

# Blue Coat Systems™ ProxySG™

## *Command Line Interface Reference*



Blue Coat Systems, Inc.	(408) 220-2200 Voice
650 Almanor Avenue	(408) 220-2250 FAX
Sunnyvale, California 94086	(866) 302-2628
Technical Support	(866) 362-2628

Copyright (c) 2002-2004 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. Without Blue Coat Systems, Inc. consent, the Software may not be modified, reproduced (except to the extent specifically allowed by local law), removed from the product on which it was installed, reverse engineered, decompiled, disassembled, or derived source code. In addition to the above restrictions, the Software may not be (i) published, distributed, rented, leased, sold, sublicensed, assigned or otherwise transferred or any part thereof, (ii) used for competitive analysis or derivative works thereof or translated, (iii) permitted application development use of the Software, (iv) used to publish or distribute the results of any benchmark tests run on the Software without the express written permission of Blue Coat Systems, Inc., or (v) removed or obscured of any Blue Coat Systems, Inc. or licensor copyrights, trademarks or other proprietary notices or legends from any portion of the Software or any associated documentation. 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. Blue Coat Systems, Inc. specifications and documentation are subject to change with notice. Information contained in this document is believed to be accurate and reliable, however, Blue Coat Systems, Inc. assumes no responsibility for its use. Blue Coat™, ProxySG™, CacheOS™, are trademarks of Blue Coat Systems, Inc. and CacheFlow®, and Accelerating The Internet® 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. The Software and all related technical information, documents and materials are subject to export controls under the U.S. Export Administration Regulations and the export regulations of other countries.

Printed in U.S.A.

Document Number: 231-02680

Document Revision: 3.1.4—06/30/04

### THIRD PARTY COPYRIGHT NOTICES

Blue Coat Systems, Inc. Security Gateway Operating System (SGOS) version 3 utilizes third party software from various sources. Portions of this software are copyrighted by their respective owners as indicated in the copyright notices below.

The following lists the copyright notices for:

BPF

Copyright (c) 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that: (1) source code distributions retain the above copyright notice and this paragraph in its entirety, (2) distributions including binary code include the above copyright notice and this paragraph in its entirety in the documentation or other materials provided with the distribution, and (3) all advertising materials mentioning features or use of this software display the following acknowledgement:

This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.

Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

DES

Software DES functions written 12 Dec 1986 by Phil Karn, KA9Q; large sections adapted from the 1977 public-domain program by Jim Gilgoly.

EXPAT

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Finjan Software

Copyright (c) 2003 Finjan Software, Inc. All rights reserved.

Flowerfire

Copyright (c) 1996-2002 Greg Ferrar

ISODE

ISODE 8.0 NOTICE

Acquisition, use, and distribution of this module and related materials are subject to the restrictions of a license agreement. Consult the Preface in the User's Manual for the full terms of this agreement.

4BSD/ISODE SMP NOTICE

Acquisition, use, and distribution of this module and related materials are subject to the restrictions given in the file SMP-READ-ME.

UNIX is a registered trademark in the US and other countries, licensed exclusively through X/Open Company Ltd.

MD5

RSA Data Security, Inc. MD5 Message-Digest Algorithm

Copyright (c) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

THE BEER-WARE LICENSE" (Revision 42):

<phk@FreeBSD.org <mailto:phk@FreeBSD.org>> wrote this file. As long as you retain this notice you can do whatever you want with this stuff. If we meet some day, and you think this stuff is worth it, you can buy me a beer in return. Poul-Henning Kamp

Microsoft Windows Media Streaming

Copyright (c) 2003 Microsoft Corporation. All rights reserved.

OpenLDAP

Copyright (c) 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

<http://www.openldap.org/software/release/license.html>

The OpenLDAP Public License Version 2.7, 7 September 2001

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

OpenSSH

Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland. All rights reserved

This file is part of the OpenSSH software.

The licences which components of this software fall under are as follows. First, we will summarize and say that all components are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

1) As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell".

[Tatu continues]

However, I am not implying to give any licenses to any patents or copyrights held by third parties, and the software includes parts that are not under my direct control. As far as I know, all included source code is used in accordance with the relevant license agreements and can be used freely for any purpose (the GNU license being the most restrictive); see below for details.

