(config) security sequence edit-realm <i>realm_sequence_name</i> .....	195
#(config) security siteminder edit-realm <i>realm_name</i> .....	196
#(config) serial-number .....	199
#(config) services .....	199
#(config services) aol-im .....	202
#(config services) dns .....	203
#(config services) epmapper .....	204
#(config services) ftp .....	205
#(config services) http .....	206
#(config services) https .....	208
#(config services) http-console .....	210
#(config services) https-console .....	211
#(config services) mms .....	213
#(config services) msn-im .....	214
#(config services) rtsp .....	215
#(config services) socks .....	217
#(config services) ssh-console .....	218
#(config services) tcp-tunnel .....	220
#(config services) telnet .....	221
#(config services) telnet-console .....	223
#(config services) yahoo-im .....	224

#(config) session-monitor .....	225
#(config) shell .....	227
#(config) show .....	227
#(config) snmp .....	228
#(config) socks-gateways.....	230
#(config socks-gateways) edit gateway_alias .....	231
#(config) socks-machine-id.....	232
#(config) socks-proxy .....	233
#(config) ssl.....	234
#(config ssl) edit ccl list_name .....	239
#(config ssl) edit ssl-client ssl_client_name .....	240
#(config) static-routes.....	242
#(config) streaming.....	243
#(config) tcp-ip .....	250
#(config) tcp-rtt .....	251
#(config) tcp-rtt-use .....	251
#(config) timezone .....	251
#(config) upgrade-path .....	252
#(config) virtual-ip.....	252
#(config) wccp .....	253

## Chapter 1: *Introduction*

To configure and manage your Blue Coat® Systems ProxySG, Blue Coat developed a software suite that includes an easy-to-use graphical interface called the Management Console and a Command Line Interface (CLI). The CLI allows you to perform the superset of configuration and management tasks; the Management Console, a subset.

This reference guide describes each of the commands available in the CLI.

### Audience for this Document

This reference guide is written for system administrators and experienced users who are familiar with network configuration. Blue Coat assumes that you have a functional network topography, that you and your Blue Coat Sales representative have determined the correct number and placement of the ProxySG Appliances, and that those appliances have been installed in an equipment rack and at least minimally configured as outlined in the Blue Coat *Installation Guide* that accompanied the ProxySG. Furthermore, Blue Coat assumes that the Blue Coat ProxySG has been configured for reverse proxy server acceleration, transparent reverse proxy server acceleration, or a variant of either.

### Organization of this Document

This document contains the following chapters:

#### Chapter 1 – Introduction

The organization of this document; conventions used; descriptions of the CLI modes; and instructions for saving your configuration.

#### Chapter 2 – Standard and Privileged Mode Commands

All of the standard mode commands, including syntax and examples, in alphabetical order. All of the privileged mode commands (except for the `configure` commands, which are described in Chapter 3), including syntax and examples, in alphabetical order.

#### Chapter 3 – #Configure Commands

The `#configure` command is the most used and most elaborate of all of the CLI commands. For better readability you will notice that in the command reference chapters, each command heading is preceded with the appropriate prompt, and for the more complicated commands, the parent command prompt is included as well.

### Related Blue Coat Documentation

You can download the following and other Blue Coat documentation in PDF format from the Blue Coat Web site at [www.bluecoat.com](http://www.bluecoat.com).

- *Blue Coat Configuration and Management Guide*
- *Blue Coat Content Policy Language Guide*

## Document Conventions

The following table lists the typographical and CLI syntax conventions used in this manual.

Convention	Definition
<i>Italics</i>	The first use of a new or Blue Coat-proprietary term.
<code>Courier font</code>	Command-line text that will appear on your administrator workstation.
<i>Courier Italics</i>	A command-line variable that should be substituted with a literal name or value pertaining to the appropriate facet of your network system.
<b>Courier Boldface</b>	A CLI literal that should be entered as shown.
{ }	One of the parameters enclosed within the braces must be supplied
[ ]	An optional parameter or parameters.
	Either the parameter before or after the pipe character can or must be selected, but not both.

## SSH and Script Considerations

Consider the following when using the CLI during an SSH session or in a script:

**Case Sensitivity.** CLI command literals and parameters are not case sensitive.

**Command Abbreviations.** You can abbreviate CLI commands, provided you supply enough command characters as to be unambiguous. For example:

```
SGOS#configure terminal
```

Can be shortened to:

```
SGOS#conf t
```

---

*Note:* You cannot use Telnet until you configure and enable it. (Enabling Telnet introduces a security risk, so it is not recommended.)

---

## Standard and Privileged Modes

The ProxySG CLI has three major modes—*standard*, *privileged*, and *configure privileged*. In addition, privileged mode has several subordinate modes. See the introduction in Chapter 2: “Standard and Privileged Mode Commands” for details about the different modes.

- Standard mode prompt: >
- Privileged mode prompt: #
- Configure Privileged mode prompt: # (config)

## Accessing Quick Command Line Help

You can access command line help at any time during a session. The following commands are available in both standard mode and privileged mode.

*To Access a Comprehensive List of Mode-Specific Commands:*

Type `help` or `?` at the prompt.



The `help` command displays how to use CLI help. For example:

```
SGOS> help
```

Help may be requested at any point in a command by typing a question mark '?'.

1. For a list of available commands, enter '?' at the prompt.
2. For a list of arguments applicable to a command, precede the '?' with a space (e.g. 'show ?')
3. For help completing a command, do not precede the '?' with a space (e.g. 'sh?')

The `?`  command displays the available commands. For example:

```
SGOS> ?
```

display	Display a text based url
enable	Turn on privileged commands
exit	Exit command line interface
help	Information on help
ping	Send echo messages
show	Show running system information
traceroute	Trace route to destination

#### *To Access a Command-Specific Parameter List:*

Type the command name, followed by a space, followed by a question mark.

Note that you must be in the correct mode—standard or privileged—to access the appropriate help information. For example, to get command completion help for `pcap`:

```
SGOS# pcap ?
```

bridge	Setup the packet capture mode for bridges
filter	Setup the current capture filter
.	
.	
.	

To get command completion for configuring SNMP:

```
SGOS#(config) clock ?
```

day	Set UTC day
hour	Set UTC hour
.	
.	
.	

#### *To Access the Correct Spelling and Syntax, Given a Partial Command:*

Type the first letter, or more, of the command, followed by a question mark (no spaces).

Note that you must be in the correct mode—standard or privileged—to access the appropriate help information. For example:

```
SGOS# p?
```

```
pcap  ping  purge-dns-cache
```



## Chapter 2: *Standard and Privileged Mode Commands*

This chapter describes and provides examples for the Blue Coat ProxySG standard and privileged mode CLI commands.

### Standard Mode Commands

Standard mode is the default mode when you first log on. From standard mode, you can view but you cannot change configuration settings. In contrast to privileged mode, this mode cannot be password-protected. Standard mode has a short list of commands.

---

*Note:* For a description of the `help` command and instructions on using the CLI help, see “Accessing Quick Command Line Help” on page 8 in Chapter 1: “Introduction”.

---

The standard mode prompt is a greater-than sign; for example:

```
telnet> open 10.25.36.47
username: admin
password: *****
SGOS>
```

### > display

Use this command to display the source code (such as HTML or Javascript) used to build the named URL. This source code is displayed one screen at a time. “—More—” at the bottom of the terminal screen indicates that there is additional code. Press the Spacebar to display the next batch of code; press the Enter key to display one additional line of code.

#### Syntax

```
display url
  where url is a valid, fully-qualified text Web address.
```

#### Example

```
SGOS> display http://www.bluecoat.com

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">

<html>
<head>
<title>Blue Coat Inc.</title>
<meta NAME="KEYWORDS" CONTENT="cache, caching, cache appliance, network cache,
web cache, Blue Coat, internet caching, active, transparent caching,
intelligent, proxy, fast, cache server, Content delivery, streaming, media
streaming, content delivery networks, CDNs, access control, Enterprise Internet
Management, turnkey, web, speed, bandwidth savings, hit rate, internet">
<meta NAME="DESCRIPTION" CONTENT="Blue Coat products are intelligent appliances
specifically architected to accelerate the Internet.">
```

```
<!-- _____  
  
Copyright 1998-2003 Blue Coat Systems Inc. All rights reserved.  
.  
.  
.
```

## > enable

Use this command to enter Privileged mode. Privileged mode commands enable you to view and change your configuration settings. In some configurations, you must provide a password.

To set username and password, please refer to the instructions provided in the *Blue Coat Configuration and Management Guide*.

### Syntax

enable

The `enable` command does not have any parameters or subcommands.

### Example

```
SGOS> enable  
Enable Password:*****  
SGOS# configure terminal  
SGOS(config)  
.  
.  
.
```

### See also

`disable` (`disable` is a Privileged mode command).

## > exit

Use this command to exit the CLI.

### Syntax

exit

The `exit` command does not have any parameters or subcommands.

### Example

```
SGOS> exit
```

## > help

See “Accessing Quick Command Line Help” on page 8 for information about this command.

## > ping

Use this command to verify that a particular IP address exists and can accept requests.

### Syntax

`ping hostname or ip_address`

Table 2.1: > ping

<i>hostname</i>	Specifies the name of the host you want to verify.
<i>ip_address</i>	Specifies the IP address you want to verify.

### Example

```
SGOS> ping 10.25.36.47
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.25.36.47, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
Number of duplicate packets received = 0
```

## > show

Use this command to display system information.

### Syntax

**option 1:** show accelerated-pac

**option 2:** show access-log

sub-option 1: [default-logging]

sub-option 2: [format [brief | *format\_name*]]

sub-option 3: [log [brief | *log\_name*]]

sub-option 4: [statistics [*log\_name*]]

**option 3:** show arp-table

**option 4:** show bandwidth-gain

**option 5:** show bridge

sub-option 1: configuration [*bridge\_name*]

sub-option 2: fwtable *bridge\_name*

sub-option 3: statistics *bridge\_name*

**option 6:** show brief

**option 7:** show bypass-list

**option 8:** show caching

**option 9:** show clock

**option 10:** show commands

sub-option 1: [delimited [all | privileged]]

sub-option 2: [formatted [all | privileged]]

**option 11:** show content-distribution

**option 12:** show cpu

**option 13:** show diagnostics  
    sub-option 1: service-info  
    sub-option 2: status

**option 14:** show disk  
    sub-option 1: disk\_number  
    sub-option 2: all

**option 15:** show dns

**option 16:** show download-paths

**option 17:** show dynamic-bypass

**option 18:** show efficiency

**option 19:** show environmental

**option 20:** show event-log [configuration]

**option 21:** show exceptions  
    sub-option 1: [built-in\_id]  
    sub-option 2: [user-defined\_id]

**option 22:** show expanded

**option 23:** show external-services [statistics]

**option 24:** show failover  
    sub-option 1: configuration [group\_address]  
    sub-option 2: statistics

**option 25:** show forwarding

**option 26:** show health-checks

**option 27:** show hostname

**option 28:** show http

**option 29:** show http-stats

**option 30:** show icp-settings

**option 31:** show identd

**option 32:** show im  
    sub-option 1: aol-statistics  
    sub-option 2: configuration  
    sub-option 3: msn-statistics  
    sub-option 4: yahoo-statistics

**option 33:** show installed-systems

**option 34:** show interface  
    sub-option 1: all  
    sub-option 2: interface\_number

**option 35:** show ip-default-gateway

**option 36:** show ip-route-table

**option 37:** show ip-rts-table

**option 38:** show ip-stats

sub-option 1: all

sub-option 2: e# (0 - 7)

sub-option 3: ip

sub-option 4: memory

sub-option 5: summary

sub-option 6: tcp

sub-option 7: udp

**option 39:** show licenses

**option 40:** show netbios

**option 41:** show noprompts

**option 42:** show ntp

**option 43:** show policy

sub-option 1: [listing]

sub-option 2: [order]

sub-option 3: [proxy-default]

**option 44:** show ports

**option 45:** show profile

**option 46:** show post-setup

**option 47:** show resources

**option 48:** show restart

**option 49:** show return-to-sender

**option 50:** show rip

sub-option 1: parameters

sub-option 2: routes

sub-option 3: statistics

**option 51:** show services

sub-option 1: [aol-im]

sub-option 2: [dns]

sub-option 3: [ftp]

sub-option 4: [http]

sub-option 5: [https]

sub-option 6: [http-console]

sub-option 7: [https-console]

sub-option 8: [mms]

```
sub-option 9: [msn-im]
sub-option 10: [rtsp]
sub-option 11: [socks]
sub-option 12: [ssh-console]
sub-option 13: [tcp-tunnel]
sub-option 14: [telnet-console]
sub-option 15: [yahoo-im]
option 52: show sessions
option 53: show snmp
option 54: show socks-gateways
option 55: show socks-machine-id
option 56: show socks-proxy
option 57: show sources
sub-option 1: bypass-list
sub-option 2: forwarding
sub-option 3: icp-settings
sub-option 4: license-key
sub-option 5: policy {central | local | forward | vpm-cpl | vpm-xml}
sub-option 6: rip-settings
sub-option 7: socks-gateways
sub-option 8: static-route-table
sub-option 9: wccp-settings
option 58: show ssl
sub-option 1: ccl [list_name]
sub-option 2: ssl-client [ssl_client]
option 59: show static-routes
option 60: show status
option 61: show streaming
sub-option 1: configuration
sub-option 2: quicktime {configuration | statistics}
sub-option 3: real-media {configuration | statistics}
sub-option 4: statistics
sub-option 5: windows-media {configuration | statistics}
option 62: show tcp-rtt
option 63: show telnet-management
option 64: show terminal
option 65: show timezones
option 66: show user-authentication
option 67: show version
```



**option 68:** show virtual-ip

**option 69:** show wccp

sub-option 1: configuration

sub-option 2: statistics

**Table 2.2:** > show

accelerated-pac		Displays accelerated PAC file information.
access-log	[default-facility   facility [brief   facility_name]   format [brief   format_name]   statistics [facility_name]]	Displays the current access log settings.
arp-table		Displays TCP/IP ARP table information.
bandwidth-gain		Displays bandwidth gain status, mode, and the status of the "substitute get for get-if-modified-since," "substitute get for HTTP 1.1 conditional get," and "never refresh before specified object expiry" features.
bridge	{configuration [bridge_name]   fwtable bridge_name   statistics bridge_name}	Displays bridge information.
brief		Displays the configuration file without expanding the inline text files.
bypass-list		Displays the current bypass list.
caching		Displays data regarding cache refresh rates and settings and caching policies.
clock		Displays the current ProxySG time setting.
commands	[delimited [all   privileged]   formatted [all   privileged]]	Displays the available CLI commands. Delimited displays commands so they can be parsed, and formatted displays commands so they can be viewed easily.
content-distribution		Displays the average sizes of objects in the cache.
cpu		Displays CPU usage.
diagnostics	service-info   status	Displays remote diagnostics information, including version number, and whether the Heartbeats feature and the ProxySG monitor are currently enabled.
disk	disk_number   all	Displays disk information, including slot number, vendor, product ID, revision and serial number, capacity, and status, about all disks or a specified disk.
dns		Displays primary and alternate DNS server data.

Table 2.2: &gt; show (Continued)

download-paths		Displays downloaded configuration path information, including the policy list, bypass list, accelerated PAC file, HTTP error page, ICP settings, RIP settings, static route table, upgrade image, and WCCP settings.
dynamic-bypass		Displays dynamic bypass configuration status information.
efficiency		Displays efficiency statistics by objects and by bytes, as well as information about non-cacheable objects and access patterns.
environmental		Displays environmental sensor information.
event-log	[start [YYYY-mm-dd] [HH:MM:SS]] [end [YYYY-mm-dd] [HH:MM:SS]] [regex regex   substring string] [configuration]	Show the event-log configuration, using show event-log configuration, or show the contents of the event-log, using the filters offered to narrow the view.
exceptions	[built-in_id]   [user-defined_id]	Displays exception definitions.
expanded		Displays the configuration file, including the contents of the inline text files.
external-services	[statistics]	Displays external services or external services statistics information.
failover	configuration [group_address]   statistics	Displays failover settings.
forwarding		Displays advanced forwarding settings, including download-via-forwarding, health check, and load balancing status, and the definition of forwarding hosts/groups and advanced forwarding rules.
health-checks		Displays health check information.
hostname		Displays the current hostname, IP address, and type.
http		Displays HTTP configuration information.
http-stats		Displays HTTP statistics, including HTTP statistics version number, number of connections accepted by HTTP, number of persistent connections that were reused, and the number of active client connections.
icp-settings		Displays ICP settings.
identd		Displays IDENTD service settings.

Table 2.2: &gt; show (Continued)

im	aol-statistics   configuration   msn-statistics   yahoo-statistics	Displays IM information.
installed-systems		Displays ProxySG system information such as version and release numbers, boot and lock status, and timestamp information.
interface	all   <i>interface_number</i>	Displays interface status and configuration information.
ip-default-gateway		Specifies the default IP gateway.
ip-route-table		Displays route table information.
ip-rts-table		Displays return-to-sender route table information.
ip-stats	all   e#   ip   memory   summary   tcp   udp	Displays TCP/IP statistics for the current session.
licenses		Displays produce license information.
netbios		Displays NETBIOS settings.
ntp		Displays NTP servers status and information.
noprompts		Displays the configuration without using the --More-- prompt.
policy	[listing   order   proxy-default]	Displays the current installed policy (no sub-option), the results of the policy load (listing), the policy files order (order), or the policy default of <i>allow</i> or <i>deny</i> (proxy-default).
ports		Displays HTTP and console port number, type, and properties.
profile		Displays the system profile.
post-setup		Displays the configuration file without those elements that are established in the setup console.
resources		Displays allocation of disk and memory resources.
restart		Displays system restart settings, including core image information and compression status.
return-to-sender		Displays "return to sender" inbound and outbound settings.
rip	parameters   routes   statistics	Displays information on RIP settings, including parameters and configuration, RIP routes, and RIP statistics.

Table 2.2: &gt; show (Continued)

services	[aol-im   dns   ftp   http   https   http-console   https-console   mms   msn-im   rtsp   socks   ssh-console   tcp-tunnel   telnet-console   yahoo-im]	Displays information about services.
sessions		Displays information about the CLI session.
snmp		Displays SNMP statistics, including status and MIB variable and trap information.
socks-gateways		Displays SOCKS gateway settings.
socks-machine-id		Displays the id of the secure sockets machine.
socks-proxy		Displays SOCKS proxy settings.
sources	bypass-list   forwarding   icp-settings   license-key   policy {central   local   forward   vpm-cpl   vpm-xml}   rip-settings   socks-gateways   static-route-table   wccp-settings	Displays source listings for installable lists, such as the bypass-list, license key, policy files, ICP settings, RIP settings, static route table, and WCCP settings files.
ssl	ccl [ <i>list_name</i> ]   ssl-client [ <i>ssl_client</i> ]	Displays SSL settings.
static-routes		Displays static route table information.
status		Displays current system status information, including configuration information and general status information.
streaming	configuration   quicktime {configuration   statistics}   real-media {configuration   statistics}   statistics   windows-media {configuration   statistics}	Displays QuickTime, RealNetworks, or Microsoft Windows Media information, and client and total bandwidth configurations and usage.
tcp-rtt		Displays default TCP round trip time ticks.
telnet-management		Displays Telnet management status and the status of SSH configuration through Telnet.
terminal		Displays terminal configuration parameters and subcommands.
timezones		Displays timezones used.

Table 2.2: &gt; show (Continued)

user-authentication		Displays Authenticator Credential Cache Statistics, including credential cache information, maximum number of clients queued for cache entry, and the length of the longest chain in the hash table.
version		Displays ProxySG hardware and software version and release information and backplane PIC status.
virtual-ip		Displays the current virtual IP addresses.
wccp	configuration   statistics	Displays WCCP configuration and statistics information.

**Examples**

```

SGOS> show caching
Refresh:
Estimated access freshness is 100.0%
Let the ProxySG Appliance manage refresh bandwidth
Current bandwidth used is 0 kilobits/sec
Policies:
Do not cache objects larger than 1024 megabytes
Cache negative responses for 0 minutes
Let the ProxySG Appliance manage freshness
FTP caching:

Caching FTP objects is enabled
FTP objects with last modified date, cached for 10% of last modified time
FTP objects without last modified date, initially cached for 24 hours

SGOS> show resources
Disk resources:
Maximum objects supported: 1119930
Cached Objects: 0
Disk used by system objects: 537533440
Disk used by access log: 0
Total disk installed: 18210036736
Memory resources:
In use by cache: 699203584
In use by system: 83230176
In use by network: 22872608
Total RAM installed: 805306368

```

**> traceroute**

Use this command to trace the route from the current host to the specified destination host.

**Syntax**

```
traceroute {ip_address | hostname}
```

Table 2.3: &gt; traceroute

<i>ip_address</i>	Specifies the IP address of the destination host.
<i>hostname</i>	Specifies the name of the destination host.

**Example**

```
SGOS> traceroute 10.25.36.47
Type escape sequence to abort.
Tracing the route to 10.25.36.47
 1 10.25.36.47 0 0 0
```

## Privileged Mode Commands

Privileged mode provides a robust set of commands that enable you to view, manage, and change ProxySG settings for features such as log files, authentication, caching, DNS, HTTPS, packet capture filters, and security.

---

**Note:** The privileged mode subcommand, *configure*, enables you to manage the ProxySG features. See Chapter 3: “Privileged Mode Configure Commands” for detailed information about this command.

---

**To Access Privileged Mode:**

From standard mode, enter privileged mode using the enable command, as shown below:

```
SGOS> enable
Enable Password:*****
SGOS#
```

If the network administrator who performed the initial network configuration assigned a privileged mode password, you are prompted to supply that also. To prevent unauthorized access to your ProxySG configuration and network, we recommend that you always require a privileged mode password. The default privileged mode password is *admin*.

It is important to note that the prompt changes from a greater than sign (>) to a pound sign (#), acting as an indicator that you are in privileged mode now.

---

**Note:** For a description of the *help* command and instructions on using the CLI help, see “Accessing Quick Command Line Help” on page 8 in Chapter 1: “Introduction”.

---

## # acquire-utc

Use this command to acquire the Universal Time Coordinates (UTC) from a Network Time Protocol (NTP) server. To manage objects, a ProxySG must know the current UTC time. Your ProxySG comes pre-populated with a list of NTP servers available on the Internet, and attempts to connect to them in the order they appear in the NTP server list on the NTP tab. If the ProxySG cannot access any of the listed NTP servers, the UTC time must be set manually. For instructions on how to set the UTC time manually, refer to the *Blue Coat Configuration and Management Guide*.

## Syntax

```
acquire-utc
```

The `acquire-utc` command does not have any parameters or subcommands.

### Example

```
SGOS# acquire-utc
ok
```

## # bridge

This command clears bridge data.

## Syntax

```
bridge
```

Table 2.4: # bridge

<code>clear-statistics</code>	<i>bridge_name</i>	Clears bridge statistics.
<code>clear-fwtable</code>	<i>bridge_name</i>	Clears bridge forward table.

### Example

```
SGOS# bridge clear-statistics testbridge
ok
```

## # cancel-upload

This command cancels a pending access-log upload. The `cancel-upload` command allows you to stop repeated upload attempts if the Web server becomes unreachable while an upload is in progress. This command sets log uploading back to idle if the log is waiting to retry the upload. If the log is in the process of uploading, a flag is set to the log. This flag sets the log back to idle if the upload fails.

## Syntax

```
cancel-upload
```

Table 2.5: # cancel-upload

<code>all</code>		Cancels upload for all logs.
<code>log</code>	<i>log_name</i>	Cancels upload for a specified log.

### Example

```
SGOS# cancel-upload all
ok
```

## # clear-arp

The `clear-arp` command clears the Address Resolution Protocol (ARP) table. ARP tables are used to correlate an IP address to a physical machine address recognized only in a local area network. ARP

provides the protocol rules for providing address conversion between a physical machine address (also known as a Media Access Control or MAC address) and its corresponding IP address, and vice versa.

## Syntax

```
clear-arp
```

The `clear-arp` command does not have any parameters or subcommands.

### Example

```
SGOS# clear-arp
ok
```

## # clear-cache

The `clear-cache` command sets all objects in the cache to *expired*. You can clear the system cache at any time. Although objects are not immediately removed from memory or disk, all subsequent first requests for objects are retrieved from the source.

## Syntax

```
clear-cache
```

### Example

```
SGOS# clear-cache
ok
```

## # clear-statistics

This command clears the bandwidth-management, Windows Media, Real Media, and QuickTime streaming statistics collected by the ProxySG. To view streaming statistics from the CLI, use either the `show streaming {quicktime | real-media | windows-media} statistics` or the `show bandwidth-management statistics [bandwidth_class]` commands. To view streaming statistics from the Management Console, go to either Statistics>Streaming History>Windows Media/Real Media/Quicktime, or to Statistics>Bandwidth Mgmt.

## Syntax

```
clear-statistics
```

Table 2.6: # clear-statistics

bandwidth-management	[class <i>class_name</i> ]	Clears bandwidth-management statistics, either for all classes at once or for the bandwidth-management class specified.
quicktime		Clears the QuickTime statistics.
real-media		Clears the Real Media statistics.
windows-media		Clears the Windows Media statistics.



*Example*

```
SGOS# clear-statistics windows-media
ok
```

## # configure

The privileged mode subcommand `configure`, enables you to manage the ProxySG features. See Chapter 3: “Privileged Mode Configure Commands” for detailed information about this command.

## # disable

The `disable` command returns you to Standard mode from Privileged mode.

### Syntax

```
disable
```

The `disable` command does not have any parameters or subcommands.

*Example*

```
SGOS# disable
SGOS>
```

### See also

`enable` (Standard mode command)

## # disk

Use the `disk` command to take a disk offline or to reinitialize a disk.

On a multi-disk ProxySG, after issuing the `disk reinitialize disk_number` command, complete the reinitialization by setting it to empty and copying pre-boot programs, boot programs and starter programs, and system images from the master disk to the reinitialized disk. The master disk is the leftmost valid disk. *Valid* indicates that the disk is online, has been properly initialized, and is not marked as invalid or unusable.

---

*Note:* If the current master disk is taken offline, reinitialized or declared invalid or unusable, the leftmost valid disk that has not been reinitialized since restart becomes the master disk. Thus as disks are reinitialized in sequence, a point is reached where no disk can be chosen as the master. At this point, the current master disk is the last disk. If this disk is taken offline, reinitialized, or declared invalid or unusable, the ProxySG is restarted.

---

Reinitialization is done without rebooting the ProxySG. The ProxySG operations, in turn, are not affected, although during the time the disk is being reinitialized, that disk is not available for caching. Note that only the master disk reinitialization might restart the ProxySG.

### Syntax

**option 1:** `disk offline disk_number`

**option 2:** disk reinitialize *disk\_number*

Table 2.7: # disk

offline	<i>disk_number</i>	Takes the disk specified by <i>disk_number</i> off line.
reinitialize	<i>disk_number</i>	Reinitializes the disk specified by <i>disk_number</i> .

#### Example

```
SGOS# disk offline 3
ok
SGOS# disk reinitialize 3
ok
```

## # display

Use this command to display the source code (such as HTML or Javascript) used to build the named URL. This source code is displayed one screen at a time. "—More—" at the bottom of the terminal screen indicates that there is additional code. Press the Spacebar to display the next batch of code; press the Enter key to display one additional line of code.

### Syntax

display *url*

where *url* is a valid, fully-qualified text Web address.

#### Example

```
SGOS# display www.company1.com
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>302 Found</TITLE>
</HEAD><BODY>
<H1>Found</H1>
The document has moved <A
HREF="http://lc2.law5.company1.passport.com/cgi-bin/log
in">here</A>.<P>
</BODY></HTML>
```

## # exit

Exits from Configuration mode to Privileged mode, from Privileged mode to Standard mode. From Standard mode, the `exit` command closes the CLI session.

### Syntax

exit

The `exit` command does not have any parameters or subcommands.

*Example*

```
SGOS# exit
```

**# help**

See “Accessing Quick Command Line Help” on page 8 for information about this command.

**# hide-advanced**

Use this command to disable advanced commands. See “# reveal-advanced” on page 40 for information about enabling advanced commands that are disabled.

---

*Note:* You can also use the `configure` command `SGOS# (config) hide-advanced {all | expand}` to hide commands.

---

**Syntax**

**option 1:** `hide-advanced all`

**option 2:** `hide-advanced expand`

Table 2.8: # hide-advanced

all	Hides all advanced commands.
expand	Disables expanded commands.

*Example*

```
SGOS# hide-advanced expand
ok
SGOS# hide-advanced all
ok
```

**See also**

reveal-advanced

**# inline**

Installs configuration elements based on your console port input. There are several ways to create a configuration file for your ProxySG. You can use the `inline` command or you can create a text file to contain the configuration commands and settings. You can also create the file locally and browse to it if you use the Management Console.

If you choose to configure using the `inline` command, see the example below:

```
SGOS# inline accelerated-pac eof_marker
.
.
.
end
eof_marker
```

Where *eof\_marker* marks the end of the inline commands.

---

*Note:* You can also use the `configure` command `SGOS#(config) inline accelerated-pac eof_marker` to create a configuration file.

---

If you choose to create a text file to contain the configuration commands and settings, be sure to assign the file the extension `.txt`. Use a text editor to create this file, noting the following ProxySG configuration file rules:

- Only one command (and any associated parameters) permitted, per line
- Comments must begin with a semicolon (;)
- Comments can begin in any column, however, all characters from the beginning of the comment to the end of the line are considered part of the comment and, therefore, are ignored

When entering input for the inline command, you can correct mistakes on the current line using the backspace key. If you detect a mistake in a line that has already been terminated using the Enter key, you can abort the inline command by typing `<Ctrl-c>`. If the mistake is detected after you terminate input to the inline command, type the same inline command again but with the correct configuration information. The corrected information replaces the information from the last inline command.

The end-of-input marker is an arbitrary string chosen by the you to mark the end of input for the current inline command. The string can be composed of standard characters and numbers, but cannot contain any spaces, punctuation marks, or other symbols.

Take care to choose a unique end-of-input string that does not match any string of characters in the configuration information.

## Syntax

**option 1:** `inline accelerated-pac eof_marker`

**option 2:** `inline authentication-form form_name eof_marker`

**option 3:** `inline authentication-forms eof_marker`

**option 4:** `inline bypass-list`

sub-option 1: `central eof_marker`

sub-option 2: `local eof_marker`

**option 5:** `inline forwarding eof_marker`

**option 6:** `inline icp-settings eof_marker`

**option 7:** `inline license-key eof_marker`

**option 8:** `inline policy`

sub-option 1: `central eof_marker`

sub-option 2: `forward eof_marker`

sub-option 3: `local eof_marker`

sub-option 4: `vpm-cpl eof_marker`

sub-option 5: `vpm-xml eof_marker`

**option 9:** `inline rip-settings eof_marker`

**option 10:** `inline socks-gateways eof_marker`

**option 11:** inline static-route-table *eof\_marker*

**option 12:** inline wccp-settings *eof\_marker*

Table 2.9: # inline

accelerated-pac	<i>eof_marker</i>	Updates the accelerated pac file with the settings you include between the beginning <i>eof_marker</i> and the ending <i>eof_marker</i> .
bypass-list	central <i>eof_marker</i>	Updates the central bypass list with the settings you include between the beginning <i>eof_marker</i> and the ending <i>eof_marker</i> .
	local <i>eof_marker</i>	Updates the local bypass list with the settings you include between the beginning <i>eof_marker</i> and the ending <i>eof_marker</i> .
forwarding	<i>eof_marker</i>	Updates the forwarding configuration with the settings you include between the beginning <i>eof_marker</i> and the ending <i>eof_marker</i> .
icp-settings	<i>eof_marker</i>	Updates the current ICP settings with the settings you include between the beginning <i>eof_marker</i> and the ending <i>eof_marker</i> .
license-key	<i>eof_marker</i>	Updates the current license key settings with the settings you include between the beginning <i>eof_marker</i> and the ending <i>eof_marker</i> .

Table 2.9: # inline (Continued)

policy	central eof_marker	Updates the current central policy file with the settings you include between the beginning eof_marker and the ending eof_marker.
	local eof_marker	Updates the current local policy file with the settings you include between the beginning eof_marker and the ending eof_marker.
	forward eof_marker	Updates the current forward policy file with the settings you include between the beginning eof_marker and the ending eof_marker.
	vpm-cpl eof_marker	Updates the VPM policy with the settings you include between the beginning eof_marker and the ending eof_marker. (This option is designed to be used with the Blue Coat Director product.)
	xml-cpl eof_marker	Updates the XML policy with the settings you include between the beginning eof_marker and the ending eof_marker. (This option is designed to be used with the Blue Coat Director product.)
rip-settings	eof_marker	Updates the current RIP settings with the settings you include between the beginning eof_marker and the ending eof_marker.
socks-gateway	eof_marker	Updates the current SOCKS gateway settings with the settings you include between the beginning eof_marker and the ending eof_marker.
static-route-table	eof_marker	Updates the current static route table settings with the settings you include between the beginning eof_marker and the ending eof_marker.
wccp-settings	eof_marker	Updates the current WCCP settings with the settings you include between the beginning eof_marker and the ending eof_marker.

**Example**

```

SGOS# inline icp-settings eof
icp_port 3130
icp_host 127.0.0.0 sibling 8080 3130
eof

```

## # kill

Terminates a CLI session.

### Syntax

```
kill session_number
```

where *session\_number* is a valid CLI session number.

### Example

```
SGOS# kill 3
ok
```

## # licensing

Use these commands to request or update licenses.

### Syntax

**option 1:** licensing {disable-trial | enable-trial}

**option 2:** licensing request-key [*user\_id*] [*password*]

**option 3:** licensing update-key

Table 2.10: # licensing

disable-trial   enable-trial		<ul style="list-style-type: none"> <li>• <b>disable-trial:</b> All licenses that are in trial mode switch from yes to no. Users cannot use these features. Furthermore, they do not receive nag dialogs warning of license expiration.</li> <li>• <b>enable-trial:</b> Users can use any feature during the trial mode.</li> </ul>
request-key	[ <i>user_id</i> ] [ <i>password</i> ]	Requests the license key from Blue Coat using the WebPower user ID and password.
update-key		Updates the license key from Blue Coat now.

### Example

```
SGOS# licensing request-key
User ID: admin
Password: *****
...
ok
```

where “...” represents license download in progress information.

## # load

Downloads installable lists or system upgrade images. These installable lists or settings can be updated using the `inline` command.

---

*Note:* You can also use the `configure` command `SGOS#(config) load` to download installable lists or system upgrade images.

---

### Syntax

**option 1:** `load accelerated-pac`

**option 2:** `load authentication-form form_name`

**option 3:** `load authentication-forms`

**option 4:** `load bypass-list`  
    sub-option 1: `central`  
    sub-option 2: `local`

**option 5:** `load exceptions`

**option 6:** `load forwarding`

**option 7:** `load icp-settings`

**option 8:** `load license-key`

**option 9:** `load policy`  
    sub-option 1: `central`  
    sub-option 2: `forward`  
    sub-option 3: `local`  
    sub-option 4: `vpm-cpl`  
    sub-option 5: `vpm-software`  
    sub-option 6: `vpm-xml`

**option 10:** `load rip-settings`

**option 11:** `load socks-gateways`

**option 12:** `load static-route-table`

**option 13:** `load upgrade [ignore-warnings]`

**option 14:** `load wccp-settings`

Table 2.11: # load

accelerated-pac		Downloads the current accelerated pac file settings.
authentication-form	<i>form_name</i>	Downloads the new authentication form.
bypass-list	central	Downloads the current central bypass list settings.
	local	Downloads the current local bypass list settings.
exceptions		Downloads new exceptions.



Table 2.11: # load (Continued)

forwarding		Downloads the current forwarding settings.
icp-settings		Downloads the current ICP settings.
license-key		Downloads the new license key.
policy	central	Downloads the current central policy file settings.
	forward	Downloads the current forward policy file settings.
	local	Downloads the current local policy file settings.
	vpm-cpl	Downloads a new VPM CPL policy.
	vpm-software	Downloads a new VPM version.
	vpm-xml	Downloads a new VPM XML policy.
rip-settings		Downloads the current RIP settings.
socks-gateways		Downloads the current SOCKS gateways settings.
static-route-table		Downloads the current static route table settings.
upgrade	[ignore-warnings]	Downloads the latest system image. The ignore-warnings option allows you to force an upgrade even if you receive policy deprecation warnings. Note that using the load upgrade ignore-warnings command to force an upgrade while the system emits deprecation warnings results in a policy load failure; all traffic is allowed or denied according to default policy.
wccp-settings		Downloads the current WCCP settings.

**Examples**

```

SGOS# load bypass-list central
  Downloading from "www.bluecoat.com/support/subscriptions/CentralBypassList.txt
"
  The new policy has been successfully downloaded and installed

SGOS# load policy central
  Downloading from "download.bluecoat.com/release/SG3/files/CentralPolicy.txt"
  The new policy has been successfully downloaded and installed with 1 warning(s)
Policy installation
Compiling new configuration file: download.bluecoat.com/release/SG3/files/Centra
lPolicy.txt
Tue, 15 Jul 2003 21:40:25 UTC

Warning:

    Dynamic bypass is enabled. Sites that are added to the dynamic
    bypass is enabled. Sites that are added to the dynamic
There were 0 errors and 1 warning

```

```
SGOS# load upgrade
      Downloading from "proteus.bluecoat.com/builds/ca_make.19892/wdir/3000.chk"
      Downloading new system software (block 2611)
      The new system software has been successfully downloaded.
      Use "restart upgrade" to install the new system software.
```

## See also

inline

## # pcap

This utility enables you to capture packets of Ethernet frames going into or leaving a ProxySG. Packet capturing allows filtering on various attributes of the frame to limit the amount of data collected. The collected data can then be transferred to the desktop for analysis.

---

**Note:** Packet capturing increases the amount of processor usage performed in TCP/IP. Before using the `pcap` utility, consider that packet capturing doubles the amount of processor usage performed in TCP/IP.

To capture packets, you must have a tool that can read Packet Sniffer Pro 1.1 files (for example, EtherReal or Packet Sniffer Pro 3.0).

---

For an in-depth discussion of PCAP, refer to the “Diagnostics” appendix in the *Blue Coat Configuration and Management Guide*.

## Syntax

```
option 1: pcap bridge capture-all {enable | disable}
option 2: pcap filter
      sub-option 1: [iface {in | out}]
      sub-option 2: [iface {in | out} interface_number]
      sub-option 3: [iface interface_number]
      sub-option 4: [bridge {in | out} name port number]
      sub-option 5: [bridge name port number]
      sub-option 6: [expr filter_expression]
option 3: pcap info
option 4: pcap coreimage keep n(k)
option 5: pcap start
      sub-option 1: [first n]
      sub-option 2: [capsize n(k)]
      sub-option 3: [trunc n]
      sub-option 4: [last n]
option 6: pcap stop
option 7: pcap transfer full_url/filename username password
```

Table 2.12: # pcap

bridge capture-all	enable   disable	Configures the bridge to capture all packets: <i>disable</i> captures packets relevant to this device; <i>enable</i> captures all packets.
filter	<cr>	No filtering specified (captures all).
	[iface {in   out}]	Specifies capture if all specifiers are true either in or out from the ProxySG.
	[iface {in   out} interface_number]	Specifies capture if all specifiers are true either in or out from a particular interface (interface number must be between 0 and 16).
	[iface interface_number]	Specifies capture if all specifiers are true both in and out from a particular interface (interface number must be between 0 and 16).
	[bridge {in   out} bridge_name port port_number]	Specifies capture if all specifiers are true either in or out on a particular bridge port.
	[bridge bridge_name port port_number]	Specifies capture if all specifiers are true both in and out on a particular bridge port.
	[expr filter_expression]	Specifies capture if all specifiers are true for the filter expression. See Table 2.13 for examples.
info		Displays the current packet capture information.
coreimage	keep kilobytes	Specifies kilobytes of packets kept in a core image.
start	[first n]	The <i>first n</i> parameter collects <i>n</i> (up to 100 MB) packets. After the number of packets <i>n</i> is reached, capturing stops. The packet capture file size is limited to 1% of total RAM, which might be reached before <i>n</i> packets have been captured. <b>Note:</b> The parameter <i>first n</i> is a specific command; it captures an exact number of packets. If no parameters are specified, the default is to capture until the stop subcommand is issued or the maximum limit reached.
	[capsize n(kilobytes)]	The <i>capsize n(k)</i> parameter stops the collection after <i>n</i> kilobytes (up to 100 MB) of packets have been captured. The packet capture file size is limited to 1% of total RAM, which might be reached before <i>n</i> packets have been captured. <b>Note:</b> The parameter <i>capsize n</i> is an approximate command; it captures an approximate number of packets. If no parameters are specified, the default is to capture until the stop subcommand is issued or the maximum limit reached.
	[trunc n]	The <i>trunc n</i> parameter collects, at most, <i>n</i> bytes of packets from each frame. This continues until the 1% of total RAM for file size limitation is reached. Range is 0 to 2147483647.
	[last n]	The <i>last n</i> parameter capture saves up to <i>n</i> bytes of packets in memory. (The maximum amount of memory used for saving packets is limited to 100 MB.) Any packet received after the memory limit is reached results in the discarding of the oldest saved packet prior to saving the new packet. The saved packets in memory are written to disk when the capture is terminated. The range is 0 to 2147483647.

Table 2.12: # pcap (Continued)

stop		Stops the capture.
transfer	<i>full_url/filename</i> <i>username password</i>	Transfers captured data to an FTP site. See the examples below for details.

---

*Note:* Once a filter is set, it remains in effect until it is redefined, or until the ProxySG is rebooted, when filtering is set to off; at this point, you must reset or redefine all filtering options.

---

The following are examples of the `pcap` parameters/subcommands `filter`, `info`, `start`, and `transfer`.

#### Example 1

Capture transactions among a ProxySG (10.1.1.1), a server (10.2.2.2), and a client (10.1.1.2).

```
SGOS# pcap filter expr "host 10.1.1.1 || host 10.2.2.2 || host 10.1.1.2"
```

#### Example 2

```
SGOS# pcap filter expr "port 80"
ok
SGOS# pcap start
ok
```

This captures outbound packets that have a source port of 80 from the interface using the IP protocol TCP.

```
SGOS# pcap info
packet capture information:
Packets captured:          381
Bytes captured:            171552
Packets written:           379
Bytes written:             182088
Max packet ram:            0
Packet ram used:           0
Packets filtered:          0
Bridge capture all:        Disabled
Current state:              Capturing
Filtering:                  Off
Filter expression:          iface out
```

This shows relevant information regarding current packet-capturing.

#### Example 3

The following command stops the capturing of packets after approximately three kilobytes of packets have been collected.

```
SGOS# pcap start capsize 3
```

#### Example 3

This transfers captured packets to the FTP site 10.25.36.47. Note that the username and password are provided.

```
SGOS# pcap transfer ftp://10.25.36.47/path/filename.cap username password
```

If the folders in the path do not exist, they are not created. An error message is generated.

## # ping

Use this command to verify that a particular IP address exists and can accept requests. Ping output will also tell you the minimum, maximum, and average time it took for the ping test data to reach the other computer and return to the origin.

### Syntax

```
ping {ip_address | hostname}
```

where *ip\_address* is the IP address and *hostname* is the hostname of the remote computer.

### Example

```
SGOS# ping 10.25.36.47
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.25.36.47, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
Number of duplicate packets received = 0
```

## # policy

Use this command to configure policy commands. Use `all` to trace all transactions by default, and use `none` to specify no tracing except as specified in policy files.

**Important:** Configuring the policy command to trace all transactions by default can significantly degrade performance.

### Syntax

```
policy trace {all | none}
```

### Example

```
SGOS# policy trace all
ok
All requests will be traced by default;
Warning: this can significantly degrade performance.
Use 'policy trace none' to restore normal operation
SGOS# policy trace none
ok
```

## # purge-dns-cache

This command clears the DNS cache. You can purge the DNS cache at any time. You might need to do so if you have experienced a problem with your DNS server, or if you have changed your DNS configuration.

## Syntax

`purge-dns-cache`

The `purge-dns-cache` command does not have any parameters or subcommands.

### Example

```
SGOS# purge-dns-cache
ok
```

## # restart

Restarts the system. The restart options determine whether the ProxySG should simply reboot the ProxySG (regular), or should reboot using the new image previously downloaded using the `load upgrade` command (upgrade).