[However, none of that term is relevant at this point in time. All of these restrictively licenced software components which he talks about have been removed from OpenSSH, i.e.,

- RSA is no longer included, found in the OpenSSL library
- IDEA is no longer included, its use is deprecated
- DES is now external, in the OpenSSL library
- GMP is no longer used, and instead we call BN code from OpenSSL
- Zlib is now external, in a library
- The make-ssh-known-hosts script is no longer included
- TSS has been removed
- MD5 is now external, in the OpenSSL library
- RC4 support has been replaced with ARC4 support from OpenSSL
- Blowfish is now external, in the OpenSSL library

[The licence continues]

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "<http://www.cs.hut.fi/crypto>".

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A

FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2) The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

Cryptographic attack detector for ssh - source code

Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained. THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

Ariel Futoransky <futo@core-sdi.com> <<http://www.core-sdi.com>>

3) ssh-keygen was contributed by David Mazieres under a BSD-style license.

Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>. Modification and redistribution in source and binary forms is permitted provided that due credit is given to the author and the OpenBSD project by leaving this copyright notice intact.

4) The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

@version 3.0 (December 2000)

Optimised ANSI C code for the Rijndael cipher (now AES)

@author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>

@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>

@author Paulo Barreto <paulo.barreto@terra.com.br>

This code is hereby placed in the public domain.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

5) One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

Copyright (c) 1983, 1990, 1992, 1993, 1995

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

6) Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

Markus Friedl  
 Theo de Raadt  
 Niels Provos  
 Dug Song  
 Aaron Campbell  
 Damien Miller  
 Kevin Steves  
 Daniel Kouril  
 Wesley Griffin  
 Per Allansson  
 Nils Nordman  
 Simon Wilkinson

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenSSL

Copyright (c) 1995-1998 Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). All rights reserved.

<http://www.openssl.org/about/>

<http://www.openssl.org/about/>

OpenSSL is based on the excellent SSLeay library developed by [Eric A. Young <mailto:ey@cryptsoft.com>](mailto:Eric.A.Young@cryptsoft.com) and [Tim J. Hudson <mailto:tjh@cryptsoft.com>](mailto:Tim.J.Hudson@cryptsoft.com).

The OpenSSL toolkit is licensed under a Apache-style license which basically means that you are free to get and use it for commercial and non-commercial purposes.

This package is an SSL implementation written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com))" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com))"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

Copyright (c) 1998-2002 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:  
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

PCRE

Copyright (c) 1997-2001 University of Cambridge

University of Cambridge Computing Service, Cambridge, England. Phone: +44 1223 334714.

Written by: Philip Hazel <ph10@cam.ac.uk>

Permission is granted to anyone to use this software for any purpose on any computer system, and to redistribute it freely, subject to the following restrictions:

1. This software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
2. Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England.

ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/

PHAOS SSLava and SSLavaThin

Copyright (c) 1996-2003 Phaos Technology Corporation. All Rights Reserved.

The software contains commercially valuable proprietary products of Phaos which have been secretly developed by Phaos, the design and development of which have involved expenditure of substantial amounts of money and the use of skilled development experts over substantial periods of time. The software and any portions or copies thereof shall at all times remain the property of Phaos.

PHAOS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE SOFTWARE, OR ITS USE AND OPERATION ALONE OR IN COMBINATION WITH ANY OTHER SOFTWARE.

PHAOS SHALL NOT BE LIABLE TO THE OTHER OR ANY OTHER PERSON CLAIMING DAMAGES AS A RESULT OF THE USE OF ANY PRODUCT OR SOFTWARE FOR ANY DAMAGES WHATSOEVER. IN NO EVENT WILL PHAOS BE LIABLE FOR SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

RealSystem

The RealNetworks® RealProxy™ Server is included under license from RealNetworks, Inc. Copyright 1996-1999, RealNetworks, Inc. All rights reserved.

SNMP

Copyright (C) 1992-2001 by SNMP Research, Incorporated.

This software is furnished under a license and may be used and copied only in accordance with the terms of such license and with the inclusion of the above copyright notice. This software or any other copies thereof may not be provided or otherwise made available to any other person. No title to and ownership of the software is hereby transferred. The information in this software is subject to change without notice and should not be construed as a commitment by SNMP Research, Incorporated.

Restricted Rights Legend:

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013; subparagraphs (c)(4) and (d) of the Commercial Computer Software-Restricted Rights Clause, FAR 52.227-19; and in similar clauses in the NASA FAR Supplement and other corresponding governmental regulations.

PROPRIETARY NOTICE

This software is an unpublished work subject to a confidentiality agreement and is protected by copyright and trade secret law. Unauthorized copying, redistribution or other use of this work is prohibited. The above notice of copyright on this source code product does not indicate any actual or intended publication of such source code.

STLport

Copyright (c) 1999, 2000 Boris Fomitchev

This material is provided "as is", with absolutely no warranty expressed or implied. Any use is at your own risk.

Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies. Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

The code has been modified.

Copyright (c) 1994 Hewlett-Packard Company

Copyright (c) 1996-1999 Silicon Graphics Computer Systems, Inc.

Copyright (c) 1997 Moscow Center for SPARC Technology

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Hewlett-Packard Company makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Silicon Graphics makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting

documentation. Moscow Center for SPARC Technology makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

SmartFilter

Copyright (c) 2003 Secure Computing Corporation. All rights reserved.

SurfControl

Copyright (c) 2003 SurfControl, Inc. All rights reserved.

Symantec AntiVirus Scan Engine

Copyright (c) 2003 Symantec Corporation. All rights reserved.

TCPIP

Some of the files in this project were derived from the 4.X BSD (Berkeley Software Distribution) source.

Their copyright header follows:

Copyright (c) 1982, 1986, 1988, 1990, 1993, 1994, 1995

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Trend Micro

Copyright (c) 1989-2003 Trend Micro, Inc. All rights reserved.

zlib

Copyright (c) 2003 by the [Open Source Initiative](#)

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

# Contents

## Chapter 1: Introduction

Audience for this Document.....	13
Organization of this Document.....	13
Related Blue Coat Documentation.....	13
Document Conventions.....	14
SSH and Script Considerations .....	14
Standard and Privileged Modes.....	14
Accessing Quick Command Line Help.....	15

## Chapter 2: Standard and Privileged Mode Commands

Standard Mode Commands.....	17
>display .....	17
>enable .....	18
>exit.....	18
>ping.....	18
>show .....	19
>traceroute .....	27
Privileged Mode Commands.....	28
#acquire-utc.....	28
#bridge.....	28
#cancel-upload.....	29
#clear-arp.....	29
#clear-cache.....	30
#clear-statistics.....	30
#configure.....	30
#disable .....	30
#disk .....	31
#display .....	31
#exit .....	32
#hide-advanced .....	32
#inline .....	33
#kill.....	36
#licensing.....	36
#load.....	36
#pcap.....	38
#ping .....	42
#policy.....	43
#purge-dns-cache .....	43
#restart .....	43
#restore-cacheos4-config.....	44
#restore-sgos2-config.....	44
#restore-defaults.....	45
#reveal-advanced .....	46
#show .....	46
#temporary-route .....	57
#test http.....	57
#traceroute .....	58

**Chapter 3: Privileged Mode Configure Commands**

#configure.....	61
#(config) accelerated-pac .....	63
#(config) access-log.....	63
#(config) archive-configuration .....	72
#(config) attack-detection .....	73
#(config) bandwidth-gain.....	74
#(config) banner .....	75
#(config) bridge.....	75
#(config) bypass-list.....	78
#(config) caching.....	79
#(config) clock .....	82
#(config) content .....	83
#(config) content-filter .....	84
#(config) diagnostics .....	90
#(config) dns.....	93
#(config) dynamic-bypass .....	95
#(config) event-log.....	96
#(config) exceptions.....	97
#(config) exit.....	100
#(config) external-services.....	100
#(config) failover.....	106
#(config) forwarding .....	109
#(config) health-check .....	115
#(config) hide-advanced .....	119
#(config) hostname .....	120
#(config) http .....	120
#(config) icp .....	124
#(config) identd.....	124
#(config) im.....	125
#(config) inline .....	125
#(config) installed-systems.....	128
#(config) interface .....	129
#(config) ip-default-gateway.....	131
#(config) license-key.....	131
#(config) line-vty.....	131
#(config) load.....	132
#(config) netbios.....	134
#(config) no .....	134
#(config) ntp .....	135
#(config) policy.....	136
#(config) profile.....	138
#(config) restart.....	138
#(config) return-to-sender .....	139
#(config) reveal-advanced .....	140
#(config) rip .....	140
#(config) security .....	141
#(config) serial-number.....	160
#(config) services .....	160
#(config) show .....	181
#(config) snmp .....	189
#(config) socks-gateways.....	191
#(config) socks-machine-id.....	194
#(config) socks-proxy .....	195