## Syntax

`restart {abrupt | regular | upgrade}`

Table 2.13: # restart

<code>abrupt</code>	Reboots the system abruptly, according to the version of the ProxySG that is currently installed.
<code>regular</code>	Reboots the version of the ProxySG that is currently installed.
<code>upgrade</code>	Reboots the entire system image.

### Example

```
SGOS# restart upgrade
ok
SGOS# Read from remote host 10.9.17.159: Connection reset by peer
Connection to 10.9.17.159 closed.
```

## See also

`load`

## # restore-sgos3-config

Restores the ProxySG to settings last used with SGOS 3.x. The ProxySG retains the network settings.

## Syntax

`restore-sgos3-config`

### Example

```
SGOS# restore-sgos3-config
Restoring SGOS 3.x configuration requires a restart to take effect.
The current configuration will be lost and the system will be restarted.
Continue with restoring? (y/n)[n]: y
Restoring configuration ...
```

Or if there is no 3.x configuration found:

```
SGOS# restore-sgos3-config
%% No SGOS 3.x configuration is available on this system.
```

## See also

`restore-defaults`

## # restore-defaults

Restores the ProxySG to the default configuration. When you restore system defaults, the ProxySG's IP address, default gateway, and the DNS server addresses are cleared. In addition, any lists (for example, forwarding or bypass) are cleared. After restoring system defaults, you need to restore the ProxySG's basic network settings, as described in the *Blue Coat Configuration and Management Guide*, and reset any customizations.

## Syntax

```
option 1: restore-defaults [factory-defaults]
option 2: restore-defaults [force]
option 3: restore-defaults [keep-console [force]]
```

Table 2.14: # restore-defaults

[factory-defaults]		Reinitializes the ProxySG to the original settings it had when it was shipped from the factory.
[force]		Restores the system defaults without confirmation. If you don't use the <code>force</code> command, you are prompted to enter <code>yes</code> or <code>no</code> before the restoration can proceed.
[keep-console]	[force]	Restores defaults except settings required for console access. Using the <code>keep-console</code> option retains the settings for all consoles (Telnet-, SSH-, HTTP-, and HTTPS-consoles), whether they are enable, disabled, or deleted.  If you use the <code>force</code> command, you will not be prompted to enter <code>yes</code> or <code>no</code> before restoration can proceed.

## Example

```
SGOS# restore-defaults
Restoring defaults requires a restart to take effect.
The current configuration will be lost and the system will be restarted.
Continue with restoring? (y/n) [n]: n
Existing configuration preserved.
```

## # reveal-advanced

The `reveal-advanced` command allows you to enable all or a subset of the advanced commands available to you when using the CLI. See “# `hide-advanced`” on page 27 for information about disabling advanced commands that are enabled.

---

**Note:** You can also use the `configure` command `SGOS#(config) reveal-advanced {all | expand}` to reveal hidden commands.

---

### Syntax

```
reveal-advanced {all | expand | tcp-ip}
```

Table 2.15: # `reveal-advanced`

all	Enables all advanced commands.
expand	Displays expanded commands.

### Example

```
SGOS# reveal-advanced all
ok
```

## # show

Use this command to display system information.

---

**Note:** You can also use the `configure` command `SGOS#(config) show` to display system information.

---

**option 1:** `show accelerated-pac`

**option 2:** `show access-log`

sub-option 1: `[default-logging]`

sub-option 2: `[format [brief | format_name]]`

sub-option 3: `[log [brief | log_name]]`

sub-option 4: `[statistics [log_name]]`

**option 3:** `show archive-configuration`

**option 4:** `show arp-table`

**option 5:** `show attack-detection`

sub-option 1: `client [blocked | connections | statistics]`

sub-option 2: `configuration`

sub-option 3: `server [statistics]`

**option 6:** `show bandwidth-gain`

**option 7:** `show bandwidth-management`

sub-option 1: `configuration [bandwidth_class]`

sub-option 2: `statistics [bandwidth_class]`



**option 8:** show bridge  
    sub-option 1: configuration [*bridge\_name*]  
    sub-option 2: fwtable *bridge\_name*  
    sub-option 3: statistics *bridge\_name*

**option 9:** show bypass-list

**option 10:** show caching

**option 11:** show clock

**option 12:** show commands  
    sub-option 1: [delimited [all | privileged]]  
    sub-option 2: [formatted [all | privileged]]

**option 13:** show configuration  
    sub-option 1: [brief]  
    sub-option 2: [expanded]  
    sub-option 3: [noprompts]

**option 14:** show content  
    sub-option 1: outstanding-requests  
    sub-option 2: priority [regex *regex* | url *url*]  
    sub-option 3: url *url*

**option 15:** show content-distribution

**option 16:** show content-filter  
    sub-option 1: bluecoat  
    sub-option 2: i-filter  
    sub-option 3: intersafe  
    sub-option 4: local  
    sub-option 5: optenet  
    sub-option 6: proventia  
    sub-option 7: smartfilter  
    sub-option 8: surfcontrol  
    sub-option 9: status  
    sub-option 10: websense  
    sub-option 11: webwasher

**option 17:** show cpu

**option 18:** show cpu-monitor

**option 19:** show diagnostics  
    sub-option 1: configuration  
    sub-option 2: cpu-monitor  
    sub-option 3: service-info  
    sub-option 4: snapshot *snapshot\_name*

**option 20:** show disk

```
sub-option 1: disk_number
sub-option 2: all
option 21: show dns
option 22: show download-paths
option 23: show dynamic-bypass
option 24: show efficiency
option 25: show environmental
option 26: show epmapper statistics
option 27: show event-log [configuration]
option 28: show exceptions
sub-option 1: [built-in_id]
sub-option 2: [user-defined_id]
option 29: show external-services [statistics]
option 30: show failover
sub-option 1: configuration [group_address]
sub-option 2: statistics
option 31: show forwarding
option 32: show ftp
option 33: show health-checks
option 34: show hostname
option 35: show http
option 36: show http-stats
option 37: show icp-settings
option 38: show identd
option 39: show im
sub-option 1: aol-statistics
sub-option 2: configuration
sub-option 3: msn-statistics
sub-option 4: yahoo-statistics
option 40: show installed-systems
option 41: show interface
sub-option 1: all
sub-option 2: interface_number
option 42: show ip-default-gateway
option 43: show ip-route-table
option 44: show ip-rts-table
option 45: show ip-stats
sub-option 1: all
```

```
sub-option 2: e# (0 - 7)
sub-option 3: ip
sub-option 4: memory
sub-option 5: summary
sub-option 6: tcp
sub-option 7: udp
option 46: show licenses
option 47: show netbios
option 48: show ntp
option 49: show p2p statistics
option 50: show policy
    sub-option 1: [listing]
    sub-option 2: [order]
    sub-option 3: [proxy-default]
option 51: show profile
option 52: show realms
option 53: show resources
option 54: show restart
option 55: show return-to-sender
option 56: show rip
    sub-option 1: parameters
    sub-option 2: routes
    sub-option 3: statistics
option 57: show security
option 58: show services
    sub-option 1: [aol-im]
    sub-option 2: [dns]
    sub-option 3: [ftp]
    sub-option 4: [http]
    sub-option 5: [https]
    sub-option 6: [http-console]
    sub-option 7: [https-console]
    sub-option 8: [mms]
    sub-option 9: [msn-im]
    sub-option 10: [rtsp]
    sub-option 11: [socks]
    sub-option 12: [ssh-console]
    sub-option 13: [tcp-tunnel]
    sub-option 14: [telnet]
```

```
sub-option 15: [telnet-console]
sub-option 16: [yahoo-im]
option 59: show sessions
option 60: show shell
option 61: show snmp
option 62: show socks-gateways
option 63: show socks-machine-id
option 64: show socks-proxy
option 65: show sources
sub-option 1: bypass-list
sub-option 2: forwarding
sub-option 3: icp-settings
sub-option 4: license-key
sub-option 5: policy {central | local | forward | vpm-cpl | vpm-xml}
sub-option 6: rip-settings
sub-option 7: socks-gateways
sub-option 8: static-route-table
sub-option 9: wccp-settings
option 66: show ssh
sub-option 1: [client-key [username]]
sub-option 2: [director-client-key [key_id]]
sub-option 3: [host-public-key [sshv1 | sshv2]]
sub-option 4: [user-list]
sub-option 5: [versions-enabled]
option 67: show ssl
sub-option 1: ccl [list_name]
sub-option 2: ssl-client [ssl_client]
sub-option 3: keypair [des | des3 | unencrypted]
option 68: show static-routes
option 69: show status
option 70: show streaming
sub-option 1: configuration
sub-option 2: quicktime {configuration | statistics}
sub-option 3: real-media {configuration | statistics}
sub-option 4: statistics
sub-option 5: windows-media {configuration | statistics}
option 71: show tcp-ip
option 72: show tcp-rtt
option 73: show terminal
```

**option 74:** show timezones  
**option 75:** show user-authentication  
**option 76:** show version  
**option 77:** show virtual-ip  
**option 78:** show wccp  
     sub-option 1: configuration  
     sub-option 2: statistics

Table 2.16: # show

accelerated-pac		Displays accelerated PAC file information.
access-log	[default-facility   facility [brief   <i>facility_name</i> ]   format [brief   <i>format_name</i> ]   statistics [ <i>facility_name</i> ]]	Displays the current access log settings.
arp-table		Displays TCP/IP ARP table information.
archive-configuration		Displays archive configuration settings.
attack-detection	client [blocked   connections   statistics]	Displays client attack-detection settings.
	configuration	Displays attack-detection configuration.
	server [statistics]	Displays server attack-detection settings.
bandwidth-gain		Displays bandwidth gain status, mode, and the status of the "substitute get for get-if-modified-since," "substitute get for HTTP 1.1 conditional get," and "never refresh before specified object expiry" features.
bandwidth-management	configuration [ <i>bandwidth_class</i> ]	Displays bandwidth-management configuration for all classes or for the specified default class.
	statistics [ <i>bandwidth_class</i> ]	Displays bandwidth-management statistics for all classes or for the specified default class.
bridge	configuration [ <i>bridge_name</i> ]   fwtable <i>bridge_name</i>   statistics <i>bridge_name</i>	Displays bridge information.
bypass-list		Displays the current bypass list.
caching		Displays data regarding cache refresh rates and settings and caching policies.
clock		Displays the current ProxySG time setting.

Table 2.16: # show (Continued)

commands	[delimited [all   privileged]   formatted [all   privileged]]	Displays the available CLI commands. Delimited displays commands so they can be parsed, and formatted displays commands so they can be viewed easily.
configuration	[brief   expanded   noprompts]	Displays the current configuration, as different from the default configuration.
content	outstanding-requests   priority [regex regex   url url]   url url	Displays content management commands—outstanding-requests displays the complete list of outstanding asynchronous content revalidation and distribute requests; priority displays the deletion priority value assigned to the regex or url, respectively; and url displays statistics of the specified URL.
content-distribution		Displays the average sizes of objects in the cache.
content-filter	bluecoat   i-filter   intersafe   local   optenet   proventia   smartfilter   surfcontrol   status   websense   webwasher	Displays the content filter configuration.
cpu		Displays CPU usage.
cpu-monitor		Displays the CPU monitor results.
diagnostics	configuration   cpu-monitor   service-info   snapshot snapshot_name	Displays remote diagnostics configuration information, as well as CPU monitor results, transfer status of service information to Blue Coat, and the status and configuration of a specified snapshot.
diagnostics	service-info   status	Displays remote diagnostics information, including version number, and whether or not the Heartbeats feature and the ProxySG monitor are currently enabled.
disk	disk_number   all	Displays disk information, including slot number, vendor, product ID, revision and serial number, capacity, and status, about all disks or a specified disk.
dns		Displays primary and alternate DNS server data.
download-paths		Displays downloaded configuration path information, including the policy list, bypass list, accelerated PAC file, HTTP error page, ICP settings, RIP settings, static route table, upgrade image, and WCCP settings.
dynamic-bypass		Displays dynamic bypass configuration status information.

Table 2.16: # show (Continued)

efficiency		Displays efficiency statistics by objects and by bytes, as well as information about non-cacheable objects and access patterns.
environmental		Displays environmental sensor information.  NOTE: You cannot view environmental statistics on a ProxySG 400 Series Appliance.
epmapper	statistics	Displays End Point Mapper statistics.
event-log	[start [YYYY-mm-dd] [HH:MM:SS]] [end [YYYY-mm-dd] [HH:MM:SS]] [regex <i>regex</i>   substring <i>string</i> ] [configuration]	Show the event-log configuration, using show event-log configuration, or show the contents of the event-log, using the filters offered to narrow the view.
exceptions	[built-in_id]   [user-defined_id]	Displays exception definitions.
external-services	[statistics]	Displays external services or external services statistics information.
failover	configuration [group_address]   statistics	Displays failover settings.
forwarding		Displays advanced forwarding settings, including download-via-forwarding, health check, and load balancing status, and the definition of forwarding hosts/groups and advanced forwarding rules.
ftp		Displays FTP settings.
health-checks		Displays health check information.
hostname		Displays the current hostname, IP address, and type.
http		Displays HTTP configuration information.
http-stats		Displays HTTP statistics, including HTTP statistics version number, number of connections accepted by HTTP, number of persistent connections that were reused, and the number of active client connections.
icp-settings		Displays ICP settings.
identd		Displays IDENTD service settings.
im	aol-statistics   configuration   msn-statistics   yahoo-statistics	Displays IM information.

Table 2.16: # show (Continued)

installed-systems		Displays ProxySG system information such as version and release numbers, boot and lock status, and timestamp information.
interface	all   <i>interface_number</i>	Displays interface status and configuration information, including IP address, subnet mask, MTU size, source for instructions, autosense information, and inbound connection disposition for the current interface, for all interfaces or for a specific interface.
ip-default-gateway		Displays default IP gateway IP address, weight, and group membership.
ip-route-table		Displays route table information.
ip-rts-table		Displays return-to-sender route table information.
ip-stats	all   e#   ip   memory   summary   tcp   udp	Displays TCP/IP statistics for the current session.
licenses		Displays produce license information.
netbios		Displays NETBIOS settings.
ntp		Displays NTP servers status and information.
p2p	statistics	Displays Peer-to-Peer client statistics.
policy	[listing   order   proxy-default]	Displays the current installed policy (no sub-option), the results of the policy load (listing), the policy files order (order), or the policy default of <i>allow</i> or <i>deny</i> (proxy-default).
profile		Displays the system profile.
realms		Displays the security realms.
resources		Displays allocation of disk and memory resources.
restart		Displays system restart settings, including core image information and compression status.
return-to-sender		Displays "return to sender" inbound and outbound settings.
rip	parameters   routes   statistics	Displays information on RIP settings, including parameters and configuration, RIP routes, and RIP statistics.



Table 2.16: # show (Continued)

services	[aol-im   dns   ftp   http   https   http-console   https-console   mms   msn-im   rtsp   socks   ssh-console   tcp-tunnel   telnet   telnet-console   yahoo-im]	Displays information about services.
sessions		Displays information about CLI sessions.
snmp		Displays SNMP statistics, including status and MIB variable and trap information.
socks-gateways		Displays SOCKS gateway settings.
socks-machine-id		Displays the ID of the secure sockets machine.
socks-proxy		Displays SOCKS proxy settings.
sources	bypass-list   forwarding   icp-settings   license-key   policy {central   local   forward   vpm-cpl   vpm-xml}   rip-settings   socks-gateways   static-route-table   wccp-settings	Displays source listings for installable lists, such as the bypass-list, license key, policy files, ICP settings, RIP settings, static route table, and WCCP settings files.
ssh		Displays the SSH service details.
	[client-key username]	Displays the client key fingerprint for the specified username.  NOTE: If you have upgraded from an older version of the ProxySG, you might not need to enter a username.
	[director-client-key [key_id]]	Displays all client key fingerprints or the client key fingerprint of the specified key ID.
	[host-public-key [sshv1  sshv2]]	Displays the sshv1 or sshv2 host public key. Both keys are displayed if you do not specify a version.
	[user-list]	Displays a list of users with imported RSA client keys.
	[versions-enabled]	Displays which SSH version or versions are enabled.

Table 2.16: # show (Continued)

ssl	ccl [ <i>list_name</i> ]   ssl-client [ <i>ssl_client</i> ]	Displays SSL settings.
	keypair {des   des3   unencrypted} <i>keyring_id</i>   <i>keyring_id</i> }	Displays the keypair. If you want to view the keypair in an encrypted format, you can optionally specify des or des3 before the keyringID. If you specify either des or des3, you are prompted for the challenge entered when the keyring was created.
static-routes		Displays static route table information.
status		Displays current system status information, including configuration information and general status information.
streaming	configuration   quicktime {configuration   statistics}   real-media {configuration   statistics}   statistics   windows-media {configuration   statistics}	Displays QuickTime, RealNetworks, or Microsoft Windows Media information, and client and total bandwidth configurations and usage.
tcp-ip		Displays TCP-IP settings.
tcp-rtt		Displays default TCP round trip time ticks.
terminal		Displays terminal configuration parameters.
timezones		Displays timezones used.
user-authentication		Displays Authenticator Credential Cache Statistics, including credential cache information, maximum number of clients queued for cache entry, and the length of the longest chain in the hash table.
version		Displays ProxySG hardware and software version and release information and backplane PIC status.
virtual-ip		Displays the current virtual IP addresses.
wccp	configuration   statistics	Displays WCCP configuration and statistics information.

**Examples**

```

SGOS# show caching
Refresh:
Estimated access freshness is 100.0%
Let the ProxySG Appliance manage refresh bandwidth
Current bandwidth used is 0 kilobits/sec
Policies:
Do not cache objects larger than 1024 megabytes

```

Cache negative responses for 0 minutes  
Let the ProxySG Appliance manage freshness  
FTP caching:  
Caching FTP objects is enabled  
FTP objects with last modified date, cached for 10% of last modified time  
FTP objects without last modified date, initially cached for 24 hours

SGOS# **show resources**

Disk resources:  
Maximum objects supported: 1119930  
Cached Objects: 0  
Disk used by system objects: 537533440  
Disk used by access log: 0  
Total disk installed: 18210036736  
Memory resources:  
In use by cache: 699195392  
In use by system: 83238368  
In use by network: 22872608  
Total RAM installed: 805306368

SGOS# **show installed-systems**

ProxySG Appliance Systems  
1. Version: SGOS 96.99.99.99, Release ID: 20042  
Thursday August 21 2003 08:08:58 UTC, Lock Status: Unlocked  
Boot Status: Last boot succeeded, Last Successful Boot: Thursday August 21 2003 17:51:50 UTC  
2. Version: SGOS 3.0.1.0, Release ID: 20050  
Friday August 22 2003 04:43:34 UTC, Lock Status: Unlocked  
Boot Status: Last boot succeeded, Last Successful Boot: Monday August 25 2003 21:00:09 UTC  
3. Version: SGOS 3.0.1.0, Release ID: 20064  
Tuesday August 26 2003 08:23:20 UTC, Lock Status: Unlocked  
Boot Status: Last boot succeeded, Last Successful Boot: Tuesday August 26 2003 20:09:51 UTC  
4. Version: SGOS 96.99.99.99, Release ID: 20072  
Wednesday August 27 2003 08:04:06 UTC, Lock Status: Unlocked  
Boot Status: Last boot succeeded, Last Successful Boot: Wednesday August 27 2003 20:10:14 UTC  
5. Version: SGOS 96.99.99.99, Release ID: 20030  
Friday August 15 2003 08:01:47 UTC, Lock Status: Unlocked  
Boot Status: Last boot succeeded, Last Successful Boot: Friday August 15 2003 19:20:32 UTC  
Default system to run on next hardware restart: 4  
Default replacement being used. (oldest unlocked system)  
Current running system: 4

When a new system is loaded, only the system number that was replaced is changed.

The ordering of the rest of the systems remains unchanged.

SGOS# **show cpu**

Current cpu usage: 0 percent

SGOS# **show dns**

Primary DNS servers:

```
216.52.23.101
Alternate DNS servers:
Imputed names:
Resolved names:
Time-to-live: 3600
```

```
SGOS# show dynamic-bypass
Dynamic bypass: disabled
Non-HTTP trigger: disabled
HTTP connect error trigger: disabled
HTTP receive error trigger: disabled
HTTP 400 trigger: disabled
HTTP 401 trigger: disabled
HTTP 403 trigger: disabled
HTTP 405 trigger: disabled
HTTP 406 trigger: disabled
HTTP 500 trigger: disabled
HTTP 502 trigger: disabled
HTTP 503 trigger: disabled
HTTP 504 trigger: disabled
```

```
SGOS# show hostname
Hostname: 10.25.36.47 - Blue Coat 5000
```

```
SGOS# show icp-settings
# Current ICP Configuration
# No update

# ICP Port to listen on (0 to disable ICP)
icp_port 0

# Neighbor timeout (seconds)
neighbor_timeout 2

# ICP and HTTP failure counts
icp_failcount 20
http_failcount 5

# Host failure/recovery notification flags
host_recover_notify on
host_fail_notify on

# 0 neighbors defined, 32 maximum

# ICP host configuration
# icp_host hostname peertype http_port icp_port [options]

# ICP access: domain configuration
# icp_access_domain allow|deny domainname
# domainname of 'all' sets default access if no match
# 0 icp access domains defined, 256 maximum

# ICP access: IP configuration
# icp_access_ip allow|deny ip[/netmask]
# ip of '0.0.0.0' sets default access if no match
# 0 icp access ip's defined, 256 maximum
```

```

SGOS# show ntp
NTP is enabled
NTP servers:
ntp.bluecoat.com
ntp2.bluecoat.com
Query NTP server every 60 minutes

SGOS# show snmp
General info:
SNMP is disabled
SNMP writing is disabled
MIB variables:
sysContact:
sysLocation:
Community strings:
Read community:  *****
Write community:  *****
Trap community:   *****
Traps:
Trap address 1:
Trap address 2:
Trap address 3:
Authorization traps: disabled

```

## # temporary-route

This command is used to manage temporary route entries.

### Syntax

```
temporary-route {add destination_address netmask gateway_address | delete
destination_address}
```

Table 2.17: # temporary-route

add	<i>destination_address netmask gateway_address</i>	Adds a temporary route entry.
delete	<i>destination_address</i>	Deletes a temporary route entry.

## # test

This command is used to test subsystems. A `test http get` command to a particular origin server or URL, for example, can verify Layer 3 connectivity and also verify upper layer functionality.

### Syntax

```
test http {get url | loopback}
```

Table 2.18: # test

http	get <i>url</i>	Performs a test Get of an HTTP object specified by <i>url</i> .
	loopback	Performs a loopback test.

## Examples

```
SGOS# test http loopback

Type escape sequence to abort.
Executing HTTP loopback test
Measured throughput rate is 16688.96 Kbytes/sec
HTTP loopback test passed

SGOS# test http get http://www.google.com

Type escape sequence to abort.
Executing HTTP get test

* HTTP request header sent:
GET http://www.google.com/ HTTP/1.0
Host: www.google.com
User-Agent: HTTP_TEST_CLIENT
* HTTP response header rcv'd:
HTTP/1.1 200 OK
Connection: close
Date: Tue, 15 Jul 2003 22:42:12 GMT
Cache-control: private
Content-Type: text/html
Server: GWS/2.1
Content-length: 2691
Set-Cookie:
PREF=ID=500ccde1707c20ac:TM=1058308932:LM=1058308932:S=du3WuiW7FC_1J
Rgn; expires=Sun, 17-Jan-2038 19:14:07 GMT; path=/; domain=.google.com

Measured throughput rate is 66.72 Kbytes/sec
HTTP get test passed
```

## # traceroute

Use this command to trace the route to a destination. The `traceroute` command can be helpful in determining where a problem might lie between two points in a network. Use `traceroute` to trace the network path from a ProxySG back to a client or to a specific origin Web server.

Note that you can also use the `trace route` command from your client station (if supported) to trace the network path between the client, a ProxySG, and a Web server. Microsoft operating systems generally support the `trace route` command from a DOS prompt. The syntax from a Microsoft-based client is:

```
tracert [ip | hostname].
```

## Syntax

```
traceroute {IP_address | hostname}
```

Table 2.19: # traceroute

<i>ip_address</i>	Indicates the IP address of the client or origin server.
<i>hostname</i>	Indicates the hostname of the origin server.

**Example**

```

SGOS# traceroute 10.25.36.47
Type escape sequence to abort.
Executing HTTP get test
HTTP response code: HTTP/1.0 503 Service Unavailable
Throughput rate is non-deterministic
HTTP get test passed
10.25.36.47# traceroute 10.25.36.47

Type escape sequence to abort.
Tracing the route to 10.25.36.47
 1 10.25.36.47 212 0 0 0

```

**# upload**

Uploads the current access log or running configuration. Archiving a ProxySG's system configuration on a regular basis is a generally prudent measure. In the rare case of a complete system failure, restoring a ProxySG to its previous state is simplified if you recently uploaded an archived system configuration to an FTP, HTTP, or HTTPS server. The archive contains all system settings differing from system defaults, along with any forwarding and security lists installed on the ProxySG. See "Restoring an Archived ProxySG" below for instructions.

**Syntax**

**option 1:** `upload access-log {all | log log_name}`

**option 2:** `upload configuration`

Table 2.20: # upload

access-log	all	Uploads all access logs to a configured host.
	log <i>log_name</i>	Uploads a specified access log to a configured host.
configuration		Uploads running configuration to a configured host.

**Example**

```

SGOS# upload configuration
ok

```

**Restoring an Archived ProxySG**

Archive and restore operations must be done from the CLI. There is no Management Console Web interface for archive and restore.

**To Restore an Archived System Configuration:**

1. At the command prompt, enter the following command:

```

SGOS# configure network url

```

The URL must be in quotation marks, if the filename contains spaces, and must be fully-qualified (including the protocol, server name or IP address, path, and filename of the archive). The configuration archive is downloaded from the server, and the ProxySG settings are updated.

If your archived configuration filename does not contain any spaces, quotation marks surrounding the URL are unnecessary.

2. Enter the following command to restart the ProxySG with the restored settings:

```
SGOS# restart mode software
```

#### *Example*

```
SGOS> enable
Enable Password:*****
SGOS# configure network ftp://10.25.36.46/path/10.25.36.47
- Blue Coat 5000 0216214521.config
% Configuring from ftp://10.25.36.46/path/10.25.36.47 - Blue Coat 5000
0216214521.config
.
.
.
ok
```



## Chapter 3: *Privileged Mode Configure Commands*

### Configure Commands

The `configure` command allows you to configure the Blue Coat Systems ProxySG settings from your current terminal session (`configure terminal`), or by loading a text file of configuration settings from the network (`configure network`).

#### Syntax

```
configure {terminal | network url}  
configure_command  
configure_command  
.  
.  
.
```

where `configure_command` is any of the configuration commands, as shown in Table 3.1. Type a question mark after each of these commands for a list of subcommands or options with definitions.

Table 3.1: # (config)

<code>accelerated-pac</code>	Configures installation parameters for PAC file.
<code>access-log</code>	Configures the log facilities used in access logging
<code>archive-configuration</code>	Saves system configuration.
<code>attack-detection</code>	Prevents Denial of Services attacks and port scanning.
<code>bandwidth-gain</code>	Configures bandwidth gain.
<code>bandwidth-management</code>	Configures bandwidth management settings.
<code>banner</code>	Defines a login banner.
<code>bridge</code>	Configures bridging.
<code>bypass-list</code>	Configures bypass list settings.
<code>caching</code>	Modifies caching parameters.
<code>clock</code>	Manages the system clock.
<code>content</code>	Adds or deletes objects from the ProxySG.
<code>content-filter</code>	Configures the content filter.
<code>diagnostics</code>	Configures remote diagnostics.
<code>dns</code>	Modifies DNS settings.
<code>dynamic-bypass</code>	Modifies dynamic bypass configuration.
<code>event-log</code>	Configures event log parameters.
<code>exceptions</code>	Configures built-in and user-defined exception response objects.
<code>exit</code>	Returns to the previous prompt.
<code>external-services</code>	Configures external services.
<code>failover</code>	Configures failover.
<code>forwarding</code>	Configures forwarding parameters.
<code>front-panel</code>	Configures front panel behavior.
<code>ftp</code>	Configures FTP parameters.

Table 3.1: # (config) (Continued)

health-check	Configures health check entries.
hide-advanced	Disables commands for advanced subsystems.
hostname	Sets the system hostname.
http	Configures HTTP parameters.
icp	Configures ICP parameters.
identd	Configures IDENTD parameters.
im	Configures IM parameters.
inline	Installs configurations from console input.
installed-systems	Maintains the list of currently installed ProxySG systems.
interface	Specifies an interface to configure.
ip-default-gateway	Specifies the default IP gateway.
license-key	Configures license key settings.
line-vty	Configures a terminal line.
load	Loads an installable list.
netbios	Configures NETBIOS parameters.
no	Clears certain parameters.
ntp	Modifies NTP parameters.
policy	Specifies CPL rules.
profile	Shows the system profile.
restart	System restart behavior.
return-to-sender	IP “return to sender” behavior.
reveal-advanced	Enables commands for advanced subsystems.
rip	Modifies RIP configuration.
security	Modifies security parameters.
serial-number	Configures serial number.
services	Configures protocol attributes.
session-monitor	Configures monitor RADIUS accounting messages and maintains a session table based on the information in these messages.
shell	Configures options for the Telnet shell.
show	Shows running system information.
snmp	Modifies SNMP parameters.
socks-gateways	Configures upstream SOCKS gateways parameters.
socks-machine-id	Specifies the machine ID for SOCKS.
socks-proxy	Configures SOCKS proxy values.
ssl	Configures SSL parameters.
static-routes	Installation parameters for static routes table.
streaming	Configures streaming parameters.
tcp-ip	Configures the TCP-IP settings.
tcp-rtt	Specifies the default TCP Round Trip Time.
tcp-rtt-use	Enables or disables the default TCP Round Trip Time.

Table 3.1: #(config) (Continued)

timezone	Sets the local timezone.
upgrade-path	Identifies the network path that should be used to download system software.
virtual-ip	Configures virtual IP addresses.
wccp	Configures WCCP parameters.

**Example**

```
SGOS#(config) hide-advanced ?
  all                Hide all advanced commands
  expand             Disable expanded commands
  tcp-ip            Disable commands for TCP-IP
```

Use the `show` command to view specific configuration settings or options. Type a space and a question mark after the `show` command to see a list of all commands available for this command.

**Example**

```
SGOS#(config) show ?
  accelerated-pac    Accelerated PAC file
  access-log         Access log settings
  archive-configuration Archive configuration settings

SGOS#(config) show accelerated-pac
; Empty Accelerated pac object
```

**#(config) accelerated-pac**

Normally, a Web server serves the PAC file to client browsers. This feature allows you to load a PAC file onto the ProxySG for high performance PAC file serving right from the ProxySG. There are two ways to create an Accelerated PAC file: (1) customize the default PAC file and save it as a new file, or (2) create a new custom PAC file. In either case, it is important that the client instructions for configuring ProxySG settings contain the URL of the Accelerated-PAC file. Clients load PAC files from:

```
http://your_ProxySG_appliance:8081/accelerated_pac_base.pac.
```

**Syntax**

**option 1:** `accelerated-pac no path`

**option 2:** `accelerated-pac path url`

Table 3.2: #(config) accelerated-pac

no path		Clears the network path to download PAC file.
path	url	Specifies the location to which the PAC file should be downloaded.

### Example

```
SGOS#(config) accelerated-pac path 10.25.36.47
ok
```

## #(config) access-log

The ProxySG can maintain an access log for each HTTP request made. The access log can be stored in one of three formats, which can be read by a variety of reporting utilities. See the “Access Log Formats” appendix in the *Blue Coat Configuration and Management Guide* for additional information on log formats.

### Syntax

```
access-log
```

This changes the prompt to:

```
SGOS#(config access-log)
```

#### -subcommands-

**option 1:** create

sub-option 1: log *log\_name*

sub-option 2: format *format\_name*

**option 2:** cancel-upload

sub-option 1: all

sub-option 2: log *log\_name*

**option 3:** default-logging {icp | ftp | http | im | mms | p2p | rtsp | socks |  
tcp-tunnel | telnet} *log\_name*

**option 4:** delete

sub-option 1: log *log\_name*

sub-option 2: format *format\_name*

**option 5:** disable

**option 6:** early-upload *megabytes*

**option 7:** edit

sub-option 1: log *log\_name*—changes the prompt (see “#(config access-log) edit log  
log\_name” on page 63)

sub-option 2: format *format\_name*—changes the prompt (see “#(config access-log) edit  
format format\_name” on page 68)

**option 8:** enable

**option 9:** exit

**option 10:** max-log-size *megabytes*

**option 11:** no default-logging {icp | ftp | http | im | mms | p2p | rtsp | socks |  
tcp-tunnel | telnet}

**option 12:** overflow-policy

sub-option 1: delete

sub-option 2: stop

**option 13:**upload

sub-option 1: all

sub-option 2: log *log\_name*

**option 14:**view

sub-option 1: [log [brief | *log\_name*]]

sub-option 2: [format [brief | *format\_name*]]

sub-option 3: [statistics [*log\_name*]]

sub-option 4: [default-logging]

**Table 3.3:** #(config access-log)

create	log <i>log_name</i>	Creates an access log.
	format <i>format_name</i>	Creates an access log format.
cancel-upload	all	Cancels upload for all logs.
	log <i>log_name</i>	Cancels upload for a log.
default-logging	icp <i>log_name</i>	Sets the default log for the ICP protocol.
	ftp <i>log_name</i>	Sets the default log for the FTP protocol.
	http <i>log_name</i>	Sets the default log for the HTTP/HTTPS protocol.
	im <i>log_name</i>	Sets the default log for the IM protocol.
	mms <i>log_name</i>	Sets the default log for the MMS protocol.
	p2p <i>log_name</i>	Sets the default log for the Peer-to-Peer protocol.
	rtsp <i>log_name</i>	Sets the default log for the Real Media/QuickTime protocol.
	socks <i>log_name</i>	Sets the default log for the SOCKS protocol.
	tcp-tunnel <i>log_name</i>	Sets the default log for the TCP-tunnel protocol.
delete	log <i>log_name</i>	Deletes an access log.
	format <i>format_name</i>	Deletes an access log format.
disable		Disables access logging.
early-upload	<i>megabytes</i>	Sets the log size in megabytes that triggers an early upload.
edit	log <i>log_name</i>	Changes the prompt. See “#(config access-log) edit log <i>log_name</i> ” on page 63.
	format <i>format_name</i>	changes the prompt. See “#(config access-log) edit format <i>format_name</i> ” on page 68.
enable		Enables access logging.

Table 3.3: #(config access-log) (Continued)

exit		Exits configure access-log mode and returns to configure mode.
max-log-size	<i>megabytes</i>	Sets the maximum size in megabytes that logs can reach.
no default-logging	icp	Disables default logging for the ICP protocol.
	ftp	Disables default logging for the FTP protocol.
	http	Disables default logging for the HTTP/HTTPS protocol.
	im	Disables default logging for the IM protocol.
	mms	Disables default logging for the MMS protocol.
	p2p	Disables default logging for the Peer-to-Peer protocol.
	rtsp	Disables default logging for the Real Media/QuickTime protocol.
	socks	Disables default logging for the SOCKS protocol.
	tcp-tunnel	Disables default logging for the TCP-tunnel protocol.
overflow-policy	telnet	Disables default logging for the Telnet protocol.
	delete	Deletes the oldest log entries (up to the entire log).
upload	stop	Stops access logging until logs are uploaded.
	all	Uploads all logs.
view	log <i>log_name</i>	Uploads a log.
		Shows access logging settings.
	[log [brief   <i>log_name</i> ]]	Shows the entire access log configuration, a brief version of the access log configuration, or the configuration for a specific access log.
	[format [brief   <i>format_name</i> ]]	Shows the entire log format configuration, a brief version of the log format configuration, or the configuration for a specific log format.
	[statistics [ <i>log_name</i> ]]	Shows access log statistics for all logs or for the specified log.
	[default-logging]	Shows the access log default policy.

**Example**

```

SGOS#(config) access-log
SGOS#(config access-log) create log test
ok
SGOS#(config access-log) max-log-size 1028
ok
SGOS#(config access-log) overflow-policy delete
ok

```

View the results. (This is a partial output.)

```
SGOS#(config access-log) view log
Settings:
Log name: main
Format name: main
Description:
Logs uploaded using FTP client
Logs upload as gzip file
Wait 60 seconds between server connection attempts
FTP client:
Filename format: SG_%f_%l%m%d%H%M%S.log
Filename uses utc time
Use PASV: yes
Use secure connections: no
Primary host site:
Host:
Port: 21
Path:
Username:
Password: *****
Alternate host site:
Host:
Port: 21
Path:
```

### **#(config access-log) edit log *log\_name***

Use these commands to edit an access log.

#### **Syntax**

```
access-log
```

This changes the prompt to:

```
SGOS#(config access-log)
```

```
edit log log_name
```

This changes the prompt to:

```
SGOS#(config log log_name)
```

#### **-subcommands-**

**option 1:** bandwidth-class *bwm\_class\_name*

**option 2:** client-type

sub-option 1: custom

sub-option 2: ftp

sub-option 3: http

sub-option 4: none

sub-option 5: websense

**option 3:** commands

sub-option 1: cancel-upload

```
sub-option 2: close-connection
sub-option 3: delete-logs
sub-option 4: open-connection
sub-option 5: rotate-remote-log
sub-option 6: send-keep-alive
sub-option 7: test-upload
sub-option 8: upload-now

option 4: connect-wait-time seconds
option 5: continuous-upload
sub-option 1: enable
sub-option 2: keep-alive seconds
sub-option 3: lag-time seconds
sub-option 4: rotate-remote {daily rotation_hour (0-23) | hourly hours [minutes] }

option 6: custom-client
sub-option 1: alternate hostname [port]
sub-option 2: primary hostname [port]
sub-option 3: secure {no | yes}

option 7: description description
option 8: early-upload megabytes
option 9: encryption certificate certificate_name
option 10: exit
option 11: format-name format_name
option 12: ftp-client
sub-option 1: alternate {encrypted-password encrypted_password | host hostname
                        [port] | password password | path path | username username}
sub-option 2: filename format
sub-option 3: no {alternate | filename | primary}
sub-option 4: pasv {no | yes}
sub-option 5: primary {encrypted-password encrypted_password | host hostname
                        [port] | password password | path path | username username}
sub-option 6: secure {no | yes}
sub-option 7: time-format {local | utc}

option 13: http-client
sub-option 1: alternate {encrypted-password encrypted_password | host hostname
                        [port] | password password | path path | username username}
sub-option 2: filename format
sub-option 3: no {alternate | filename | primary}
sub-option 4: primary {encrypted-password encrypted_password | host hostname
                        [port] | password password | path path | username username}
sub-option 5: secure {no | yes}
```



```

sub-option 6: time-format {local | utc}
option 14:no {encryption | bandwidth-class}
option 15:periodic-upload
sub-option 1: enable
sub-option 2: upload-interval {daily upload_hour (0-23) | hourly hours [minutes]}
option 16:remote-size megabytes
option 17:signing keyring_id
option 18:upload-type {gzip | text}
option 19:view
option 20:websense-client
sub-option 1: alternate hostname [port]
sub-option 2: primary hostname [port]

```

Table 3.4: #(config access-log log *log\_name*)

bandwidth-class	<i>bwm_class_name</i>	Specifies a bandwidth-management class for managing the bandwidth of this log. <b>IMPORTANT:</b> In order to bandwidth-manage this log, bandwidth management must be enabled. Bandwidth management is enabled by default if you have a valid bandwidth-management license. You must also create a bandwidth class for this access log (in bandwidth-management mode) before you can select it here. See “#(config) bandwidth-management” on page 75 for more information.
client-type	custom	Uploads log using the custom client.
	ftp	Uploads log using the FTP client.
	http	Uploads log using the HTTP client.
	none	Disables uploads for this log.
	websense	Uploads log using the Websense LogServer protocol.

Table 3.4: #(config access-log log *log\_name*) (Continued)

commands	cancel-upload	Cancels a pending access log upload.
	close-connection	Closes a manually opened connection to the remote server.
	delete-logs	Permanently deletes all access logs on the ProxySG.
	open-connection	Manually opens a connection to the remote server.
	rotate-remote-log	Switches to a new remote logfile.
	send-keep-alive	Sends a keep-alive log packet to the remote server.
	test-upload	Tests the upload configuration by uploading a verification file.
	upload-now	Uploads access log now.
connect-wait-time	<i>seconds</i>	Sets time to wait between server connect attempts.
continuous-upload	enable	Uploads access log continuously to remote server.
	keep-alive <i>seconds</i>	Sets the interval between keep-alive log packets.
	lag-time <i>seconds</i>	Sets the maximum time between log packets (text upload only).
	rotate-remote {daily <i>rotation_hour</i> (0-23)   hourly <i>hours</i> [ <i>minutes</i> ]}	Specifies when to switch to new remote logfile.
custom-client	alternate <i>hostname</i> [ <i>port</i> ]	Configures the alternate custom server address.
	primary <i>hostname</i> [ <i>port</i> ]	Configures the primary custom server address.
	secure {no   yes}	Selects whether to use secure connections (SSL). The default is no. If yes, the <i>hostname</i> must match the hostname in the certificate presented by the server.
description	<i>description</i>	Sets the log description.
early-upload	<i>megabytes</i>	Sets log size in MB which triggers an early upload.
encryption	certificate <i>certificate_name</i>	Specifies access-log encryption settings.
exit		Exits configure log <i>log_name</i> mode and returns to access-log mode.
format-name	<i>format_name</i>	Sets the log format.

Table 3.4: #(config access-log log log\_name) (Continued)

ftp-client	alternate {encrypted-password encrypted_password   host hostname [port]   password password   path path   username username}	Configures the alternate FTP host site.
	filename format	Configures the remote filename format.
	no {alternate   filename   primary}	Deletes FTP client parameters.
	pasv {no   yes}	Sets whether PASV command is sent.
	primary {encrypted-password encrypted_password   host hostname [port]   password password   path path   username username}	Configures the primary FTP host site.
	secure {no   yes}	Selects whether to use secure connections (FTPS). The default is no. If yes, the hostname must match the hostname in the certificate presented by the server.
	time-format {local   utc}	Selects the time format to use within upload filename.
http-client	alternate {encrypted-password encrypted_password   host hostname [port]   password password   path path   username username}	Configures the alternate HTTP host site.
	filename format	Configures the remote filename format.
	no {alternate   filename   primary}	Deletes HTTP client parameters.
	primary {encrypted-password encrypted_password   host hostname [port]   password password   path path   username username}	Configures the primary HTTP host site.
	secure {no   yes}	Selects whether to use secure connections (HTTPS). The default is no. If yes, the hostname must match the hostname in the certificate presented by the server.
	time-format {local   utc}	Selects the time format to use within upload filename.

Table 3.4: #(config access-log log log\_name) (Continued)

no	encryption	Disables access-log encryption for this log.
	bandwidth-class	Disables bandwidth management for this log.
	signing	Disables digital signing for this log.
periodic-upload	enable	Uploads access log daily/hourly to remote server.
	upload-interval {daily upload_hour (0-23)   hourly hours [minutes]}	Specifies access log upload interval.
remote-size	megabytes	Sets maximum size in MB of remote log files.
signing	keyring_id	Specifies the keyring to be used for digital signatures.
upload-type	{gzip   text}	Sets upload file type (gzip or text).
view		Shows log settings.
websense-client	alternate hostname [port]	Configures the alternate websense server address.
	primary hostname [port]	Configures the primary websense server address.

**Example**

```

SGOS#(config) access-log
SGOS#(config access-log) edit log testlog
SGOS#(config log testlog) upload-type gzip
ok
SGOS#(config log testlog) exit
SGOS#(config access-log) exit
SGOS#(config)

```

**#(config access-log) edit format format\_name**

Use these commands to edit an access log format.

**Syntax**

```
access-log
```

This changes the prompt to:

```
SGOS#(config access-log)
```

```
edit format format_name
```

This changes the prompt to:

```
SGOS#(config format format_name)
```

**-subcommands-**

**option 1:** exit

**option 2:** multi-valued-header-policy

sub-option 1: log-all-headers

```

sub-option 2: log-first-header
sub-option 3: log-last-header
option 3: type
sub-option 1: custom format_string
sub-option 2: elff format_string
option 4: view

```

Table 3.5: #(config format *format\_name*)

exit		Exits configure format <i>format_name</i> mode and returns to access-log mode.
multi-valued-header-policy	log-all-headers	Sets multi-valued header policy to log all headers.
	log-first-header	Sets multi-valued header policy to log the first header.
	log-last-header	Sets multi-valued header policy to log the last header.
type	custom <i>format_string</i>	Specifies custom logging format.
	elff <i>format_string</i>	Specifies W3C extended log file format.
view		Shows the format settings.