#(config) splash-generator.....	195
#(config) ssl.....	198
#(config) static-routes.....	202
#(config) streaming.....	203
#(config) tcp-ip.....	209
#(config) tcp-rtt.....	210
#(config) telnet-management.....	211
#(config) timezone.....	211
#(config) upgrade-path.....	211
#(config) virtual-ip.....	212
#(config) wccp.....	212



## 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

*Blue Coat 600 and 700 Installation Guide*

*Blue Coat 6000 and 7000 Installation Guide*

*Blue Coat 400 Installation Guide*

*Blue Coat 800 Installation Guide*

*Blue Coat Configuration and Management Guide*

*Blue Coat Content Policy Language Reference Manual*

## 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.
<code>Courier Italics</code>	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 may 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. Refer to the introduction in Chapter 2: *Standard and Privileged Mode Commands* 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
info            Display current capture information
coreimage       Include packets within a core image
start           Start the capture
stop            Stop the capture
transfer        Transfer captured data to ftp site
```

To get command completion for configuring SNMP:

```
SGOS# (config) snmp ?
<cr>
```

### *To View 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                policy              purge-dns-cache
```

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

This chapter describes and provides examples for the Blue Coat Systems 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, refer to *Accessing Quick Command Line Help*.

---

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 ProxySG 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
```

## >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 bypass-list
option 7: show caching
option 8: show clock
option 9: show commands
    sub-option 1: [delimited [all | privileged]]
    sub-option 2: [formatted [all | privileged]]
option 10: show content-distribution
option 11: show cpu
option 12: show diagnostics
    sub-option 1: service-info
```

sub-option 2: status

**option 13:** show disk  
sub-option 1: *disk\_number*  
sub-option 2: all

**option 14:** show dns

**option 15:** show download-paths

**option 16:** show dynamic-bypass

**option 17:** show efficiency

**option 18:** show environmental

**option 19:** show event-log

**option 20:** show exceptions  
sub-option 1: [*built-in\_id*]  
sub-option 2: [*user-defined\_id*]

**option 21:** show external-services [statistics]

**option 22:** show failover  
sub-option 1: configuration [*group\_address*]  
sub-option 2: statistics

**option 23:** show forwarding

**option 24:** show health-checks

**option 25:** show hostname

**option 26:** show http

**option 27:** show http-stats

**option 28:** show icp-settings

**option 29:** show identd

**option 30:** show im  
sub-option 1: aol-statistics  
sub-option 2: configuration  
sub-option 3: msn-statistics  
sub-option 4: yahoo-statistics

**option 31:** show installed-systems

**option 32:** show interface  
sub-option 1: all  
sub-option 2: *interface\_number*

**option 33:** show ip-default-gateway

**option 34:** show ip-route-table

**option 35:** show ip-rts-table

**option 36:** 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 37: show licenses
option 38: show netbios
option 39: show ntp
option 40: show policy
sub-option 1: [listing]
sub-option 2: [order]
sub-option 3: [proxy-default]
option 41: show ports
option 42: show profile
option 43: show resources
option 44: show restart
option 45: show return-to-sender
option 46: show rip
sub-option 1: parameters
sub-option 2: routes
sub-option 3: statistics
option 47: 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 48: show sessions
```

**option 49:** show snmp

**option 50:** show socks-gateways

**option 51:** show socks-machine-id

**option 52:** show socks-proxy

**option 53:** 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 54:** show ssl

- sub-option 1: ccl [*list\_name*]
- sub-option 2: ssl-client [*ssl\_client*]

**option 55:** show static-routes

**option 56:** show status

**option 57:** 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 58:** show tcp-rtt

**option 59:** show telnet-management

**option 60:** show terminal

**option 61:** show timezones

**option 62:** show user-authentication

**option 63:** show version

**option 64:** show virtual-ip

**option 65:** show wccp

- sub-option 1: configuration
- sub-option 2: statistics

Table 2.2: &gt; 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.
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 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 2.2: &gt; 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.
event-log		Displays event log settings, including event level and event log size, and event recipients.
exceptions	[ <i>built-in_id</i> ]   [ <i>user-defined_id</i> ]	Displays exception definitions.
external-services	[ <i>statistics</i> ]	Displays external services or external services statistics information.
failover	configuration [ <i>group_address</i> ]   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.
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.

Table 2.2: &gt; show (Continued)

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.
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.
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.
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 Telnet connections.
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.

Table 2.2: &gt; show (Continued)

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.
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: > 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. Refer to 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 will be 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, refer to *Accessing Quick Command Line Help*.

---

## #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 ProxySG 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

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

all		Cancels upload for all logs.
log	<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 will be retrieved from the source.

### Syntax

```
clear-cache
```

### Example

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

## #clear-statistics

This command clears the Windows Media, Real Media, and QuickTime streaming statistics collected by the ProxySG. You can also clear the streaming statistics through the Streaming applet. To view streaming statistics from the Management Console, go to **Statistics>Streaming History>Windows Media/Real Media/Quicktime**.

### Syntax

```
clear-statistics
```

Table 2.6: # clear-statistics

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. Refer to 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

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

*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
```

## #hide-advanced

The `hide-advanced` command enables you to disable all or a subset of the advanced commands available to you when using the CLI. The advanced commands that you can disable include: HTTP, and TCP/IP commands.

## Syntax

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

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

**option 3:** `hide-advanced tcp-ip`

Table 2.8: # hide-advanced

all	Hides all advanced commands.
-----	------------------------------

Table 2.8: # hide-advanced (Continued)

expand	Disables expanded commands.
tcp-ip	Disables commands for TCP-IP.

**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 two ways to create a configuration file for your ProxySG. You can use the `inline` command or you can create a text file to house the configuration commands and settings.

To configure using the CLI and the `inline` command, refer to the example below:

```
SGOS# configure terminal
SGOS# (config) inline accelerated-pac eof_marker
.
.
.
end
eof_marker
```

Where `eof_marker` marks the end of the inline commands.

**Syntax**

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

**option 2:** `inline bypass-list`

sub-option 1: `central eof_marker`

sub-option 2: `local eof_marker`

**option 3:** `inline forwarding eof_marker`

**option 4:** `inline icp-settings eof_marker`

**option 5:** `inline license-key eof_marker`

**option 6:** `inline policy`

sub-option 1: `central eof_marker`

sub-option 2: `local eof_marker`

sub-option 3: `forward eof_marker`

sub-option 4: `vpm-cpl eof_marker`

sub-option 5: `vpm-xml eof_marker`

- option 7:** inline rip-settings *token*
- option 8:** inline socks-gateways *eof\_marker*
- option 9:** inline static-route-table *eof\_marker*
- option 10:** 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 <i>eof_marker</i>	Updates the current central policy file 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 current local policy file with the settings you include between the beginning <i>eof_marker</i> and the ending <i>eof_marker</i> .
	forward <i>eof_marker</i>	Updates the current forward policy file with the settings you include between the beginning <i>eof_marker</i> and the ending <i>eof_marker</i> .
	vpm-cpl <i>eof_marker</i>	Updates the VPM policy with the settings you include between the beginning <i>eof_marker</i> and the ending <i>eof_marker</i> . (This option is designed to be used with the Blue Coat Director product.)
	xml-cpl <i>eof_marker</i>	Updates the XML policy with the settings you include between the beginning <i>eof_marker</i> and the ending <i>eof_marker</i> . (This option is designed to be used with the Blue Coat Director product.)
rip-settings	<i>eof_marker</i>	Updates the current RIP settings with the settings you include between the beginning <i>eof_marker</i> and the ending <i>eof_marker</i> .
socks-gateway	<i>eof_marker</i>	Updates the current SOCKS gateway settings with the settings you include between the beginning <i>eof_marker</i> and the ending <i>eof_marker</i> .
static-route-table	<i>eof_marker</i>	Updates the current static route table settings with the settings you include between the beginning <i>eof_marker</i> and the ending <i>eof_marker</i> .
wccp-settings	<i>eof_marker</i>	Updates the current WCCP settings with the settings you include between the beginning <i>eof_marker</i> and the ending <i>eof_marker</i> .