**Example**

```

SGOS#(config) access-log
SGOS#(config access-log) edit format testformat
SGOS#(config format testformat) multi-valued-header-policy log-all-headers
ok
SGOS#(config format testformat) exit
SGOS#(config access-log) exit
SGOS#(config)

```

 **#(config) archive-configuration**

Archiving a ProxySG system configuration on a regular basis is always a good idea. In the rare case of a complete system failure, restoring a ProxySG to its previous state is simplified by loading an archived system configuration from an FTP, HTTP, or HTTPS server. The archive contains all system settings differing from system defaults, along with any forwarding and security lists installed on the ProxySG.

Archive and restore operations must be done from the CLI. There is no Management Console Web interface for archive and restore. For details, see “Restoring an Archived ProxySG” on page 55.

**Syntax**

```

option 1: archive-configuration encrypted-password encrypted_password
option 2: archive-configuration filename-prefix filename
option 3: archive-configuration host host_name
option 4: archive-configuration password password
option 5: archive-configuration path path

```

**option 6:** archive-configuration protocol {ftp | tftp}

**option 7:** archive-configuration username *username*

Table 3.6: #(config) archive-configuration

encrypted-password	<i>encrypted_password</i>	Encrypted password for upload host (not required for TFTP).
filename-prefix	<i>filename</i>	Specifies the prefix that should be applied to the archive configuration on upload.
host	<i>host_name</i>	Specifies the FTP host to which the archive configuration should be uploaded.
password	<i>password</i>	Specifies the password for the FTP host to which the archive configuration should be uploaded.
path	<i>path</i>	Specifies the path to the FTP host to which the archive configuration should be uploaded.
protocol	ftp	Indicates the upload protocol to be used for the archive configuration using FTP.
	tftp	Indicates the upload protocol to be used for the archive configuration using TFTP.
username	<i>username</i>	Specifies the username for the FTP or FTP host to which the archive configuration should be uploaded.

#### Example

```
SGOS#(config) archive-configuration host host3
ok
```

## #(config) attack-detection

The ProxySG can reduce the effects of distributed denial of service (DDoS) attacks and port scanning, two of the most common virus infections.

The ProxySG prevents attacks by limiting the number of TCP connections from each client IP address and either will not respond to connection attempts from a client already at this limit or will reset the connection.

### Syntax

attack-detection

This changes the prompt to:

```
SGOS#(config attack-detection)
```

#### -subcommands-

**option 1:** client—changes the prompt to (config client)

sub-option 1: block *ip\_address* [*minutes*]

sub-option 2: create *ip\_address* or *ip\_address\_and\_length*

```
sub-option 3: default {block-action {drop | send-tcp-rst} | connection-limit
number_of_tcp_connections | failure-limit number_of_requests | unblock-time
minutes | warning-limit number_of_warnings}
sub-option 4: delete ip_address or ip_address_and_length
sub-option 5: disable-limits
sub-option 6: edit ip_address—changes the prompt to (config client ip_address)
{block-action {drop | send-tcp-rst} | connection-limit number_of_tcp_connections |
exit | failure-limit number_of_requests | no {connection-limit | failure-limit |
warning-limit | unblock-time} | unblock-time minutes | view | warning-limit
number_of_warnings}
sub-option 7: enable-limits
sub-option 8: exit
sub-option 9: interval minutes
sub-option 10: no default {connection-limit | failure-limit | warning-limit |
unblock-time}
sub-option 11: view [blocked | connections | statistics]
sub-option 12: unblock ip_address
```

**option 2:** exit

**option 3:** server—changes the prompt to (config server)

```
sub-option 1: create hostname
sub-option 2: delete hostname
sub-option 3: edit hostname—changes the prompt to (config server hostname) {add
hostname | exit | remove hostname | request-limit number_of_requests | view}
sub-option 4: exit
sub-option 5: view [statistics]
```

**option 4:** view

```
sub-option 1: client [blocked | connections | statistics]
sub-option 2: configuration
sub-option 3: server [statistics]
```

Table 3.7: #(config attack-detection)

client			Changes the prompt to (config client).
	block <i>ip_address</i> [ <i>minutes</i> ]		Blocks a specific IP address for the number of minutes listed. If the optional <i>minutes</i> argument is omitted, the client is blocked until explicitly unblocked.
	create <i>ip_address</i> or <i>ip_address_and_length</i>		Creates a client with the specified IP address or subnet.
	default block-action {drop   send-tcp-rst}   connection-limit <i>integer_between_1_and_65535</i>   failure-limit <i>integer_between_1_and_500</i>   unblock-time <i>minutes_between_10_and_1440</i>   warning-limit <i>integer_between_1_and_100</i>		<p><i>Default</i> indicates the values that are used if a client does not have specific limits set. These settings can be overridden on a per-client basis.</p> <p>If they are modified on a per-client basis, the specified limits become the default for new clients. To change the limits on a per-client basis, see <i>edit</i>, below.</p> <p>System defaults for attack-detection limits are:</p> <ul style="list-style-type: none"> <li>• block-action: drop</li> <li>• connection-limit: 100</li> <li>• failure-limit: 50</li> <li>• unblock-time: unlimited</li> <li>• warning-limit: 10</li> </ul>
	delete <i>ip_address</i> or <i>ip_address_and_length</i>		Deletes the specified client.
	disable-limits		Disables attack detection.
	edit <i>ip_address</i>		Changes the prompt to (config client <i>ip_address</i> ).
		block-action {drop   send-tcp-rst}	Indicates the behavior when the client is at the maximum number of connections or exceeds the warning limit: drop connections that are over the limit or send TCP RST for connections over the limit. The default is drop.
		connection-limit <i>integer</i>	Indicates the number of simultaneous connections between 1 and 65535. The default is 100.
		exit	Exits the (config client <i>ip_address</i> ) submode and returns to (config client) mode.
		failure-limit <i>integer</i>	Indicates the maximum number of failed requests a client is allowed before the proxy starts issuing warnings. Default is 50. This limit can be modified on a per-client basis.
		no {connection-limit   failure-limit   unblock-time   warning-limit}	<p>Clears the specified limits on a per-client basis.</p> <p>If you edit an existing client's limits to a smaller value, the new value only applies to new connections to that client. For example, if the old value was 10 simultaneous connections and the new value is 5, existing connections above 5 will not be dropped.</p>



Table 3.7: #(config attack-detection) (Continued)

	unblock-time <i>minutes</i>	Indicates the amount of time a client is blocked at the network level when the client-warning-limit is exceeded. Time must be a multiple of 10 minutes, up to a maximum of 1440. The default is unlimited.
	view	Displays the limits for this client.
	warning-limit <i>integer</i>	Indicates the number of warnings sent to the client before the client is blocked at the network level and the administrator is notified. The default is 10; the maximum is 100.
	enable-limits	Enables attack detection. This is a global setting and cannot be configured individually for specific clients.
	exit	Exits the (config client <i>ip_address</i> ) mode and returns to (config attack-detection) mode.
	interval <i>integer</i>	Indicates the amount of time, in multiples of 10 minutes, that client activity is monitored. The default is 20. Note that this is a global limit and cannot be modified for individual clients.
	no default {connection-limit   failure-limit   unblock-time   warning-limit}	Clears the specified limit settings. These settings are applied to all new clients.
	view [blocked   connections   statistics]	Views all limits for all clients, or you can show clients blocked at the network level, view the client connection table, or view client request failure statistics.
	unblock <i>ip_address</i>	Releases a specific IP address.
exit		Exits (config attack-detection) mode and returns to (config) mode.

Table 3.7: #(config attack-detection) (Continued)

server			Changes the prompt to (config server) .
	create <i>hostname</i>		Creates a server or server group that is identified by the hostname.
	delete <i>hostname</i>		Deletes a server or server group.
	edit <i>hostname</i>		Changes the prompt to (config server <i>hostname</i> ) .
		add <i>hostname</i>	Adds an additional server to this server group.
		exit	Exits the (config server <i>hostname</i> ) submode and returns to (config server) mode.
		remove <i>hostname</i>	Removes a server from this group. You cannot remove the original server from the group.
		request-limit <i>integer</i>	Indicates the number of simultaneous requests allowed from this server or server group. The default is 1000.
		view	Displays the request limit for this server or server group.
view	exit		Exits the (config server <i>hostname</i> ) submode and returns to (config server) mode.
	view		Displays the request limit for all servers or server groups.
	client [blocked   connections   statistics]		Displays client information. The <code>blocked</code> option displays the clients blocked at the network level, the <code>connections</code> option displays the client connection table, and the <code>statistics</code> option displays client request failure statistics.
	configuration		Allows you to view attack-detection configuration settings or the number of current connections.
	server [statistics]		Displays server information. The <code>statistics</code> option displays server-connection failure statistics.

**Example**

```

SGOS#(config) attack-detection
SGOS#(config attack-detection) client
SGOS#(config client) view
Client limits enabled:           true
Client interval:                 20 minutes

Default client limits:
Client connection limit:         700
Client failure limit:            50
Client warning limit:            10
Blocked client action:           Drop
Client connection unblock time:  unlimited

Client limits for 10.9.17.159:
Client connection limit:         unlimited
Client failure limit:            unlimited
Client warning limit:            unlimited

```

```

Blocked client action:      Drop
Client connection unblock time: unlimited

Client limits for 10.9.17.134:
Client connection limit:    700
Client failure limit:       50
Client warning limit:       10
Blocked client action:      Drop
Client connection unblock time: unlimited

```

## #(config) bandwidth-gain

Bandwidth gain is a measure of the effective increase of server bandwidth resulting from the client's use of a content accelerator. For example, a bandwidth gain of 100% means that traffic volume from the ProxySG to its clients is twice as great as the traffic volume being delivered to the ProxySG from the origin server(s). Using bandwidth gain mode can provide substantial gains in apparent performance.

Keep in mind that bandwidth gain is a relative measure of the ProxySG's ability to amplify traffic volume between an origin server and the clients served by the ProxySG.

### Syntax

#### -subcommands-

**option 1:** bandwidth-gain disable

**option 2:** bandwidth-gain enable

Table 3.8: #(config) bandwidth-gain

disable		Disables bandwidth-gain mode.
enable		Enables bandwidth-gain mode.

#### Example

```

SGOS#(config) bandwidth-gain enable
ok

```

## #(config) bandwidth-management

Bandwidth management allows you to classify, control, and, if required, limit the amount of bandwidth used by a class of network traffic flowing into or out of the ProxySG.

### Syntax

```
bandwidth-management
```

This changes the prompt to:

```
SGOS#(config bandwidth-management)
```

#### -subcommands-

**option 1:** create *class\_name*

**option 2:** delete *class\_name*

**option 3:** disable

**option 4:** edit *class\_name*—changes the prompt (see “#(config bandwidth-management) edit *class\_name*” on page 76)

**option 5:** enable

**option 6:** exit

**option 7:** view

sub-option 1: configuration [*bandwidth\_class*]

sub-option 2: statistics [*bandwidth\_class*]

Table 3.9: #(config bandwidth-management)

create	<i>class_name</i>	Creates a bandwidth-management class.
delete	<i>class_name</i>	Deletes the specified bandwidth-management class.
delete	<i>class_name</i>	Deletes a bandwidth-management class. Note that if another class has a reference to the specified class, this command will fail.
disable		Disables bandwidth-management.
edit	<i>class_name</i>	Puts you into a submode that allows you to configure settings for the specified class. See “#(config bandwidth-management) edit <i>class_name</i> ” on page 76 for information.
enable		Enables bandwidth-management.
exit		Exits configure bandwidth-management mode and returns to configure mode.
view	configuration [ <i>bandwidth_class</i> ]	Displays bandwidth-management configuration for all bandwidth-management classes or for the class specified.
	statistics [ <i>bandwidth_class</i> ]	Displays bandwidth-management statistics for all bandwidth-management classes or for the class specified.

### Example

```
SGOS#(config) bandwidth-management
SGOS#(config bandwidth-management) enable
ok
SGOS#(config bandwidth-management) create Office_A
ok
SGOS#(config bandwidth-management) edit Office_A
SGOS#(config bw-class Office_A) exit
SGOS#(config bandwidth-management) exit
SGOS#(config)
```

## #(config bandwidth-management) edit *class\_name*

This command allows you to edit a bandwidth-management class.

## Syntax

bandwidth-management

This changes the prompt to:

```
SGOS#(config bandwidth-management)
```

```
edit class_name
```

This changes the prompt to:

```
SGOS#(config bandwidth-management class_name)
```

### -subcommands-

**option 1:** exit

**option 2:** max-bandwidth *maximum\_in\_kbps*

**option 3:** min-bandwidth *minimum\_in\_kbps*

**option 4:** no

sub-option 1: max-bandwidth

sub-option 2: min-bandwidth

sub-option 3: parent

**option 5:** parent *class\_name*

**option 6:** priority *value\_from\_0\_to\_7*

**option 7:** view [children]

Table 3.10: #(config bandwidth-management *class\_name*)

exit		Exits configure bandwidth-management <i>class_name</i> mode and returns to configure bandwidth-management mode.
max-bandwidth	<i>maximum_in_kbps</i>	Sets the maximum bandwidth for this class.
min-bandwidth	<i>maximum_in_kbps</i>	Sets the minimum bandwidth for this class.
no	max-bandwidth	Resets the maximum bandwidth of this bandwidth-management class to the default (unlimited—no maximum).
	min-bandwidth	Resets the minimum bandwidth of this bandwidth-management class to the default (no minimum).
	parent	Clears the parent from this bandwidth-management class.
parent	<i>class_name</i>	Makes the specified class a parent of the class being configured.
priority	<i>value_from_0_to_7</i>	Sets the priority for this bandwidth-management class. The lowest priority level is 0 and the highest is 7.
view	[children]	Displays the settings for this bandwidth-management class or displays the settings for the children of this bandwidth-management class.

### Example

```
SGOS#(config) bandwidth-management
SGOS#(config bandwidth-management) edit CEO_A
SGOS#(config bw-class CEO_A) parent Office_A
    ok
SGOS#(config bw-class CEO_A) priority 2
    ok
SGOS#(config bw-class CEO_A) exit
SGOS#(config bandwidth-management) exit
SGOS#(config)
```

## #(config) banner

This command enables you to define a login banner for your users.

### Syntax

**option 1:** banner login *string*

**option 2:** banner no login

Table 3.11: #(config) banner

login	<i>string</i>	Sets the login banner to the value of <i>string</i> .
no login		Sets the login banner to null.

### Example

```
SGOS#(config) banner login "Sales and Marketing Intranet Web"
    ok
```

## #(config) bridge

This command allows you to configure bridging.

### Syntax

bridge

This changes the prompt to:

```
SGOS#(config bridge)
```

#### -subcommands-

**option 1:** bandwidth-class *bw\_class\_name*

**option 2:** create

**option 3:** delete

**option 4:** edit—changes the prompt (see “#(config bridge) edit bridge\_name” on page 79)

**option 5:** exit

**option 6:** no bandwidth-class

**option 7:** view

```

sub-option 1: configuration [bridge_name]
sub-option 2: statistics bridge_name
sub-option 3: fwtable bridge_name

```

**Table 3.12:** # (config bridge)

bandwidth-class	<i>bw_class_name</i>	Sets a bandwidth class for this bridge.  IMPORTANT: In order to bandwidth-manage this bridge, bandwidth management must be enabled. Bandwidth management is enabled by default if you have a valid bandwidth-management license.  You must also create a bandwidth class for bridging (in bandwidth-management mode) before you can select it here. See “# (config) bandwidth-management” on page 75 for more information.
create	<i>bridge_name</i>	Creates a bridge.
delete	<i>bridge_name</i>	Deletes a bridge.
edit	<i>bridge_name</i>	Changes the prompt. See “# (config bridge) edit bridge_name” on page 79.
exit		Exits configure bridge mode and returns to configure mode.
view	configuration [bridge_name]	Displays the bridge configuration for the specified bridge or for all bridges at once.
	statistics <i>bridge_name</i>	Displays the bridge statistics for the specified bridge.
	fwtable <i>bridge_name</i>	Displays the forwarding table for the specified bridge.

**Example**

```

SGOS# (config) bridge
SGOS# (config bridge) create test
ok
SGOS# (config bridge) exit
SGOS# (config)

```

**#(config bridge) edit *bridge\_name***

This command allows you to edit a bridge.

**Syntax**

```
bridge
```

This changes the prompt to:

```

SGOS# (config bridge)
edit bridge_name

```

This changes the prompt to:

SGOS#(config bridge *bridge\_name*)

**-subcommands-**

**option 1:** accept-inbound

**option 2:** clear-fwtable

**option 3:** clear-statistics

**option 4:** exit

**option 5:** failover

**option 6:** instructions {accelerated-pac | central-pac *url* | default-pac | proxy}

**option 7:** ip-address *ip\_address*

**option 8:** mtu-size *mtu\_size*

**option 9:** no {accept-inbound | port *port\_num* | failover}

**option 10:** port *port\_number*

**option 11:** subnet-mask *subnet\_mask*

**option 12:** view {configuration | fwtable | statistics}

Table 3.13: #(config bridge *bridge\_name*)

accept-inbound		Allows inbound connections on this interface.
clear-fwtable		Clears bridge forwarding table.
clear-statistics		Clears bridge statistics.
exit		Exits configure bridge <i>bridge_name</i> mode and returns to configure bridge mode.
failover	<i>failover_group</i>	Associates this bridge to a failover group.
instructions	accelerated-pac	Helps configure browser to use your accelerated pac file.
	central-pac <i>url</i>	Helps configure browser to use your pac file.
	default-pac	Helps configure browser to use Blue Coat Systems pac file.
	proxy	Helps configure browser to use a proxy.
ip-address	<i>ip_address</i>	Sets IP address for interface.
mtu-size	<i>mtu_size</i>	Specifies MTU (maximum transmission unit) size.
no	accept-inbound	Disallows inbound connections on this interface.
	port <i>port#</i>	Negates port settings.
	failover	Negates failover settings.
port	<i>port_number</i>	Changes the prompt. See “#(config bridge <i>bridge_name</i> ) port <i>port_number</i> ” on page 81.
subnet-mask	<i>subnet_mask</i>	Sets subnet mask for interface.
view	configuration	Shows bridge configuration.
	fwtable	Shows bridge forwarding table.
	statistics	Shows bridge statistics.



**Example**

```

SGOS#(config) bridge
SGOS#(config bridge) edit b_1
SGOS#(config bridge b_1) accept-inbound
    ok
SGOS#(config bridge b_1) instructions accelerated-pac
    ok
SGOS#(config bridge b_1) exit
SGOS#(config bridge) exit
SGOS#(config)

```

**#(config bridge *bridge\_name*) port\_number****Syntax**

```
bridge
```

This changes the prompt to:

```
SGOS#(config bridge)
```

```
edit bridge_name
```

This changes the prompt to:

```
SGOS#(config bridge bridge_name)
```

```
port_number
```

This changes the prompt to:

```
SGOS#(config bridge bridge_name port_number)
```

**-subcommands-**

**option 1:** attach-interface *interface\_number*

**option 2:** exit

**option 3:** full-duplex

**option 4:** half-duplex

**option 5:** link-autosense

**option 6:** speed {10 | 100 | 1gb}

**option 7:** view

Table 3.14: #(config bridge *bridge\_name port\_number*)

attach-interface	<i>interface_number</i>	Attaches an interface for this port.
exit		Exits configure bridge <i>bridge_name port_number</i> mode and returns to configure <i>bridge_name</i> mode.
full-duplex		Configures this port for full duplex.

Table 3.14: #(config bridge *bridge\_name* *port\_number*) (Continued)

half-duplex		Configures this port for half duplex.
link-autosense		Specifies that this port should autosense network speed and duplex.
speed	10   100   1gb	Specifies the speed for this port (10 or 100 megabits/second or 1 gigabits/second).
view		Displays the bridge port settings.

**Example**

```
SGOS#(config) bridge
SGOS#(config bridge) bridge testname
SGOS#(config bridge testname) port 23
SGOS#(config bridge testname port 23) attach-interface 0
ok
SGOS#(config bridge testname port 23) full-duplex
ok
SGOS#(config bridge testname port 23) speed 100
ok
SGOS#(config bridge testname port 23) exit
SGOS#(config bridge testname) exit
SGOS#(config)
```

## #(config) bypass-list

A bypass list prevents the ProxySG from transparently accelerating requests to servers that perform IP authentication with clients. The bypass list contains IP addresses, subnet masks, and gateways. When a request matches an IP address and subnet mask specification in the bypass list, the request is sent to the designated gateway. A bypass list is only used for transparent caching.

There are two types of bypass lists: local and central.

To use bypass routes, create a text file that contains a list of address specifications. The file should be named with a .txt extension. Once you have created the bypass list, place it on an HTTP server so it can be installed onto the ProxySG.

You can create your own central bypass list to manage multiple ProxySG Appliances, or you can use the central bypass list maintained by Blue Coat Systems Technical Support at:

<http://www.bluecoat.com/support/subscriptions/CentralBypassList.txt>

The central bypass list maintained by Blue Coat Systems contains addresses Blue Coat Systems has identified as using client authentication.

### Syntax

```
option 1: bypass-list central-path url
option 2: bypass-list local-path url
option 3: bypass-list no {central-path | local-path | notify | subscribe}
option 4: bypass-list notify
option 5: bypass-list poll-now
```

**option 6:** `bypass-list subscribe`

**Table 3.15:** `#(config) bypass-list`

<code>central-path</code>	<code>url</code>	Specifies the network path used to download the central bypass list.
<code>local-path</code>	<code>url</code>	Specifies the network path used to download the local bypass list.
<code>no</code>	<code>central-path</code>	Sets the central bypass list path to null.
	<code>local-path</code>	Sets the local bypass list path to null.
	<code>notify</code>	Instructs the ProxySG to not send an e-mail notification if the central bypass list changes.
	<code>subscribe</code>	Specifies that you do not want to change the bypass list when changes are made to the central bypass list.
<code>notify</code>		Instructs the ProxySG to send an e-mail notification if the central bypass list changes.
<code>poll-now</code>		Checks the central bypass list for changes.
<code>subscribe</code>		Specifies to change the bypass list when changes are made to the central bypass list.

#### Example

```
SGOS#(config) bypass-list local-path 10.25.36.47/files/bypasslist.txt
ok
```

## #(config) caching

When a stored HTTP object expires, it is placed in a refresh list. The ProxySG processes the refresh list in the background, when it is not serving requests. Refresh policies define how the ProxySG handles the refresh process.

The HTTP caching options allow you to specify:

- Maximum object size
- Negative responses
- Refresh parameters

In addition to HTTP objects, the ProxySG can store objects requested using FTP. When the ProxySG retrieves and stores an FTP object, it uses two methods to determine how long the object should stay cached.

- If the object has a last-modified date, the ProxySG assigns a refresh date to the object that is a percentage of the last-modified date.
- If the object does not have a last-modified date, the ProxySG assigns a refresh date to the object based on a fixed period of time.

## Syntax

`caching`

This changes the prompt to:

```
SGOS#(config caching)
```

**-subcommands-**

**option 1:** `always-verify-source`

**option 2:** `exit`

**option 3:** `ftp`—changes the prompt (see “#(config caching) ftp” on page 85)

**option 4:** `max-cache-size` *megabytes*

**option 5:** `negative-response` *minutes*

**option 6:** `no` `always-verify-source`

**option 7:** `refresh` {`automatic` | `bandwidth` *kbps* | `no automatic`}

**option 8:** `view`

Table 3.16: #(config caching)

<code>always-verify-source</code>		Specifies the ProxySG to always verify the freshness of an object with the object source.
<code>ftp</code>		Changes the prompt. See “#(config caching) ftp” on page 85.
<code>max-cache-size</code>	<i>megabytes</i>	Specifies the maximum size of the cache to the value indicated by <i>megabytes</i> .
<code>negative-response</code>	<i>minutes</i>	Specifies that negative responses should be cached for the time period identified by <i>minutes</i> .
<code>no</code>	<code>always-verify-source</code>	Specifies that the ProxySG should never verify the freshness of an object with the object source.
<code>refresh</code>	<code>automatic</code>	Specifies that the ProxySG should manage the refresh bandwidth.
	<code>bandwidth</code> <i>kbps</i>	Specifies the amount of bandwidth in kilobits to utilize for maintaining object freshness.
	<code>no automatic</code>	Specifies that the ProxySG should not manage the refresh bandwidth.

**Example**

```
SGOS#(config) caching
SGOS#(config caching) always-verify-source
ok
SGOS#(config caching) max-cache-size 100
ok
SGOS#(config caching) negative-response 15
```

```

ok
SGOS#(config caching) refresh automatic
ok
SGOS#(config caching) exit
SGOS#(config)

```

## #(config caching) ftp

The FTP caching options allow you to specify:

- Transparency
- Maximum object size
- Caching objects by date
- Caching objects without a last-modified date: if an FTP object is served without a last modified date, the ProxySG caches the object for a set period of time.

### Syntax

```
caching
```

This changes the prompt to:

```
SGOS#(config caching)
```

```
ftp
```

This changes the prompt to:

```
SGOS#(config caching ftp)
```

#### -subcommands-

**option 1:** disable

**option 2:** enable

**option 3:** exit

**option 4:** type-m-percent *percent*

**option 5:** type-n-initial *hours*

**option 6:** view

Table 3.17: #(config caching ftp)

disable		Disables caching FTP objects.
enable		Enables caching FTP objects.
exit		Exits configure caching ftp mode and returns to configure caching mode.
type-m-percent	<i>percent</i>	Specifies the TTL for objects with a last-modified time.
type-n-initial	<i>hours</i>	Specifies the TTL for objects with no expiration.
view		Shows the current FTP caching settings.

### Example

```
SGOS#(config caching) ftp
SGOS#(config caching ftp) enable
ok
SGOS#(config caching ftp) max-cache-size 200
ok
SGOS#(config caching ftp) type-m-percent 20
ok
SGOS#(config caching ftp) type-n-initial 10
ok
SGOS#(config caching ftp) exit
SGOS#(config caching) exit
SGOS#(config)
```

## #(config) clock

To manage objects in the cache, a ProxySG must know the current Universal Time Coordinates (UTC) time. By default, the ProxySG attempts to connect to a Network Time Protocol (NTP) server to acquire the UTC time. The ProxySG includes a list of NTP servers available on the Internet, and attempts to connect to them in the order they appear in the NTP server list on the NTP tab. If the ProxySG cannot access any of the listed NTP servers, you must manually set the UTC time using the `clock` command.

### Syntax

**option 1:** `clock day day`

**option 2:** `clock hour hour`

**option 3:** `clock minute minute`

**option 4:** `clock month month`

**option 5:** `clock second second`

**option 6:** `clock year year`

Table 3.18: #(config) clock

day	<i>day</i>	Sets the Universal Time Code (UTC) day to the day indicated by <i>day</i> . The value can be any integer from 1 through 31.
hour	<i>hour</i>	Sets the UTC hour to the hour indicated by <i>hour</i> . The value can be any integer from 0 through 23.

Table 3.18: # (config) clock (Continued)

minute	<i>minute</i>	Sets the UTC minute to the minute indicated by <i>minute</i> . The value can be any integer from 0 through 59.
month	<i>month</i>	Sets the UTC month to the month indicated by <i>month</i> . The value can be any integer from 1 through 12.
second	<i>second</i>	Sets the UTC second to the second indicated by <i>second</i> . The value can be any integer from 0 through 59.
year	<i>year</i>	Sets the UTC year to the year indicated by <i>year</i> . The value must take the form <i>xxxx</i> .

**Example**

```

SGOS# (config) clock year 2003
ok
SGOS# (config) clock month 4
ok
SGOS# (config) clock day 1
ok
SGOS# (config) clock hour 0
ok
SGOS# (config) clock minute 30
ok
SGOS# (config) clock second 59
ok

```

**#(config) content**

Use this command to manage and manipulate content distribution requests and re-validate requests.

---

*Note:* The `content` command options are not compatible with transparent FTP.

---

**Syntax**

```

option 1: content cancel {outstanding-requests | url url}
option 2: content delete {regex regex | url url}
option 3: content distribute url [from_url]
option 4: content priority {regex priority_0-7 regex | url priority_0-7 url}
option 5: content revalidate {regex regex | url url [from_url]}

```

Table 3.19: #(config) content

cancel	outstanding-requests	Specifies to cancel all outstanding content distribution requests and re-validate requests.
	url <i>url</i>	Specifies to cancel outstanding content distribution requests and re-validate requests for the URL identified by <i>url</i> .
delete	regex <i>regex</i>	Specifies to delete content based on the regular expression identified by <i>regex</i> .
	url <i>url</i>	Specifies to delete content for the URL identified by <i>url</i> .
distribute	url [ <i>from_url</i> ]	Specifies that the content associated with <i>url</i> should be distributed from the origin server.
priority	regex <i>priority_0-7</i> <i>regex</i>	Specifies to add a content deletion policy based on the regular expression identified by <i>regex</i> .
	url <i>priority_0-7 url</i>	Specifies to add a content deletion policy for the URL identified by <i>url</i> .
revalidate	regex <i>regex</i>	Revalidates the content associated with the regular expression identified by <i>regex</i> with the origin server.
	url [ <i>from_url</i> ]	Revalidates the content associated with the <i>url</i> .

**Example**

```

SGOS#(config) content distribute http://www.bluecoat.com
Current time: Mon, 01 Apr 2003 00:34:07 GMT
ok
SGOS#(config) content revalidate url http://www.bluecoat.com
Last load time: Mon, 01 Apr 2003 00:34:07 GMT
ok
SGOS#(config) content distribute http://www.bluecoat.com
Current time: Mon, 01 Apr 2003 00:35:01 GMT
ok
SGOS#(config) content priority url 7 http://www.bluecoat.com
ok
SGOS#(config) content cancel outstanding-requests
ok
SGOS#(config) content delete url http://www.bluecoat.com
ok

```

 **#(config) content-filter**

The ProxySG offers the option of using content filtering to control the type of retrieved content and to filter requests made by clients. The ProxySG supports these content filtering methods:

- Local database

This method allows you to produce and maintain your own content-filtering list locally, through the ProxySG CLI or Management Console.



- Blue Coat Web Filter (BCWF)

BCWF is a highly effective content filtering service that can quickly learn and adapt to the working set of its users. Also, BCWF can use dynamic categorization to analyze requested Web pages in real time, blocking new unrated content on the fly, while providing the database with instant updates that impact all users without service interruption.

- Vendor-based content filtering

This method allows you to block URLs using vendor-defined categories. For this method, use content filtering solutions from the following vendors:

- i-FILTER
- InterSafe™
- Optenet
- Proventia™
- SmartFilter™
- SurfControl™
- Websense® (locally on the ProxySG and or remotely on a separate Websense Enterprise Server)
- WebWasher®

You can also combine this type of content filtering with the ProxySG policies, which use the Blue Coat Systems Policy Language.

- Denying access to URLs through policy

This method allows you to block by URL, including filtering by scheme, domain, or individual host or IP address. For this method, you define ProxySG policies, which use the Blue Coat Systems Policy Language.

Refer to the “Content Filtering” chapter of the *Blue Coat Configuration and Management Guide* and the *Blue Coat Content Policy Language Guide* for complete descriptions of these features.

## Syntax

`content-filter`

This changes the prompt to:

`SGOS#(config content-filter)`

- *subcommands*-

**option 1:** `bluecoat`—changes the prompt (see “`#(config content-filter) bluecoat`” on page 92)

**option 2:** `categories`

**option 3:** `exit`

**option 4:** `i-filter`—changes the prompt (see “`#(config content-filter) i-filter`” on page 94)

- option 5:** intersafe—changes the prompt (see “#(config content-filter) intersafe” on page 96)
- option 6:** local—changes the prompt (see “#(config content-filter) local” on page 98)
- option 7:** no review-message
- option 8:** optenet—changes the prompt (see “#(config content-filter) optenet” on page 100)
- option 9:** proventia—changes the prompt (see “#(config content-filter) proventia” on page 102)
- option 10:** provider
- sub-option 1: bluecoat {disable | enable}
  - sub-option 2: local {disable | enable}
  - sub-option 3: 3rd-party {intersafe | none | proventia | smartfilter | surfcontrol | websense | webwasher}
- option 11:** review-message
- option 12:** smartfilter—changes the prompt (see “#(config content-filter) smartfilter” on page 104)
- option 13:** surfcontrol—changes the prompt (see “#(config content-filter) surfcontrol” on page 106)
- option 14:** test-url url
- option 15:** websense—changes the prompt (see “#(config content-filter) websense” on page 108)
- option 16:** webwasher—changes the prompt (see “#(config content-filter) webwasher” on page 111)
- option 17:** view

Table 3.20: #(config content-filter)

bluecoat		Enters configuration mode for Blue Coat Web Filter. See “#(config content-filter) bluecoat” on page 92.
categories		Shows available categories.
exit		Exits configure content filter mode and returns to configure mode.
i-filter		Enters configuration mode for i-FILTER. See “#(config content-filter) i-filter” on page 94.
intersafe		Enters configuration mode for InterSafe. See “#(config content-filter) intersafe” on page 96.
local		Enters configuration mode for Local database. See “#(config content-filter) local” on page 98.
no	review message	Specifies that vendor categorization review be turned off.
optenet		Enters configuration mode for Optenet. See “#(config content-filter) optenet” on page 100.

Table 3.20: # (config content-filter) (Continued)

proventia		Enters configuration mode for Proventia. See “# (config content-filter) proventia” on page 102.
review-message		Used for categorization review for certain Content Filtering vendors. The review-message setting enables two substitutions that can be used in exceptions pages to allow users to review or dispute content categorization results.
provider	bluecoat   local {enable   disable}	Enables or disables Blue Coat Web Filter or a local user database.
provider 3rd-party	i-filter	Selects i-FILTER content filtering.
	intersafe	Selects InterSafe content filtering.
	none	Specifies that a third-party vendor not be used for content filtering.
	optenet	Selects Optenet content filtering.
	proventia	Selects Proventia Web Filter content filtering.
	smartfilter	Selects SmartFilter content filtering.
	surfcontrol	Selects SurfControl content filtering.
	websense	Selects Websense content filtering.
	webwasher	Selects Webwasher URL Filter content filtering.
smartfilter		Enters configuration mode for SmartFilter. See “# (config content-filter) smartfilter” on page 104.
surfcontrol		Enters configuration mode for SurfControl. See “# (config content-filter) surfcontrol” on page 106.
test-url	url	Displays categories for a URL assigned by the current configuration.
websense		Enters configuration mode for Websense. See “# (config content-filter) websense” on page 108.
webwasher		Enters configuration mode for WebWasher. See “# (config content-filter) webwasher” on page 111.
view		Shows the current settings for the local database (if it is in use) and the selected provider (if one is selected).

### Example

```
SGOS#(config) content-filter
SGOS#(config content-filter) provider 3rd-party proventia

loading database....
ok
SGOS#(config content-filter) exit
SGOS#(config)
```

## #(config content-filter) bluecoat

Use this command to configure Blue Coat Web Filter content filtering.

### Syntax

```
content-filter
```

This changes the prompt to:

```
SGOS#(config content-filter)
```

```
bluecoat
```

This changes the prompt to:

```
SGOS#(config bluecoat)
```

### - subcommands-

#### option 1: download

```
sub-option 1: auto
sub-option 2: day-of-week {all | friday | monday | none | saturday | sunday |
                        thursday | tuesday | wednesday}
sub-option 3: encrypted-password encrypted_password
sub-option 4: full-get-now
sub-option 5: get-now
sub-option 6: password password
sub-option 7: time-of-day 0-23
sub-option 8: url {default | url}
sub-option 9: username username
```

#### option 2: exit

#### option 3: no download

```
sub-option 1: auto
sub-option 2: day-of-week {friday | monday | saturday | sunday | thursday |
                        tuesday | wednesday}
sub-option 3: encrypted-password
sub-option 4: password
sub-option 5: url
sub-option 6: username
```

**option 4:** service

sub-option 1: disable

sub-option 2: enable

sub-option 3: mode {background | realtime | none}

**option 5:** view**Table 3.21:** # (config bluecoat)

download	auto	Enables automatic database downloads.
	day-of-week {all   friday   monday   none   saturday   sunday   thursday   tuesday   wednesday}	Specifies the day of the week for automatic downloads.
	encrypted-password <i>encrypted_password</i>	Specifies the encrypted password for the database download server.
	full-get-now	Initiates an immediate full-size database download.
	get-now	Initiates an immediate database download.
	password <i>password</i>	Specifies the password for the database download server.
	time-of-day 0-23	Specifies the time of day for automatic downloads.
	url {default   <i>url</i> }	Specifies using either the default URL or a specific URL for the database download server.
	username <i>username</i>	Specifies the username for the database download server.
exit		Exits configure bluecoat mode and returns to configure content-filter mode.
no download	auto	Disables automatic download.
	day-of-week {friday   monday   saturday   sunday   thursday   tuesday   wednesday}	Clears day(s) of the week for automatic download.
	encrypted-password	Clears the encrypted password for the database download server.
	password	Clears the password for the database download server.
	url	Clears the URL for the database download server.
	username	Clears the username for the database download server.
service	disable   enable	Enables or disables dynamic categorization.
	mode {background   realtime   none}	Configures dynamic categorization to run in the background, run in real time, or to not run.
view		Shows the current Blue Coat settings.

### Example

```
SGOS#(config) content-filter
SGOS#(config content-filter) bluecoat
SGOS#(config bluecoat) service mode background
    ok
SGOS#(config bluecoat) exit
SGOS#(config content-filter) exit
SGOS#(config)
```

## #(config content-filter) i-filter

Use this command to configure i-FILTER content filtering

### Syntax

```
content-filter
```

This changes the prompt to:

```
SGOS#(config content-filter)
```

```
i-filter
```

This changes the prompt to:

```
SGOS#(config i-filter)
```

#### - subcommands-

**option 1:** download

sub-option 1: auto

sub-option 2: day-of-week {all | friday | monday | none | saturday | sunday |  
thursday | tuesday | wednesday}

sub-option 3: encrypted-password *encrypted\_password*

sub-option 4: full-get-now

sub-option 5: get-now

sub-option 6: password *password*

sub-option 7: time-of-day *0-23*

sub-option 8: url {default | *url*}

sub-option 9: username *username*

**option 2:** exit

**option 3:** no download

sub-option 1: auto

sub-option 2: day-of-week {friday | monday | saturday | sunday | thursday | tuesday  
| wednesday}

sub-option 3: encrypted-password

sub-option 4: password

sub-option 5: url

sub-option 6: username

**option 4:** view

Table 3.22: #(config i-filter)

download	auto	Enables automatic database downloads.
	day-of-week {all   friday   monday   none   saturday   sunday   thursday   tuesday   wednesday}	Specifies the day of the week for automatic downloads.
	encrypted-password <i>encrypted_password</i>	Specifies the encrypted password for the database download server.
	full-get-now	Initiates an immediate full-size database download.
	get-now	Initiates an immediate database download.
	password <i>password</i>	Specifies the password for the database download server.
	time-of-day 0-23	Specifies the time of day for automatic downloads.
	url {default   url}	Specifies using either the default URL or a specific URL for the database download server.
	username <i>username</i>	Specifies the username for the database download server.
exit		Exits configure intersafe mode and returns to configure content-filter mode.
no download	auto	Disables automatic download.
	day-of-week {friday   monday   saturday   sunday   thursday   tuesday   wednesday}	Clears day(s) of the week for automatic download.
	encrypted-password	Clears the encrypted password for the database download server.
	password	Clears the password for the database download server.
	url	Clears the URL for the database download server.
	username	Clears the username for the database download server.
view		Shows the current InterSafe settings.

### Example

```
SGOS#(config) content-filter
SGOS#(config content-filter) i-filter
SGOS#(config i-filter) no download day-of-week mon
ok
SGOS#(config i-filter) no download day-of-week wed
ok
SGOS#(config i-filter) exit
```

```
SGOS#(config content-filter) exit  
SGOS#(config)
```

## #(config content-filter) intersafe

Use this command to configure InterSafe content filtering.

### Syntax

```
content-filter
```

This changes the prompt to:

```
SGOS#(config content-filter)
```

```
intersafe
```

This changes the prompt to:

```
SGOS#(config intersafe)
```

#### - subcommands-

**option 1:** download

```
sub-option 1: auto
```

```
sub-option 2: day-of-week {all | friday | monday | none | saturday | sunday |  
thursday | tuesday | wednesday}
```

```
sub-option 3: encrypted-password encrypted_password
```

```
sub-option 4: full-get-now
```

```
sub-option 5: get-now
```

```
sub-option 6: password password
```

```
sub-option 7: time-of-day 0-23
```

```
sub-option 8: url {default | url}
```

```
sub-option 9: username username
```

**option 2:** exit

**option 3:** no download

```
sub-option 1: auto
```

```
sub-option 2: day-of-week {friday | monday | saturday | sunday | thursday | tuesday  
| wednesday}
```

```
sub-option 3: encrypted-password
```

```
sub-option 4: password
```

```
sub-option 5: url
```

```
sub-option 6: username
```

**option 4:** view



Table 3.23: #(config intersafe)

download	auto	Enables automatic database downloads.
	day-of-week {all   friday   monday   none   saturday   sunday   thursday   tuesday   wednesday}	Specifies the day of the week for automatic downloads.
	encrypted-password <i>encrypted_password</i>	Specifies the encrypted password for the database download server.
	full-get-now	Initiates an immediate full-size database download.
	get-now	Initiates an immediate database download.
	password <i>password</i>	Specifies the password for the database download server.
	time-of-day 0-23	Specifies the time of day for automatic downloads.
	url {default   url}	Specifies using either the default URL or a specific URL for the database download server.
	username <i>username</i>	Specifies the username for the database download server.
exit		Exits configure intersafe mode and returns to configure content-filter mode.
no download	auto	Disables automatic download.
	day-of-week {friday   monday   saturday   sunday   thursday   tuesday   wednesday}	Clears day(s) of the week for automatic download.
	encrypted-password	Clears the encrypted password for the database download server.
	password	Clears the password for the database download server.
	url	Clears the URL for the database download server.
	username	Clears the username for the database download server.
view		Shows the current InterSafe settings.

**Example**

```

SGOS#(config) content-filter
SGOS#(config content-filter) intersafe
SGOS#(config intersafe) no download day-of-week mon
ok
SGOS#(config intersafe) no download day-of-week wed
ok
SGOS#(config intersafe) exit
SGOS#(config content-filter) exit
SGOS#(config)

```

## #(config content-filter) local

Use this command to configure local content filtering.

### Syntax

```
content-filter
```

This changes the prompt to:

```
SGOS#(config content-filter)
```

```
local
```

This changes the prompt to:

```
SGOS#(config local)
```

### - subcommands -

**option 1:** clear

**option 2:** download

sub-option 1: auto

sub-option 2: day-of-week {all | friday | monday | none | saturday | sunday |  
thursday | tuesday | wednesday}

sub-option 3: encrypted-password *encrypted\_password*

sub-option 4: full-get-now

sub-option 5: get-now

sub-option 6: password *password*

sub-option 7: time-of-day 0-23

sub-option 8: url *url*

sub-option 9: username *username*

**option 3:** exit

**option 4:** no download

sub-option 1: auto

sub-option 2: day-of-week {friday | monday | saturday | sunday | thursday |  
tuesday | wednesday}

sub-option 3: encrypted-password

sub-option 4: password

sub-option 5: url

sub-option 6: username

**option 5:** source

**option 6:** view

Table 3.24: # (config local)

clear		Clears the local database from the system.
download	auto	Enables automatic database downloads.
	day-of-week {all   friday   monday   none   saturday   sunday   thursday   tuesday   wednesday}	Specifies the day of the week for automatic downloads.
	encrypted-password <i>encrypted_password</i>	Specifies the encrypted password for the database download server.
	full-get-now	Initiates an immediate full-size database download.
	get-now	Initiates an immediate database download. If the previously downloaded database is up-to-date, no download is necessary and none is performed.
	password <i>password</i>	Specifies the password for the database download server.
	time-of-day 0-23	Specifies the time of day for automatic downloads.
	url <i>url</i>	Specifies the URL for the database download server.
	username <i>username</i>	Specifies the username for the database download server.
exit		Exits configure local mode and returns to configure content-filter mode.
no download	auto	Disables automatic download.
	day-of-week {friday   monday   saturday   sunday   thursday   tuesday   wednesday}	Clears day(s) of the week for automatic download.
	encrypted-password	Clears the encrypted password for the database download server.
	password	Clears the password for the database download server.
	url	Clears the URL for the database download server.
	username	Clears the username for the database download server.
source		Shows the database source file.
view		Shows the current local settings.