**Example**

```

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

```

## #kill

Terminates a Telnet session.

### Syntax

```
kill session_number
```

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

### Example

```
SGOS# kill 3
ok
```

## #licensing

Use these commands to request or update licenses.

### Syntax

**option 1:** licensing request-key [*user\_id*] [*password*]

**option 2:** licensing update-key

Table 2.10: # licensing

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.

### Syntax

**option 1:** load accelerated-pac

**option 2:** load bypass-list

sub-option 1: central

sub-option 2: local

**option 3:** load forwarding  
**option 4:** load icp-settings  
**option 5:** load license-key  
**option 6:** load policy  
     sub-option 1: central  
     sub-option 2: local  
     sub-option 3: forward  
     sub-option 4: vpm-cpl  
     sub-option 5: vpm-software  
     sub-option 6: vpm-xml  
**option 7:** load rip-settings  
**option 8:** load socks-gateways  
**option 9:** load static-route-table  
**option 10:** load upgrade  
**option 11:** load wccp-settings

Table 2.11: # load

accelerated-pac		Downloads the current accelerated pac file settings.
bypass-list	central	Downloads the current central bypass list settings.
	local	Downloads the current local bypass list settings.
forwarding		Downloads the current forwarding settings.
icp-settings		Downloads the current ICP settings.
policy	central	Downloads the current central policy file settings.
	local	Downloads the current local policy file settings.
	forward	Downloads the current forward 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		Downloads the latest system image.
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 command 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:* Before using the `pcap` command, consider that packet capturing doubles the amount of processor usage performed in TCP/IP.

---

---

*Note:* 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).

---

### 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} iface-num]`

sub-option 3: `[iface iface-num]`

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	[iface {in   out}]	Captures either in or out from a interface.
	[iface {in   out} <i>iface-num</i> ]	Captures either in or out from a particular interface.
	[iface <i>iface-num</i> ]	Captures both in and out from a particular interface.
	[bridge {in   out} <i>name</i> port <i>number</i> ]	Captures either in or out on a particular bridge port.
	[bridge <i>name</i> port <i>number</i> ]	Captures both in and out on a particular bridge port.
	[expr <i>filter_expression</i> ]	Defines the filter expression. See Table 2.13 and Table 2.14 for details.
info		Displays the current packet capture information.
coreimage	keep <i>n(k)</i>	Includes packets within a core image.

Table 2.12: # pcap (Continued)

start	[first <i>n</i> ]	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 <i>n</i> ( <i>k</i> ) ]	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 <i>n</i> ]	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 <i>n</i> ]	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.
stop		Stops the capture.
transfer	<i>full_url/filename</i> <i>username password</i>	Transfers captured data to an FTP site. Refer to the examples for details.

Table 2.13: Filter Expressions

expr	{"host name"   "net number"   "port number" }	Type qualifier. host is the default.
------	---	--------------------------------------

Table 2.13: (Continued)Filter Expressions

expr	{"src name"   "dst number"   "src name or dst name"   "src name and dst name"}	Direction qualifier; specifies the transfer direction. <code>src</code> or <code>dst</code> is the default.
expr	{ether   ip   arp   rarp   tcp   udp} expr	Proto qualifier; restrict matches to a specific protocol. For example: "tcp src name".

Table 2.14 provides more parameters that can be used to create complex filter expressions.

**Important:** Define filter `expr` parameters with double-quotes to avoid confusion with special characters.

Table 2.14: Filter Expression Parameters.

{dst host   src host   host} ip_address [ip_address ...]	If multiple IP addresses are specified, each address is checked for a match.
{ether dst   ether dst   ether host} ehost [ehost ...]	<i>ehost</i> is a valid Ethernet address. If multiple <i>ehost</i> addresses are specified, each address is checked for a match.
{dst net   src net   net} net	True if either the IP address of the packet has a network number of <i>net</i> .
{dst port   src port   port} port	True if packet has source or destination value of <i>port</i> . Maybe prepended with <code>tcp</code> or <code>udp</code> .
net net mask mask	True if the IP address matches the <i>net</i> value with the specified <i>netmask</i> value. May be qualified with <code>src</code> or <code>dst</code> .
less length	True if the packet length is less than or equal to <i>length</i> .
greater length	True if the packet length is greater than or equal to <i>length</i> .
ip proto protocol	<i>protocol</i> can be a number or name ( <code>icmp</code> , <code>udp</code> , <code>tcp</code> ), but since these identifiers are also keywords within the filter expression parser, they must be escaped with a backslash.
{ether   ip} broadcast	True if the packet is an Ethernet broadcast or IP broadcast packet.
{ether   ip} multicast	True if the packet is an Ethernet multicast or IP multicast packet.
ether proto protocol	<i>protocol</i> can be a number or name ( <code>ip</code> , <code>arp</code> , <code>rarp</code> ), but since these identifiers are also keywords within the filter expression parser, they must be escaped with a backslash.
! or not	Negation.
&& or and	Concatenation
or or	Alternation.

*Note:* Once a filter is set, it remains in effect until it is redefined. Also, if the ProxySG is rebooted, filtering is set to off; 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 between 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  
ok
```

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 host name 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 2.15: # restart

abrupt	Reboots the system abruptly, according to the version of the ProxySG that is currently installed.
regular	Reboots the version of the ProxySG that is currently installed.
upgrade	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-cacheos4-config

Restores the ProxySG to the initial configuration derived upon an upgrade from Cache OS 4.x to SGOS 2.x. The ProxySG retains the network settings.

### Syntax

```
restore-cacheos4-config
```

### Example

```
SGOS# restore-cacheos4-config
% "restore-cacheos4-configuration" requires a restart to take effect.
% Use "restart regular" to restart the system.
```

Or if there is no 4.x configuration found:

```
SGOS# restore-cacheos4-config
% No CacheOS 4.x configuration is available on this system.
```

### See also

restore-defaults

## #restore-sgos2-config

Restores the ProxySG to settings last used with SGOS 2.x. The ProxySG retains the network settings.

### Syntax

```
restore-sgos2-config
```

**Example**

```
SGOS# restore-sgos2-config
% "restore-sgos2-configuration" requires a restart to take effect.
% Use "restart regular" to restart the system.
```

Or if there is no 2.x configuration found:

```
SGOS# restore-sgos2-config
%% No SGOS 2.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 2.16: # 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 will be 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.

### Syntax

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

Table 2.17: # reveal-advanced

all	Enables all advanced commands.
expand	Displays expanded commands.
tcp-ip	Enables only the TCP/IP advanced commands; the status of the other advanced commands remains unchanged.