**Example**

```

SGOS#(config) content-filter
SGOS#(config content-filter) local
SGOS#(config local) download day-of-week all
ok

```

```
SGOS#(config local) exit
SGOS#(config content-filter) exit
SGOS#(config)
```

## #(config content-filter) optenet

Use this command to configure Optenet content filtering.

### Syntax

```
content-filter
```

This changes the prompt to:

```
SGOS#(config content-filter)
```

```
optenet
```

This changes the prompt to:

```
SGOS#(config optenet)
```

#### - subcommands-

**option 1:** download

```
sub-option 1: auto
```

```
sub-option 2: day-of-week {all | friday | monday | none | saturday | sunday |
                        thursday | tuesday | wednesday}
```

```
sub-option 3: encrypted-password encrypted_password
```

```
sub-option 4: full-get-now
```

```
sub-option 5: get-now
```

```
sub-option 6: password password
```

```
sub-option 7: time-of-day 0-23
```

```
sub-option 8: url {default | url}
```

```
sub-option 9: username username
```

**option 2:** exit

**option 3:** no download

```
sub-option 1: auto
```

```
sub-option 2: day-of-week {friday | monday | saturday | sunday | thursday |
                        tuesday | wednesday}
```

```
sub-option 3: encrypted-password
```

```
sub-option 4: password
```

```
sub-option 5: url
```

```
sub-option 6: username
```

**option 4:** view

Table 3.25: #(config optenet)

download	auto	Enables automatic database downloads.
	day-of-week {all   friday   monday   none   saturday   sunday   thursday   tuesday   wednesday}	Specifies the day of the week for automatic downloads.
	encrypted-password <i>encrypted_password</i>	Specifies the encrypted password for the database download server.
	full-get-now	Initiates an immediate full-size database download.
	get-now	Initiates an immediate database download. If a full download is unnecessary, an incremental download is initiated.
	password <i>password</i>	Specifies the password for the database download server.
	time-of-day 0-23	Specifies the time of day for automatic downloads.
	url {default   <i>url</i> }	Specifies using either the default URL or a specific URL for the database download server.
	username <i>username</i>	Specifies the username for the database download server.
exit		Exits configure optenet mode and returns to configure content-filter mode.
no download	auto	Disables automatic download.
	day-of-week {friday   monday   saturday   sunday   thursday   tuesday   wednesday}	Clears day(s) of the week for automatic download.
	encrypted-password	Clears the encrypted password for the database download server.
	password	Clears the password for the database download server.
	url	Clears the URL for the database download server.
	username	Clears the username for the database download server.
view		Shows the current optenet Web Filter settings.

**Example**

```

SGOS#(config) content-filter
SGOS#(config content-filter) optenet
SGOS#(config optenet) download time-of-day 20
ok
SGOS#(config optenet) exit

```

```
SGOS#(config content-filter) exit
SGOS#(config)
```

## #(config content-filter) proventia

Use this command to configure Proventia Web Filter content filtering.

### Syntax

```
content-filter
```

This changes the prompt to:

```
SGOS#(config content-filter)
proventia
```

This changes the prompt to:

```
SGOS#(config proventia)
```

#### - subcommands-

##### **option 1:** download

```
sub-option 1: auto
sub-option 2: day-of-week {all | friday | monday | none | saturday | sunday |
                        thursday | tuesday | wednesday}
sub-option 3: encrypted-password encrypted_password
sub-option 4: full-get-now
sub-option 5: get-now
sub-option 6: password password
sub-option 7: time-of-day 0-23
sub-option 8: url {default | url}
sub-option 9: username username
```

##### **option 2:** exit

##### **option 3:** no download

```
sub-option 1: auto
sub-option 2: day-of-week {friday | monday | saturday | sunday | thursday |
                        tuesday | wednesday}
sub-option 3: encrypted-password
sub-option 4: password
sub-option 5: url
sub-option 6: username
```

##### **option 4:** view

Table 3.26: #(config proventia)

download	auto	Enables automatic database downloads.
	day-of-week {all   friday   monday   none   saturday   sunday   thursday   tuesday   wednesday}	Specifies the day of the week for automatic downloads.
	encrypted-password <i>encrypted_password</i>	Specifies the encrypted password for the database download server.
	full-get-now	Initiates an immediate full-size database download.
	get-now	Initiates an immediate database download. If a full download is unnecessary, an incremental download is initiated.
	password <i>password</i>	Specifies the password for the database download server.
	time-of-day 0-23	Specifies the time of day for automatic downloads.
	url {default   url}	Specifies using either the default URL or a specific URL for the database download server.
	username <i>username</i>	Specifies the username for the database download server.
exit		Exits configure proventia mode and returns to configure content-filter mode.
no download	auto	Disables automatic download.
	day-of-week {friday   monday   saturday   sunday   thursday   tuesday   wednesday}	Clears day(s) of the week for automatic download.
	encrypted-password	Clears the encrypted password for the database download server.
	password	Clears the password for the database download server.
	url	Clears the URL for the database download server.
	username	Clears the username for the database download server.
view		Shows the current Proventia Web Filter settings.

**Example**

```

SGOS#(config) content-filter
SGOS#(config content-filter) proventia
SGOS#(config proventia) download time-of-day 20
    ok
SGOS#(config proventia) exit

```

```
SGOS#(config content-filter) exit
SGOS#(config)
```

## #(config content-filter) smartfilter

Use this command to configure SmartFilter filters that control the type of content retrieved by the ProxySG and filter requests made by clients.

### Syntax

```
content-filter
```

This changes the prompt to:

```
SGOS#(config content-filter)
smartfilter
```

This changes the prompt to:

```
SGOS#(config smartfilter)
```

#### - subcommands-

**option 1:** allow-rdns

**option 2:** download

sub-option 1: auto

sub-option 2: day-of-week {all | friday | monday | none | saturday | sunday |  
thursday | tuesday | wednesday}

sub-option 3: encrypted-password *encrypted\_password*

sub-option 4: full-get-now

sub-option 5: get-now

sub-option 6: license *license\_key*

sub-option 7: password *password*

sub-option 8: server *IP\_address\_or\_hostname*

sub-option 9: time-of-day *0-23*

sub-option 10:url {premier-list {ftp | http} | standard-list {ftp | http} | *url*}

sub-option 11:username *username*

**option 3:** exit

**option 4:** list-version {3 | 4}

**option 5:** no

sub-option 1: allow-rdns

sub-option 2: download {auto | day-of-week {friday | monday | saturday | sunday |  
thursday | tuesday | wednesday} | encrypted-password | password |  
url | username}

sub-option 3: use-search-keywords

**option 6:** use-search-keywords

**option 7:** view



Table 3.27: # (config smartfilter)

allow-rdns		Allow reverse DNS for lookups.
download	auto	Enables automatic download.
	day-of-week {all   friday   monday   none   saturday   sunday   thursday   tuesday   wednesday}	Sets day(s) of the week for automatic download.
	encrypted-password <i>encrypted_password</i>	Version 3.x only. Specifies the encrypted password for the database download server.
	full-get-now	Initiates an immediate full-size database download.
	get-now	Initiates immediate database download. If a full download is unnecessary, an incremental download is initiated.
	license <i>license_key</i>	Version 4.x only. The customer serial number assigned you by SmartFilter.
	password <i>password</i>	Version 3.x only. Specifies the password for the database download server.
	server <i>IP_address_or_hostname</i>	Version 4.x only. Enter the IP address or hostname of the server you should use for downloads if requested.
	time-of-day <i>0-23</i>	Sets time of day (UTC) for automatic download.
	url {premier-list {ftp   http}   standard-list {ftp   http}   url}	Version 3.x only. Specifies the download URL. Select the type of control list (standard-list or premier-list) and the protocol (ftp or http).
	username <i>username</i>	Version 3.x only. Specifies the username for the database download server.
exit		Exits configure smartfilter mode and returns to configure content-filter mode.
list-version	3   4	Specifies the version (3.x or 4.x) of the SmartFilter control list.

Table 3.27: #(config smartfilter) (Continued)

no	allow-rdns	Disallows reverse DNS for lookups.
	download {auto   day-of-week {friday   monday   saturday   sunday   thursday   tuesday   wednesday}   encrypted-password   password   url   username}	Negates download commands.
	use-search-keywords	Disables the ability to categorize search engines based on keywords in the URL query.
use-search-keywords	no	Allows you to categorize search engines based on keywords in the URL query.
view		Shows the current SmartFilter settings.

**Example**

```

SGOS#(config) content-filter
SGOS#(config content-filter) smartfilter
SGOS#(config smartfilter) allow-rdns
    ok
SGOS#(config smartfilter) exit
SGOS#(config content-filter) exit
SGOS#(config)

```

**#(config content-filter) surfcontrol**

Use this command to configure SurfControl filters that control the type of content retrieved by the ProxySG and filter requests made by clients.

**Syntax**

```
content-filter
```

This changes the prompt to:

```
SGOS#(config content-filter)
```

```
surfcontrol
```

This changes the prompt to:

```
SGOS#(config surfcontrol)
```

**- subcommands-**

**option 1:** download

sub-option 1: auto

sub-option 2: day-of-week {all | friday | monday | none | saturday | sunday | thursday | tuesday | wednesday}

sub-option 3: encrypted-password *encrypted\_password*

```

sub-option 4: full-get-now
sub-option 5: get-now
sub-option 6: password password
sub-option 7: time-of-day 0-23
sub-option 8: url {default | url}
sub-option 9: username username

```

**option 2:** exit

**option 3:** no download {auto | day-of-week {friday | monday | saturday | sunday | thursday | tuesday | wednesday} | encrypted-password | username | password | url}

**option 4:** view

**Table 3.28:** # (config surfcontrol)

download	auto	Enables automatic download.
	day-of-week {all   friday   monday   none   saturday   sunday   thursday   tuesday   wednesday}	Sets day(s) of the week for automatic download.
	encrypted-password <i>encrypted-password</i>	Sets the download encrypted password. The username/password is assigned by Blue Coat.
	full-get-now	Initiates an immediate full-size database download.
	get-now	Initiates an immediate database download. If the previously downloaded database is up-to-date, no download is necessary and none is performed.
	password <i>password</i>	Sets the download password. The username/password is assigned by Blue Coat.
	time-of-day <i>0-23</i>	Sets time of day (UTC) for automatic download.
	url {default   <i>url</i> }	Specifies the URL from which to download database.

Table 3.28: #(config surfcontrol) (Continued)

	<code>username username</code>	Sets the download username. The username/password is assigned by Blue Coat.
<code>exit</code>		Exits configure surfcontrol mode and returns to configure content-filter mode.
<code>no download</code>	<code>auto   day-of-week {friday   monday   saturday   sunday   thursday   tuesday   wednesday}   encrypted-password   password   url   username</code>	Negates download commands.
<code>view</code>		Shows the current SurfControl settings.

**Example**

```
SGOS#(config) content-filter
SGOS#(config content-filter) surfcontrol
SGOS#(config surfcontrol) no download url
    ok
SGOS#(config surfcontrol) exit
SGOS#(config content-filter) exit
SGOS#(config)
```

**#(config content-filter) websense**

Use this command to configure Websense filters that control the type of content retrieved by the ProxySG and filter requests made by clients.

**Syntax**

```
content-filter
```

This changes the prompt to:

```
SGOS#(config content-filter)
```

```
websense
```

This changes the prompt to:

```
SGOS#(config websense)
```

**- subcommands-**

**option 1:** `always-apply-regexes`

**option 2:** `download`

sub-option 1: `auto`

sub-option 2: `day-of-week {all | friday | monday | none | saturday | sunday | thursday | tuesday | wednesday}`

sub-option 3: `email-contact email_address`

```

sub-option 4: full-get-now
sub-option 5: get-now
sub-option 6: license license_key
sub-option 7: server {ip_address | hostname}
sub-option 8: time-of-day 0-23

```

**option 3:** exit

**option 4:** integration-service

```

sub-option 1: disable
sub-option 2: enable
sub-option 3: host (hostname or IP_address)
sub-option 4: port {integer between 0 and 65535}

```

**option 5:** no

```

sub-option 1: always-apply-regexes
sub-option 2: download {auto | day-of-week {friday | monday | saturday | sunday |
                                         thursday | tuesday | wednesday} | email-contact | license | server}
sub-option 3: integration-service

```

**option 6:** view

**Table 3.29:** # (config websense)

always-apply-regexes		Forces an additional regular expression lookup for each URL to be categorized. Normally, regular expression lookups are only performed when no category is found in the Websense database. This option causes them to be performed always, even for categorized URLs. This can reduce lookup performance, but can allow certain sites (such as translation, search engine, and link-cache sites) to be categorized more accurately.
----------------------	--	---

Table 3.29: # (config websense) (Continued)

download	auto	Enables automatic download.
	day-of-week	Sets day(s) of the week for automatic download.
	email-contact <i>email_address</i>	Specifies an e-mail address that is sent to Websense when downloading the database.
	full-get-now	Initiates an immediate full-size database download.
	get-now	Initiates immediate database download. If a full download is unnecessary, an incremental download is initiated.
	license <i>license_key</i>	Specifies the license key for the database download server.
	server { <i>ip_address</i>   <i>hostname</i> }	Specifies the server location of the database.
	time-of-day	Sets time of day (UTC) for automatic download.
exit		Exits configure websense mode and returns to configure content-filter mode.
integration-service	disable	Disables the integration service.
	enable	Enables the integration service.
	host <i>hostname</i> or <i>IP_address</i>	Set the integration service hostname or IP address. The IP address must match the IP address of the Websense Log Server.
	port <i>integer</i>	Configure the integration service port. Accepted values are between 0 and 65535
no	always-apply-regexes	Specifies to not apply regular expression filters to categorized URLs.
	download {auto   day-of-week {friday   monday   saturday   sunday   thursday   tuesday   wednesday}   email-contact   license   server}	Clears the download parameters.
	integration-service {host   port}	Clears the integration-service host or port
view		Shows the current SurfControl settings.

### Example

```
SGOS#(config) content-filter
SGOS#(config content-filter) websense
SGOS#(config websense) no always-apply-regexes
ok
SGOS#(config websense) exit
SGOS#(config content-filter) exit
SGOS#(config)
```

## #(config content-filter) webwasher

Use this command to configure Webwasher URL Filter content filtering.

### Syntax

```
content-filter
```

This changes the prompt to:

```
SGOS#(config content-filter)
```

```
webwasher
```

This changes the prompt to:

```
SGOS#(config webwasher)
```

### - subcommands-

#### option 1: download

```
sub-option 1: auto
```

```
sub-option 2: day-of-week {all | friday | monday | none | saturday | sunday |
                        thursday | tuesday | wednesday}
```

```
sub-option 3: encrypted-password encrypted_password
```

```
sub-option 4: full-get-now
```

```
sub-option 5: get-now
```

```
sub-option 6: password password
```

```
sub-option 7: time-of-day 0-23
```

```
sub-option 8: url {default | url}
```

```
sub-option 9: username username
```

#### option 2: exit

#### option 3: no download

```
sub-option 1: auto
```

```
sub-option 2: day-of-week {friday | monday | saturday | sunday | thursday | tuesday
                        | wednesday}
```

```
sub-option 3: encrypted-password
```

```
sub-option 4: password
```

```
sub-option 5: url
```

```
sub-option 6: username
```

**option 4:** view

Table 3.30: # (config webwasher)

download	auto	Enables automatic database downloads.
	day-of-week {all   friday   monday   none   saturday   sunday   thursday   tuesday   wednesday}	Specifies the day of the week for automatic downloads.
	encrypted-password <i>encrypted_password</i>	Specifies the encrypted password for the database download server.
	full-get-now	Initiates an immediate full-size database download.
	get-now	Initiates an immediate database download. If a full download is unnecessary, an incremental download is initiated.
	password <i>password</i>	Specifies the password for the database download server.
	time-of-day <i>0-23</i>	Specifies the time of day for automatic downloads.
	url {default   <i>url</i> }	Specifies using either the default URL or a specific URL for the database download server.
	username <i>username</i>	Specifies the username for the database download server.
exit		Exits configure webwasher mode and returns to configure content-filter mode.
no download	auto	Disables automatic download.
	day-of-week {friday   monday   saturday   sunday   thursday   tuesday   wednesday}	Clears day(s) of the week for automatic download.
	encrypted-password	Clears the encrypted password for the database download server.
	password	Clears the password for the database download server.
	url	Clears the URL for the database download server.
	username	Clears the username for the database download server.
view		Shows the current webwasher Web Filter settings.

### Example

```
SGOS#(config) content-filter
SGOS#(config content-filter) webwasher
SGOS#(config webwasher) download time-of-day 20
ok
SGOS#(config webwasher) exit
```



```
SGOS#(config content-filter) exit  
SGOS#(config)
```

## #(config) diagnostics

This command enables you to configure the remote diagnostic feature Heartbeat.

### Syntax

```
diagnostics
```

This changes the prompt to:

```
SGOS#(config diagnostics)
```

#### - subcommands-

**option 1:** cpu-monitor

sub-option 1: disable

sub-option 2: enable

sub-option 3: interval *seconds*

**option 2:** exit

**option 3:** heartbeat {disable | enable}

**option 4:** monitor {disable | enable}

**option 5:** send-heartbeat

**option 6:** service-info—changes the prompt (see “#(config diagnostics) service-info” on page 114)

**option 7:** snapshot

sub-option 1: create *snapshot\_name*

sub-option 2: delete *snapshot\_name*

sub-option 3: edit *snapshot\_name*—changes the prompt (see “#(config diagnostics) snapshot *snapshot\_name*” on page 116)

**option 8:** view

sub-option 1: configuration

sub-option 2: cpu-monitor

sub-option 3: service-info

sub-option 4: snapshot *snapshot\_name*

Table 3.31: # (config diagnostics)

cpu-monitor	disable   enable	Enables or disables the CPU monitor (the CPU monitor is disabled by default).
	interval <i>seconds</i>	Sets the periodic interval of the CPU monitor from 1 to 59 seconds (the default setting is 5 seconds).
exit		Exits configure diagnostics mode and returns to configure mode.
heartbeat	disable   enable	Enables or disables the ProxySG Heartbeat features.
monitor	disable   enable	Enables or disables the Blue Coat monitoring feature.
send-heartbeat		Triggers a heartbeat report.
service-info		Changes the prompt. See “# (config diagnostics) service-info” on page 114.
snapshot	create <i>snapshot_name</i>	Creates a new snapshot job.
	delete <i>snapshot_name</i>	Deletes a snapshot job.
	edit <i>snapshot_name</i>	Changes the prompt. See “# (config diagnostics) snapshot <i>snapshot_name</i> ” on page 116.
view	configuration	Displays diagnostics settings for Heartbeats, CPU monitor, automatic service-info, and snapshots.
	cpu-monitor	Displays the CPU Monitor results.
	service-info	Displays service-info settings and progress.
	snapshot <i>snapshot_name</i>	Displays the snapshot settings (target, status, interval, to keep, to take, and next snapshot) for the snapshot name specified.
	status	Displays the diagnostic settings.

**Example**

```

SGOS#(config) diagnostics
SGOS#(config diagnostics) heartbeat enable
    ok
SGOS#(config diagnostics) exit
SGOS#(config)

```

**#(config diagnostics) service-info**

This command allows you to send service information to Blue Coat Systems.

**Syntax**

```
diagnostics
```

This changes the prompt to:

```
SGOS#(config diagnostics)
```

```
service-info
```

This changes the prompt to:

```
SGOS#(diagnostics service-info)
```

**- subcommands-**

**option 1:** auto

```
sub-option 1: disable
```

```
sub-option 2: enable
```

```
sub-option 3: no sr-number
```

```
sub-option 4: sr-number sr_number
```

**option 2:** bandwidth-class *bw\_class\_name*

**option 3:** cancel

```
sub-option 1: all
```

```
sub-option 2: one_or_more_from_view_status
```

**option 4:** exit

**option 5:** no bandwidth-class

**option 6:** send *sr\_number one\_or\_more\_commands\_from\_view\_available*

**option 7:** view

```
sub-option 1: available
```

```
sub-option 2: status
```

**Table 3.32:** # (config diagnostics service-info)

auto	disable	Disables the automatic service information feature.
	enable	Enables the automatic service information feature.
	no sr-number	Clears the service-request number for the automatic service information feature.
	sr-number <i>sr_number</i>	Sets the service-request number for the automatic service information feature.
bandwidth-class	<i>bw_class_name</i>	Sets a bandwidth class used to manage the bandwidth of service-information transfers. <b>IMPORTANT:</b> In order to bandwidth-manage service-information transfers, bandwidth management must be enabled. Bandwidth management is enabled by default if you have a valid bandwidth-management license. You must also create a bandwidth class for service-information transfers (in bandwidth-management mode) before you can select it here. See “# (config) bandwidth-management” on page 75 for more information.

Table 3.32: # (config diagnostics service-info) (Continued)

cancel	all	Cancel all service information being sent to Blue Coat Systems.
	<i>one_or_more_from_view_status</i>	Cancel certain service information being sent to Blue Coat Systems.
exit		Exits configure diagnostics service-info mode and returns to configure diagnostics mode.
no	bandwidth-class	Disables bandwidth-management for service-information transfers.
send	<i>sr_num</i> <i>one_or_more_commands_from_view_available</i>	Sends a specific service request number along with a specific command or commands (chosen from the list provided by the view available command) to Blue Coat Systems.
	<i>one_or_more_commands_from_view_available</i>	Sends certain commands to Blue Coat Systems.
view	available	Shows list of service information than can be sent to Blue Coat Systems.
	status	Shows transfer status of service information to Blue Coat Systems.

**Example**

```

SGOS#(config) diagnostics
SGOS#(config diagnostics) service-info
SGOS#(diagnostics service-info) view available
Service information that can be sent to Blue Coat

Name                                     Approx Size (bytes)
Event_log                               188,416
System_information                       Unknown
Snapshot_sysinfo                         Unknown
Snapshot_sysinfo_stats                   Unknown
SGOS#(diagnostics service-info) send 1-4974446 event_log system_information
snapshot_sysinfo
Sending the following reports
Event_log
System_information
Snapshot_sysinfo
SGOS#(diagnostics service-info) view status
Name                                     Transferred      Total Size      % Done
Event_log                               Transferred successfully
Snapshot_sysinfo                         Transferred successfully
Event_log                               Transferred successfully
System_information                       Transferred successfully
SGOS#(diagnostics service-info) exit
SGOS#(config diagnostics) exit
SGOS#(config)

```

**#(config diagnostics) snapshot *snapshot\_name***

This command allows you to edit a snapshot job.

## Syntax

diagnostics

This changes the prompt to:

```
SGOS#(config diagnostics)
```

```
snapshot edit snapshot_name
```

This changes the prompt to:

```
SGOS#(config snapshot snapshot_name)
```

- *subcommands* -

**option 1:** clear-reports

**option 2:** disable

**option 3:** enable

**option 4:** exit

**option 5:** interval *minutes*

**option 6:** keep *number\_to\_keep* (from 1 - 100)

**option 7:** take {infinite | *number\_to\_take*}

**option 8:** target *object\_to\_fetch*

**option 9:** view

Table 3.33: #(config snapshot *snapshot\_name*)

clear-reports		Clears all stored snapshots reports.
disable		Disables this snapshot job.
enable		Enables this snapshot job.
exit		Exits configure diagnostics snapshot name mode and returns to configure diagnostics service-info mode.
interval	<i>minutes</i>	Specifies the interval between snapshots reports in minutes.
keep	<i>number_to_keep</i> (from 1 - 100)	Specifies the number of snapshot reports to keep.
take	infinite   <i>number_to_take</i>	Specifies the number of snapshot reports to take.
target	<i>object_to_fetch</i>	Specifies the object to snapshot.
view		Displays snapshot status and configuration.

### Example

```
SGOS#(config) diagnostics
SGOS#(config diagnostics) snapshot testshot
SGOS#(diagnostics snapshot testshot) enable
    ok
SGOS#(diagnostics service-info) interval 1440
    ok
SGOS#(diagnostics snapshot testshot) exit
SGOS#(config diagnostics) exit
SGOS#(config)
```

## #(config) dns

The `dns` command enables you to modify the DNS settings for the ProxySG. Note that the alternate DNS servers are only checked if the servers in the standard DNS list return: “Name not found.”

### Syntax

**option 1:** `dns alternate ip_address`

**option 2:** `dns clear {alternate | imputing | resolving | server}`

**option 3:** `dns imputing name`

**option 4:** `dns no {alternate ip_address | imputing imputed_name | server ip_address}`

**option 5:** `dns server ip_address`

Table 3.34: #(config) dns

alternate	<i>ip_address</i>	Adds the new alternate domain name server indicated by <i>ip_address</i> to the alternate DNS server list.
clear	alternate	Sets all entries in the alternate DNS server list to null.
	imputing	Sets all entries in the name imputing list to null.
	server	Sets all entries in the primary DNS server list to null.
imputing	<i>name</i>	Identifies the file indicated by <i>name</i> as the name imputing list.
no	alternate <i>ip_address</i>	Removes the alternate DNS server identified by <i>ip_address</i> from the alternate DNS server list.
	imputing <i>imputed_name</i>	Removes the imputed name identified by <i>imputed_name</i> from the name imputing list.
	server <i>ip_address</i>	Removes the primary DNS server identified by <i>ip_address</i> from the primary DNS server list.
server	<i>ip_address</i>	Adds the new primary domain name server indicated by <i>ip_address</i> to the primary DNS server list.

*Example*

```

SGOS#(config) dns clear server
ok
SGOS#(config) dns server 10.253.220.249
ok
SGOS#(config) dns clear alternate
ok
SGOS#(config) dns alternate 216.52.23.101
ok

```

 **#(config) dynamic-bypass**

Dynamic bypass provides a maintenance-free method for improving performance of the ProxySG by automatically compiling a list of requested URLs that return various kinds of errors.

With dynamic bypass, the ProxySG adds dynamic bypass entries, containing the server IP address of sites that have returned an error, to the ProxySG's local bypass list. For a configured period of time, further requests for the error-causing URL are sent immediately to the origin server, saving the ProxySG processing time. The amount of time a dynamic bypass entry stays in the list, and the types of errors that cause the ProxySG to add a site to the list, along with several other settings, is configurable from the CLI.

Once the dynamic bypass timeout for a URL has ended, the ProxySG removes the URL from the bypass list. On the next client request for the URL, the ProxySG attempts to contact the origin server. If the origin server still returns an error, the URL is once again added to the local bypass list for the configured dynamic bypass timeout. If the URL does not return an error, the request is handled in the normal manner.

The performance gains realized with this feature are substantial if the client base is large, and clients are requesting many error-causing URLs in a short period of time (for example, many users clicking a browser's refresh button over and over to get an overloaded origin server to load a URL). Dynamic bypass increases efficiency because redundant attempts to contact the origin server are minimized.

**Syntax**

**option 1:** dynamic-bypass clear

**option 2:** dynamic-bypass disable

**option 3:** dynamic-bypass enable

**option 4:** dynamic-bypass no trigger {all | connect-error | non-http | receive-error | 400 | 401 | 403 | 405 | 406 | 500 | 502 | 503 | 504}

**option 5:** dynamic-bypass trigger {all | connect-error | non-http | receive-error | 400 | 401 | 403 | 405 | 406 | 500 | 502 | 503 | 504}

Table 3.35: #(config) dynamic-bypass

clear		Clears all entries in the dynamic bypass list.
disable		Disables the current dynamic bypass list.
enable		Enables the current dynamic bypass list.
no trigger	all   connect-error   non-http   receive-error   400   403   405   406   500   502   503   504	Disables dynamic bypass for the specified HTTP response code, all HTTP response codes, or all non-HTTP responses.
trigger	all   connect-error   non-http   receive-error   400   403   405   406   500   502   503   504	Enables dynamic bypass for the specified HTTP response code, all HTTP response codes, or all non-HTTP responses.

**Example**

```

SGOS#(config) dynamic-bypass clear
ok
SGOS#(config) dynamic-bypass enable
WARNING:
    Requests to sites that are put into the dynamic bypass list will
    bypass future policy evaluation. This could result in subversion
    of on-box policy. The use of dynamic bypass is cautioned.
ok
SGOS#(config) dynamic-bypass trigger all
ok

```

**#(config) event-log**

You can configure the ProxySG to log system events as they occur. Event logging allows you to specify the types of system events logged, the size of the event log, and to configure Syslog monitoring. The ProxySG can also notify you by e-mail if an event is logged.

**Syntax**

```
event-log
```

This changes the prompt to:

```
SGOS#(config event-log)
```

**- subcommands-**

**option 1:** exit

**option 2:** level {configuration | informational | policy | severe | verbose}

**option 3:** log-size *megabytes*

**option 4:** mail {add *email\_address* | clear | no smtp-gateway | remove *email\_address* | smtp-gateway {*domain\_name* | *ip\_address*}}

**option 5:** syslog {disable | enable | facility {auth | daemon | kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail



```
| news | syslog | user | uucp} | loghost {domain_name | ip_address} | no
loghost}
```

**option 6:** view [configuration]

**option 7:** when-full {overwrite | stop}

**Table 3.36:** # (config event-log)

exit		Exits configure event-log mode and returns to configure mode.
level	configuration	Writes severe and configuration change error messages to the event log.
	informational	Writes severe, configuration change, policy event, and information error messages to the event log.
	policy	Writes severe, configuration change, and policy event error messages to the event log.
	severe	Writes only severe error messages to the event log.
	verbose	Writes all error messages to the event log.
log-size	<i>megabytes</i>	Specifies the maximum size of the event log in megabytes.
mail	add <i>email_address</i>	Specifies an e-mail recipient for the event log output.
	clear	Removes all e-mail recipients from the event log e-mail output distribution list.
	no smtp-gateway	Clears the SMTP gateway used for notifications.
	remove <i>email_address</i>	Removes the e-mail recipient indicated by <i>email_address</i> from the event log e-mail output distribution list.
	smtp-gateway { <i>domain_name</i>   <i>ip_address</i> }	Specifies the SMTP gateway to use for event log e-mail output notifications.

Table 3.36: # (config event-log) (Continued)

syslog	disable	Disables the collection of system log messages.
	enable	Enables the collection of system log messages.
	facility {auth   daemon   kernel   local0   local1   local2   local3   local4   local5   local6   local7   lpr   mail   news   syslog   user   uucp}	Specifies the types of system log messages to be collected in the system log.
	loghost {domain_name   ip_address}	Specifies the host domain used for system log notifications.
	no loghost	Clears the loghost setting.
view	[start [YYYY-mm-dd] [HH:MM:SS]] [end [YYYY-mm-dd] [HH:MM:SS]] [regex regex   substring string] [configuration]	View the event-log configuration, using configuration, or view the contents of the event-log, using the filters offered to narrow the view.
when-full	{overwrite   stop}	Specifies what should happen to the event log when the maximum size has been reached. overwrite overwrites the oldest information in a FIFO manner; stop disables event logging.

**Note:** You must replace the default Blue Coat Systems SMTP gateway with your gateway. If you do not have access to an SMTP gateway, you can use the Blue Coat Systems gateway to send event messages to Blue Coat Systems (the Blue Coat Systems SMTP gateway will only send mail to Blue Coat Systems; it will not forward mail to other domains).

#### Example

```
SGOS# (config) event-log
SGOS# (config event-log) syslog enable
ok
```

## #(config) exceptions

These commands allow you to configure built-in and user-defined exception response objects.

### Syntax

```
exceptions
```

This changes the prompt to:

```
SGOS# (config exceptions)
```

**- subcommands-****option 1:** create *exception\_id***option 2:** company-name *name***option 3:** delete *exception\_id***option 4:** edit *exception\_id* or *user\_defined\_exception\_id*—changes the prompt (see “#(config exceptions) edit [user-defined.]exception\_id” on page 124)**option 5:** exit**option 6:** inline {contact | details | format | help | http {contact | details | format | help | summary} | summary} eof\_marker**option 7:** load exceptions**option 8:** no path**option 9:** path *url***option 10:** user-defined inline {contact | details | format | help | http {contact | details | format | help | summary} | summary} eof\_marker**Table 3.37:** #(config exceptions)

create	<i>exception_id</i>	Creates the given exception.
company-name	<i>name</i>	Sets the name used for the \$(exception.company_name) substitution.
delete	<i>exception_id</i>	Deletes the exception specified by <i>exception_id</i> .
edit	<i>exception_id</i>   <i>user_defined_exception_id</i>	Changes the prompt. See “#(config exceptions) edit [user-defined.]exception_id” on page 124.
exit		Exits configure exceptions mode and returns to configure mode.
inline	{contact   details   format   help   http {contact   details   format   help   summary}   summary} eof_marker	Configures defaults for all exception objects.
load	exceptions	Downloads new exceptions.
no	path	Clears the network path to download exceptions.
path	<i>url</i>	Specifies the network path to download exceptions.
user-defined	inline {contact   details   format   help   http {contact   details   format   help   summary}   summary} eof_marker	Configures the top-level values for user-defined exceptions.

### Example

```
SGOS#(config) exceptions
SGOS#(config exceptions) default contact
    ok
SGOS#(config exceptions) exit
SGOS#(config)
```

## **#(config exceptions) edit [user-defined.]exception\_id**

These commands allow you to edit an exception or a user-defined exception.

### Syntax

exceptions

This changes the prompt to:

```
SGOS#(config exceptions)
exception_id or user_defined_exception_id
```

This changes the prompt to:

```
SGOS#(config exceptions [user-defined.]exception_id)
```

- *subcommands*-

**option 1:** exit

**option 2:** http-code *numeric\_http\_response\_code*

**option 3:** inline {contact | details | format | help | http {contact | details |  
format | help | summary} | summary} *eof\_marker*

Table 3.38: #(config exceptions [user-defined.]exception\_id)

exit		Exits configure exceptions [user-defined] exception_id mode and returns to configure exceptions mode.
http-code	<i>numeric_http_response_code</i>	Configures this exception's HTTP response code.
inline	{contact   details   format   help   http {contact   details   format   help   summary}   summary} <i>eof_marker</i>	Configures this exception's substitution values.

### Example

```
SGOS#(config) exceptions
SGOS#(config exceptions) edit testname
SGOS#(config exceptions user-defined testname) http-code 000
    ok
SGOS#(config exceptions user-defined testname) exit
SGOS#(config exceptions) exit
SGOS#(config)
```

## #(config) exit

Exits from Configuration mode to Privileged mode, from Privileged mode to Standard mode. From Standard mode, the `exit` command closes the CLI session.

### Syntax

```
exit
```

The `exit` command does not have any parameters or subcommands.

## #(config) external-services

These commands allow you to configure your external services.

Use the edit ICAP commands to configure the ICAP service used to integrate the ProxySG with a virus scanning server. The configuration is specific to the virus scanning server and includes the server IP address, as well as the supported number of connections. If you are using the ProxySG with multiple virus scanning servers or multiple scanning services on the same server, add an ICAP service for each server or scanning service.

---

**Note:** When you define virus scanning policies, use the same service name. Make sure you type the ICAP service name accurately, whether you are configuring the service on the ProxySG or defining policies since the name retrieves the other configuration settings for that service.

---

### Syntax

```
external-services
```

This changes the prompt to:

```
SGOS#(config external-services)
```

- *subcommands*-

**option 1:** create {icap icap\_service\_name | service-group service\_group\_name | websense websense\_service\_name}

**option 2:** delete name

**option 3:** edit—changes the prompt to one of three external service edit commands:

sub-option 1: icap\_service\_name (see “#(config external-services) edit icap\_service\_name” on page 127)

sub-option 2: `service_group_name` (see “#(config external-services) edit `service_group_name`” on page 128)

sub-option 3: `websense_service_name` (see “#(config external-services) edit `websense_service_name`” on page 130)

**option 4:** `exit`

**option 5:** `inline`

sub-option 1: `http {icap-patience-details | icap-patience-header | icap-patience-help | icap-patience-summary}`

sub-option 2: `ftp icap-patience-details`

**option 6:** `view`

**Table 3.39:** #(config external-services)

create	<code>icap icap_service_name</code>	Creates an ICAP service.
	<code>service-group service_group_name</code>	Creates a service group.
	<code>websense websense_service_name</code>	Creates a Websense service.
delete	<code>name</code>	Deletes an external service.
edit	<code>icap_service_name</code>	Changes the prompt. See “#(config external-services) edit <code>icap_service_name</code> ” on page 127.
	<code>service_group_name</code>	Changes the prompt. See “#(config external-services) edit <code>service_group_name</code> ” on page 128.
	<code>websense_service_name</code>	Changes the prompt. See “#(config external-services) edit <code>websense_service_name</code> ” on page 130.
exit		Exits configure external-services mode and returns to configure mode.
inline	<code>http {icap-patience- details eof_marker   icap-patience-header eof_marker}   icap-patience-help eof_marker   icap-patience-summary eof_marker}</code>	Customizes ICAP patience page details for HTTP connections.
	<code>ftp icap-patience-details</code>	Customizes ICAP patience page details for FTP connections.
view		Shows external services and external service groups.

### Example

```
SGOS#(config) external-services
SGOS#(config external-services) create websense testwebsense
      ok
SGOS#(config external-services) exit
SGOS#(config)
```

## **#(config external-services) edit icap\_service\_name**

These commands allow you to edit ICAP parameters.

### Syntax

external-services

This changes the prompt to:

```
SGOS#(config external-services)
```

```
edit icap_service_name
```

This changes the prompt to:

```
SGOS#(config icap icap_service_name)
```

#### **- subcommands-**

**option 1:** exit

**option 2:** max-conn *max\_num\_connections*

**option 3:** methods {REQMOD | RESPMOD}

**option 4:** no

sub-option 1: send {client-address | server-address}

sub-option 2: notify virus-detected

sub-option 3: patience-page

sub-option 4: preview

**option 5:** notify virus-detected

**option 6:** patience-page *seconds*

**option 7:** preview-size *bytes*

**option 8:** send {client-address | server-address}

**option 9:** sense-settings

**option 10:** timeout *seconds*

**option 11:** url *url*

**option 12:** view

Table 3.40: #(config icap icap\_service\_name)

exit		Exits configure ICAP name mode and returns to configure external-services mode.
max-conn	<i>max_num_connections</i>	Sets the maximum number of connections for the ICAP service.
methods	REQMOD   RESPMOD	Sets the method supported by the ICAP service. REQMOD is request modification and RESPMOD is response modification.
no	send {client-address   server-address}	Specifies what should not be sent to the ICAP server.
	notify virus-detected	Specifies no notification to the administrator when a virus is detected.
	patience-page	Specifies that patience pages do not get served.
	preview	Specifies that previews do not get sent.
notify virus-detected		Specifies notification when viruses are found.
patience-page	<i>seconds</i>	Sets the number of seconds (5 to 65535) to wait before serving a patience page.
preview-size	<i>bytes</i>	Sets the preview size for the ICAP service.
send	client-address	Specifies that the client address be sent to the ICAP service.
	server-address	Specifies that the server address be sent to the ICAP service.
sense-settings		Senses the service's setting by contacting the server.
timeout	<i>seconds</i>	Sets the connection timeout for the ICAP services.
url	<i>url</i>	Sets the URL for the ICAP services.
view		Displays the service's current configuration.

**Example**

```

SGOS#(config) external-services
SGOS#(config external-services) edit testicap
SGOS#(config icap testicap) send client-address
    ok
SGOS#(config icap testicap) exit
SGOS#(config external-services) exit
SGOS#(config)

```

**#(config external-services) edit service\_group\_name**

These commands allow you to edit service group parameters.

**Syntax**

```
external-services
```

This changes the prompt to:



```
SGOS#(config external-services)
```

```
edit service_group_name
```

This changes the prompt to:

```
SGOS#(config service-group service_group_name)
```

- *subcommands*-

**option 1:** add *entry\_name*

**option 2:** edit *entry\_name*—changes the prompt (see “#(config service-group service\_group\_name) edit entry\_name” on page 129)

**option 3:** exit

**option 4:** remove *entry\_name*

**option 5:** view

Table 3.41: #(config service-group service\_group\_name)

add	<i>entry_name</i>	Adds an entry to this service group.
edit	<i>entry_name</i>	Edits an entry in this service group. Changes the prompt (see “#(config service-group service_group_name) edit entry_name” on page 129).
exit		Exits configure service-group name mode and returns to configure external-services mode.
remove	<i>entry_name</i>	Removes an entry from this service group.
view		Displays this service group’s configuration.

### Example

```
SGOS#(config) external-services
SGOS#(config external-services) edit testgroup
SGOS#(config service-group testgroup) add testentry
ok
SGOS#(config service-group testgroup) exit
SGOS#(config external-services) exit
SGOS#(config)
```

### **#(config service-group service\_group\_name) edit entry\_name**

These commands allow you to edit a service group entry.

### Syntax

```
external-services
```

This changes the prompt to:

```
SGOS#(config external-services)
```

```
edit service_group_name
```

This changes the prompt to:

```
SGOS#(config service-group service_group_name)
```

```
edit entry_name
```

This changes the prompt to:

```
SGOS#(config service-group service_group_name entry_name)
```

- *subcommands*-

**option 1:** exit

**option 2:** view

**option 3:** weight 0 to 255

Table 3.42: #(config service-group service\_group\_name entry\_name)

exit		Exits configure service-group name/entry name mode and returns to configure service-group name mode.
view		Shows this entry's configuration.
weight	0 to 255	Modifies this entry's weight.

*Example*

```
SGOS#(config) external-services
SGOS#(config external-services) edit testgroup
SGOS#(config service-group testgroup) edit testentry
SGOS#(config service-group testgroup testentry) weight 223
ok
SGOS#(config service-group testgroup testentry) exit
SGOS#(config service-group testgroup) exit
SGOS#(config external-services) exit
SGOS#(config)
```

## **#(config external-services) edit websense\_service\_name**

These commands allow you to edit Websense parameters.

### **Syntax**

```
external-services
```

This changes the prompt to:

```
SGOS#(config external-services)
```

```
edit websense_service_name
```

This changes the prompt to:

```
SGOS#(config websense websense_service_name)
```

- *subcommands*-

**option 1:** apply-by-default

**option 2:** exit

**option 3:** fail-open

**option 4:** host host

**option 5:** max-conn *max\_num\_connections*

**option 6:** no {apply-by-default | fail-open | send {client-address | client-info} | serve-exception-page}

**option 7:** port *port*

**option 8:** send {client-address | client-info}

**option 9:** sense-categories

**option 10:** serve-exception-page

**option 11:** test-url *url*

**option 12:** timeout *seconds*

**option 13:** version {4.3 | 4.4}

**option 14:** view

Table 3.43: # (config websense *websense\_service\_name*)

apply-by-default		Applies Websense by default.
exit		Exits configure websense name mode and returns to configure external-services mode.
fail-open		Fail open if service is applied by default.
host	<i>host</i>	Remote Websense hostname or IP address.
max-conn	<i>max_num_connections</i>	Specifies the maximum number of concurrent connections.
no	apply-by-default	Will not apply service by default.
	fail-open	Fail closed if service is applied by default.
	send {client-address   client-info}	Negates send options.
	serve-exception-page	Serves Websense message when content is blocked.
port	<i>port</i>	Port number of remote Websense server.
send	client-address	Sends the client address to the Websense server.
	client-info	Sends the client information to the Websense server.
sense-categories		Sense categories configured on the Websense server.
serve-exception-page		Serves built-in exception page when content is blocked.
test-url	<i>url</i>	Tests a url against the Websense server.
timeout	<i>seconds</i>	Sets the receive timeout in seconds.
version	4.3   4.4	Sets the version of the Websense server.
view		Displays the service's current configuration.

### Example

```
SGOS#(config) external-services
SGOS#(config external-services) edit testwebsense
SGOS#(config websense testwebsense) send client-address
    ok
SGOS#(config websense testwebsense) exit
SGOS#(config external-services) exit
SGOS#(config)
```

## #(config) failover

These commands allow you to configure redundancy into your network.

### Syntax

failover

This changes the prompt to:

SGOS#(config failover)

- *subcommands*-

**option 1:** create *group\_address*

**option 2:** edit *group\_address*—changes the prompt (see “#(config failover) edit *group\_address*” on page 132)

**option 3:** exit

**option 4:** delete *group\_address*

Table 3.44: #(config failover)

create	<i>group_address</i>	Creates a failover group.
edit	<i>group_address</i>	Changes the prompt. See “#(config failover) edit <i>group_address</i> ” on page 132.
exit		Exits configure failover mode and returns to configure mode.
delete	<i>group_address</i>	Deletes a failover group.

### Example

```
SGOS#(config) failover
SGOS#(config failover) create 10.9.17.135
    ok
SGOS#(config failover) exit
SGOS#(config)
```

## #(config failover) edit *group\_address*

These commands allow you to edit your failover group settings.

## Syntax

```
failover
```

This changes the prompt to:

```
SGOS#(config failover)
```

```
edit group_address
```

This changes the prompt to:

```
SGOS#(config failover group_address)
```

### - subcommands-

**option 1:** disable

**option 2:** enable

**option 3:** encrypted-secret *encrypted\_secret*

**option 4:** exit

**option 5:** interval *interval\_in\_seconds*

**option 6:** master

**option 7:** multicast-address *multicast\_address*

**option 8:** no {interval | multicast-address | master | priority | secret}

**option 9:** priority *relative\_priority*

**option 10:** secret *secret*

**option 11:** view

Table 3.45: #(config failover *group\_address*)

disable		Disables failover group indicated by <i>group_address</i> .
enable		Enables failover group indicated by <i>group_address</i> .
encrypted-secret	<i>encrypted_secret</i>	(Optional but recommended) Refers to an encrypted password shared only with the group.
exit		Exits configure failover <i>group_address</i> mode and returns to configure failover mode.
interval	<i>interval_in_seconds</i>	(Optional) Refers to the time between advertisements from the master to the multicast address. The default is 40 seconds.
master		Defines the current system as the master and all other systems as slaves.
multicast-address	<i>multicast_address</i>	Refers to a multicast address where the master sends the keepalives (advertisements) to the slave systems.

Table 3.45: #(config failover group\_address) (Continued)

no	interval	Resets the interval to the default value (40 seconds).
	multicast-address	Removes the multicast address from the failover group.
	master	Removes as configured master.
	priority	Resets the priority to the default value (100).
	secret	Clears the secret from the failover group.
priority	relative_priority	(Optional) Refers to the rank of slave systems. The range is from 1 to 253. (The master system, the one whose IP address matches the group address, gets 254.)
secret	secret	(Optional but recommended) Refers to a password shared only with the group. You can create a secret, which will then be hashed.
view		Shows the current settings for the failover group indicated by <i>group_address</i> .

**Example**

```

SGOS#(config) failover
SGOS#(config failover) edit 10.9.17.135
SGOS#(config failover 10.9.17.135) master
    ok
SGOS#(config failover 10.9.17.135) exit
SGOS#(config failover) exit
SGOS#(config)

```

 **#(config) forwarding**

The ProxySG supports the forwarding of content requests to defined hosts and groups through policy. You must add each host and group to use in forwarding content requests. To define a group, add a host and use the `group=` subcommand to add a group. Add up to 512 hosts and up to 32 groups.

To set the default load-balancing and host-affinity values, use the `(config forwarding) load-balance` or `(config forwarding) host-affinity` commands. However, three methods are available to set per host or per group settings. You can:

- Use the `(config forwarding) create` command.
- Use the `(config forwarding) load-balance` or `(config forwarding) host-affinity` commands.
- Use the `(config forwarding host_alias)` or `(config forwarding group_alias)` commands (see “#(config forwarding) edit host\_alias” on page 139 or “#(config forwarding) edit group\_alias” on page 138).

After adding forwarding hosts and groups, you can create a default sequence, which provides you with default forwarding and failover capabilities in the event that no policy gestures apply. However, Blue Coat does not recommend that you use the default sequence as a substitute for fully specifying forwarding behavior in policy.

A default failover sequence (and any sequence specified in policy) works by allowing healthy hosts to take over for an unhealthy host (one that is failing its DNS Resolution or its health check). The sequence specifies the order of failover, with the second host taking over for the first host, the third taking over for the second, and so on. All members must be pre-existing hosts and groups, and no member can be in the group more than once.

---

*Note:* The default sequence replaces the deprecated `default` and `backup` settings. The default sequence (if present) is applied only if no applicable forwarding gesture is in policy.

---

The ProxySG automatically performs health checks for all forwarding hosts. When the ProxySG performs a health check, it determines whether the host returns a response and is available to fulfill a content request. A positive health check indicates:

- An end-to-end connection exists.
- The host is up and running and will most likely be able to return a response.

## Syntax

forwarding

This changes the prompt to:

SGOS#(config forwarding)

- *subcommands* -

**option 1:** create {*host\_alias* *host\_name* [default-schemes] [http[=*port* | =no]] [https[=*port* | =no]] [ftp[=*port* | =no]] [mms[=*port* | =no]] [rtsp[=*port* | =no]] [tcp=*port*] [telnet[=*port* | =no]] [ssl-verify-server[=yes | =no]] [group=*group\_name*] [server | proxy] [load-balance={no | round-robin | least-connections}] [host-affinity={no | client-ip-address | accelerator-cookie}] [host-affinity-ssl={no | client-ip-address | accelerator-cookie | ssl-session-id}]}

**option 2:** delete {all | group *group\_name* | host *host\_alias*}

**option 3:** download-via-forwarding {disable | enable}

**option 4:** edit *host\_or\_group\_alias*—changes the prompt (see either “#(config forwarding) edit *group\_alias*” on page 138 or “#(config forwarding) edit *host\_alias*” on page 139)

**option 5:** exit

**option 6:** failure-mode {closed | open}

**option 7:** host-affinity

sub-option 1: method {accelerator-cookie [*host\_or\_group\_alias*] | client-ip-address [*host\_or\_group\_alias*] | default *host\_or\_group\_alias* | no [*host\_or\_group\_alias*]}

sub-option 2: ssl-method {accelerator-cookie [*host\_or\_group\_alias*] | client-ip-address [*host\_or\_group\_alias*] | default *host\_or\_group\_alias* | no [*host\_or\_group\_alias*] | ssl-session-id [*host\_or\_group\_alias*]}

sub-option 3: timeout *minutes*

**option 8:** integrated-host-timeout *minutes*

**option 9:** load-balance

sub-option 1: hash {default *group\_alias* | domain [*group\_alias*] | no [*group\_alias*] | url [*group\_alias*]}

sub-option 2: method {default *host\_or\_group\_alias* | least-connections [*host\_or\_group\_alias*] | no [*host\_or\_group\_alias*] | round-robin [*host\_or\_group\_alias*]}

**option 10:**no path

**option 11:**path *url*

**option 12:**sequence

sub-option 1: add *host\_or\_group\_alias*

sub-option 2: clear

sub-option 3: demote *host\_or\_group\_alias*

sub-option 4: promote *host\_or\_group\_alias*

sub-option 5: remove *host\_or\_group\_alias*

**option 13:**view

Table 3.46: # (config forwarding)

create		Creates a forwarding host/group. The only required entries under the <code>create</code> option (for a host) are <i>host_alias</i> , <i>host_name</i> , a protocol, and a port number. The port number can be defined explicitly (i.e., <code>http=8080</code> ), or it can take on the default port value of the protocol, if one exists (i.e., enter <code>http</code> , and the default port value of 80 is entered automatically).  To create a host group, you must also include the <code>group=group_name</code> command. If this is the first mention of the group, <i>group_name</i> , then that group is automatically created with this host as its first member. Do not use this command when creating an independent host.
delete	all	Deletes all forwarding hosts and groups.
	group <i>group_name</i>	Deletes only the group identified by <i>group_name</i> .
	host <i>host_alias</i>	Deletes only the host identified by <i>host_alias</i> .
download-via-forwarding	disable   enable	Disables or enables configuration file downloading using forwarding.
edit	<i>host_or_group_alias</i>	Changes the prompt. See either “# (config forwarding) edit <i>group_alias</i> ” on page 138 or “# (config forwarding) edit <i>host_alias</i> ” on page 139.



Table 3.46: # (config forwarding) (Continued)

exit		Exits configure forwarding mode and returns to configure mode.
failure-mode	closed   open	Sets the default forwarding failure mode to closed or open.
host-affinity	method {accelerator-cookie [host_or_group_alias]   client-ip-address [host_or_group_alias]   default host_or_group_alias   no [host_or_group_alias]}	Selects a host affinity method (non-SSL). If a host or group alias is not specified for the accelerator-cookie, client-ip-address, or no options, the global default is used. Use the default option to specify default configurations for all the settings for a specified host or group.
	ssl-method {accelerator-cookie [host_or_group_alias]   client-ip-address [host_or_group_alias]   default host_or_group_alias   no [host_or_group_alias]   ssl-session-id [host_or_group_alias]}	Selects a host affinity method for SSL. If a host or group alias is not specified for the accelerator-cookie, client-ip-address, no, or ssl-session-id options, the global default is used. Use the default option to specify default configurations for all the settings for a specified host or group.
	timeout minutes	Sets the timeout in minutes for the host affinity.
integrated-host-timeout	minutes	Sets the timeout for aging out unused integrated hosts.
load-balance	hash {default group_alias   domain [group_alias]   url [group_alias]   no [group_alias]}	Sets if and how load balancing hashes between group members. If a group alias is not specified for the domain, url, or no options, the global default is used. Use the default option to specify default configurations for all the settings for a specified group
	method {default host_or_group_alias   least-connections [host_or_group_alias]   round-robin [host_or_group_alias]   no [host_or_group_alias]}	Sets the load balancing method. If a host or group alias is not specified for the least-connections, round-robin, or no options, the global default is used. Use the default option to specify default configurations for all the settings for a specified host or group.
no path		Negates certain forwarding settings.
path	url	Sets the network path to download forwarding settings.

Table 3.46: #(config forwarding) (Continued)

sequence	add <i>host_or_group_alias</i>	Adds an alias to the end of the default failover sequence.
	clear	Clears the default failover sequence.
	demote <i>host_or_group_alias</i>	Demotes an alias one place towards the end of the default failover sequence.
	promote <i>host_or_group_alias</i>	Promotes an alias one place towards the start of the default failover sequence.
	remove <i>host_or_group_alias</i>	Removes an alias from the default failover sequence.
view		Displays the currently defined forwarding groups or hosts.

**Example**

```
SGOS#(config) forwarding
SGOS#(config forwarding) download-via-forwarding disable
ok
SGOS#(config forwarding) failure-mode closed
ok
SGOS#(config forwarding) host-affinity method client-ip-address
ok
SGOS#(config forwarding) load-balance hash domain group_name1
ok
SGOS#(config forwarding) exit
SGOS#(config)
```

 **#(config forwarding) edit group\_alias**

These commands allow you to edit the settings of a specific forwarding group.

**Syntax**

forwarding

This changes the prompt to:

```
SGOS#(config forwarding)
```

```
edit group_alias
```

This changes the prompt to:

```
SGOS#(config forwarding group_alias)
```

**- subcommands-**

**option 1:** exit

**option 2:** host-affinity

sub-option 1: method {accelerator-cookie | client-ip-address | default}

sub-option 2: ssl-method {accelerator-cookie | client-ip-address | default |  
ssl-session-id}

**option 3:** load-balance

```

sub-option 1: hash {default | domain | url}
sub-option 2: method {default | least-connections | round-robin}

```

**option 4:** no

```

sub-option 1: host-affinity {method | ssl-method}
sub-option 2: load-balance {hash | method}

```

**option 5:** view**Table 3.47:** # (config forwarding *group\_alias*)

exit		Exits configure forwarding <i>group_alias</i> mode and returns to configure forwarding mode.
host-affinity	method {accelerator-cookie   client-ip-address   default}	Changes the host affinity method (non-SSL) for this group.
	ssl-method {accelerator-cookie   client-ip-address   default   ssl-session-id}	Changes the host affinity method (SSL) for this group.
load-balance	hash {default   domain   url}	Changes if and how load balancing hashes between group members.
	method {default   least-connections   round-robin}	Changes the load balancing method.
no	host-affinity {method   ssl-method}	Disables a host affinity setting for this group.
	load-balance {hash   method}	Disables a load balancing setting for this group.
view		Shows the current settings for this forwarding group.

**Example**

```

SGOS#(config) forwarding
SGOS#(config forwarding) edit test_group
SGOS#(config forwarding test_group) load-balance hash domain
ok
SGOS#(config forwarding test_group) exit
SGOS#(config forwarding) exit
SGOS#(config)

```

**#(config forwarding) edit *host\_alias***

These commands allow you to edit the settings of a specific forwarding host.

**Syntax**

```
forwarding
```

This changes the prompt to:

```
SGOS#(config forwarding)
edit host_alias
```

This changes the prompt to:

```
SGOS#(config forwarding host_alias)
```

**- subcommands-**

**option 1:** exit

**option 2:** ftp [port]

**option 3:** group group\_name

**option 4:** host host\_name

**option 5:** host-affinity

sub-option 1: method {accelerator-cookie | client-ip-address | default}

sub-option 2: ssl-method {accelerator-cookie | client-ip-address | default |  
ssl-session-id}

**option 6:** http [port]

**option 7:** https [port]

**option 8:** load-balance method {default | least-connections | round-robin}

**option 9:** mms [port]

**option 10:** no {ftp | group | host-affinity {method | ssl-method} | http | https |  
load-balance method | mms | rtsp | ssl-verify-server | tcp | telnet}

**option 11:** proxy

**option 12:** rtsp [port]

**option 13:** server

**option 14:** ssl-verify-server

**option 15:** tcp port

**option 16:** telnet [port]

**option 17:** view

Table 3.48: #(config forwarding *host\_alias*)

exit		Exits configure forwarding <i>host_alias</i> mode and returns to configure forwarding mode.
ftp	[ <i>port</i> ]	Changes the FTP port to the default port or to a port that you specify.
group	<i>group_name</i>	Specifies the group (or server farm or group of proxies) to which this host belongs.  The ProxySG uses load balancing to evenly distribute forwarding requests to the origin servers or group of proxies. Do not use the <i>group</i> option when creating independent hosts.
host	<i>host_name</i>	Changes the host name.
host-affinity	method { <i>accelerator-cookie</i>   <i>client-ip-address</i>   default}	Changes the host affinity method (non-SSL) for this host.
	ssl-method { <i>accelerator-cookie</i>   <i>client-ip-address</i>   default   <i>ssl-session-id</i> }	Changes the host affinity method (SSL) for this host.
http	[ <i>port</i> ]	Changes the HTTP port to the default port or to a port that you specify.
https	[ <i>port</i> ]	Changes the HTTPS port to the default port or to a port that you specify.
load-balance	method {default   <i>least-connections</i>   <i>round-robin</i> }	Changes the load balancing method.
mms	[ <i>port</i> ]	Changes the MMS port to the default port or to a port that you specify.
no	ftp   group   host-affinity {method   ssl-method}   http   https   load-balance method   mms   rtsp   ssl-verify-server   tcp   telnet	Deletes a setting for this host.
proxy		Makes the host a proxy instead of a server; any HTTPS or TCP port are deleted.
rtsp	[ <i>port</i> ]	Changes the RTSP port to the default port or to a port that you specify.
server		Makes the host a server instead of a proxy.

Table 3.48: #(config forwarding *host\_alias*) (Continued)

ssl-verify-server		Sets SSL to verify server certificates.
tcp	<i>port</i>	Changes the TCP port.
telnet	[ <i>port</i> ]	Changes the Telnet port to the default port or to a port that you specify.
view		Shows the current settings for this forwarding host.

**Example**

```
SGOS#(config) forwarding
SGOS#(config forwarding) edit test_host
SGOS#(config forwarding test_host) server
ok
SGOS#(config forwarding test_host) exit
SGOS#(config forwarding) exit
SGOS#(config)
```

## #(config) front-panel

Use this command to configure the front panel. For instance, the front-panel LCD behavior can be configured using the `backlight` command.

### Syntax

```
front-panel
```

This changes the prompt to:

```
SGOS#(config front-panel)
```

**- subcommands-**

**option 1:** backlight

sub-option 1: flash

sub-option 2: state {off | on | timeout}

sub-option 3: timeout *seconds*

**option 2:** exit

**option 3:** hashed-pin *hashed\_PIN*

**option 4:** no backlight flash

**option 5:** pin *PIN*

**option 6:** view

Table 3.49: #(config front-panel)

backlight	flash	The front-panel LCD is configured to flash, which can, for instance, help you locate a particular appliance in a room full of appliances.
	state {off   on   timeout}	The front-panel LCD is configured to be always turned on, always turned off, or to turn off after a specified length of time (use the <code>backlight timeout</code> command to configure the length of time).
	timeout <i>seconds</i>	Configures the length of time before the front-panel LCD turns off. You must also set the <code>backlight state timeout</code> command to configure timeout mode.
exit		Exits configure front-panel mode and returns to configure mode.
hashed-pin	<i>hashed_PIN</i>	Specifies a front-panel PIN in hashed format.
no	backlight flash	Stops the front-panel LCD from flashing.
pin	<i>PIN</i>	Sets a four-digit PIN to restrict access to the front panel of the ProxySG. To clear the PIN, specify 0000 instead of a real PIN.
view		Displays the front panel settings.

**Example**

```

SGOS#(config) front-panel
SGOS#(config front-panel) backlight state timeout
ok
SGOS#(config front-panel) backlight timeout 60
ok
SGOS#(config front-panel) exit
SGOS#(config)

```

 **#(config) ftp**

Use this command to configure FTP parameters.

**Syntax**

**option 1:** ftp login-syntax {raptor | checkpoint}  
**option 2:** ftp no welcome-banner

**option 3:** ftp welcome-banner *banner*

Table 3.50: # (config) ftp

login-syntax	{raptor   checkpoint}	Toggles between Raptor and Checkpoint login syntax. The default is raptor.
no welcome-banner		No text is displayed to an FTP client when a connection occurs.
welcome-banner	<i>banner</i>	Customizes the text displayed to an FTP client when a connection occurs.

## #(config) health-check

Use this command to configure health check settings.

---

**Note:** Using the `pause` command to temporarily pause the forwarding or SOCKS gateways health checks causes the system to stay in `pause` mode until you use the `resume` command to end it—rebooting the system will not cause paused health checks to resume.

---

### Syntax

health-check

This changes the prompt to:

SGOS# (config health-check)

- subcommands-

**option 1:** create *entry\_name*

**option 2:** delete *entry\_name*

**option 3:** edit *entry\_name*—changes the prompt (see “# (config health-check) edit *entry\_name*” on page 146)

**option 4:** exit

**option 5:** forwarding

sub-option 1: failcount *count*

sub-option 2: interval *seconds*

sub-option 3: pause

sub-option 4: resume

sub-option 5: type {http *object* | https *object* | layer-3 | layer-4}

**option 6:** socks-gateways

sub-option 1: failcount *count*

sub-option 2: interval *seconds*

sub-option 3: pause

sub-option 4: resume

sub-option 5: type {layer-3 | layer-4}

**option 7:** statistics



**option 8:** view

**Table 3.51:** # (config health-check)

create	<i>entry_name</i>	Adds a health check entry specified by <i>entry_name</i> .
delete	<i>entry_name</i>	Deletes the specified health check entry.
edit	<i>entry_name</i>	Changes the prompt. See “# (config health-check) edit <i>entry_name</i> ” on page 146.
exit		Exits configure health check mode and returns to configure mode.
forwarding	<i>failcount count</i>	Configures the forwarding health check failure count.
	<i>interval seconds</i>	Configures the forwarding health check interval in seconds.
	pause	Pauses the forwarding health checks temporarily (the system remains in pause mode until you use the <code>resume</code> command to end it).
	resume	Resumes the forwarding health checks.
	type {http object   https object   layer-3   layer-4}	Configures the forwarding health check type.
socks-gateways	<i>failcount count</i>	Configures the SOCKS gateways health check failure count.
	<i>interval seconds</i>	Configures the SOCKS gateways health check interval in seconds.
	pause	Pauses the SOCKS gateways health checks temporarily (the system remains in pause mode until you use the <code>resume</code> command to end it).
	resume	Resumes the SOCKS gateways health checks.
	type {layer-3   layer-4}	Configures the SOCKS gateways health check type.
show health-check		Displays health check settings for layer-3 and layer-4 types. This command does not show ICAP or Websense 4 settings.
statistics		Displays health check statistics.
view		Displays the current health check configurations for forwarding and SOCKS gateways settings.

### Example

```
SGOS#(config) health-check
SGOS#(config health-check) socks-gateways type layer-3
    ok
SGOS#(config health-check) exit
SGOS#(config)
```

## #(config health-check) edit *entry\_name*

Use this command to edit health check entries.

### Syntax

health-check

This changes the prompt to:

```
SGOS#(config health-check)
```

```
edit entry_name
```

This changes the prompt to:

```
SGOS#(config health-check entry_name)
```

#### - subcommands-

**option 1:** exit

**option 2:** failure-trigger *trigger*

**option 3:** http url *url*

**option 4:** https url *url*

**option 5:** icap service-name *service\_name*

**option 6:** interval

sub-option 1: healthy *interval\_in\_seconds*

sub-option 2: sick *interval\_in\_seconds*

**option 7:** layer-3 hostname *hostname*

**option 8:** layer-4

sub-option 1: hostname *hostname*

sub-option 2: port *port*

**option 9:** no notify

**option 10:** notify

**option 11:** perform-health-check

**option 12:** statistics

**option 13:** threshold

sub-option 1: healthy *threshold*

sub-option 2: sick *threshold*

**option 14:** type {layer-3 | layer-4 | http | https | icap | websense4-offbox}

**option 15:**view

**option 16:**websense-offbox {default-url | service-name *service\_name* | url *test\_url*}

Table 3.52: #(config health-check *entry\_name*)

exit		Exits configure health check <i>entry_name</i> mode and returns to configure health check mode.
failure-trigger	<i>trigger</i>	Sets failure count to trigger a health check.
http url	<i>url</i>	Configures HTTP health check parameters.
https url	<i>url</i>	Configures HTTPS health check parameters.
icap service-name	<i>service_name</i>	Configures ICAP health check parameters.
interval	healthy <i>interval_in_seconds</i>	Configures the health check healthy intervals.
	sick <i>interval_in_seconds</i>	Configures the health check sick intervals.
layer-3 hostname	<i>hostname</i>	Configures layer-3 health check parameters.
layer-4 hostname	<i>hostname</i>	Configures layer-4 health check parameters.
no notify		Disables e-mail notification of state changes.
notify		Enables e-mail notification of state changes.
perform-health-check		Performs a health check.
statistics		Shows current health check statistics.
threshold	healthy <i>threshold</i>	The number of successful checks before a transition to healthy.
	sick <i>threshold</i>	The number of failed checks before a transition to sick.
type	layer-3	Performs layer-3 health checks.
	layer-4	Performs layer-4 health checks.
	http	Performs HTTP health checks.
	https	Performs HTTPS health checks.
	icap	Performs ICAP health checks.
	websense4-offbox	Performs Websense health checks.
view		Shows the entry's current configuration.
websense-offbox	default-url	Uses the default Websense URL for health checks.
	service-name <i>service_name</i>	Configures the Websense service-name to health check.
	url <i>test_url</i>	Configures the Websense URL to health check.

### Example

```
SGOS#(config) health-check
SGOS#(config health-check) edit testhealthcheck
SGOS#(config health-check testhealthcheck) type https
ok
SGOS#(config health-check testhealthcheck) exit
SGOS#(config health-check) exit
SGOS#(config)
```

## #(config) hide-advanced

See “# hide-advanced” on page 27 in Chapter 2: “Standard and Privileged Mode Commands”.

## #(config) hostname

Use this command to assign a name to a ProxySG. Any descriptive name that helps identify the system will do.

### Syntax

**option 1:** hostname *name*

Table 3.53: #(config) hostname

<i>name</i>	Associates <i>name</i> with the current ProxySG.
-------------	--

### Example

```
SGOS#(config) hostname "Blue Coat Systems Demo"
ok
```

## #(config) http

Use this command to configure HTTP settings.

### Syntax

**option 1:** http add-header {client-ip | front-end-https | via | x-forwarded-for}

**option 2:** http byte-ranges

**option 3:** http cache {authenticated-data | expired | personal-pages}

**option 4:** http force-ntlm

**option 5:** http ftp-proxy-url {root-dir | user-dir}

**option 6:** http no

sub-option 1: add-header {client-ip | front-end-https | via | x-forwarded-for}

sub-option 2: byte-ranges

sub-option 3: cache {authenticated-data | expired | personal-pages}

sub-option 4: force-ntlm

sub-option 5: parse meta-tag cache-control | expires | pragma-no-cache

```

sub-option 6: persistent {client | server}
sub-option 7: pipeline {client {requests | redirects} | prefetch {requests |
    redirects}}
sub-option 8: proprietary-headers bluecoat
sub-option 9: revalidate-pragma-no-cache
sub-option 10: ssl-verify-server
sub-option 11: strict-expiration {refresh | serve}
sub-option 12: strip-from-header
sub-option 13: substitute {conditional | ie-reload | if-modified-since |
    pragma-no-cache}
sub-option 14: tolerant-request-parsing
sub-option 15: www-redirect
sub-option 16: xp-rewrite-redirect
option 7: http parse meta-tag cache-control | expires | pragma-no-cache
option 8: http persistent {client | server}
option 9: http persistent-timeout {client | server}
option 10: http pipeline {client {requests | redirects} | prefetch {requests |
    redirects}}
option 11: http proprietary-headers bluecoat
option 12: http receive-timeout {client | refresh | server}
option 13: http revalidate-pragma-no-cache
option 14: http ssl-verify-server
option 15: http strict-expiration {refresh | serve}
option 16: http strip-from-header
option 17: http substitute {conditional | ie-reload | if-modified-since |
    pragma-no-cache}
option 18: http tolerant-request-parsing
option 19: http upload-with-pasv {disable | enable}
option 20: http version {1.0 | 1.1}
option 21: http www-redirect
option 22: xp-rewrite-redirect

```

Table 3.54: #(config) http

add-header	client-ip	Adds the client-ip header to forwarded requests.
	front-end-https	Adds the front-end-https header to forwarded requests.
	via	Adds the via header to forwarded requests.
	x-forwarded-for	Adds the x-forwarded-for header to forwarded requests.

Table 3.54: # (config) http (Continued)

byte-ranges		<p>Enables HTTP byte-range support.</p> <p>If byte-range support is disabled, then HTTP will treat all byte range requests as non-cacheable. This means that HTTP will never even check to see whether the object is in the cache, but will forward the request to the origin-server and not cache the result. So the range request will have no affect on the cache. For instance, if the object was in the cache before a range request, then it would still be in the cache afterward—the range request will not delete any currently cached objects. Also, the Range header is not modified when forwarded to the origin-server.</p> <p>If the requested byte range is type 3 or 4, then the request is treated as if byte-range support is disabled. That is, the request is treated as non-cacheable and will not have any affect on objects in the cache.</p>
cache	authenticated-data	Caches any data that appears to be authenticated.
	expired	Retains cached objects older than the explicit expiration.
	personal-pages	Caches objects that appear to be personal pages.
force-ntlm		Uses NTLM for Microsoft Internet Explorer proxy.
ftp-proxy-url	root-dir	URL path is absolute in relation to the root.
	user-dir	URL path is relative to the user's home directory.
no	<i>parameter</i>	Negates the specified command.
parse meta-tag	cache-control   expires   pragma-no-cache	Parses HTML objects for the cache-control, expires, and pragma-no-cache meta-tags.
persistent	client	Enables support for persistent client requests from the browser.
	server	Enables support for persistent server requests to the Web server.
persistent-timeout	client <i>num_seconds</i>	Sets persistent connection timeout for the client to <i>num_seconds</i> .
	server <i>num_seconds</i>	Sets persistent connection timeout for the server to <i>num_seconds</i> .

Table 3.54: # (config) http (Continued)

pipeline	client {redirects   requests}	Prefetches either embedded objects in client requests or redirected responses to client requests.
	prefetch {redirects   requests}	Prefetches either embedded objects in pipelined objects or redirected responses to pipelined requests.
proprietary-headers	bluecoat	Enables the Blue Coat Systems proprietary HTTP header extensions.
receive-timeout	client <i>num_seconds</i>	Sets receive timeout for client to <i>num_seconds</i> .
	refresh <i>num_seconds</i>	Sets receive timeout for refresh to <i>num_seconds</i> .
	server <i>num_seconds</i>	Sets receive timeout for server to <i>num_seconds</i> .
revalidate-pragma-no-cache		Revalidates "Pragma: no-cache."
ssl-verify-server		Enables verification of server certificate during an HTTPS connection (overridden by forwarding).
strict-expiration	refresh	Forces compliance with explicit expirations by never refreshing objects before their explicit expiration.
	serve	Forces compliance with explicit expirations by never serving objects after their explicit expiration.
strip-from-header		Removes HTTP information from headers.
substitute	conditional	Uses an HTTP "get" in place of HTTP 1.1 conditional get
	ie-reload	Uses an HTTP "get" for Microsoft Internet Explorer reload requests.
	if-modified-since	Uses an HTTP "get" instead of "get-if-modified."
	pragma-no-cache	Uses an HTTP "get" instead of "get pragma: no-cache."
tolerant-request-parsing	no	Enables or disables the HTTP tolerant-request-parsing flag.
upload-with-pasv	disable	Disables uploading with Passive FTP.
	enable	Enables uploading with Passive FTP.
version	1.0	Indicates the version of HTTP that should be used by the ProxySG.
	1.1	
www-redirect		Redirects to <i>www.host.com</i> if host not found.
xp-rewrite-redirect		Rewrites origin server 302s to 307s for Windows XP IE requests.

### Example

```
SGOS#(config) http version 1.1
ok
SGOS#(config) http byte-ranges
ok
SGOS#(config) http no force-ntlm
ok
SGOS#(config)
```

## #(config) icp

ICP is a caching communication protocol. It allows a cache to query other caches for an object, without actually requesting the object. By using ICP, the ProxySG determines if the object is available from a neighboring cache, and which ProxySG will provide the fastest response.

Once you have created the ICP or advanced forwarding configuration file, place the file on an FTP or HTTP server so it can be downloaded to the ProxySG.

### Syntax

**option 1:** `icp no path`

**option 2:** `icp path url`

Table 3.55: #(config) icp

no path		Negates the path previously set using the command <code>icp path url</code> .
path	url	Specifies the network location of the ICP configuration file to download.

### Example

```
SGOS#(config) icp path 10.25.36.47/files/icpconfig.txt
ok
```

## #(config) identd

IDENTD implements the TCP/IP IDENT user identification protocol. IDENTD operates by looking up specific TCP/IP connections and returning the user name of the process owning the connection.

### Syntax

`identd`

This changes the prompt to:

```
SGOS#(config identd)
```

**-subcommands-**

**option 1:** `disable`

**option 2:** `enable`

**option 3:** `exit`



**option 4:** view

Table 3.56: #(config identd)

disable		Disables IDENTD.
enable		Enables IDENTD.
exit		Exits configure identd mode and returns to configure mode.
view		Displays current IDENTD settings.

#### Example

```
SGOS#(config) identd
SGOS#(config identd) enable
ok
SGOS#(config identd) exit
SGOS#(config)
```

## #(config) im

You can configure the IM proxy settings, assign an administrator buddy name for each client type, and determine how exception messages are sent.

### Syntax

```
option 1: im aol-admin-buddy buddy
option 2: im aol-direct-proxy-host host
option 3: im aol-http-host host
option 4: im aol-native-host host
option 5: im buddy-spoof-message message_text
option 6: im exceptions {in-band | out-of-band}
option 7: im explicit-proxy-vip virtual_IP_address
option 8: im msn-admin-buddy buddy
option 9: im msn-http-host host
option 10: im msn-native-host host
option 11: no
option 12: im yahoo-admin-buddy buddy
option 13: im yahoo-download-host host
option 14: im yahoo-http-host host
option 15: im yahoo-http-chat-host host
option 16: im yahoo-native-host host
option 17: im yahoo-upload-host host
```

Table 3.57: #(config) im

aol-admin-buddy	<i>buddy</i>	Set AOL admin buddy name.
aol-direct-proxy-host	<i>host</i>	Set AOL direct proxy host.
aol-http-host	<i>host</i>	Set AOL HTTP host.
aol-native-host	<i>host</i>	Set AOL native host.
buddy-spoof-message	<i>message_text</i>	Set buddy spoof message.
exceptions	<i>in-band</i>	Deliver IM exceptions in band.
	<i>out-of-band</i>	Deliver IM exceptions out of band.
explicit-proxy-vip	<i>virtual_IP_address</i>	Set explicit proxy virtual IP address.
msn-admin-buddy	<i>buddy</i>	Set MSN admin buddy name.
msn-http-host	<i>host</i>	Set MSN HTTP host.
msn-native-host	<i>host</i>	Set MSN native host.
yahoo-admin-buddy	<i>buddy</i>	Set Yahoo admin buddy name.
yahoo-download-host	<i>host</i>	Set Yahoo download host.
http-host	<i>host</i>	Set Yahoo HTTP host.
http-http-chat-host	<i>host</i>	Set Yahoo HTTP chat host.
yahoo-native-host	<i>host</i>	Set Yahoo native host.
yahoo-upload-host	<i>host</i>	Set Yahoo upload host.

**Example**

```
SGOS#(config) im exceptions in-band
ok
SGOS#(config) im yahoo-admin-buddy testname
ok
```

## #(config) inline

See “# inline” on page 27 in Chapter 2: “Standard and Privileged Mode Commands”.

## #(config) installed-systems

Use this command to manage the list of installed ProxySG systems.

**Syntax**

```
installed-systems
```

This changes the prompt to:

```
SGOS#(config installed-systems)
```

**-subcommands-**

**option 1:** default *system\_number*

**option 2:** delete *system\_number*

**option 3:** exit

**option 4:** lock *system\_number*  
**option 5:** no {lock *system\_number* | replace}  
**option 6:** replace *system\_number*  
**option 7:** view

Table 3.58: #(config installed-systems)

default	<i>system_number</i>	Sets the default system to the system indicated by <i>system_number</i> .
delete	<i>system_number</i>	Deletes the system indicated by <i>system_number</i> .
exit		Exits configure installed-systems mode and returns to configure mode.
lock	<i>system_number</i>	Locks the system indicated by <i>system_number</i> .
no	lock <i>system_number</i>	Unlocks the system indicated by <i>system_number</i> if it is currently locked.
	replace	Specifies that the system currently tagged for replacement should not be replaced. The default replacement is used (oldest unlocked system).
replace	<i>system_number</i>	Specifies that the system identified by <i>system_number</i> is to be replaced next.
view		Shows installed ProxySG systems.

**Example**

```
SGOS#(config) installed-systems
SGOS#(config installed-systems) default 2
ok
SGOS#(config installed-systems) lock 1
ok
SGOS#(config installed-systems) exit
SGOS#(config)
```

 **#(config) interface**

This command enables you to configure the network interfaces.

The built-in Ethernet adapter is configured for the first time using the setup console. If you want to modify the built-in adapter configuration, or if you have multiple adapters, you can configure each one using the command-line interface.

**Syntax**

```
interface fast-ethernet interface_number
```

Table 3.59: # (config) interface

fast-ethernet	<i>interface_number</i>	Sets the number of the fast Ethernet connection to <i>interface_number</i> . Valid values for <i>interface_number</i> are 0 through 3, inclusive.
---------------	-------------------------	---

This changes the prompt to:

```
SGOS#(config interface interface_number)
```

**- subcommands-**

**option 1:** accept-inbound

**option 2:** exit

**option 3:** full-duplex

**option 4:** half-duplex

**option 5:** ip-address *ip\_address*

**option 6:** instructions {accelerated-pac | central-pac *url* | default-pac | proxy}

**option 7:** link-autosense

**option 8:** mtu-size *mtu\_size*

**option 9:** no {accept-inbound | link-autosense}

**option 10:** speed {10 | 100 | 1gb}

**option 11:** subnet-mask *mask*

Table 3.60: # (config interface *interface\_number*)

accept-inbound		Permits inbound connections to this interface.
exit		Exits configure interface number mode and returns to configure mode.
full-duplex		Configures this interface for full duplex.
half-duplex		Configures this interface for half duplex.
ip-address	<i>ip_address</i>	Sets the IP address for this interface to <i>ip_address</i> .
instructions	accelerated-pac	Configures browser to use your accelerated pac file.
	central-pac <i>url</i>	Configures browser to use your pac file.
	default-pac	Configures browser to use a Blue Coat Systems pac file.
	proxy	Configures browser to use a proxy.
link-autosense		Specifies that the interface should autosense speed and duplex.
mtu-size	<i>mtu_size</i>	

Table 3.60: # (config interface *interface\_number*) (Continued)

no	accept-inbound	Negates the current accept-inbound settings.
	link-autosense	Negates the current link-autosense settings.
speed	10   100   1gb	Specifies the interface speed.
subnet-mask	<i>subnet_mask</i>	Sets the subnet mask for the interface.
view		Shows the interface settings.

**Example**

```

SGOS#(config) interface 0
SGOS#(config interface 0) ip-address 10.252.10.54
ok
SGOS#(config interface 0) instructions accelerated-pac
ok
SGOS#(config interface 0) subnet-mask 255.255.255.0
ok
SGOS#(config interface 0) exit
SGOS#(config) interface 1
SGOS#(config interface 1) ip-address 10.252.10.72
ok
SGOS#(config interface 1) subnet-mask 255.255.255.0
ok
SGOS#(config interface 1) exit
SGOS#(config)

```

**#(config) ip-default-gateway**

A key feature of the ProxySG is the ability to distribute traffic originating at the cache through multiple IP gateways. Further, you can fine tune how the traffic is distributed among gateways. This feature works with any routing protocol (for example, static routes or RIP).

*Note:* Load balancing through multiple IP gateways is independent from the per-interface load balancing that the ProxySG automatically does when more than one network interface is installed.

**Syntax**

```
ip-default-gateway ip_address [preference group (1-10)] [weight (1-100)]
```

Table 3.61: # (config) ip-default-gateway

<i>ip_address</i>	[preference group (1-10)] [weight (1-100)]	Specifies the IP address of the default gateway to be used by the ProxySG.
-------------------	--	--

### Example

```
SGOS#(config) ip-default-gateway 10.25.36.47
ok
```

## #(config) license-key

Use this command to configure license key settings.

### Syntax

**option 1:** license-key auto-update {disable | enable}

**option 2:** license-key no path

**option 3:** license-key path *url*

Table 3.62: #(config) license-key

auto-update	disable   enable	Disables or enables auto-update of the Blue Coat Systems license key.
no path		Negates certain license key settings.
path	<i>url</i>	Specifies the network path to download the license key.

### Example

```
SGOS#(config) license-key no path
ok
```

## #(config) line-vty

When you have a CLI session, that session will remain open as long as there is activity. If you leave the session idle, the connection will eventually timeout and you will have to reconnect. The default timeout is five minutes. You can set the timeout and other session-specific options using the `line-vty` command.

### Syntax

```
line-vty
```

This changes the prompt to:

```
SGOS#(config line-vty)
```

- *subcommands* -

**option 1:** exit

**option 2:** length *num\_lines\_on\_screen*

**option 3:** no length

**option 4:** telnet {no transparent | transparent}

**option 5:** timeout *minutes*

**option 6:** view

Table 3.63: #(config) line-vty

exit		Exits configure line-vty mode and returns to configure mode.
length	<i>num_lines_on_screen</i>	Specifies the number of lines of code that should appear on the screen at once. Specify 0 to scroll without pausing.
no	length	Disables screen paging.
telnet	no transparent   transparent	Indicates that this is a Telnet protocol-specific configuration. If you specify <i>no transparent</i> , carriage returns are sent to the console as a carriage return plus linefeed. If you specify <i>transparent</i> , carriage returns are sent to the console as a carriage return.
timeout	<i>minutes</i>	Sets the line timeout to the number of minutes indicated by <i>minutes</i> .
view		Displays running system information.

**Example**

```

SGOS#(config) line-vty
SGOS#(config line-vty) timeout 60
ok
SGOS#(config line-vty) exit
SGOS#(config)

```

 **#(config) load**

See “# load” on page 32 in Chapter 2: “Standard and Privileged Mode Commands”.

 **#(config) netbios**

Use this command to configure NETBIOS.

**Syntax**

```
netbios
```

This changes the prompt to:

```
SGOS#(config netbios)
```

**option 1:** exit

**option 2:** nbstat requester {retries | timeout} | responder {enable | disable}

**option 3:** view

Table 3.64: #(config netbios)

exit		Exits configure netbios mode and returns to configure mode.
nbstat	requester retries   timeout responder enable   disable	Requester is enabled by default, with three retries and a five-second timeout. Responder is disabled by default.
view		Shows the NETBIOS settings.

**Example**

```

SGOS#(config) netbios
SGOS#(config netbios) nbstat responder enable
ok
SGOS#(config netbios) exit
SGOS#(config)
ok

```

 **#(config) no**

Use this command to negate the current settings for the archive configuration, content priority, IP default gateway, SOCKS machine, or system upgrade path.

**Syntax**

**option 1:** no archive-configuration

**option 2:** no bridge *bridge\_name*

**option 3:** no content {priority {regex *regex* | url *url*} | outstanding-requests {delete | priority | revalidate} *regex*}

**option 4:** no ip-default-gateway *ip\_address*

**option 5:** no serial-number

**option 6:** no socks-machine-id

**option 7:** no upgrade-path

Table 3.65: #(config) no

archive-configuration		Clears the archive configuration upload site.
bridge	<i>bridge_name</i>	Clears the bridge configuration.
content	priority {regex <i>regex</i>   url <i>url</i> }	Removes a deletion regular expression policy or a deletion URL policy.
	outstanding-requests {delete   priority   revalidate} <i>regex</i>	Deletes a specific, regular expression command in-progress (revalidation, priority, or deletion).



Table 3.65: # (config) no (Continued)

ip-default-gateway	<i>ip_address</i>	Sets the default gateway IP address to zero.
serial-number		Removes the serial number.
socks-machine-id		Removes the SOCKS machine ID from the configuration.
upgrade-path		Clears the upgrade image download path.

**Example**

```

SGOS# (config) no archive-configuration
ok
SGOS# (config) no content priority regex http://.*cnn.com
ok
SGOS# (config) no content priority url http://www.bluecoat.com
ok
SGOS# (config) no ip-default-gateway 10.252.10.50
ok
SGOS# (config) no socks-machine-id
ok
SGOS# (config) no upgrade-path
ok

```

**#(config) ntp**

Use this command to set NTP parameters. Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock times in a network of computers. The ProxySG sets the UTC time by connecting to an NTP server. The ProxySG includes a list of NTP servers available on the Internet. If an NTP server is not available, you can set the time manually using the Management Console.

**Syntax**

```

option 1: ntp clear
option 2: ntp disable
option 3: ntp enable
option 4: ntp interval minutes
option 5: ntp no server domain_name
option 6: ntp server domain_name

```

Table 3.66: # (config) ntp

clear		Removes all entries from the NTP server list.
disable		Disables NTP.

Table 3.66: # (config) ntp (Continued)

enable		Enables NTP.
interval	<i>minutes</i>	Specifies how often to perform NTP server queries.
no server	<i>domain_name</i>	Removes the NTP server named <i>domain_name</i> from the NTP server list.
server	<i>domain_name</i>	Adds the NTP server named <i>domain_name</i> from the NTP server list.

**Example**

```
SGOS#(config) ntp server clock.tricity.wsu.edu
ok
```

## #(config) policy

Use this command to specify central and local policy file location, status, and other options.

**Syntax**

```
option 1: policy central-path url
option 2: policy forward-path url
option 3: policy local-path url
option 4: policy no
    sub-option 1: central-path
    sub-option 2: forward-path
    sub-option 3: local-path
    sub-option 4: notify
    sub-option 5: subscribe
    sub-option 6: vpm-cpl-path
    sub-option 7: vpm-software
    sub-option 8: vpm-xml-path
option 5: policy notify
option 6: policy order order of v)pm, l)ocal, c)entral
option 7: policy poll-interval minutes
option 8: policy poll-now
option 9: policy proxy-default {allow | deny}
option 10: policy reset
option 11: policy subscribe
option 12: policy vpm-cpl-path url
option 13: policy vpm-software url
option 14: policy vpm-xml-path url
```

Table 3.67: # (config) policy

central-path	<i>url</i>	Specifies the network path (indicated by <i>url</i> ) from which the central policy file can be downloaded.
forward-path	<i>url</i>	Specifies the network path (indicated by <i>url</i> ) from which the forward policy file can be downloaded.
local-path	<i>url</i>	Specifies the network path (indicated by <i>url</i> ) from which the local policy file can be downloaded.
vpm-cpl-path	<i>url</i>	Specifies the network path (indicated by <i>url</i> ) from which the vpm-cpl policy file can be downloaded.
vpm-xml-path	<i>url</i>	Specifies the network path (indicated by <i>url</i> ) from which the vpm-xml policy file can be downloaded.
no	central-path	Specifies that the current central policy file URL setting should be cleared.
	forward-path	Specifies that the current forward policy file URL setting should be cleared.
	local-path	Specifies that the current local policy file URL setting should be cleared.
	notify	Specifies that no e-mail notification should be sent if the central policy file should change.
	subscribe	Specifies that the current policy should not be automatically updated in the event of a central policy change.
	vpm-cpl-path	Clears the network path to download VPM CPL policy.
	vpm-software	Clears the network path to download VPM software.
notify	vpm-xml-path	Clears the network path to download VPM XML policy.
		Specifies that an e-mail notification should be sent if the central policy file should change.
order	<i>order of v)pm, l)ocal, c)entral</i>	Specifies the policy evaluation order.
poll-interval	<i>minutes</i>	Specifies the number of minutes that should pass between tests for central policy file changes.
poll-now		Tests for central policy file changes immediately.

Table 3.67: # (config) policy (Continued)

proxy-default	allow	The default proxy policy is allow.
	deny	The default proxy policy is deny.
reset		Clears all policies.
subscribe		Indicates that the current policy should be automatically updated in the event of a central policy change.
vpm-software	url	Specifies the network path to download the VPM software.

**Example**

```
SGOS# (config) policy local-path http://www.server1.com/local.txt
ok
SGOS# (config) policy central-path http://www.server2.com/central.txt
ok
SGOS# (config) policy poll-interval 10
ok
```

## #(config) profile

Sets your system profile to normal (the default setting) or portal (to accelerate the server).

**Syntax**

**option 1:** profile bwgain  
**option 2:** profile normal  
**option 3:** profile portal

Table 3.68: # (config) profile

bwgain		Sets your system profile to bandwidth gain.
normal		Sets your system profile to normal.
portal		Sets your system profile to portal.

**Example**

```
SGOS# (config) profile normal
ok
```

## #(config) restart

Use this command to set restart options for the ProxySG.

**Syntax**

**option 1:** restart core-image {context | full | keep *number* | none}  
**option 2:** restart mode {hardware | software}

Table 3.69: `#(config) restart`

core-image	context	Indicates only core image context should be written on restart.
	full	Indicates full core image should be written on restart.
	keep <i>number</i>	Specifies a number of core images to keep on restart.
	none	Indicates no core image should be written on restart.
mode	hardware	Specifies a hardware restart.
	software	Specifies a software restart.

**Example**

```
SGOS#(config) restart mode software
ok
```

**#(config) return-to-sender**

The return-to-sender feature eliminates unnecessary network traffic when the three following conditions are met:

- The ProxySG has connections to clients or servers on a different subnet.
- The shortest route to the clients or servers is not through the default gateway.
- There are no static routes or RIP routes defined that apply to the IP addresses of the clients and servers.

Under these conditions, if the return-to-sender feature is enabled, the ProxySG remembers the MAC address of the last hop for a packet from the client or server and sends any responses or requests to the MAC address instead of the default gateway.

Under the same conditions, if return-to-sender is disabled, the ProxySG sends requests or responses to the default gateway, which then sends the packets to the gateway representing the last hop to the ProxySG for the associated connection. This effectively doubles the number of packets transmitted on the LAN compared to when return-to-sender is enabled.

Inbound return-to-sender affects connections initiated to the ProxySG by clients. Outbound return-to-sender affects connections initiated by the ProxySG to origin servers.

---

*Note:* Return-to-sender functionality should only be used if static routes cannot be defined for the clients and servers or if routing information for the clients and servers is not available through RIP packets.

---

**Syntax**

**option 1:** `return-to-sender inbound {disable | enable}`

**option 2:** `return-to-sender outbound {disable | enable}`

**option 3:** `return-to-sender version {1 | 2}`

Table 3.70: #(config) return-to-sender

inbound	disable   enable	Enables or disables return-to-sender for inbound sessions.
outbound	disable   enable	Enables or disables return-to-sender for outbound sessions.
version	1   2	<p>Enables return-to-sender (RTS) versions 1 or 2.</p> <p>In version 1, the RTS route is created at Layer-3 and stored globally, thus being interface agnostic.</p> <p>RTS version 2 was introduced to get around this multi-interface limitation. With version 2, TCP now stores a per-socket RTS route that contains both the destination MAC address and interface information. Once the SYN is received by the ProxySG all subsequent packets on that socket will traverse the interface on which the SYN was received.</p> <p><b>Note:</b>All current sockets tied to that interface will time out. However, subsequent and existing TCP connections continue to function normally on the other interfaces.</p>

**Example**

```
SGOS#(config) return-to-sender inbound enable
ok
```

## #(config) reveal-advanced

See “# reveal-advanced” on page 40 in Chapter 2: “Standard and Privileged Mode Commands”.

## #(config) rip

Use this command to set RIP (Routing Information Protocol) configuration options.

Using RIP, a host and router can send a routing table list of all other known hosts to its closest neighbor host every 30 seconds. The neighbor host passes this information on to its next closest neighbor and so on until all hosts have perfect knowledge of each other. (RIP uses the hop count measurement to derive network distance.) Each host in the network can then use the routing table information to determine the most efficient route for a packet.

The RIP configuration is defined in a configuration file. To configure RIP, first create a text file of RIP commands and then load the file by using the `load` command.

### Syntax

**option 1:** rip disable

**option 2:** `rip enable`  
**option 3:** `rip no path`  
**option 4:** `rip path url`

Table 3.71: `#(config) rip`

<code>disable</code>		Disables the current RIP configuration.
<code>enable</code>		Enables the current RIP configuration.
<code>no path</code>		Clears the current RIP configuration path as determined using the <code>rip path url</code> command.
<code>path</code>	<code>url</code>	Sets the path to the RIP configuration file to the URL indicated by <code>url</code> .

**Example**

```
SGOS#(config) rip path 10.25.36.47/files/rip.txt
ok
```

**#(config) security**

The ProxySG provides the ability to authenticate and authorize explicit and transparent proxy users using industry-standard authentication services. The supported authentication services are:

- Certificate—Authentication using X.509 Certificates
- Oblix COREid—Authentication using an Oblix COREid Access Server
- Forms-based Authentication—Authentication using forms-based authentication exceptions
- LDAP—Lightweight Directory Access Protocol
- Local—Users and groups stored locally on the ProxySG
- Netegrity SiteMinder—Authentication using a Netegrity SiteMinder server
- NTLM—Windows NT Challenge Response
- Policy Substitution—Identifying and authorizing users based on information in the request to the ProxySG
- RADIUS—Remote Authentication for Dialup Users
- Sequence—Associating realms with other realms to allow Blue Coat to search for the proper authentication credentials

The ProxySG provides a flexible authentication architecture that supports multiple services (LDAP, NTLM, and the like) with multiple backend servers (for example, LDAP directory servers together with NT domains with no trust relationship, and so forth) within each authentication scheme with the introduction of the realm.

A realm authenticates and authorizes users for access to Blue Coat Systems ProxySG services using either explicit proxy or transparent proxy mode. Note that multiple authentication realms can be used on a single ProxySG. Multiple realms are essential if the enterprise is a Managed Service provider, or the company has merged with or acquired another company, for example. Even for companies using only one protocol, multiple realms might be necessary—as in the case of a company using an LDAP

server with multiple authentication boundaries. You can use realm sequencing to search the multiple realms all at once.

A realm configuration includes:

- **realm name**
- **authentication service**—(LDAP, Local, NTLM, RADIUS, Certificate).
- **external server configuration**—backend server configuration information, such as host, port, and other relevant information based on the selected service.
- **authentication schema**—the definition used to authenticate users.
- **authorization schema**—the definition used to (1) authorize users for membership in defined groups, and (2) check for attributes that trigger evaluation against any defined policy rules.

For details, refer to the “Using Authentication Services” chapter of the *Blue Coat Configuration and Management Guide*.

## Syntax

**option 1:** security allowed-access {add | remove} *source\_ip* [*ip\_mask*]

**option 2:** security authentication-form

sub-option 1: create *form\_name*

sub-option 2: delete *form\_name*

sub-option 3: inline *form\_name* *eof\_marker*

sub-option 4: load *form\_name*

sub-option 5: no path *form\_name*

sub-option 6: path [*form\_name*] *path*

**option 3:** security certificate

sub-option 1: create-realm *realm\_name*

sub-option 2: delete-realm *realm\_name*

sub-option 3: edit-realm *realm\_name*—changes the prompt (see “#(config) security certificate edit-realm *realm\_name*” on page 175)

sub-option 4: view [*realm\_name*]

**option 4:** security coreid

sub-option 1: create-realm *realm\_name*

sub-option 2: delete-realm *realm\_name*

sub-option 3: edit-realm *realm\_name*—changes the prompt (see “#(config) security coreid edit-realm *realm\_name*” on page 177)

sub-option 4: view [*realm\_name*]

**option 5:** security default-authenticate-mode {auto | sg2}

**option 6:** security destroy-old-password [*force*]

**option 7:** security enable-password “*password*”

**option 8:** security enforce-acl {disable | enable}

**option 9:** security flush-credentials



```
sub-option 1: [on-policy-change {disable | enable}]
sub-option 2: [realm realm_name]
option 10:security front-panel-pin PIN
option 11:security hashed-enable-password hashed_password
option 12:security hashed-front-panel-pin
option 13:security hashed-password hashed_password
option 14:security ldap
    sub-option 1: create-realm {ad | iplanet | nds | other} realm_name [base_dn]
        primary_host [primary_port]
    sub-option 2: delete-realm realm_name
    sub-option 3: edit-realm realm_name—changes the prompt (see “#(config) security ldap
        edit-realm realm_name” on page 180)
    sub-option 4: view [realm_name]
option 15:security local
    sub-option 1: create-realm realm_name
    sub-option 2: delete-realm realm_name
    sub-option 3: edit-realm realm_name—changes the prompt (see “#(config) security local
        edit-realm realm_name” on page 185)
    sub-option 4: view [realm_name]
option 16:security local-user-list
    sub-option 1: clear [force]
    sub-option 2: create local_user_list
    sub-option 3: default {append-to-default {disable | enable} | list
        local_user_list}
    sub-option 4: delete local_user_list [force]
    sub-option 5: edit local_user_list—changes the prompt (see “#(config) security
        local-user-list edit local_user_list” on page 186)
option 17:security management
    sub-option 1: auto-logout-timeout seconds
    sub-option 2: display-realm name
    sub-option 3: no {auto-logout-timeout | display-realm}
option 18:security ntlm
    sub-option 1: create-realm realm_name primary_server_host [primary_server_port]
    sub-option 2: delete-realm realm_name
    sub-option 3: edit-realm realm_name—changes the prompt (see “#(config) security ntlm
        edit-realm realm_name” on page 189)
    sub-option 4: view [realm_name]
option 19:security password “password”
option 20:security password-display {encrypted | keyring keyring | none | view}
option 21:security policy-substitution
```

```
sub-option 1: create-realm realm_name
sub-option 2: delete-realm realm_name
sub-option 3: edit-realm realm_name—changes the prompt (see “# (config) security
policy-substitution edit-realm realm_name” on page 190)
sub-option 4: view [realm_name]
```

**option 22:**security radius

```
sub-option 1: create-realm realm_name secret primary_server_host
[primary_server_port]
sub-option 2: create-realm-encrypted realm_name encrypted-secret
primary_server_host [primary_server_port]
sub-option 3: delete-realm realm_name
sub-option 4: edit-realm realm_name—changes the prompt (see “# (config) security radius
edit-realm realm_name” on page 192)
sub-option 5: view [realm_name]
```

**option 23:**security request-storage

```
sub-option 1: allow-redirects {disable | enable}
sub-option 2: expiry-time seconds
sub-option 3: max-size megabytes
sub-option 4: verify-ip {disable | enable}
```

**option 24:**security sequence

```
sub-option 1: create-realm realm_sequence_name
sub-option 2: delete-realm realm_sequence_name
sub-option 3: edit-realm realm_sequence_name—changes the prompt (see “# (config)
security sequence edit-realm realm_sequence_name” on page 195)
sub-option 4: view [realm_sequence_name]
```

**option 25:**security siteminder

```
sub-option 1: create-realm realm_name
sub-option 2: delete-realm realm_name
sub-option 3: edit-realm realm_name—changes the prompt (see “# (config) security
siteminder edit-realm realm_name” on page 196)
sub-option 4: view [realm_name]
```

**option 26:**security transparent-proxy-auth

```
sub-option 1: cookie {persistent | session}
sub-option 2: method {ip | cookie}
sub-option 3: time-to-live {ip | persistent-cookie} minutes
sub-option 4: virtual-url url
```

**option 27:**security username *user\_name*

Table 3.72: # (config) security

allowed-access	add <i>source_ip</i> [ <i>ip_mask</i> ]	Adds the specified IP to the access control list.
	remove <i>source_ip</i> [ <i>ip_mask</i> ]	Removes the specified IP from the access control list.
authentication-form	create <i>form_name</i>	Creates a new authentication form.
	delete <i>form_name</i>	Deletes an authentication form.
	inline <i>form_name</i> <i>eof_marker</i>	Installs an authentication form from console input.
	load <i>form_name</i>	Downloads a new authentication form.
	no path [ <i>form_name</i> ]	Negates authentication-form configuration.
	path [ <i>form_name</i> ] <i>path</i>	Specifies the path (URL or IP address) from which to load an authentication form, or the entire set of authentication forms.
certificate	create-realm <i>realm_name</i>	Creates a new certificate realm with the name specified. The maximum number of certificate realms is 40.
	delete-realm <i>realm_name</i>	Deletes the specified certificate realm.
	edit-realm <i>realm_name</i>	Changes the prompt. See “# (config) security certificate edit-realm <i>realm_name</i> ” on page 175.
	view [ <i>realm_name</i> ]	Displays the configuration of all certificate realms or just the configuration for <i>realm_name</i> if specified.
coreid	create-realm <i>realm_name</i>	Creates a new Oblix COREid realm with the name specified. The maximum number of Oblix COREid realms is 40.
	delete-realm <i>realm_name</i>	Deletes the specified Oblix COREid realm.
	edit-realm <i>realm_name</i>	Enters edit mode for the Oblix COREid realm. See “# (config) security coreid edit-realm <i>realm_name</i> ” on page 177.
	view [ <i>realm_name</i> ]	Displays the configuration of all Oblix COREid realms or, if specified, just the configuration for <i>realm_name</i> .
default-authenticate-mode	auto	Sets the default <code>authenticate.mode</code> to <code>auto</code> .
	sg2	Sets the default <code>authenticate.mode</code> to <code>sg2</code> .
destroy-old-passwords	[ <i>force</i> ]	Destroys recoverable passwords in configuration used by previous versions. Do not use this command if you intend to downgrade as the old passwords are destroyed. Specify “ <i>force</i> ” to destroy the passwords without a prompt for confirmation.

Table 3.72: # (config) security (Continued)

enable-password	"password"	Sets the console enable password to the password specified. Note that the password must be in quotes. This is the password required to enter enable mode from the CLI when using console credentials, the serial console or RSA SSH.
enforce-acl	disable	Disables the console access control list.
	enable	Enables the console access control list.
flush-credentials	[on-policy-change {disable   enable}]	Disables/enables the flushing of the credential cache when policy is compiled.
	[realm realm]	Flushes the credentials for a particular realm now.
front-panel-pin	PIN	Sets a four-digit PIN to restrict access to the front panel of the ProxySG. To clear the PIN, specify 0000 instead of a real PIN.
hashed-enable-password	hashed_password	Specifies the console enable password in hashed format.
hashed-front-panel-pin	hashed_PIN	Specifies a front-panel PIN in hashed format.
hashed-password	hashed_password	Specifies the console password in hashed format.
ldap	create-realm {ad   iplanet   nds   other} realm_name [base_DN] primary_host [primary_port]	Creates a new LDAP realm of the type specified with the name, base DN, primary host and port specified. The base DN and port are optional. A base DN must be defined for LDAP authentication to succeed. The maximum number of LDAP realms is 40.
	delete-realm realm_name	Deletes the specified LDAP realm.
	edit-realm	Changes the prompt. See "# (config) security ldap edit-realm realm_name" on page 180.
	view [realm_name]	Displays the configuration of all LDAP realms or just the configuration for realm_name if specified.
local	create-realm realm_name	Creates a new local realm with the name specified. The maximum number of local realms is 40.
	delete-realm realm_name	Deletes the specified local realm.
	edit-realm	Changes the prompt. See "# (config) security local edit-realm realm_name" on page 185.
	view [realm_name]	Displays the configuration of all local realms or just the configuration for realm_name if specified.

Table 3.72: # (config) security (Continued)

local-user-list	clear [force]	Clears all local user lists. Lists referenced by local realms and the default local user list are recreated but empty. Specify “force” to clear realms without a prompt for confirmation.
	create local_user_list	Creates the local user list with the name specified.
	default append-to-default {disable   enable}	Disables/enables appending uploaded users to the default local user list.
	default list local_user_list	Specifies the default local user list. The default list is populated during password file uploads. The default list is also the default list used by local realms when they are created.
	delete local_user_list [force]	Deletes the specified local user list. The default list and any lists used by local realms cannot be deleted. Specify “force” to delete the list without a prompt for confirmation.
	edit	Changes the prompt. See “# (config) security local-user-list edit local_user_list” on page 186.
management	auto-logout-timeout seconds	Specifies the length of a management console session before the administrator is required to re-enter credentials. The default is 900 seconds (15 minutes).
	display-realm name	Specifies the realm to display in the management console challenge. The default value is the IP of the ProxySG.
	no auto-logout-timeout	Disables the automatic session logout.
	no display-realm	Resets the display realm to be the IP of the ProxySG.
ntlm	create-realm realm_name primary_server_host [primary_server_port]	Creates a new NTLM realm with the name, primary server host and port specified. The maximum number of NTLM realms is 40.
	delete-realm realm_name	Deletes the specified NTLM realm.
	edit-realm	Changes the prompt. See “# (config) security ntlm edit-realm realm_name” on page 189.
	view [realm_name]	Displays the configuration of all NTLM realms or just the configuration for realm_name if specified.
password	“password”	Specifies the console password. Note that the password must be in quotes.

Table 3.72: # (config) security (Continued)

password-display	encrypted   none	Specifies format to display passwords in “show config” output. Specify “encrypted” to display encrypted passwords. Specify “none” to display no passwords.
	keyring	Specifies the keyring to use for password encryption.
	view	Displays the current password display settings.
policy-substitution	create-realm <i>realm_name</i>	Create a new Policy Substitution realm.
	delete-realm <i>realm_name</i>	Deletes the specified Policy Substitution realm.
	edit-realm	Changes the prompt. See “# (config) security policy-substitution edit-realm <i>realm_name</i> ” on page 190.
	view [ <i>realm_name</i> ]	Displays the configuration of all Policy Substitution realms or just the configuration for <i>realm_name</i> if specified.
radius	create-realm <i>realm_name</i> secret <i>primary_server_host</i> [ <i>primary_server_port</i> ]	Creates a new RADIUS realm with the name, secret, primary server host and port specified. Only 1 RADIUS realm can be created.
	create-realm-encrypted <i>realm_name</i> encrypted-secret <i>primary_server_host</i> [ <i>primary_server_port</i> ]	Creates a new RADIUS realm with the name, secret (in encrypted format), primary server host and port specified. Only 1 RADIUS realm can be created.
	delete-realm <i>realm_name</i>	Deletes the specified RADIUS realm.
	edit-realm	Changes the prompt. See “# (config) security radius edit-realm <i>realm_name</i> ” on page 192.
	view [ <i>realm_name</i> ]	Displays the configuration of all RADIUS realms or just the configuration for <i>realm_name</i> if specified.
request-storage	allow-redirects {disable   enable}	Sets whether to allow stored request to be redirected.
	expiry-time <i>seconds</i>	Sets the expiry time of stored requests requiring authentication.
	max-size <i>megabytes</i>	Sets the maximum size of a stored request requiring authentication.
	verify-ip {disable   enable}	Sets whether to compare the client IP with the IP in the stored request.

Table 3.72: # (config) security (Continued)

sequence	create-realm <i>realm_sequence_name</i>	Creates a new realm sequence with the name specified. The maximum number of realm sequences is 40.
	delete-realm <i>realm_sequence_name</i>	Deletes the specified realm sequence.
	edit-realm <i>realm_sequence_name</i>	Changes the prompt. See “# (config) security sequence edit-realm <i>realm_sequence_name</i> ” on page 195.
	view [ <i>realm_name</i> ]	Displays the configuration of all realm sequences or just the configuration for <i>realm_name</i> if specified.
siteminder	create-realm <i>realm_siteminder_name</i>	Creates a new SiteMinder realm with the name specified. The maximum number of SiteMinder realms is 40.
	delete-realm <i>realm_sequence_name</i>	Deletes the specified SiteMinder realm.
	edit-realm <i>realm_sequence_name</i>	Changes the prompt. See “# (config) security siteminder edit-realm <i>realm_name</i> ” on page 196.
	view [ <i>realm_name</i> ]	Displays the configuration of all SiteMinder realms or just the configuration for <i>realm_name</i> if specified.
transparent-proxy-auth	cookie {persistent   session}	Specifies whether to use persistent or session cookies.
	method {ip   cookie}	Specifies whether to use IP or cookie surrogate credentials.
	time-to-live {ip   persistent-cookie} <i>minutes</i>	Specifies the length of time that the surrogate credentials are considered valid.
	virtual-url <i>url</i>	Specifies the virtual URL to which requests requiring authentication are redirected.
username	<i>username</i>	Specifies the console account username.

**Example**

```

SGOS# (config) security local create-realm testlocal
ok
SGOS# (config) security allowed-access add 10.253.101.23 255.255.255.255
ok
SGOS# (config) security enable-password enable
ok

```

**#(config) security certificate edit-realm *realm\_name*****Syntax**

```
security certificate edit-realm realm_name
```

This changes the prompt to:

SGOS#(config certificate *realm\_name*)

**- subcommands-**

**option 1:** authorization

sub-option 1: append-base-dn {disable | dn *dn\_to\_append* | enable}

sub-option 2: container-attr-list *list\_of\_attribute\_names*

sub-option 3: no {container-attr-list | realm-name}

sub-option 4: realm-name *authorization\_realm\_name*

sub-option 5: username-attribute *username\_attribute*

**option 2:** cache-duration *seconds*

**option 3:** display-name *display\_name*

**option 4:** exit

**option 5:** rename *new\_realm\_name*

**option 6:** view

**option 7:** virtual-url *url*

Table 3.73: #(config certificate *realm\_name*)

authorization	append-base-dn {disable   dn <i>DN_to_append</i>   enable}	Disables or enables appending of the base DN to the authenticated username, or specifies the base DN to append. If no base DN is specified, then the first base DN in the LDAP authorization realm is used. Applies to LDAP authorization realms only.
	container-attr-list <i>list_of_attribute_names</i>	Specifies the attributes from the certificate subject to use in constructing the user DN. E.g. "o,ou". The list needs to be quoted if it contains spaces.
	no {container-attr-list   realm-name}	Clears the container attribute list or the authorization realm.
	realm-name <i>authorization_realm_name</i>	Specifies the authorization realm to use. Only LDAP and local realms are valid authorization realms.
	username-attribute <i>username_attribute</i>	Specifies the attribute in the certificate subject that identifies the user's relative name. The default is "cn".
cache-duration	<i>seconds</i>	Specifies the length of time to cache credentials for this realm.
display-name	<i>display_name</i>	Specifies the display name for this realm.
exit		Exits configure security certificate mode and returns to configure mode.
rename	<i>new_realm_name</i>	Renames this realm to <i>new_realm_name</i> .
view		Displays this realm's configuration.
virtual-url	<i>url</i>	Specifies the virtual URL to use for this realm. If no URL is specified the global transparent proxy virtual URL is used.



**Example**

```

SGOS#(config) security certificate edit-realm testcert
SGOS#(config certificate testcert) no container-attr-list
ok
SGOS#(config certificate testcert) cache-duration 800
ok
SGOS#(config certificate testcert) exit
SGOS#(config)

```

 **#(config) security coreid edit-realm realm\_name****Syntax**

```
security coreid edit-realm realm_name
```

This changes the prompt to:

```
SGOS#(config coreid realm_name)
```

**- subcommands-**

**option 1:** access-server-hostname hostname

**option 2:** access-server-id id

**option 3:** access-server-port port

**option 4:** add-header-responses disable | enable

**option 5:** alternate-agent

sub-option 1: accessgate-id name

sub-option 2: encrypted-secret encrypted\_shared\_secret

sub-option 3: host hostname

sub-option 4: port port

sub-option 5: secret shared\_secret

**option 6:** always-redirect-offbox disable | enable

**option 7:** cache-duration seconds

**option 8:** case-sensitive disable | enable

**option 9:** certificate-path certificate\_path

**option 10:** display-name display\_name

**option 11:** encrypted-transport-pass-phrase encrypted\_pass\_phrase

**option 12:** exit

**option 13:** no alternate-agent | certificate-path

**option 14:** primary-agent

sub-option 1: accessgate-id name

sub-option 2: encrypted-secret encrypted\_shared\_secret

sub-option 3: host hostname

sub-option 4: port port

```

sub-option 5: secret shared_secret
option 15: protected-resource-name resource_name
option 16: rename new_realm_name
option 17: security-mode cert | open | simple
option 18: ssl disable | enable
option 19: ssl-verify-agent disable | enable
option 20: timeout seconds
option 21: transport-pass-phrase pass_phrase
option 22: validate-client-IP disable | enable
option 23: view
option 24: virtual-url virtual_URL

```

Table 3.74: # (config coreid *realm\_name*)

access-server-hostname	<i>hostname</i>	The hostname of the primary Access Server.
access-server-id	<i>id</i>	The ID of the primary Access Server.
access-server-port	<i>port</i>	The port of the primary Access Server.
add-header-responses	disable   enable	When enabled, authorization actions from the policy domain obtained during authentication are added to each request forwarded by the ProxySG. Note that header responses will replace any existing header of the same name; if no such header exists, the header is added. Cookie responses will replace a cookie header with the same cookie name; if no such cookie header exists, one is added.
alternate-agent	accessgate-id <i>name</i>	The id of the alternate AccessGate agent
	encrypted-secret <i>encrypted_shared_secret</i>	The encrypted password associated with the alternate AccessGate. (Passwords can be up to 64 characters long and are always case sensitive.) The primary use of the encrypted-secret command is to allow the ProxySG to reload a password that it encrypted. If you choose to use a third-party encryption application, be sure it supports RSA encryption, OAEP padding, and is Base64 encoded with no newlines.
	host <i>hostname</i>	The hostname or the IP address of the alternate system that contains the agent.
	port <i>port</i>	The port where the alternate agent listens.
	secret <i>shared_secret</i>	The password associated with the alternate AccessGate. (Passwords can be up to 64 characters long and are always case sensitive.)
always-redirect-offbox	disable   enable	Forces authentication challenges to always be redirected to an off-box URL.

Table 3.74: #(config coreid realm\_name) (Continued)

cache-duration	<i>seconds</i>	Specifies the length of time in seconds that user and administrator credentials received are cached. Credentials can be cached for up to 3932100 seconds. The default value is 900 seconds (15 minutes).
case-sensitive	disable   enable	Specifies whether the username and group comparisons on the ProxySG should be case-sensitive.
certificate-path	<i>certificate_path</i>	If Cert mode is used, the location on the BCAA host machine where the key, server and CA chain certificates reside. The certificate files must be named aaa_key.pem, aaa_cert.pem and aaa_chain.pem respectively.
display-name	<i>display_name</i>	Equivalent to the display-name option in the CPL authenticate action. The default value for the display name is the realm name. The display name cannot be longer than 128 characters and it cannot be null.
encrypted-transport-pass-phrase	<i>encrypted_pass_phrase</i>	If Simple or Cert mode is used, the Transport encrypted pass phrase configured in the Access System.
exit		Exits the edit mode and returns to configuration mode.
no	alternate-agent   certificate-path	Removes the alternate agent configuration or the certificate path.
primary-agent	accessgate-id <i>name</i>	The id of the primary AccessGate agent
	encrypted-secret <i>encrypted_shared_secret</i>	The encrypted password associated with the primary AccessGate. (Passwords can be up to 64 characters long and are always case sensitive.) The primary use of the encrypted-secret command is to allow the ProxySG to reload a password that it encrypted. If you choose to use a third-party encryption application, be sure it supports RSA encryption, OAEP padding, and is Base64 encoded with no newlines.
	host <i>hostname</i>	The hostname or the IP address of the primary system that contains the agent.
	port <i>port</i>	The port where the primary agent listens.
	secret <i>shared_secret</i>	The password associated with the primary AccessGate. (Passwords can be up to 64 characters long and are always case sensitive.)
protected-resource-name	<i>resource_name</i>	The resource name defined in the Access System policy domain.
rename	<i>new_realm_name</i>	Renames the realm to your request.

Table 3.74: #(config coreid realm\_name) (Continued)

security-mode	cert   open   simple	The Security Transport Mode for the AccessGate to use when communicating with the Access System.
ssl-verify-client	disable   enable	Enable or disable verification of BCAA's certificate.
timeout	seconds	The length of time to elapse before timeout if a response from BCAA is not received
transport-pass-phrase	pass_phrase	If Simple or Cert mode is used, the Transport pass phrase configured in the Access System.
validate-client-IP	disable   enable	Enables validation of the client IP address in SSO cookies. If the client IP address in the SSO cookie can be valid yet different from the current request client IP address due to downstream proxies or other devices, then disable client IP address validation. The WebGates participating in SSO with the ProxySG should also be modified. The WebGateStatic.lst file should be modified to either set the ipvalidation parameter to false or to add the downstream proxy/device to the IPValidationExceptions lists.
view		Views the realm configuration.
virtual-url	virtual_URL	The URL to redirect to when the user needs to be challenged for credentials. If the ProxySG is participating in SSO, the virtual hostname must be in the same cookie domain as the other servers participating in the SSO. It cannot be an IP address or the default.

**Example**

```

SGOS#(config) security coreid edit-realm coreid_1
SGOS#(config coreid coreid_1) access-server-hostname AccessServer_1
SGOS#(config coreid coreid_1) cache-duration 800
SGOS#(config coreid coreid_1) exit
SGOS#(config)

```

**#(config) security ldap edit-realm realm\_name****Syntax**

```
security ldap edit-realm realm_name
```

This changes the prompt to:

```
SGOS#(config ldap realm_name)
```

**- subcommands-**

**option 1:** alternate-server host [port]

**option 2:** cache-duration seconds

**option 3:** case-sensitive {disable | enable}  
**option 4:** default-group-name *default\_group\_name*  
**option 5:** display-name *display\_name*  
**option 6:** distinguished-name  
    sub-option 1: user-attribute-type *user\_attribute\_type*  
    sub-option 2: base-dn {add | demote | promote | remove} *base\_dn* | clear  
**option 7:** exit  
**option 8:** membership-attribute *attribute\_name*  
**option 9:** membership-type group | user  
**option 10:** membership-username (full | relative)  
**option 11:** no  
    sub-option 1: alternate-server  
    sub-option 2: default-group-name  
    sub-option 3: membership-attribute  
**option 12:** objectclass  
    sub-option 1: container {add | remove} *container\_objectclass* | clear  
    sub-option 2: group {add | remove} *group\_objectclass* | clear  
    sub-option 3: user {add | remove} *user\_objectclass* | clear  
**option 13:** primary-server *host* [*port*]  
**option 14:** protocol-version {2 | 3}  
**option 15:** referrals-follow {disable | enable}  
**option 16:** rename *new\_realm\_name*  
**option 17:** search  
    sub-option 1: anonymous {disable | enable}  
    sub-option 2: dereference {always | finding | never | searching}  
    sub-option 3: encrypted-password *encrypted\_password*  
    sub-option 4: password *password*  
    sub-option 5: user-dn *user\_dn*  
**option 18:** server-type {ad | iplanet | nds | other}  
**option 19:** spoof-authentication {none | origin | proxy}  
**option 20:** ssl {disable | enable}  
**option 21:** ssl-verify-server {disable | enable}  
**option 22:** timeout *seconds*  
**option 23:** view  
**option 24:** virtual-url *url*

Table 3.75: #(config ldap realm\_name)

alternate-server	host [port]	Specifies the alternate server host and port.
cache-duration	seconds	Specifies the length of time to cache credentials for this realm.
case-sensitive	disable   enable	Specifies whether or not the LDAP server is case-sensitive.
default-group-name	default_group_name	If the validate-authorized-user command is disabled and a default-group-name is configured, the default-group-name is used as the group name for non-existent users.
display-name	display_name	Specifies the display name for this realm.
distinguished-name	user-attribute-type user_attribute_type	Specifies the attribute type that defines the relative user name.
	base-dn {add   demote   promote   remove} base_dn	Adds/demotes/promotes/removes a base DN from the base DN list, or clears the base DN list.
exit		Exits configure security ldap mode and returns to configure mode.
membership-attribute	attribute_name	Specifies the attribute that defines group membership.
membership-type	group   user	Specifies the membership type. Specify group if user memberships are specified in groups. Specify user if memberships are specified in users.
membership-username	full   relative	Specifies the username type to use during membership lookups. The full option specifies that the user's FQDN is used during membership lookups, and relative option specifies that the user's relative username is used during membership lookups. Only one can be selected at a time.
no	alternate-server	Clears the alternate-server or membership-attribute values.
	default-group-name	Clears the default group name.
	membership-attribute	Clears the membership-attribute values.

Table 3.75: #(config ldap realm\_name) (Continued)

objectclass	container {add   remove} <i>container_objectclass</i>   clear	Adds/removes container objectclass values from the list (these values are used during VPM searches of the LDAP realm), or clears all values from the container objectclass list.
	group {add   remove} <i>group_objectclass</i>   clear	Adds/removes group objectclass values from the list (these values are used during VPM searches of the LDAP realm), or clears all values from the group objectclass list.
	user {add   remove} <i>user_objectclass</i>   clear	Adds/removes user objectclass values from the list (these values are used during VPM searches of the LDAP realm), or clears all values from the user objectclass list.
primary-server	<i>host</i> [ <i>port</i> ]	Specifies the primary server host and port.
protocol-version	2   3	Specifies the LDAP version to use. SSL and referral processing are not available in LDAP v2.
referrals-follow	disable   enable	Disables/enables referral processing. This is available in LDAP v3 only.
rename	<i>new_realm_name</i>	Renames this realm to <i>new_realm_name</i> .
search	anonymous {disable   enable}	Disables/enables anonymous searches.
	dereference {always   finding   never   searching}	Specifies the dereference level. Specify always to always dereference aliases. Specify finding to dereference aliases only while locating the base of the search. Specify searching to dereference aliases only after locating the base of the search. Specify never to never dereference aliases.
	encrypted-password <i>encrypted_password</i>	Specifies the password to bind with during searches in encrypted format.
	password <i>password</i>	Specifies the password to bind with during searches.
	user-dn <i>user_dn</i>	Specifies the user DN to bind with during searches.
server-type	{ad   iplanet   nds   other}	Specifies the LDAP server type for this realm.

Table 3.75: #(config ldap realm\_name) (Continued)

spoof-authentication	none   origin   proxy	<p>Enables/disables the forwarding of authenticated credentials to the origin content server or for proxy authentication. You can only choose one.</p> <ul style="list-style-type: none"> <li>• If set to <i>origin</i>, the spoofed header is an Authorization: header.</li> <li>• If set to <i>proxy</i>, the spoofed header is a Proxy-Authorization: header.</li> <li>• If set to <i>none</i>, no spoofing is done.</li> </ul> <p>Flush the entries for a realm if the spoof-authentication value is changed to ensure that the spoof-authentication value is immediately applied.</p>
ssl	disable   enable	Disables/enables SSL communication between the ProxySG and the LDAP server. This is only available in LDAP v3.
ssl-verify-server	disable   enable	Specifies whether or not to verify the LDAP server's certificate.
timeout	seconds	Specifies the LDAP server's timeout.
validate-authorized-user	disable   enable	<p>When validate-authorized-user is enabled, an <i>authorization</i> (not authentication) request will verify that the user exists in the LDAP server. If the user does not exist, the authorization request fails (authentication requests always require the user to exist).</p> <p>When validate-authorized-user is disabled, no user existence check is made for an authorization request. If the user does not exist, the authorization request succeeds.</p>
view		Displays this realm's configuration.
virtual-url	url	Specifies the virtual URL to use for this realm. If no URL is specified the global transparent proxy virtual URL is used.



**Example**

```

SGOS#(config) security ldap edit-realm testldap
SGOS#(config ldap testldap) server-type iplanet
ok
SGOS#(config ldap testldap) spoof-authentication origin
ok
SGOS#(config ldap testldap) exit
SGOS#(config)

```

**#(config) security local edit-realm *realm\_name*****Syntax**

```
security local edit-realm realm_name
```

This changes the prompt to:

```
SGOS#(config local realm_name)
```

**- subcommands-**

**option 1:** cache-duration *seconds*

**option 2:** default-group-name *default\_group\_name*

**option 3:** display-name *display\_name*

**option 4:** exit

**option 5:** local-user-list *local\_user\_list\_name*

**option 6:** rename *new\_realm\_name*

**option 7:** spoof-authentication {none | origin | proxy}

**option 8:** view

**option 9:** virtual-url *url*

Table 3.76: #(config local *realm\_name*)

cache-duration	seconds	Specifies the length of time to cache credentials for this realm.
default-group-name	<i>default_group_name</i>	If the validate-authorized-user command is disabled and a default-group-name is configured, the default-group-name is used as the group name for non-existent users.
display-name	<i>display_name</i>	Specifies the display name for this realm.
exit		Exits configure security local mode and returns to configure mode.
local-user-list	<i>local_user_list_name</i>	Specifies the local user list to for this realm.
no	default-group-name	Clears the default group name.
rename	<i>new_realm_name</i>	Renames this realm to <i>new_realm_name</i> .

Table 3.76: `#(config local realm_name)` (Continued)

<code>spoof-authentication</code>	<code>none   origin   proxy</code>	<p>Enables/disables the forwarding of authenticated credentials to the origin content server or for proxy authentication. You can only choose one.</p> <ul style="list-style-type: none"> <li>• If set to <i>origin</i>, the spoofed header is an Authorization: header.</li> <li>• If set to <i>proxy</i>, the spoofed header is a Proxy-Authorization: header.</li> <li>• If set to <i>none</i>, no spoofing is done.</li> </ul> <p>Flush the entries for a realm if the spoof-authentication value is changed to ensure that the spoof-authentication value is immediately applied.</p>
<code>validate-authorized-user</code>	<code>disable   enable</code>	<p>When <code>validate-authorized-user</code> is enabled, an <i>authorization</i> (not authentication) request will verify that the user exists in the local user list. If the user does not exist in the list, the authorization request fails (authentication requests always require the user to exist).</p> <p>When <code>validate-authorized-user</code> is disabled, no user existence check is made for an authorization request. If the user does not exist, the authorization request succeeds.</p>
<code>view</code>		Displays this realm's configuration.
<code>virtual-url</code>	<code>url</code>	Specifies the virtual URL to use for this realm. If no URL is specified the global transparent proxy virtual URL is used.

**Example**

```

SGOS#(config) security local edit-realm testlocal
SGOS#(config local testlocal) cache-duration 1500
ok
SGOS#(config local testlocal) spoof-authentication proxy
ok
SGOS#(config local testlocal) exit
SGOS#(config)

```

**`#(config) security local-user-list edit local_user_list`****Syntax**

```
security local-user-list edit local_user_list
```

This changes the prompt to:

```
SGOS#(config local-user-list local_user_list)
```

**- subcommands-****option 1:** disable-all**option 2:** enable-all**option 3:** exit**option 4:** group

sub-option 1: clear

sub-option 1: create *group\_name*sub-option 2: delete *group\_name* [force]**option 5:** lockout-duration *seconds***option 6:** max-failed-attempts *attempts***option 7:** no [lockout-duration | max-failed-attempts | reset-interval]**option 8:** reset-interval *seconds***option 9:** user

sub-option 1: clear

sub-option 2: create *user\_name*sub-option 3: delete *user\_name* [force]sub-option 4: edit *user\_name*—changes the prompt to #SGOS (config local-user-list  
*local\_user\_list user\_name*)

disable | enable

exit

group {add | remove} *group\_name*hashed-password *hashed\_password*password *password*

view

sub-option 5: view

Table 3.77: #(config local-user-list *local\_user\_list*)

disable-all		Disables all user accounts in the specified list
enable-all		Enables all user accounts in the specified list.
exit		Exits configure local-user-list mode and returns to configure mode.
group	clear	Clears all groups from the list. The users remain but do not belong to any groups.
	create <i>group_name</i>	Creates the specified group in the local user list.
	delete <i>group_name</i>	Deletes the specified group in the local user list.
lockout-duration	<i>seconds</i>	The length of time a user account is locked out after too many failed password attempts. The default is 3600.

Table 3.77: `#(config local-user-list local_user_list)` (Continued)

<code>max-failed-attempts</code>	<code>attempts</code>	The number of failed attempts to login to a ProxySG before the user account is locked. The default is 60 attempts.
<code>no</code>	<code>lockout-duration  </code> <code>max-failed-attempts  </code> <code>reset-interval</code>	Disables the settings for this user list.
<code>reset-interval</code>	<code>seconds</code>	The length of seconds to wait after the last failed attempt before resetting the failed counter to zero.
<code>user</code>	<code>clear</code>	Clears all users from the list The groups remain but do not have any users.
	<code>create user_name</code>	Creates the specified user in the local user list.
	<code>delete user_name</code>	Deletes the specified user in the local user list.
	<code>edit user_name</code>	Edits the specified user in the local user list. Changes the prompt to <code>#(config local-user-list local_user_list user_name)</code> .
	<code>disable   enable</code>	Disables/enables the user account.
	<code>exit</code>	Exits configure local-user-list <code>user_list</code> mode and returns to configure local-user-list mode.
	<code>group add   remove</code> <code>group_name</code>	Adds/removes the specified group from the user.
	<code>hashed-password</code> <code>hashed_password</code>	Specifies the user's password in hashed format.
<code>view</code>	<code>password password</code>	Specifies the user's password.
	<code>view</code>	Displays the user account.
		Displays all users and groups in the local user list.

### Example

```
SGOS#(config) security local-user-list edit testlul
SGOS#(config local-user-list testlul) user create testuser
ok
SGOS#(config local-user-list testlul) user edit testuser
SGOS#(config local-user-list testlul testuser) enable
ok
SGOS#(config local-user-list testlul testuser) exit
SGOS#(config local-user-list testlul) exit
SGOS#(config)
```

## **#(config) security ntlm edit-realm *realm\_name***

Edits the NTLM realm specified by *realm\_name*.

### Syntax

```
security ntlm edit-realm realm_name
```

This changes the prompt to:

```
SGOS#(config ntlm realm_name)
```

#### **- subcommands-**

```
option 1: alternate-server host [port]
option 2: cache-duration seconds
option 3: credentials-basic {disable | enable}
option 4: credentials-ntlm {disable | enable}
option 5: display-name display_name
option 6: exit
option 7: no alternate-server
option 8: primary-server host [port]
option 9: rename new_realm_name
option 10: timeout seconds
option 11: ssl {disable | enable}
option 12: ssl-verify-server {disable | enable}
option 13: view
option 14: virtual-url url
```

**Table 3.78:** `#(config ntlm realm_name)`

<code>alternate-server</code>	<code>host [port]</code>	Specifies the alternate server host and port.
<code>cache-duration</code>	<code>seconds</code>	Specifies the length of time to cache credentials for this realm.
<code>credentials-basic</code>	<code>disable   enable</code>	Disables/enables support for Basic credentials in this realm. At least one of Basic or NTLM credentials must be supported.
<code>credentials-ntlm</code>	<code>disable   enable</code>	Disables/enables support for NTLM credentials in this realm. At least one of Basic or NTLM credentials must be supported.
<code>display-name</code>	<code>display_name</code>	Specifies the display name for this realm.
<code>exit</code>		Exits configure ntlm-realm mode and returns to configure mode.
<code>no alternate-server</code>		Clears the alternate-server.
<code>primary-server</code>	<code>host [port]</code>	Specifies the primary server host and port.
<code>rename</code>	<code>new_realm_name</code>	Renames this realm to <code>new_realm_name</code> .
<code>timeout</code>	<code>seconds</code>	Specifies the NTLM request timeout.
<code>ssl</code>	<code>disable   enable</code>	Disables/enables SSL communication between the ProxySG and BCAA.
<code>ssl-verify-server</code>	<code>disable   enable</code>	Specifies whether or not to verify the BCAA certificate.
<code>view</code>		Displays this realm's configuration.
<code>virtual-url</code>	<code>url</code>	Specifies the virtual URL to use for this realm. If no URL is specified the global transparent proxy virtual URL is used.

**Example**

```
SGOS#(config) security ntlm edit-realm testntlm
SGOS#(config ntlm testntlm) cache-duration 1500
ok
SGOS#(config ntlm testntlm) no alternate server
ok
SGOS#(config ntlm testntlm) exit
SGOS#(config)
```

**`#(config) security policy-substitution edit-realm realm_name`**

Edits the Policy Substitution realm specified by `realm_name`.

**Syntax**

```
security policy-substitution edit-realm realm_name
```

This changes the prompt to:

```

SGOS# (config policy-substitution realm_name)
option 1: authorization-realm-name realm_name
option 2: cache-duration seconds
option 3: exit
option 4: full-username construction_rule
option 5: no authorization-realm-name
option 6: rename new_realm_name
option 7: username construction_rule
option 8: view
option 9: virtual-url

```

Table 3.79: # (config policy-substitution realm\_name)

authorization-realm-name	realm_name	This option is only required if you are associating an authorization realm with the Policy Substitution realm.
cache-duration	seconds	Specifies the length of time to cache credentials for this realm.
exit		Exits configure policy-substitution mode and returns to configure mode.
full-username	construction_rule	<p>The full username as created through policy substitutions. The construction rule is made up any of the substitutions whose values are available at client logon, listed in Appendix D, "CPL Substitutions," in the <i>Blue Coat Content Policy Language Guide</i>.</p> <p><b>Note:</b>The username and full username attributes are character strings that contain policy substitutions. When authentication is required for the transaction, these character strings are processed by the policy substitution mechanism, using the current transaction as input. The resulting string is stored in the user object in the transaction, and becomes the user's identity.</p> <p>To create full usernames for various uses in Policy Substitution realms, see the <i>Blue Coat Content Policy Language Guide</i>.</p>
no authorization-realm-name		Clears the authorization realm name.

Table 3.79: #(config policy-substitution *realm\_name*) (Continued)

rename	<i>new_realm_name</i>	Renames this realm to <i>new_realm_name</i> .
username	<i>construction_rule</i>	<p>The username as created through policy substitutions. Note that the username is only required if you are using an authorization realm. The construction rule is made up any of the policy substitutions whose values are available at client logon, listed in Appendix D, “CPL Substitutions,” in the <i>Blue Coat Content Policy Language Guide</i>.</p> <p>Note: The username and full username attributes are character strings that contain policy substitutions. When authentication is required for the transaction, these character strings are processed by the policy substitution mechanism, using the current transaction as input. The resulting string is stored in the user object in the transaction, and becomes the user’s identity.</p> <p>To create usernames for the various uses of Policy Substitution realms, see the <i>Blue Coat Content Policy Language Guide</i></p>
view		Displays this realm’s configuration.
virtual-url	<i>url</i>	Specifies the virtual URL to use for this realm. If no URL is specified the global transparent proxy virtual URL is used.

**Example**

```

SGOS#(config) security policy-substitution edit-realm PS1
SGOS#(config policy-substitution PS1) authorization-realm-name LDAP1
SGOS#(config policy-substitution PS1) username $(netbios.messenger-username)
SGOS#(config policy-substitution PS1) full-username
cn=$(netbios.messenger-username),cn=users,dc=$(netbios.computer-domain),
dc=company,dc=com

```

**#(config) security radius edit-realm *realm\_name***

Edits the RADIUS realm specified by *realm\_name*.

**Syntax**

```
security radius edit-realm realm_name
```



This changes the prompt to:

```
SGOS#(config radius realm_name)
```

**option 1:** alternate-server

sub-option 1: encrypted-secret *encrypted\_secret*

sub-option 2: host [port]

sub-option 3: secret *secret*

sub-option 4: service-type *type*

**option 2:** cache-duration *seconds*

**option 3:** case-sensitive {disable | enable}

**option 4:** display-name *display\_name*

**option 5:** exit

**option 6:** no alternate-server

**option 7:** one-time-passwords enable | disable

**option 8:** primary-server

sub-option 1: encrypted-secret *encrypted\_secret*

sub-option 2: host [port]

sub-option 3: secret *secret*

sub-option 4: service-type *type*

**option 9:** rename *new\_realm\_name*

**option 10:** timeout *seconds*

**option 11:** server-retry *count*

**option 12:** spoof-authentication {none | origin | proxy}

**option 13:** view

**option 14:** virtual-url *url*

Table 3.80: #(config radius realm\_name)

alternate-server	host [port]	Specifies the alternate server host and port.
	encrypted-secret <i>encrypted_secret</i>	Specifies the alternate server secret in encrypted format.
	secret <i>secret</i>	Specifies the alternate server secret.
	service-type <i>type</i>	Specifies the service-type to send to the alternate server.
cache-duration	<i>seconds</i>	Specifies the length of time to cache credentials for this realm.
case-sensitive	disable   enable	Specifies whether or not the RADIUS server is case-sensitive.
display-name	<i>display_name</i>	Specifies the display name for this realm.
exit		Exits configure radius-realm mode and returns to configure mode.
no alternate-server		Clears the alternate-server.

Table 3.80: #(config radius realm\_name) (Continued)

one-time-passwords	enable   disable	Allows you to use one-time passwords for authentication. The default is disabled.
primary-server	host [port]	Specifies the primary server host and port.
	encrypted-secret encrypted_secret	Specifies the primary server secret in encrypted format.
	secret secret	Specifies the primary server secret.
	service-type type	Specifies the service-type to send to the primary server.
rename	new_realm_name	Renames this realm to new_realm_name.
timeout	seconds	Specifies the RADIUS request timeout.
server-retry	count	Specifies the number of authentication retry attempts.
spoof-authentication	none   origin   proxy	<p>Enables/disables the forwarding of authenticated credentials to the origin content server or for proxy authentication. You can only choose one.</p> <ul style="list-style-type: none"> <li>• If set to <i>origin</i>, the spoofed header is an Authorization: header.</li> <li>• If set to <i>proxy</i>, the spoofed header is a Proxy-Authorization: header.</li> <li>• If set to <i>none</i>, no spoofing is done.</li> </ul> <p>Flush the entries for a realm if the spoof-authentication value is changed to ensure that the spoof-authentication value is immediately applied.</p>
view		Displays this realm's configuration.
virtual-url	url	Specifies the virtual URL to use for this realm. If no URL is specified the global transparent proxy virtual URL is used.

**Example**

```

SGOS#(config) security radius edit-realm testradius
SGOS#(config radius testradius) server-retry 8
ok
SGOS#(config radius testradius) spoof-authentication proxy
ok
SGOS#(config radius testradius) exit
SGOS#(config)

```

**#(config) security sequence edit-realm *realm\_sequence\_name***

Edits the realm sequence specified by *realm\_sequence\_name*.

**Syntax**

```
security sequence edit-realm realm_sequence_name
```

This changes the prompt to:

```
SGOS#(config sequence realm_sequence_name)
```

**option 1:** display-name *display\_name*

**option 2:** exit

**option 3:** ntlm-only-once {disable | enable}

**option 4:** realm {add | demote | promote | remove} *realm\_name* | clear

**option 5:** rename *new\_realm\_name*

**option 6:** view

**option 7:** virtual-url *url*

**Table 3.81:** #(config sequence *realm\_sequence\_name*)

display-name	<i>display_name</i>	Specifies the display name for this realm.
exit		Exits configure sequence-realm mode and returns to configure mode.
ntlm-only-once	disable   enable	Specifies whether or not to challenge for credentials for the NTLM realm once or multiple times.
realm	{add   demote   promote   remove} <i>realm_name</i> clear	Adds/demotes/promotes/removes a realm from the realm sequence, or clears all realms from the realm sequence.
rename	<i>new_realm_sequence_name</i>	Renames this realm to <i>new_realm_sequence_name</i> .
view		Displays this realm's configuration.
virtual-url	<i>url</i>	Specifies the virtual URL to use for this realm sequence. If no URL is specified the global transparent proxy virtual URL is used.

### Example

```
SGOS#(config) security sequence edit-realm testsequence
SGOS#(config sequence testsequence) ntlm-only-once disable
ok
SGOS#(config sequence testsequence) realm clear
ok
SGOS#(config sequence testsequence) exit
SGOS#(config)
```

## #(config) security siteminder edit-realm *realm\_name*

Edits the SiteMinder realm sequence specified by *realm\_name*.

### Syntax

```
security siteminder edit-realm realm_name
```

This changes the prompt to:

```
SGOS#(config siteminder realm_name)
```

- *subcommands*-

**option 1:** add-header-responses {enable | disable}  
**option 2:** alternate-agent {agent-name | encrypted-shared-secret | host | port | shared-secret | always-redirect-offbox}  
**option 3:** always-redirect-offbox {enable | disable}  
**option 4:** cache-duration seconds  
**option 5:** case-sensitive {enable | disable}  
**option 6:** display-name *display\_name*  
**option 7:** exit  
**option 8:** no  
**option 9:** primary-agent {agent-name | encrypted-shared-secret | host | port | shared-secret | always-redirect-offbox}  
**option 10:** protected-resource-name *resource-name*  
**option 11:** rename *new\_realm\_name*  
**option 12:** server-mode {failover | round-robin}  
**option 13:** siteminder-server {create | delete | edit}  
**option 14:** ssl {enable | disable}  
**option 15:** ssl-verify-agent {enable | disable}  
**option 16:** timeout *seconds*  
**option 17:** view  
**option 18:** virtual-url *url*

Table 3.82: #(config siteminder realm\_name)

add-header-responses	enable   disable	Enable if your Web applications need information from the SiteMinder policy server responses.
alternate-agent	agent-name	Specifies the alternate agent.
	encrypted-secret encrypted_secret	Specifies the alternate agent secret in encrypted format.
	host	The host ID or the IP address of the system that contains the alternate agent.
	port	The port where the agent listens.
	shared-secret secret	Specifies the alternate agent secret.
always-redirect-offbox	enable   disable	Enables or disables SSO.
cache-duration	seconds	Specifies the length of time to cache credentials for this realm.
case-sensitive		Specifies whether or not the SiteMinder server is case-sensitive.
display-name	display_name	Specifies the display name for this realm.
exit		Exits configure siteminder-realm mode and returns to configure mode.
no	alternate-agent	Clears the alternate agent configuration.
primary-agent	agent-name	Specifies the primary agent.
	encrypted-secret encrypted_secret	Specifies the primary agent secret in encrypted format.
	host	The host ID or the IP address of the system that contains the primary agent.
	port	The port where the agent listens.
	shared-secret secret	Specifies the primary agent secret.
	always-redirect-offbox (enable   disable)	Enables or disables the SSO-Only mode.
protected-resource-name	resource-name	The protected resource name is the same as the resource name on the SiteMinder server that has rules and policy defined for it.
rename	new_realm_name	Renames this realm to new_realm.
server-mode	failover   round-robin	Behavior of the server. Failover mode falls back to one of the other servers if the primary one is down. Round-robin modes specifies that all of the servers should be used together in a round-robin approach. Failover is the default.

Table 3.82: # (config siteminder realm\_name) (Continued)

validate-client-IP	disable   enable	Enables validation of the client IP address. If the client IP address in the SSO cookie might be valid yet different from the current request client IP address, due to downstream proxies or other devices, disable client IP validation. The SiteMinder agents participating in SSO with the ProxySG should also be modified. The TransientIPCheck variable should be set to <i>yes</i> to enable IP validation and <i>no</i> to disable it. Enable is the default
siteminder-server	create	Create a SiteMinder server.
	delete	Delete a SiteMinder server.
	edit	Enter the SiteMinder server edit mode.
	authentication port <i>port_number</i>	The default is 44442. The ports should be the same as the ports configured on the SiteMinder server. The valid port range is 1-65535.
	authorization port <i>port_number</i>	The default is 44443. The ports should be the same as the ports configured on the SiteMinder server. The valid port range is 1-65535.
	accounting port <i>port_number</i>	The default is 44441. The ports should be the same as the ports configured on the SiteMinder server. The valid port range is 1-65535.
	connection-increment <i>number</i>	The default is 1. The connection increment specifies how many connections to open at a time if more are needed and the maximum is not exceeded.
	exit	Takes you out of the siteminder-server edit mode.
	ip-address	The IP address of the SiteMinder server.
	max-connections <i>number</i>	The default is 256. The maximum number of connections is 32768
	min-connections <i>number</i>	The default is 1.
	timeout <i>seconds</i>	The default is 60.
	view	Displays the server's configuration.

Table 3.82: # (config siteminder realm\_name) (Continued)

ssl	disable   enable	Disables/enables SSL communication between the ProxySG and BCAAA.
ssl-verify-agent	disable   enable	Specifies whether or not to verify the BCAAA certificate.
timeout	seconds	
view		Displays this realm's configuration.
virtual-url	url	Specifies the virtual URL to use for this SiteMinder realm. If no URL is specified the global transparent proxy virtual URL is used.

**Example**

```

SGOS#(config) security siteminder edit-realm test2
SGOS#(config siteminder test2) server-mode round-robin
ok
SGOS#(config siteminder test2) ssl enable
ok
SGOS#(config siteminder test2) exit
SGOS#(config)

```

**#(config) serial-number**

This command configures the ProxySG serial number.

**Syntax**

**option 1:** serial-number serial\_number

Table 3.83: #(config) serial-number

serial_number		Configures the ProxySG serial number.
---------------	--	---------------------------------------

**Example**

```

SGOS#(config) serial-number xxx
ok

```

**#(config) services**

Use this command to configure DNS, Endpoint Mapper FTP, HTTPS, IM, SSH, and Telnet services.

**Syntax**

services

This changes the prompt to:

```
SGOS#(config services)
```

**- subcommands-**

- option 1:** aol-im—changes the prompt (see “#(config services) aol-im” on page 202)
- option 2:** dns—changes the prompt (see “#(config services) dns” on page 203)
- option 3:** exit
- option 4:** epmapper—changes the prompt (see “#(config services) epmapper” on page 204)
- option 5:** ftp—changes the prompt (see “#(config services) ftp” on page 205)
- option 6:** http—changes the prompt (see “#(config services) http” on page 206)
- option 7:** https—changes the prompt (see “#(config services) https” on page 208)
- option 8:** http-console—changes the prompt (see “#(config services) http-console” on page 210)
- option 9:** https-console—changes the prompt (see “#(config services) https-console” on page 211)
- option 10:** mms—changes the prompt (see “#(config services) mms” on page 213)
- option 11:** msn-im—changes the prompt (see “#(config services) msn-im” on page 214)
- option 12:** rtsp—changes the prompt (see “#(config services) rtsp” on page 215)
- option 13:** socks—changes the prompt (see “#(config services) socks” on page 217)
- option 14:** ssh-console—changes the prompt (see “#(config services) ssh-console” on page 218)
- option 15:** tcp-tunnel—changes the prompt (see “#(config services) tcp-tunnel” on page 220)
- option 16:** telnet—changes the prompt (see “#(config services) telnet” on page 221)
- option 17:** telnet-console—changes the prompt (see “#(config services) telnet-console” on page 223)
- option 18:** view
- option 19:** yahoo-im—changes the prompt (see “#(config services) yahoo-im” on page 224)

Table 3.84: #(config services)

aol-im		Configures AOL IM services. See “#(config services) aol-im” on page 202.
dns		Configures DNS services. See “#(config services) dns” on page 203.
epmapper		Configures Endpoint Mapper services. See “#(config services) epmapper” on page 204.
exit		Exits the config services mode and returns to the config prompt.
ftp		Configures transparent or explicit FTP services. See “#(config services) ftp” on page 205.
http		Configures HTTP services. See “#(config services) http” on page 206.



Table 3.84: #(config services) (Continued)

https		Configures HTTPS services. See “#(config services) https” on page 208.
http-console		Configures HTTP Console services. See “#(config services) http-console” on page 210.
https-console		Configures HTTPS Console services. See “#(config services) https-console” on page 211.
mms		Configures MMS services. See “#(config services) mms” on page 213.
msn-im		Configures MSN IM services. See “#(config services) msn-im” on page 214.
rtsp		Configures RTSP services. See “#(config services) rtsp” on page 215.
socks		Configures SOCKS services. See “#(config services) socks” on page 217.
ssh-console		Configures SSH services. See “#(config services) ssh-console” on page 218.
tcp-tunnel		Configures TCP-tunneling services. See “#(config services) tcp-tunnel” on page 220.
telnet		Configures Telnet services. See “#(config services) telnet” on page 221.
telnet-console		Configures Telnet Console services. See “#(config services) telnet-console” on page 223.
view		Displays all services-related configuration information.
yahoo-im		Configures Yahoo IM services. See “#(config services) yahoo-im” on page 224.

### Example

```
SGOS#(config services) view
Port:      8080   Type: http
Properties: enabled, explicit-proxy
Port:      80     Type: http
Properties: enabled, transparent, explicit-proxy
Port:      21     Type: ftp
Properties: enabled, transparent
SGOS#(config services) exit
SGOS#(config)
```

## #(config services) aol-im

Use this command to configure AOL instant messaging services.

### Syntax

services

This changes the prompt to:

```
SGOS#(config services)
```

aol-im

This changes the prompt to:

```
SGOS#(config services aol-im)
```

#### - subcommands-

**option 1:** attribute send-client-ip {disable | enable} *port*

**option 2:** create *port*

**option 3:** delete *port*

**option 4:** disable *port*

**option 5:** enable *port*

**option 6:** exit

**option 7:** view

Table 3.85: #(config services aol-im)

attribute send-client-ip	disable <i>port</i>	Disables spoof attribute for listener.
	enable <i>port</i>	Enables spoof attribute for listener.
create	<i>port</i>	Creates an AOL-IM services listener.
delete	<i>port</i>	Deletes an AOL-IM services listener.
disable	<i>port</i>	Disables an AOL-IM services listener. This is the default setting.
enable	<i>port</i>	Enables an AOL-IM services listener.
exit		Exits configure services aol-im mode and returns to configure services mode.
view		Shows the AOL-IM services configuration.

**Example**

```

SGOS#(config) services
SGOS#(config services) aol-im
SGOS#(config services aol-im) create 2003
    ok
SGOS#(config services aol-im) exit
SGOS#(config services)

```

**#(config services) dns**

Use this command to configure DNS services.

**Syntax**

```
services
```

This changes the prompt to:

```
SGOS#(config services)
```

```
dns
```

This changes the prompt to:

```
SGOS#(config services dns)
```

**- subcommands-**

**option 1:** attribute

sub-option 1: explicit {disable | enable} [ip:]port

sub-option 2: transparent {disable | enable} [ip:]port

**option 2:** create [ip:]port

**option 3:** delete [ip:]port

**option 4:** disable [ip:]port

**option 5:** enable [ip:]port

**option 6:** exit

**option 7:** view

**Table 3.86:** #(config services dns)

attribute	explicit {disable   enable} [ip:]port	Disables or enables explicit-proxy attribute for listener.
	transparent {disable   enable} [ip:]port	Disables or enables transparent attribute of listener.
create	[ip:]port	Creates a DNS services listener.
delete	[ip:]port	Deletes a DNS services listener.
disable	[ip:]port	Disables a DNS services listener.
enable	[ip:]port	Enables a DNS services listener.
exit		Exits configure services dns mode and returns to configure services mode.
view		Shows the DNS services configuration.

### Example

```
SGOS#(config) services
SGOS#(config services) dns
SGOS#(config services dns) create 1
    ok
SGOS#(config services dns) exit
SGOS#(config services) exit
SGOS#(config)
```

## #(config services) epmapper

Use this command to configure Endpoint Mapper services.

### Syntax

services

This changes the prompt to:

```
SGOS#(config services)
```

epmapper

This changes the prompt to:

```
SGOS#(config services epmapper)
```

### Subcommands

**option 1:** attribute send-client-ip {disable | enable} port

**option 2:** create port

**option 3:** delete port

**option 4:** disable port

**option 5:** enable port

**option 6:** exit

**option 7:** view

Table 3.87: #(config services-epmapper)

attribute	send-client-ip {disable   enable port}	Enables or disables sending of the client's IP address instead of the ProxySG's IP address.
create	port	Creates an Endpoint Mapper services port.
delete	port	Deletes the specified Endpoint Mapper port.

Table 3.87: #(config services-epmapper) (Continued)

disable	<i>port</i>	Disables the Endpoint Mapper services on the specified port.
enable	<i>port</i>	Enables the Endpoint Mapper services on the specified port.
exit		Exits configure services Endpoint Mapper mode and returns to configure services mode.
view		Displays the Endpoint Mapper services configuration.

**Example**

```

SGOS#(config) services
SGOS#(config services) epmapper
SGOS#(config services epmapper) create 136
    ok
SGOS#(config services epmapper) attribute send-client-ip enable 136
    ok
SGOS#(config services) view
Port:      136      IP: 0.0.0.0      Type: epmapper
Properties: transparent, explicit, enabled, send-client-ip

```

**#(config services) ftp**

Use this command to configure transparent FTP services.

**Syntax**

```
services
```

This changes the prompt to:

```
SGOS#(config services)
```

```
ftp
```

This changes the prompt to:

```
SGOS#(config services ftp)
```

**- subcommands-**

**option 1:** attribute {explicit {disable | enable} [*ip*:]*port* | passive-mode {disable | enable} [*ip*:]*port* | transparent {disable | enable} [*ip*:]*port*}

**option 2:** create [*ip*:]*port*

**option 3:** delete [*ip*:]*port*

**option 4:** disable [*ip*:]*port*

**option 5:** enable [*ip*:]*port*

**option 6:** exit

**option 7:** view

Table 3.88: #(config services ftp)

attribute	explicit {disable   enable} [ip:]port	Disables or enables explicit-proxy attribute for listener.
	passive-mode {disable   enable}	Disables or enables support for passive mode to clients.
	transparent {disable   enable} [ip:]port	Disables or enables transparent attribute of listener.
create	[ip:]port	Creates a transparent FTP services port.
delete	[ip:]port	Deletes a transparent FTP services port.
disable	[ip:]port	Disables the transparent FTP services port.
enable	[ip:]port	Enables the transparent FTP services port.
exit		Exits configure services ftp mode and returns to configure services mode.
view		Displays the transparent FTP services configuration.

**Example**

```
SGOS#(config) services
SGOS#(config services) ftp
SGOS#(config services ftp) create 2003
ok
SGOS#(config services ftp) exit
SGOS#(config services) exit
SGOS#(config)
```

**#(config services) http**

Use this command to create and configure HTTP services.

**Syntax**

```
services
```

This changes the prompt to:

```
SGOS#(config services)
```

```
http
```

This changes the prompt to:

```
SGOS#(config services http)
```

**- subcommands-**

**option 1:** attribute

```
sub-option 1: authenticate-401 {disable | enable} [ip:]port
sub-option 2: explicit {disable | enable} [ip:]port
sub-option 3: send-client-ip {disable | enable} [ip:]port
sub-option 4: transparent {disable | enable} [ip:]port
```

```

sub-option 5: head {disable {drop | error} [ip:]port | enable [ip:]port}
sub-option 6: connect {disable {drop | error} [ip:]port | enable [ip:]port}
option 2: create [ip:]port
option 3: delete [ip:]port
option 4: disable [ip:]port
option 5: enable [ip:]port
option 6: exit
option 7: view

```

Table 3.89: # (config services-http)

attribute	authenticate-401 {disable   enable [ip:]port}	Enables or disables transparent authentication.
	explicit {disable   enable [ip:]port}	Accepts or rejects requests for non-transparent content.
	send-client-ip {disable   enable [ip:]port}	Enables or disables the spoof attribute.
	transparent {disable   enable [ip:]port}	Accepts or rejects requests for transparent content.
	head {disable {drop   error} [ip:]port   enable [ip:]port}	Allows or prevents blocking of HEAD requests.
	connect {disable {drop   error} [ip:]port   enable [ip:]port}	Allows or blocks CONNECT requests.
create	[ip:]port	Creates an HTTP services listener port.
delete	[ip:]port	Deletes the specified HTTP services listener port.
disable	[ip:]port	Disables the HTTP services on the specified port.
enable	[ip:]port	Enables the HTTP services on the specified port.
exit		Exits configure services HTTP mode and returns to configure services mode.
view		Displays the HTTP services configuration.

### Example

```
SGOS#(config) services
SGOS#(config services) http
SGOS#(config services http) create 8085
    ok
SGOS#(config services http) attribute authenticate-401 enable 8085
    ok
SGOS#(config services http) exit
SGOS#(config services) exit
SGOS#(config)
```

## #(config services) https

Use this command to create and configure HTTPS services.

### Syntax

services

This changes the prompt to:

```
SGOS#(config services)
```

https

This changes the prompt to:

```
SGOS#(config services https)
```

#### - subcommands-

**option 1:** attribute

sub-option 1: ccl *ip:port*

sub-option 2: cipher-suite *ip:port* [*cipher-suite*]

sub-option 3: forward-client-cert {disable | enable} *ip:port*

sub-option 4: send-client-ip {disable | enable} *ip:port*

sub-option 5: ssl-protocol-version {ssl2 | ssl3 | tls1 | ssl2v3 | ssl2tls1 |  
ssl3tls1 | ssl2v3tls1} *ip:port*

sub-option 6: verify-client {disable | enable} *ip:port*

**option 2:** create *ip:port* keyring *id*

**option 3:** delete

sub-option 1: attribute ccl *ip:port*

sub-option 2: *ip:port*

**option 4:** disable *ip:port*

**option 5:** enable *ip:port*

**option 6:** exit

**option 7:** view



Table 3.90: # (config services https)

attribute	<code>cipher-suite ip:port</code> <code>cipher-suite</code>	Specifies the cipher suite to use. The default is to use all cipher suites. If you want to change the default, you have two choices: <ul style="list-style-type: none"> <li>• interactive mode</li> <li>• non-interactive mode</li> </ul> Director uses non-interactive commands in profiles and overlays to create cipher suites. The optional <code>cipher-suite</code> refers to the cipher-suites you want to use, space separated, such as <code>rc4-md5</code> <code>exp-des-cbc-sha</code> . If you want to use the interactive mode, do not specify a cipher suite. For a list of cipher suites available, refer to “Using Secure Services” in the <i>Blue Coat Configuration and Management Guide</i> .
	<code>ccl ip:port</code>	Sets CA Certificate List to use for verifying certificates.
	<code>forward-client-cert</code> {disable   enable} <code>ip:port</code>	Enables or disables client certificate forwarding
	<code>send-client-ip</code> {disable   enable} <code>ip:port</code>	Enables or disables sending client's IP as source IP address.
	<code>ssl-protocol-version</code> { <code>ssl2</code>   <code>ssl3</code>   <code>tlsv1</code>   <code>ssl2v3</code>   <code>ssl2tlsv1</code>   <code>ssl3tlsv1</code>   <code>ssl2v3tlsv1</code> } <code>ip:port</code>	Specifies the SSL protocol version.
	<code>verify-client</code> {disable   enable} <code>ip:port</code>	Enables or disables client verification.
create	<code>ip:port keyring id</code>	Creates an HTTPS services listener port.
delete	<code>attribute ccl ip:port</code>   <code>ip:port</code>	Deletes the HTTPS services settings.
disable	<code>ip:port</code>	Disables the HTTPS services listener port.
enable	<code>ip:port</code>	Enables the HTTPS services listener port.
exit		Exits configure services HTTPS mode and returns to configure services mode.
view		Displays the HTTPS services configuration.

### Example

```
SGOS#(config) services
SGOS#(config services) https
SGOS#(config services https) create 10.25.36.47:8085 default
ok
SGOS#(config services https) view

Port:      8085      IP: 10.25.36.47 Type: https
Keyring: default
Properties: transparent, explicit, enabled
SSL Protocol version: SSLv2v3TLSv1
CA Certificate List: not configured

Cipher suite:
RC4-MD5:RC4-SHA:DES-CBC3-SHA:DES-CBC3-MD5:RC2-CBC-MD5:RC4-64-MD5:DES-CBC-SHA:DES-CBC-MD5:EXP1024-RC4-MD5:EXP1024-RC4-SHA:EXP1024-RC2-CBC-MD5:EXP1024-DES-CBC-SHA:EXP-RC4-MD5:EXP-RC2-CBC-MD5:EXP-DES-CBC-SHA:+SSLv2:+SSLv3+LOW:+SSLv2+LOW:+EXPO

SGOS#(config services https) exit
SGOS#(config services) exit
SGOS#(config)
```

## #(config services) http-console

Use this command to create and configure an HTTP management console.

### Syntax

```
services
```

This changes the prompt to:

```
SGOS#(config services)
```

```
http-console
```

This changes the prompt to:

```
SGOS#(config services http-console)
```

#### - subcommands-

**option 1:** create [*ip*:]*port*

**option 2:** delete [*ip*:]*port*

**option 3:** disable [*ip*:]*port*

**option 4:** enable [*ip*:]*port*

**option 5:** exit

**option 6:** view

Table 3.91: #(config services http-console)

create	[ip:]port	Creates an HTTP Console services listener.
delete	[ip:]port	Deletes an HTTP Console services listener.
disable	[ip:]port	Disables an HTTP Console services listener. This is the default setting.
enable	[ip:]port	Enables an HTTP Console services listener.
exit		Exits configure services http-console mode and returns to configure services mode.
view		Displays the HTTP Console services configuration.

**Example**

```

SGOS#(config) services
SGOS#(config services) http-console
SGOS#(config services http-console) create 9000
ok
SGOS#(config services http-console) enable 9000
ok
SGOS#(config services http-console) view
Port:      9000      IP: 0.0.0.0      Type: management
Properties: explicit, enabled
SGOS#(config services http-console) exit
SGOS#(config services) exit
SGOS#(config)

```

**#(config services) https-console**

Use this command to create and configure an HTTPS management console.

**Syntax**

```
services
```

This changes the prompt to:

```
SGOS#(config services)
```

```
https-console
```

This changes the prompt to:

```
SGOS#(config services https-console)
```

**- subcommands-**

**option 1:** attribute cipher-suite [ip:]port cipher-suite

**option 2:** create [ip:]port [keyring\_id]

**option 3:** delete [ip:]port

**option 4:** disable [ip:]port

**option 5:** enable `[ip:]port`

**option 6:** exit

**option 7:** view

Table 3.92: # (config services https-console)

attribute cypher-suite	<code>[ip:]port</code> <code>[cipher-suite]</code>	<p>Configures HTTPS Console services cypher suite. The default is to use all ciphers.</p> <p>If you want to change the default, you have two choices:</p> <ul style="list-style-type: none"><li>• interactive mode</li><li>• non-interactive mode</li></ul> <p>Director uses non-interactive commands in profiles and overlays to create cipher suites.</p> <p>The optional <code>cipher-suite</code> refers to the cipher-suites you want to use, space separated, such as <code>rc4-md5 exp-des-cbc-sha</code>. If you want to use the interactive mode, do not specify a cipher suite.</p> <p>For a list of cipher suites available, refer to “Using Secure Services” in the <i>Blue Coat Configuration and Management Guide</i>.</p>
create	<code>[ip:]port [keyring_id]</code>	Creates an HTTPS Console services listener.
delete	<code>[ip:]port</code>	Deletes an HTTPS Console services listener.
disable	<code>[ip:]port</code>	Disables an HTTPS Console services listener.
enable	<code>[ip:]port</code>	Enables an HTTPS Console services listener.
exit		Exits configure services https-console mode and returns to configure services mode.
view		Displays the HTTPS Console services configuration.

*Example*

```

SGOS#(config) services
SGOS#(config services) https-console
SGOS#(config services https-console) create 9000
    ok
SGOS#(config services https-console) enable 9000
    ok
SGOS#(config services https-console) view
Port:      9000      IP: 0.0.0.0      Type: management

    Properties: explicit, enabled

SGOS#(config services https-console) exit
SGOS#(config services) exit
SGOS#(config)

```

 **#(config services) mms**

Use this command to create and configure MMS services.

**Syntax**

```
services
```

This changes the prompt to:

```
SGOS#(config services)
```

```
mms
```

This changes the prompt to:

```
SGOS#(config services mms)
```

**- subcommands-**

**option 1:** attribute

```
sub-option 1: explicit {disable | enable} [ip:]port
```

```
sub-option 2: send-client-ip {disable | enable} [ip:]port
```

```
sub-option 3: transparent {{disable | enable} [ip:]port
```

**option 2:** create [ip:]port

**option 3:** delete [ip:]port

**option 4:** disable [ip:]port

**option 5:** enable [ip:]port

**option 6:** exit

**option 7:** view

Table 3.93: #(config services mms)

attribute	explicit {disable   enable} [ip:]port	Disables or enables explicit-proxy attribute for listener.
	send-client-ip {disable   enable} [ip:]port	Disables or enables spoof attribute for listener.
	transparent {disable   enable} [ip:]port	Disables or enables transparent attribute for listener.
create	[ip:]port	Creates an MMS services listener port.
delete	[ip:]port	Deletes the specified MMS services listener port.
disable	[ip:]port	Disables the MMS services on the specified port. This is the default setting.
enable	[ip:]port	Enables the MMS services on the specified port.
exit		Exits configure services mms mode and returns to configure services mode.
view		Displays the MMS services configuration.

**Example**

```
SGOS#(config) services
SGOS#(config services) mms
SGOS#(config services mms) create 8085
ok
SGOS#(config services mms) attribute explicit enable 8085
ok
SGOS#(config services mms) exit
SGOS#(config services) exit
SGOS#(config)
```

 **#(config services) msn-im**

Use this command to create and configure MSN instant messaging services.

**Syntax**

```
services
```

This changes the prompt to:

```
SGOS#(config services)
```

```
msn-im
```

This changes the prompt to:

```
SGOS#(config services msn-im)
```

**- subcommands-**

**option 1:** attribute send-client-ip {disable | enable} port

**option 2:** create port

**option 3:** delete *port*  
**option 4:** disable *port*  
**option 5:** enable *port*  
**option 6:** exit  
**option 7:** view

Table 3.94: # (config services msn-im)

attribute send-client-ip	{disable   enable} <i>port</i>	Disables or enables spoof attribute for listener.
create	<i>port</i>	Creates an MSN IM services listener port.
delete	<i>port</i>	Deletes the specified MSN IM services listener port.
disable	<i>port</i>	Disables the MSN IM services on the specified port. This is the default setting.
enable	<i>port</i>	Enables the MSN IM services on the specified port.
exit		Exits configure services msn-im mode and returns to configure services mode.
view		Displays the MSN IM services configuration.

**Example**

```
SGOS#(config) services
SGOS#(config services) msn-im
SGOS#(config services msn-im) create 8085
ok
SGOS#(config services msn-im) attribute send-client-ip enable 8085
ok
SGOS#(config services msn-im) exit
SGOS#(config services) exit
SGOS#(config)
```

**#(config services) rtsp**

Use this command to create and configure RTSP services.

**Syntax**

```
services
```

This changes the prompt to:

```
SGOS#(config services)
```

```
rtsp
```

This changes the prompt to:

```
SGOS#(config services rtsp)
```

**- subcommands-****option 1:** attribute

sub-option 1: explicit {disable | enable} [ip:]port

sub-option 2: send-client-ip {disable | enable} [ip:]port

sub-option 3: transparent {disable | enable} [ip:]port

**option 2:** create [ip:]port**option 3:** delete [ip:]port**option 4:** disable [ip:]port**option 5:** enable [ip:]port**option 6:** exit**option 7:** view

Table 3.95: #(config services rtsp)

attribute	explicit {disable   enable} [ip:]port	Disables or enables explicit-proxy attribute for listener.
	send-client-ip {disable   enable} [ip:]port	Disables or enables spoof attribute for listener.
	transparent {disable   enable} [ip:]port	Disables or enables transparent attribute for listener.
create	[ip:]port	Creates an RTSP services listener port.
delete	[ip:]port	Deletes the specified RTSP services listener port.
disable	[ip:]port	Disables the RTSP services on the specified port. This is the default setting.
enable	[ip:]port	Enables the RTSP services on the specified port.
exit		Exits configure services rtsp mode and returns to configure services mode.
view		Displays the RTSP services configuration.

**Example**

```

SGOS#(config) services
SGOS#(config services) rtsp
SGOS#(config services rtsp) create 8085
ok
SGOS#(config services rtsp) attribute explicit enable 8085
ok
SGOS#(config services rtsp) exit
SGOS#(config services) exit
SGOS#(config)

```



## #(config services) socks

Use this command to create and configure SOCKS services.

### Syntax

```
services
```

This changes the prompt to:

```
SGOS#(config services)
```

```
socks
```

This changes the prompt to:

```
SGOS#(config services socks)
```

### - subcommands-

**option 1:** create *[ip]:port*

**option 2:** delete *[ip]:port*

**option 3:** disable *[ip]:port*

**option 4:** enable *[ip]:port*

**option 5:** exit

**option 6:** view

Table 3.96: #(config services socks)

create	<i>[ip]:port</i>	Creates a SOCKS services listener port.
delete	<i>[ip]:port</i>	Deletes a SOCKS services listener.
disable	<i>[ip]:port</i>	Disables a SOCKS services listener. This is the default setting.
enable	<i>[ip]:port</i>	Enables a SOCKS services listener.
exit		Exits configure services socks mode and returns to configure services mode.
view		Displays the SOCKS services configuration.

### Example

```
SGOS#(config) services
SGOS#(config services) socks
SGOS#(config services socks) create 8085
ok
SGOS#(config services socks) enable 8085
ok
SGOS#(config services socks) exit
SGOS#(config services) exit
SGOS#(config)
```

## #(config services) ssh-console

The default connection to the ProxySG is SSH and HTTPS. All data transmitted between the SSH client and SSH host is encrypted and decrypted using public and private keys established on the ProxySG and by the SSH application on the client.

---

*Note:* The ProxySG supports a combined maximum of 16 Telnet and SSH sessions. It also supports up to 24 keys per user.

---

## Before You Begin

SSHv2 is enabled and ready for use. You must create and enable SSHv1 if you want to use it. To use SSH with RSA authentication, you must create a keypair in OpenSSH format through the SSH client application, copy the keypair to the clipboard, and use the `import client-key` command to import the key onto the ProxySG.

## Syntax

services

This changes the prompt to:

```
SGOS#(config services)
```

ssh-console

This changes the prompt to:

```
SGOS#(config services ssh-console)
```

### - subcommands-

#### option 1: create

sub-option 1: host-keypair {[sshv1] | [sshv2]}

sub-option 2: [ip]:port

#### option 2: delete

sub-option 1: client-key username key\_id

sub-option 2: director-client-key key\_id

sub-option 3: legacy-client-key key\_id

sub-option 4: host-keypair {[sshv1] | [sshv2]}

```

sub-option 5: [ip]:port
option 3: disable [ip]:port
option 4: enable [ip]:port
option 5: exit
option 6: import client-key username | director-client-key
option 7: view
sub-option 1: [client-key username]
sub-option 2: [director-client-key [key_id]]
sub-option 3: [host-public-key {[sshv1] | [sshv2]}]
sub-option 4: [user-list]
sub-option 5: [versions-enabled]

```

Table 3.97: # (config services ssh-console)

create	host-keypair {[sshv1]   [sshv2]}	Allows you to create a host keypair if one has been deleted. Only two keypairs—SSHv1 and SSV2—are allowed on the ProxySG. The port number is required.
	[ip]:port	
delete	client-key <i>username</i> <i>key_id</i>	Deletes either the host keypair or the client key associated with the indicated <i>username</i> .
	director-client-key <i>key_id</i>	Deletes the client key associated with the indicated <i>username</i> of a ProxySG that is being used in Blue Coat Systems Director configurations.
	legacy-client-key <i>key_id</i>	Deletes the client-key file (if you upgraded from a previous version) with all its client keys. This file does not contain client keys created in SGOS v3.
	host-keypair {[sshv1]   [sshv2]}	Deletes the host-keypair associated with SSHv1 or SSHv2.
	[ip]:port	Deletes the SSH-console at the port specified.
exit		Exits configure services ssh-console mode and returns to configure services mode.
import	client-key <i>username</i>	Imports the client key associated with the indicated <i>username</i> .
	director-client-key	Imports the Director client key, automatically determined from the imported key.

Table 3.97: #(config services ssh-console) (Continued)

view		Displays the SSH service details.
	[client-key username]	Displays the client key associated with the indicated <i>username</i> .  NOTE: If you have upgraded from an older version of the ProxySG, you might not need to enter a username.
	director-client-key [key_id]	Displays the client key associated with the indicated Director <i>key_id</i> or all client fingerprints.
	host-public-key {[sshv1]   [sshv2]}	Displays the host-keypair associated with SSHv1 or SSHv2.
	user-list	Displays the list of users with imported RSA client keys.
	versions-enabled	Displays which SSH version(s) is enabled.

**Example**

```

SGOS#(config) services
SGOS#(config services) ssh-console
SGOS#(config services ssh-console) import client-key username
Paste client key here, end with "... " (three periods)
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAlV/xvN21VrOOK6sNuAnavWy9RsI8xgfD7OXQ4rocXrNm9kdnYB1
OzaDWgZ4mHUnTmBkmAJKaGJRfZMIQt2ZXF+biVHbOWyinzbiDMkXEEI4PHXoqyWp5Bq7bI2RgDOVaM
MlvQT9uyenKymwZE1DNe/tlRiGkdUN3/s3kX6xv0M= admin@GLYPH
...
ok

SGOS#(config services ssh-console) view client-key username
admin@adminPC 45:5C:3F:5F:EA:65:6E:CF:EE:4A:05:58:9A:C5:FB:4F
admin@GLYPH BB:20:21:4D:E0:BC:32:39:13:55:2E:B4:07:81:4F:AV
SGOS#(config services socks) exit
SGOS#(config services) exit
SGOS#(config)

```

 **#(config services) tcp-tunnel**

Use this command to create, enable, and configure TCP-tunnel services. Multiple TCP-tunnel services are supported.

---

*Note:* TCP-tunnel services are not created by default—you must create and enable them.

---

**Syntax**

```
services
```

This changes the prompt to:

```
SGOS#(config services)
```

```
tcp-tunnel
```

This changes the prompt to:

```
SGOS#(config services tcp-tunnel)
```

- *subcommands*-

**option 1:** attribute

```
sub-option 6: explicit {disable | enable} [ip:]port
```

```
sub-option 7: transparent {disable | enable} [ip:]port
```

**option 2:** create [ip:]port

**option 3:** delete [ip:]port

**option 4:** disable [ip:]port

**option 5:** enable [ip:]port

**option 6:** exit

**option 7:** view

Table 3.98: #(config services tcp-tunnel)

attribute	explicit {disable   enable} [ip:]port	Enables or disables the explicit TCP-tunnel port.
	transparent {disable   enable} [ip:]port	Enables or disables the transparent TCP-tunnel port.
create	[ip:]port	Creates a TCP-tunnel port.
delete	[ip:]port	Deletes the TCP-tunnel services settings.
disable	[ip:]port	Disables the TCP-tunnel port.
enable	[ip:]port	Enables the TCP-tunnel port.
exit		Exits configure services tcp-tunnel mode and returns to configure services mode.
view		Displays the TCP-tunnel services configuration.

### Example

```
SGOS#(config) services
SGOS#(config services) tcp-tunnel
SGOS#(config services tcp-tunnel) create 0.0.0.0:9001
ok
SGOS#(config services tcp-tunnel) view
Port:      9001      IP: 0.0.0.0      Type: tcp-tunnel
Properties: transparent, enabled
SGOS#(config services tcp-tunnel) exit
SGOS#(config services) exit
SGOS#(config)
```

## #(config services) telnet

Use this command to create and configure Telnet services.

## Syntax

services

This changes the prompt to:

```
SGOS#(config services)
```

telnet

This changes the prompt to:

```
SGOS#(config services telnet)
```

### - subcommands-

**option 1:** attribute

sub-option 1: explicit

sub-option 2: send-client-ip

sub-option 3: transparent

**option 2:** create [*ip*:]*port*

**option 3:** delete [*ip*:]*port*

**option 4:** disable [*ip*:]*port*

**option 5:** enable [*ip*:]*port*

**option 6:** exit

**option 7:** view

Table 3.99: #(config services telnet)

attribute	explicit {disable   enable} [ <i>ip</i> :] <i>port</i>	Specifies whether to accept or not to accept explicit proxy requests for the port and optional IP address specified.
	send-client-ip {disable   enable} [ <i>ip</i> :] <i>port</i>	Enables or disables the spoof attribute for the port and optional IP address specified.
	transparent {disable   enable} [ <i>ip</i> :] <i>port</i>	Enables or disables the transparent proxy attribute for the port and optional IP address specified.
create	[ <i>ip</i> :] <i>port</i>	Creates a Telnet services port indicated by [ <i>ip</i> :] <i>port</i> . Note that if you also enable the Telnet-Console you must use a different port for the Telnet service.
delete	[ <i>ip</i> :] <i>port</i>	Deletes the Telnet services port indicated by [ <i>ip</i> :] <i>port</i> .
disable	[ <i>ip</i> :] <i>port</i>	Disables the Telnet services port.
enable	[ <i>ip</i> :] <i>port</i>	Enables the Telnet services port.
exit		Exits configure services telnet-console mode and returns to configure services mode.
view		Displays the Telnet services configuration.

**Example**

```

SGOS#(config) services
SGOS#(config services) telnet
SGOS#(config services telnet) create 10.25.36.47:24
ok
SGOS#(config services telnet) attribute send-client-ip enable 10.25.36.47:24
ok
SGOS#(config services telnet) view
Port:      23      IP: 0.0.0.0      Type: telnet
Properties: transparent, explicit, disabled
Port:      24      IP: 10.25.36.47:24      Type: telnet
Properties: explicit, enabled, send-client-ip

```

 **#(config services) telnet-console**

Use this command to enable and configure the Telnet Console, which allows you to connect to the ProxySG with the Telnet protocol. Remember that Telnet is an insecure protocol that should not be used in insecure conditions.

**Syntax**

```
services
```

This changes the prompt to:

```
SGOS#(config services)
```

```
telnet-console
```

This changes the prompt to:

```
SGOS#(config services telnet-console)
```

- *subcommands* -

**option 1:** create [*ip*:]*port*

**option 2:** delete [*ip*:]*port*

**option 3:** disable [*ip*:]*port*

**option 4:** enable [*ip*:]*port*

**option 5:** exit

**option 6:** view

Table 3.100: #(config services telnet-console)

create	[ <i>ip</i> :] <i>port</i>	Creates a Telnet-Console services port indicated by [ <i>ip</i> :] <i>port</i> . Note that if you also enable Telnet you must use a different port for the Telnet-Console service.
delete	[ <i>ip</i> :] <i>port</i>	Deletes the Telnet-Console services port indicated by [ <i>ip</i> :] <i>port</i> .

Table 3.100: #(config services telnet-console) (Continued)

disable	[ip:]port	Disables the Telnet-Console services port.
enable	[ip:]port	Enables the Telnet-Console services port.
exit		Exits configure services Telnet-Console mode and returns to configure services mode.
view		Displays the Telnet-Console services configuration.

**Example**

```
SGOS#(config) services
SGOS#(config services) telnet-console
SGOS#(config services telnet-console) create 10.25.36.47:25
ok
SGOS#(config services telnet-console) view
Port:      25      IP: 10.25.36.47 Type: telnet-console
Properties: enabled
```

 **#(config services) yahoo-im**

Use this command to create and configure Yahoo instant messaging services.

**Syntax**

```
services
```

This changes the prompt to:

```
SGOS#(config services)
```

```
yahoo-im
```

This changes the prompt to:

```
SGOS#(config services yahoo-im)
```

**- subcommands-**

**option 1:** attribute send-client-ip {disable | enable} port

**option 2:** create port

**option 3:** delete port

**option 4:** disable port

**option 5:** enable port

**option 6:** exit

**option 7:** view



Table 3.101: #(config services yahoo-im)

attribute	send-client-ip {disable <i>port</i>   enable <i>port</i> }	Disables or enables spoof attribute for listener.
create	<i>port</i>	Creates a Yahoo IM services listener port.
delete	<i>port</i>	Deletes the specified Yahoo IM services listener port.
disable	<i>port</i>	Disables the Yahoo IM services on the specified port.
enable	<i>port</i>	Enables the Yahoo IM services on the specified port.
exit		Exits configure services yahoo-im mode and returns to configure services mode.
view		Displays the Yahoo IM services configuration.

**Example**

```

SGOS#(config) services
SGOS#(config services) yahoo-im
SGOS#(config services yahoo-im) create 8085
ok
SGOS#(config services yahoo-im) attribute transparent enable 8085
ok
SGOS#(config services yahoo-im) exit
SGOS#(config services) exit
SGOS#(config)

```

 **#(config) session-monitor**

Use this command to configure options to monitor RADIUS accounting messages and to maintain a session table based on the information in these messages.

**Syntax**

```
session-monitor
```

This changes the prompt to:

```
#(config session-monitor)
```

**-subcommands-**

**option 1:** cluster {disable | enable | grace-period *seconds* | group-address  
*IP\_Address* | no | port *port*| synchronization-delay *seconds*}

**option 2:** disable

**option 3:** enable

**option 4:** max-entries *integer*

**option 5:** radius {acct-listen-port *port* | authentication {disable | enable}|  
encrypted-shared-secret *encrypted-secret* | no | respond {disable |  
enable}| shared-secret *secret*}

**option 6:** timeout *minutes*

**option 7:** view

Table 3.102: (config session-monitor)

cluster	disable		Disables cluster support.
	enable		Enables cluster support. The group address must be set before the cluster can be enabled.
	grace-period	<i>seconds</i>	Set the time to keep session transactions in memory while waiting for slave logins. This can be set to allow session table synchronization to occur after the synchronization-delay has expired. The default is 30 seconds; the range is 0 to $2^{31}-1$ seconds.
	group-address no group-address	<i>IP_Address</i>	Set or clear (the default) the failover group IP address. This must be an existing failover group address.
	port	<i>port</i>	Set the TCP/IP port for the session replication control. The default is 55555.
	synchronization-delay	<i>seconds</i>	Set the maximum time to wait for session table synchronization. The default is zero; the range is from 0 to $2^{31}-1$ seconds. During this time evaluation of <code>\$(session.username)</code> is delayed, so proxy traffic might also be delayed.
disable			Enable session monitoring.
enable			Disable (the default) session monitoring
max-entries	integer		The maximum number of entries in the session table. The default is 500,000; the range is from 1 to 2,000,000. If the table reaches the maximum, additional START messages are ignored.
radius	acct-listen-port	<i>port</i>	The port number where the ProxySG listens for accounting messages.
	authentication	disable   enable	Enable or disable (the default) the authentication of RADIUS messages using the shared secret. Note that the shared secret must be configured before authentication is enabled.
	encrypted-shared-secret	<i>encrypted-secret</i>	Specify the shared secret (in encrypted form) used for RADIUS protocol authentication. The secret is decrypted using the configuration-passwords-key.
	no shared-secret		Clears the shared secret used for RADIUS protocol authentication.
	respond	disable   enable	Enable (the default) or disable generation of RADIUS responses.
	shared-secret	<i>plaintext_secret</i>	Specify the shared secret used for RADIUS protocol in plaintext.

Table 3.102: (config session-monitor) (Continued)

cluster	disable		Disables cluster support.
timeout	minutes		The amount of time before a session table entry assumes a STOP message has been sent. The default is 120 minutes; the range is from 0 to 65535 minutes. Zero indicates no timeout.
view			View the session-monitor configuration.

## #(config) shell

Use this command to configure options for the shell.

**option 1:** shell max-connections

**option 2:** shell no

**option 3:** shell prompt

**option 4:** shell realm-banner

**option 5:** shell welcome-banner

Table 3.103: #(config) shell

max-connections	<i>number</i>	Maximum number of shell connections. Allowed values are between 1 and 65535.
no	<i>string</i>	Disables the prompt, realm-banner, and welcome-banner strings.
prompt	<i>string</i>	Sets the prompt that the user sees in the shell. If the string includes white space, enclose the string in quotes.
realm-banner	<i>string</i>	Sets the realm banner that the user sees when logging into a realm through the shell. If the string includes white space, enclose the string in quotes.
welcome-banner	<i>string</i>	Sets the welcome banner that the users sees when logging into the shell. If the string includes white space, enclose the string in quotes.

### Example

```
SGOS#(config) shell prompt "Telnet Shell >"
ok
SGOS#(config) shell welcome-banner "Welcome to the Blue Coat Systems Telnet
Shell"
ok
```

## #(config) show

See “# show” on page 40 in Chapter 2: “Standard and Privileged Mode Commands”.

## #(config) snmp

Use this command to set SNMP (Simple Network Management Protocol) options for the ProxySG.

The ProxySG can be viewed using an SNMP management station. The ProxySG supports MIB-2 (RFC 1213).

### Syntax

snmp

This changes the prompt to:

SGOS#(config snmp)

#### - subcommands-

**option 1:** authorize-traps

**option 2:** disable

**option 3:** enable

**option 4:** encrypted-read-community *encrypted\_password*

**option 5:** encrypted-trap-community *encrypted\_password*

**option 6:** encrypted-write-community *encrypted\_password*

**option 7:** exit

**option 8:** no

sub-option 1: authorize-traps

sub-option 2: sys-contact

sub-option 3: sys-location

sub-option 4: trap-address {1 | 2 | 3}

**option 9:** read-community *password*

**option 10:** reset-configuration

**option 11:** snmp-writes {disable | enable}

**option 12:** sys-contact *string*

**option 13:** sys-location *string*

**option 14:** trap-address {1 | 2 | 3} *ip\_address*

**option 15:** trap-community *password*

**option 16:** view

**option 17:** write-community *password*

Table 3.104: #(config snmp)

authorize-traps		Enables SNMP authorize traps.
disable		Disables SNMP for the ProxySG.
enable		Enables SNMP for the ProxySG.
encrypted-read-communit y	<i>encrypted_password</i>	Specifies encrypted read community string.

Table 3.104: #(config snmp) (Continued)

encrypted-trap-community	<i>encrypted_password</i>	Specifies encrypted trap community string.
encrypted-write-community	<i>encrypted_password</i>	Specifies encrypted write community string.
exit		Exits configure snmp mode and returns to configure mode.
no	authorize-traps	Disables the current authorize traps settings.
	sys-contact	Disables the current system contact settings.
	sys-location	Disables the current system location settings.
	trap-address {1   2   3}	Disables the current trap address settings (for trap address 1, 2, or 3).
read-community	<i>password</i>	Sets the read community password or encrypted-password.
reset-configuration		Resets the SNMP configuration to the default settings.
snmp-writes	{disable   enable}	Enables or disables SNMP write capability.
sys-contact	<i>string</i>	Sets the "sysContact" MIB variable to <i>string</i> .
sys-location	<i>string</i>	Sets the "sysLocation" MIB variable to <i>string</i> .
trap-address	{1   2   3} <i>ip_address</i>	Indicates which IP address(es) can receive traps and in which priority.
trap-community	<i>password</i>	Sets the trap community password or encrypted-password.
view		Displays SNMP settings.
write-community	<i>password</i>	Sets the write community password or encrypted-password.

**Example**

```

SGOS#(config) snmp
SGOS#(config snmp) authorize-traps
ok
SGOS#(config snmp) exit
SGOS#(config)

```

## #(config) socks-gateways

Use this command to set the SOCKS gateways settings.

### Syntax

socks-gateways

This changes the prompt to:

SGOS#(config socks-gateways)

#### - subcommands-

**option 1:** create *gateway\_alias gateway\_host SOCKS\_port* [version={4 | 5  
[user=username password=password] [request-compression={yes | no}]]]

**option 2:** delete {all | gateway *gateway\_alias*}

**option 3:** edit *gateway\_alias*—changes the prompt (see “#(config socks-gateways) edit *gateway\_alias*” on page 231)

**option 4:** exit

**option 5:** failure-mode {closed | open}

**option 6:** no path

**option 7:** path *url*

**option 8:** sequence

sub-option 1: add *gateway\_alias*

sub-option 2: clear

sub-option 3: demote *gateway\_alias*

sub-option 4: promote *gateway\_alias*

sub-option 5: remove *gateway\_alias*

**option 9:** view

Table 3.105: #(config socks-gateways)

create	<i>gateway_alias gateway_host SOCKS_port</i> [version={4   5 [user=username password=password] [request-compression= {yes   no}]]]	Creates a SOCKS gateway.
delete	all   gateway <i>gateway_alias</i>	Deletes a SOCKS gateway.
edit	<i>gateway_alias</i>	Changes the prompt. See “#(config socks-gateways) edit <i>gateway_alias</i> ” on page 231.
exit		Exits configure socks-gateways mode and returns to configure mode.
failure-mode	closed   open	Sets the default failure mode (which can be overridden by policy).

Table 3.105: # (config socks-gateways) (Continued)

no path		Clears network path to download SOCKS gateway settings.
path	url	Specifies the network path to download SOCKS gateway settings.
sequence	add gateway_alias	Adds an alias to the end of the default failover sequence.
	clear	Clears the default failover sequence.
	demote gateway_alias	Demotes an alias one place towards the end of the default failover sequence.
	promote gateway_alias	Promotes an alias one place towards the start of the default failover sequence.
	remove gateway_alias	Removes an alias from the default failover sequence.
view		Displays all SOCKS gateways.

**Example**

```

SGOS#(config) socks-gateways
SGOS#(config socks-gateways) failure-mode open
ok
SGOS#(config socks-gateways) exit
SGOS#(config)

```

**#(config socks-gateways) edit gateway\_alias**

These commands allow you to edit the settings of a specific SOCKS gateway.

**Syntax**

```
socks-gateways
```

This changes the prompt to:

```
SGOS#(config socks-gateways)
```

```
edit gateway_alias
```

This changes the prompt to:

```
SGOS#(config socks-gateways gateway_alias)
```

- subcommands-

**option 1:** exit

**option 2:** host

**option 3:** no

**option 4:** password

**option 5:** port

**option 6:** request-compression

**option 7:** user

**option 8:** version

**option 9:** view

Table 3.106: # (config socks-gateways gateway\_alias)

exit		Exits configure socks-gateways gateway_alias mode and returns to configure socks-gateways mode.
host	gateway_host	Changes the host name.
no	password   user	Optional, and only if you use version 5. Deletes the version 5 password or username.
password	password	Optional, and only if you use version 5. Changes the version 5 password. If you specify a password, you must also specify a username.
port	SOCKS_port	Changes the SOCKS port.
request-compression	enable   disable	Enables or disables SOCKS compression. Disable is the default.
user	user_name	Optional, and only if you use version 5. Changes the version 5 username. If you specify a username, you must also specify a password.
version	4   5	Changes the SOCKS version.
view		Shows the current settings for this SOCKS gateway.

### Example

```
SGOS# (config) socks-gateways
SGOS# (config socks-gateways) edit testgateway
SGOS# (config socks-gateways testgateway) version 5
ok
SGOS# (config socks-gateways testgateway) exit
SGOS# (config socks-gateways) exit
SGOS# (config)
```

## #(config) socks-machine-id

Use this command to set the machine ID for SOCKS.

If you are using a SOCKS server for the primary or alternate gateway, you must specify the ProxySG machine ID for the Identification (Ident) protocol used by the SOCKS gateway.

### Syntax

```
socks-machine-id machine_id
```

Table 3.107: # (config) socks-machine-id

machine_id		Indicates the machine ID for the SOCKS server.
------------	--	--



*Example*

```
SGOS# (config) socks-machine-id 10.25.36.47
ok
```

 **#(config) socks-proxy**

Use this command to configure a SOCKS proxy on a ProxySG. Only one server is permitted per ProxySG. Both SOCKSv4 and SOCKSv5 are supported by Blue Coat Systems, and both are enabled by default.

---

**Note:** The version of SOCKS used is only configurable through policy. For example, to use only SOCKSv5:

---

```
<proxy>
socks.version=4 deny
```

**Syntax**

```
socks-proxy
```

**- subcommands-**

**option 1:** socks-proxy accept-timeout *seconds*

**option 2:** socks-proxy connect-timeout *seconds*

**option 3:** socks-proxy max-connections *num\_connections*

**option 4:** socks-proxy max-idle-timeout *seconds*

**option 5:** socks-proxy min-idle-timeout *seconds*

**Table 3.108:** #(config) socks-proxy

accept-timeout	<i>seconds</i>	Sets maximum time to wait on an inbound BIND.
connect-timeout	<i>seconds</i>	Sets maximum time to wait on an outbound CONNECT.
max-connections	<i>num_connections</i>	Sets maximum allowed SOCKS client connections.
max-idle-timeout	<i>seconds</i>	Specifies the minimum timeout after which SOCKS can consider the connection for termination when the max connections are reached.
min-idle-timeout	<i>seconds</i>	Specifies the max idle timeout value after which SOCKS should terminate the connection.

### Example

```
SGOS#(config) socks-proxy accept-timeout 120
ok
```

## #(config) ssl

Use this command to configure HTTPS termination, including managing certificates, both self-signed and those from a Certificate Signing Authority (CSA).

To configure HTTPS termination, you must complete the following tasks:

- Configure a keyring
- Configure the SSL client
- Configure the HTTPS service

---

*Note:* To perform these steps, you must have a serial or SSH connection; you cannot use Telnet.

---

### Syntax

```
ssl
```

This changes the prompt to:

```
SGOS#(config ssl)
```

#### - subcommands-

##### option 1: create

```
sub-option 1: ccl list_name
sub-option 2: certificate keyring_id
sub-option 3: keyring {show | show-director | no-show} keyring_id [key_length]
sub-option 4: signing-request keyring_id
sub-option 5: ssl-client ssl_client_name (only default is permitted)
```

##### option 2: delete

```
sub-option 1: ca-certificate name
sub-option 2: ccl list_name
sub-option 3: certificate keyring_id
sub-option 4: external-certificate name
sub-option 5: keyring keyring_id
sub-option 6: signing-request keyring_id
sub-option 7: ssl-client ssl_client_name
```

##### option 3: edit

```
sub-option 1: ccl list_name—changes the prompt (see “#(config ssl) edit ccl list_name”
on page 239)
sub-option 2: ssl-client ssl_client_name (only default is permitted)—changes the
prompt (see “#(config ssl) edit ssl-client ssl_client_name” on page 240)
```

**option 4:** exit

**option 5:** inline

sub-option 1: ca-certificate *name eof*

sub-option 2: certificate *keyring\_id eof*

sub-option 3: external-certificate *name eof*

sub-option 4: keyring {show | show-director | no-show} *keyring\_id eof*

sub-option 5: signing-request *keyring\_id eof*

**option 6:** ssl-nego-timeout *seconds*

**option 7:** view

sub-option 1: ca-certificate *name*

sub-option 2: ccl

sub-option 3: certificate *keyring\_id*

sub-option 4: external-certificate *name*

sub-option 5: keypair {des | des3 | unencrypted} *keyring\_id | keyring\_id*

sub-option 6: keyring [*keyring\_id*]

sub-option 7: signing-request *keyring\_id*

sub-option 8: ssl-client

sub-option 9: ssl-nego-timeout

sub-option 10:summary {ca-certificate | external-certificate} [*name*]

Table 3.109: # (config ssl)

create	ccl list_name	Creates a list to contain CA certificates.
	certificate keyring_id	Creates a certificate. Certificates can be associated with a keyring.  You can create a self-signed certificate two ways: interactively or non-interactively.  Director uses non-interactive commands in profiles and overlays to create certificates.  For information on the two forms of create, refer to the <i>Blue Coat Configuration and Management Guide</i> .
	keyring {show   show-director   no-show} keyring_id [key_length]	Creates a keyring, with a keypair, where: <ul style="list-style-type: none"> <li>• show: Keyrings created with this attribute are displayed in the show configuration output, meaning that the keyring can be included as part of a profile or overlay pushed by Director.</li> <li>• show-director: Keyrings created with this attribute are part of the show configuration output if the CLI connection is secure (SSH/RSA) and the command is issued from Director.</li> <li>• no-show: Keyrings created with this attribute are not displayed in the show configuration output and cannot be part of a profile. The no-show option is provided as additional security for environments where the keys will never be used outside of the particular ProxySG.</li> </ul>
	signing-request keyring_id	Creates a certificate signing request. The request must be associated with a keyring.  You can create a signing request two ways: interactively or non-interactively.  Director uses non-interactive commands in profiles and overlays to create signing requests.  For information on the two forms of create, refer to the <i>Blue Coat Configuration and Management Guide</i> .
	ssl-client ssl_client_name	Associates the SSL client with a keyring. Only the default is permitted.

Table 3.109: # (config ssl) (Continued)

delete	ca-certificate <i>name</i>	Deletes a CA-certificate from the ProxySG.
	ccl <i>list_name</i>	Deletes a CCL list from the ProxySG.
	certificate <i>keyring_id</i>	Deletes the certificate associated with a keyring.
	external-certificate <i>name</i>	Deletes an external certificate from the ProxySG.
	keyring <i>keyring_id</i>	Deletes a keyring, with a keypair.
	signing-request <i>keyring_id</i>	Deletes a certificate signing request.
	ssl-client <i>ssl_client_name</i>	Deletes an SSL client.
edit	ccl <i>list_name</i>	Changes the prompt. See “# (config ssl) edit ccl <i>list_name</i> ” on page 239.
	ssl-client <i>ssl_client_name</i>	Changes the prompt. See “# (config ssl) edit ssl-client <i>ssl_client_name</i> ” on page 240.
exit		Exits configure ssl mode and returns to configure mode.
inline	ca-certificate <i>name eof</i>	Imports a CA certificate.
	certificate <i>keyring_id eof</i>	Imports a certificate.

Table 3.109: # (config ssl) (Continued)

	<code>external-certificate name eof</code>	Imports a certificate without the corresponding private key.
	<code>keyring {show   show-director   no-show} keyring_id eof</code>	Imports a keyring, where: <ul style="list-style-type: none"> <li>• <code>show</code>: Keyrings created with this attribute are displayed in the <code>show</code> configuration output, meaning that the keyring can be included as part of a profile or overlay pushed by Director.</li> <li>• <code>show-director</code>: Keyrings created with this attribute are part of the <code>show</code> configuration output if the CLI connection is secure (SSH/RSA) and the command is issued from Director.</li> <li>• <code>no-show</code>: Keyrings created with this attribute are not displayed in the <code>show</code> configuration output and cannot be part of a profile. The <code>no-show</code> option is provided as additional security for environments where the keys will never be used outside of the particular ProxySG.</li> <li>• <code>eof</code>: End-of-file marker. This can be anything, as long as it doesn't also appear in the inline text. (If the <code>eof</code> appears in the inline text, the <code>inline</code> command completes at that point.)</li> </ul>
	<code>signing-request keyring_id eof</code>	Imports a signing request.
<code>ssl-nego-timeout</code>	<code>seconds</code>	Configures the SSL-negotiation timeout period. The default is 300 seconds.

Table 3.109: #(config ssl) (Continued)

view	ca-certificate <i>name</i>	Displays the Certificate Authority certificate.
	ccl	Displays the CA-certificate lists.
	certificate <i>keyring_id</i>	Displays the certificate.
	external-certificate <i>name</i>	Displays the external certificate.
	keypair {des   des3   unencrypted} <i>keyring_id</i>   <i>keyring_id</i>	Displays the keypair. If you want to view the keypair in an encrypted format, you can optionally specify des or des3 before the keyringID. If you specify either des or des3, you are prompted for the challenge entered when the keyring was created.
	keyring [ <i>keyring_id</i> ]	Displays the keyring.
	signing-request <i>keyring_id</i>	Displays the certificate signing request.
	ssl-client	Displays summary information of SSL clients.
	ssl-nego-timeout	Displays SSL negotiation timeout period status summary.
	summary {ca-certificate   external-certificate} [ <i>name</i> ]	Displays a summary for all CA-certificate or external-certificate commands, or for the certificate name specified.

**Examples:**

```

SGOS#(config) ssl
SGOS#(config ssl) create keyring show keyring id [key length]
ok
SGOS#(config ssl) view keyring keyring id
KeyringID: default
Is private key showable? yes
Have CSR? no
Have certificate? yes
Is certificate valid? yes
CA: Blue Coat Systems SG3000
Expiration Date: Jan 23 23:57:21 2013 GMT
Fingerprint: EB:BD:F8:2C:00:25:84:02:CB:82:3A:94:1E:7F:0D:E3
SGOS#(config ssl) exit
SGOS#(config)

```

**#(config ssl) edit ccl *list\_name***

Allows you to edit the CCL parameters.

**Syntax**

```
ssl
```

This changes the prompt to:

```
SGOS#(config ssl)
edit ccl list_name
```

This changes the prompt to:

```
SGOS#(config ssl ccl list_name)
```

**- subcommands-**

**option 1:** add *ca\_certificate\_name*  
**option 2:** clear  
**option 3:** exit  
**option 4:** remove *ca\_certificate\_name*  
**option 5:** view

Table 3.110: #(config ssl ccl list\_name)

add	<i>ca_certificate_name</i>	Adds a CA certificate to this list. (The CA certificate must first be imported in configure ssl mode.)
clear		Clears all CA certificates from the specified list.
exit		Exits configure ssl ccl <i>list_name</i> mode and returns to ssl configure mode.
remove	<i>ca_certificate_name</i>	Deletes a CA certificate from this list.
view		Shows a summary of CA certificates in this list.

**Examples:**

```
SGOS#(config) ssl
SGOS#(config ssl) edit ccl list_name
SGOS#(config ssl ccl list_name) add CACert1
ok
SGOS#(config ssl ccl list_name) exit
SGOS#(config ssl) exit
SGOS#(config)
```

## **#(config ssl) edit ssl-client ssl\_client\_name**

Allows you to edit the SSL client parameters. Only the default is permitted.

### **Syntax**

```
ssl
```

This changes the prompt to:

```
SGOS#(config ssl)
edit ssl-client ssl_default_client_name
```

This changes the prompt to:

```
SGOS#(config ssl ssl_default_client_name)
```



**- subcommands-****option 1:** cipher-suite**option 2:** exit**option 3:** keyring-id *keyring\_id***option 4:** protocol *ssl*v2 | *ssl*v3 | *tl*sv1 | *ssl*v2v3 | *ssl*v2*tl*sv1| *ssl*v3*tl*sv1 | *ssl*v2v3*tl*sv1**option 5:** view**Table 3.111:** #(*config ssl ssl\_default\_client\_name*)

cipher-suite	<i>cipher-suite</i>	<p>Specifies the cipher suite to use. The default is to use all cipher suites. If you want to change the default, you have two choices:</p> <ul style="list-style-type: none"> <li>• interactive mode</li> <li>• non-interactive mode</li> </ul> <p>Director uses non-interactive commands in profiles and overlays to create cipher suites.</p> <p>The optional <i>cipher-suite</i> refers to the cipher-suites you want to use, space separated, such as <i>rc4-md5</i> <i>exp-des-cbc-sha</i> . If you want to use the interactive mode, do not specify a cipher suite.</p> <p>For a list of cipher suites available, refer to “Using Secure Services” in the <i>Blue Coat Configuration and Management Guide</i>.</p>
exit		Exits configure ssl ssl-client <i>ssl_default_client_name</i> mode and returns to ssl configure mode.
keyring-id	<i>keyring_id</i>	Configures SSL client keyring id.
protocol	<i>ssl</i> v2   <i>ssl</i> v3   <i>tl</i> sv1   <i>ssl</i> v2v3   <i>ssl</i> v2 <i>tl</i> sv1  <i>ssl</i> v3 <i>tl</i> sv1   <i>ssl</i> v2v3 <i>tl</i> sv1	Configures SSL client protocol version.
view		Displays the SSL client details.

**Examples:**

```
SGOS#(config) ssl
SGOS#(config ssl) edit ssl-client ssl_default_client_name
SGOS#(config ssl ssl-client ssl_default_client_name) cipher-suite rc4-md5
exp-des-cbc-sha
ok
SGOS#(config ssl ssl-client ssl_default_client_name) exit
SGOS#(config ssl) exit
SGOS#(config)
```

## #(config) static-routes

Use this command to set the network path to download the static routes configuration file.

To use static routes on the ProxySG, you must create a routing table and place it on an HTTP server accessible to the ProxySG. The routing table is a text file that contains a list of IP addresses, subnet masks, and gateways. When you download a routing table, the table is stored in the device until it is replaced by downloading a new table.

The routing table is a simple text file containing a list of IP addresses, subnet masks, and gateways. A sample routing table is illustrated below:

```
10.63.0.0      255.255.0.0      10.63.158.213
10.64.0.0      255.255.0.0      10.63.158.213
10.65.0.0      255.255.0.0      10.63.158.226
```

When a routing table is loaded, all requested addresses are compared to the list, and routed based on the best match.

Once the routing table is created, place it on an HTTP server so it can be downloaded to the device. To download the routing table to the ProxySG, use the `load` command.

### Syntax

**option 1:** `static-routes no path`

**option 2:** `static-routes path url`

Table 3.112: #(config) static-routes

<code>no path</code>		Clears the network path location of the static route table.
<code>path</code>	<code>url</code>	Sets the network path location of the static route table to the specified URL.

**Example**

```
SGOS#(config) static-routes path 10.25.36.47/files/routes.txt
ok
```

## #(config) streaming

Use this command to configure general streaming settings and Microsoft Windows Media or RealNetworks Real Media settings.

### Syntax

**option 1:** streaming max-client-bandwidth *kbps*

**option 2:** streaming max-gateway-bandwidth *kbps*

**option 3:** streaming multicast

sub-option 1: address-range *first\_address - last\_address*

sub-option 2: port-range *first\_port - last\_port*

sub-option 3: ttl *ttl*

**option 4:** streaming no

sub-option 1: max-client-bandwidth

sub-option 2: max-gateway-bandwidth

**option 5:** streaming quicktime

sub-option 1: http-handoff {disable | enable}

sub-option 2: max-client-bandwidth *kbps*

sub-option 3: max-connections *number*

sub-option 4: max-gateway-bandwidth *kbps*

sub-option 5: no {max-client-bandwidth | max-connections | max-gateway-bandwidth}

**option 6:** streaming real-media

sub-option 1: http-handoff {disable | enable}

sub-option 2: log-forwarding {disable | enable}

sub-option 3: max-client-bandwidth *kbps*

sub-option 4: max-connections *number*

sub-option 5: max-gateway-bandwidth *kbps*

sub-option 6: multicast {disable | enable}

sub-option 7: no {max-client-bandwidth | max-connections | max-gateway-bandwidth | refresh-interval}

sub-option 8: refresh-interval *hours*

**option 7:** streaming windows-media

sub-option 1: asx-rewrite *number in\_addr cache\_proto cache\_addr* [cache-port]

sub-option 2: broadcast-alias *alias url loops date time*

sub-option 3: http-handoff {disable | enable}

sub-option 4: live-retransmit {disable | enable}

sub-option 5: log-compatibility {disable | enable}

sub-option 6: log-forwarding {disable | enable}

sub-option 7: max-client-bandwidth *kbps*

sub-option 8: max-connections *number*

```

sub-option 9: max-fast-bandwidth kpbs
sub-option 10: max-gateway-bandwidth kpbs
sub-option 11: multicast-alias alias url [preload]
sub-option 12: multicast-station name {alias | url} ip port ttl
sub-option 13: no {asx-rewrite number | broadcast-alias alias |
    max-client-bandwidth | max-connections | max-gateway-bandwidth |
    multicast-alias alias | multicast-station name | refresh-interval |
    server-auth-type cache_ip_address | unicast-alias alias}
sub-option 14: refresh-interval hours
sub-option 15: server-auth-type {basic | ntlm} cache_ip_address
sub-option 16: server-thinning {disable | enable}
sub-option 17: unicast-alias alias url

```

Table 3.113: #(config) streaming

max-client-bandwidth	<i>kpbs</i>	Sets the maximum client bandwidth permitted to <i>kpbs</i> .
max-gateway-bandwidth	<i>kpbs</i>	Sets the maximum gateway bandwidth permitted to <i>kpbs</i> .
multicast	address-range <i>first_address-last_address</i>	The IP address range for the ProxySG's multicast-station. Default is from 224.2.128.0 and 224.2.255.255.
	port-range <i>first_port-last_port</i>	Port range for the ProxySG's multicast-station. Default is between 32768 and 65535.
	ttl <i>ttl</i>	Time to live value for the multicast-station on the ProxySG, expressed in hops. Default is 5; a valid number is between 1 and 255.
no	max-client-bandwidth	Clears the current maximum client bandwidth setting.
	max-gateway-bandwidth	Clears the current maximum gateway bandwidth setting.
quicktime	http-handoff {disable   enable}	Disables or enables QuickTime HTTP handoff.
	max-client-bandwidth <i>kpbs</i>	Sets the maximum connections allowed.
	max-connections <i>number</i>	Sets the maximum client bandwidth allowed.
	max-gateway-bandwidth <i>kpbs</i>	Sets the maximum gateway bandwidth allowed.
	no {max-client-bandwidth   max-connections   max-gateway-bandwidth}	Negates QuickTime parameters.

Table 3.113: # (config) streaming (Continued)

real-media	http-handoff {disable   enable}	Disables or enables Real Media HTTP handoff.
	log-forwarding {disable   enable}	Sets Real Media client log forwarding.
	max-client-bandwidth <i>kbps</i>	Limits the total bandwidth used by all connected clients. Changing the setting to no max-client-bandwidth uses the maximum available bandwidth. Zero (0) is not an accepted value.
	max-connections <i>number</i>	Limits the concurrent number of client connections. Changing the setting to no max-connections uses the maximum available bandwidth. Zero (0) is not an accepted value.
	max-gateway-bandwidth <i>kbps</i>	Limits the total bandwidth used between the proxy and the gateway. Changing the setting to no max-gateway-bandwidth, uses the maximum available bandwidth. Zero (0) is not an accepted value.
	multicast {disable   enable}	Disables or enables Real Media client multicast support.
	no {max-client-bandwidth   max-connections   max-gateway-bandwidth   refresh-interval}	Negates Real Media parameters.
	refresh-interval <i>hours</i>	Sets the streaming content refresh interval.

Table 3.113: #(config) streaming (Continued)

windows-media	<code>asx-rewrite number in_addr cache_proto cache_addr [cache_port]</code>	<p>Provides proxy support for Windows Player 6.4.</p> <p>If your environment does not use a Layer 4 switch or WCCP, the ProxySG can operate as a proxy for Windows Media Player 6.4 clients by rewriting the .asx file (which links Web pages to Windows Media ASF files) to point to the Windows Media streaming media cache rather than the Windows Media server.</p> <p><i>number</i> can be any positive number. It defines the priority of all the asx-rewrite rules. Smaller numbers indicate higher priority. <i>in_addr</i> specifies the hostname. It can have a maximum of one wildcard character. <i>cache_proto</i> rewrites the protocol on the ProxySG and can take any of the following forms:</p> <ul style="list-style-type: none"><li>mmsu (MMS-UDP)</li><li>mmst (MMS-TCP)</li><li>http (HTTP)</li><li>mms (MMS-UDP or MMS-TCP)</li></ul> <p><i>cache_addr</i> rewrites the address on the ProxySG.</p>
---------------	---	--

Table 3.113: # (config) streaming (Continued)

windows-media, continued	broadcast-alias <i>alias</i> <i>url loops date time</i>	Enables scheduled live unicast or multicast transmission of video-on-demand content.  <i>alias</i> must be unique. <i>url</i> specifies the address of the video-on-demand stream. <i>loops</i> specifies the number of times the stream should be played back. 0 means forever. <i>date</i> specifies the broadcast alias starting date. To specify multiple starting dates, enter the date as a comma-separated string. <i>date</i> can take any of the following formats:  yyyy-mm-dd today  <i>time</i> specifies the broadcast-alias starting time. To specify multiple starting times within the same date, enter the time as a comma-separated string. No spaces are permitted. <i>time</i> can take any of the following formats:  hh:mm  midnight, 12am, 1am, 2am, 3am, 4am, 5am, 6am, 7am, 8am, 9am, 10am, 11am, noon, 12pm, 1pm, 2pm, 3pm, 4pm, 5pm, 6pm, 7pm, 8pm, 9pm, 10pm, 11pm.
	http-handoff {enable   disable}	Allows the Windows Media module to control the HTTP port when Windows Media streaming content is present. The default is enabled.
	live-retransmit {enable   disable}	Allows the ProxySG to retransmit dropped packets sent through MMS-UDP for unicast. The default is enabled.
	log-compatibility {enable   disable}	Disables or enables access log compatibility. When log-compatibility is enabled, ProxySG generates the MMS log the same way as Windows Media Server does. Three fields are affected when log-compatibility is enabled: <ul style="list-style-type: none"> <li>• c-ip            x-wm-c-ip (client address derived from client log)</li> <li>• c-dns           x-wm-c-dns (client hostname derived from client log)</li> <li>• c-uri-stem    cs-uri (use full URI instead of just the path)</li> </ul>
	log-forwarding {enable   disable}	Enables forwarding of the client log to the origin media server.
	max-client-bandwidth <i>kbps</i>	Sets the maximum client bandwidth permitted to <i>kbps</i> .

Table 3.113: #(config) streaming (Continued)

windows-media, continued	max-connections <i>number</i>	Limits the concurrent number of client connections. If this variable is set to 0, you effectively lock out all client connections to the ProxySG. To allow maximum client bandwidth, enter <b>streaming windows-media no max-connections</b> .
	max-fast-bandwidth <i>kpbs</i>	Sets the maximum fast start bandwidth per player.
	max-gateway-bandwidth <i>kpbs</i>	Sets the maximum limit, in kilobits per second (Kbps), for the amount of bandwidth Windows Media uses to send requests to its gateway. If this variable is set to 0, you effectively prevent the ProxySG from initiating any connections to the gateway. To allow maximum gateway bandwidth, enter <b>streaming windows-media no max-gateway-bandwidth</b> .
	multicast-alias <i>alias url</i> [preload]	Creates an alias on the ProxySG that reflects the multicast station on the origin content server.
	multicast-station <i>name</i> [ <i>alias</i>   <i>url</i> ] <i>ip port ttl</i>	Enables multicast transmission of Windows Media content from the ProxySG. <i>name</i> specifies the name of the alias. It must be unique. <i>alias</i> can be a unicast alias, a multicast-alias or a broadcast alias, as well as a <i>url</i> to a live stream source. <i>ip</i> is an optional parameter and specifies the multicast station's IP address. <i>port</i> specifies the multicast station's port value address. <i>ttl</i> specifies the multicast-station's time-to-live value, expressed in hops (and must be a valid number between 1 and 255). The default <i>ttl</i> is 5.
	no (see "windows-media no")	
	refresh-interval <i>hours</i>	Checks the refresh interval for cached streaming content. <i>hours</i> must be a floating point number to specify refresh interval. 0 means always check for freshness.
	server-auth-type {basic   ntlm} cache_ip_address	Sets the authentication type of the ProxySG indicated by <i>cache_ip_address</i> to BASIC or NTLM.
	server-thinning {disable   enable}	Disables or enables server thinning.



Table 3.113: #(config) streaming (Continued)

windows-media, continued	unicast-alias <i>alias url</i>	Creates an alias on the ProxySG that reflects the content specified by the URL. When a client requests the alias content, the ProxySG uses the URL specified in the unicast-alias command to request the content from the origin streaming server.
windows-media no	asx-rewrite <i>number</i>	Deletes the ASX rewrite rule associated with <i>number</i> .
	broadcast-alias <i>alias</i>	Deletes the broadcast alias rule associated with <i>alias</i> .
	max-client-bandwidth	Negates maximum client bandwidth settings.
	max-connections	Negates maximum connections settings.
	max-gateway-bandwidth	Negates maximum gateway bandwidth settings.
	multicast-alias <i>alias</i>	Deletes the multicast alias rule associated with <i>alias</i> .
	multicast-station <i>name</i>	Deletes the multicast station rule associated with <i>name</i> .
	refresh-interval	Sets the current Windows Media refresh interval to “never refresh.”
	server-auth-type <i>cache_ip_address</i>	Clears the authentication type associated with <i>cache_ip_address</i> .
	unicast-alias <i>alias</i>	Deletes the unicast alias rule associated with <i>alias</i> . The name of the alias, such as “welcome1” that is created on the ProxySG and reflects the content specified by the URL. The protocol is specified by the URL if the protocol is mmst, mmsu, or http. If the protocol is mms, the same protocol as the client is used.

### Example

```
SGOS#(config) streaming windows-media http-handoff enable
ok

SGOS#(config) streaming windows-media live-retransmit disable
ok

SGOS#(config) streaming windows-media log-forwarding disable
ok

SGOS#(config) streaming windows-media max-connections 1600
ok

SGOS#(config) streaming windows-media no max-connections
ok
```

## #(config) tcp-ip

Use the following commands to configure your TCP-IP settings.

### Syntax

**option 1:** tcp-ip icmp-bcast-echo {disable | enable}  
**option 2:** tcp-ip icmp-tstamp-echo {disable | enable}  
**option 3:** tcp-ip ip-forwarding {disable | enable}  
**option 4:** tcp-ip pmtu-discovery {disable | enable | expire-period *seconds* | probe-interval *seconds*}  
**option 5:** tcp-ip rfc-1323 {disable | enable}  
**option 6:** tcp-ip tcp-newreno {disable | enable}  
**option 7:** tcp-ip tcp-2msl *seconds*  
**option 8:** tcp-ip window-size *window\_size*

Table 3.114: #(config) tcp-ip

icmp-bcast-echo	disable   enable	Enables or disables ICMP broadcast echo responses.
icmp-tstamp-echo	disable   enable	Enables or disables ICMP timestamp echo responses.
ip-forwarding	disable   enable	Enables or disables IP-forwarding.
pmtu-discovery	disable   enable   expire-period <i>seconds</i>   probe-interval <i>seconds</i>	Enables or disables Path MTU Discovery, and configures the PMTU expiration period and probe interval.
rfc-1323	disable   enable	Enables or disables RFC-1323 support (satellite communications).
tcp-newreno	disable   enable	Enables or disables TCP NewReno support (improved fast recovery).
tcp-2msl	<i>seconds</i>	Specifies the time_wait value for a TCP connection before completely closing.
window-size	<i>window_size</i>	Specifies the TCP window size for satellite communications.

**Example**

```
SGOS#(config) tcp-ip ip-forwarding enable
ok
SGOS#(config) tcp-ip rfc-1323 enable
ok
```

 **#(config) tcp-rtt**

Use this command to configure the number of TCP round trip time ticks.

**Syntax**

```
tcp-rtt num_500ms_ticks
```

**Table 3.115:** #(config) tcp-rtt

<i>num_500ms_ticks</i>		Indicates the default TCP Round Trip Time in ticks.
------------------------	--	---

**Example**

```
SGOS#(config) tcp-rtt 500
ok
```

 **#(config) tcp-rtt-use**

Use this command to enable or disable the default TCP Round Trip Time.

**Syntax**

```
tcp-rtt-use {disable | enable}
```

**Table 3.116:** #(config) tcp-rtt-use

disable		Disables using fixed RTT.
enable		Enables using fixed RTT.

**Example**

```
SGOS#(config) tcp-rtt-use enable
ok
```

 **#(config) timezone**

Use this command to set the local time zone on the ProxySG.

**Syntax**

```
timezone timezone_number
```

Table 3.117: # (config) timezone

<i>timezone_number</i>		Enables you to set the local time zone. (Use (config) show timezones to display a list of supported timezones.)
------------------------	--	---

**Example**

```
SGOS# (config) timezone 3
ok
```

## #(config) upgrade-path

Use this command to specify the network path to download system software.

**Syntax**

```
upgrade-path url
```

Table 3.118: # (config) upgrade-path

<i>url</i>		Indicates the network path to use to download ProxySG system software.
------------	--	--

**Example**

```
SGOS# (config) upgrade-path 10.25.36.47
ok
```

## #(config) virtual-ip

This command allows you to configure virtual IP addresses.

**Syntax**

**option 1:** virtual-ip address *ip\_address*

**option 2:** virtual-ip clear

**option 3:** virtual-ip no address *ip\_address*

Table 3.119: # (config) virtual-ip

address	<i>ip_address</i>	Specifies the virtual IP to add.
clear		Removes all virtual IP addresses.
no address	<i>ip_address</i>	Removes the specified virtual IP from the list.

*Example*

```
SGOS#(config) virtual-ip address 10.25.36.47
ok
```

**#(config) wccp**

The ProxySG can be configured to participate in a WCCP (Web Cache Control Protocol) scheme, where a WCCP-capable router collaborates with a set of WCCP-configured ProxySG Appliances to service requests. WCCP is a Cisco-developed protocol. For more information about WCCP, refer to the *Blue Coat Configuration and Management Guide*.

Once you have created the WCCP configuration file, place the file on an HTTP server so it can be downloaded to the ProxySG. To download the WCCP configuration to the ProxySG, use the `load` command.

**Syntax**

```
option 1: wccp disable
option 2: wccp enable
option 3: wccp no path
option 4: wccp path url
```

Table 3.120: #(config) wccp

disable		Disables WCCP.
enable		Enables WCCP.
no path		Negates certain WCCP settings.
path	url	Specifies the network path from which to download WCCP settings.

*Example*

```
SGOS#(config) wccp path 10.25.36.47/files/wccp.txt
ok
```