### Example

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

## #show

Use this command 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 bandwidth-gain
option 6: show bridge
    sub-option 1: configuration [bridge_name]
    sub-option 2: fwtable bridge_name
    sub-option 3: statistics bridge_name
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 configuration
sub-option 1: [brief]
sub-option 2: [expanded]
sub-option 3: [noprompts]
option 12: show content
sub-option 1: outstanding-requests
sub-option 2: priority [regex regex | url url]
sub-option 3: url url
option 13: show content-distribution
option 14: show content-filter
sub-option 1: smartfilter
sub-option 2: surfcontrol
sub-option 3: status
sub-option 4: websense
option 15: show cpu
option 16: show diagnostics
sub-option 1: service-info
sub-option 2: status
option 17: show disk
sub-option 1: disk_number
sub-option 2: all
option 18: show dns
option 19: show download-paths
option 20: show dynamic-bypass
option 21: show efficiency
option 22: show environmental
option 23: show event-log
option 24: show exceptions
sub-option 1: [built-in_id]
sub-option 2: [user-defined_id]
option 25: show external-services [statistics]
option 26: show failover
sub-option 1: configuration [group_address]
sub-option 2: statistics
option 27: show forwarding
option 28: show health-checks
```

**option 29:** show hostname

**option 30:** show http

**option 31:** show http-stats

**option 32:** show icp-settings

**option 33:** show identd

**option 34:** show im

- sub-option 1: aol-statistics
- sub-option 2: configuration
- sub-option 3: msn-statistics
- sub-option 4: yahoo-statistics

**option 35:** show installed-systems

**option 36:** show interface

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

**option 37:** show ip-default-gateway

**option 38:** show ip-route-table

**option 39:** show ip-rts-table

**option 40:** 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 41:** show licenses

**option 42:** show netbios

**option 43:** show ntp

**option 44:** show policy

- sub-option 1: [listing]
- sub-option 2: [order]
- sub-option 3: [proxy-default]

**option 45:** show ports

**option 46:** show profile

**option 47:** show realms

**option 48:** show resources

**option 49:** show restart

**option 50:** show return-to-sender

**option 51:** show rip  
sub-option 1: parameters  
sub-option 2: routes  
sub-option 3: statistics

**option 52:** show security

**option 53:** 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 54:** show sessions

**option 55:** show snmp

**option 56:** show socks-gateways

**option 57:** show socks-machine-id

**option 58:** show socks-proxy

**option 59:** 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 60:** show splash-generator

**option 61:** show ssl  
sub-option 1: ccl [*list\_name*]

```

    sub-option 2: ssl-client [ssl_client]
option 62: show static-routes
option 63: show status
option 64: 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 65: show tcp-rtt
option 66: show telnet-management
option 67: show terminal
option 68: show timezones
option 69: show user-authentication
option 70: show version
option 71: show virtual-ip
option 72: show wccp
    sub-option 1: configuration
    sub-option 2: statistics

```

Table 2.18: # 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.
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 [ <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 2.18: # 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	smartfilter   surfcontrol   status   websense	Displays the content filter configuration.
cpu		Displays CPU usage.
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.
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		Displays event log settings, including event level and event log size, and event recipients.
exceptions	[built-in_id]   [user-defined_id]	Displays exception definitions.

Table 2.18: # show (Continued)

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.
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   interface_number	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.

Table 2.18: # show (Continued)

ntp		Displays NTP servers status and information.
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.
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.
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 Telnet connections.
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.
splash-generator		Displays general, radius accounting and TACACS accounting information.

Table 2.18: # show (Continued)

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.
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 2.19: # 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 http

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 2.20: # 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_lJ
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 may 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 2.21: # traceroute

<i>ip_address</i>	Indicates the IP address of the client or origin server.
<i>hostname</i>	Indicates the host name 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
 0 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

```
upload {access-log | configuration}
```

Table 2.22: # 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> enable
Enable Password:*****
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

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>	Configures the ProxySG to prevent distributed Denial of Service attacks.
<code>bandwidth-gain</code>	Configures bandwidth gain.
<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>health-check</code>	Configures health check entries.
<code>hide-advanced</code>	Disables commands for advanced subsystems.
<code>hostname</code>	Sets the system hostname.

Table 3.1: # (config) (Continued)

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.
show	Shows running system information.
snmp	Modifies SNMP parameters.
socks-gateways	Configures SOCKS gateways.
socks-machine-id	Specifies the machine ID for SOCKS.
socks-proxy	Configures SOCKS proxy values.
splash-generator	Configures splash pages.
ssl	Configures SSL parameters.
static-routes	Installation parameters for static routes table.
streaming	Configures streaming parameters.
tcp-rtt	Specifies the default TCP Round Trip Time.
telnet-management	Enables or disables SSHD configuration via Telnet.
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 is kept around to serve 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`

<code>no path</code>		Clears the network path to download PAC file.
<code>path</code>	<code>url</code>	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 chapter for additional information on log formats.

## Syntax

access-log

This changes the prompt to:

SGOS#(config access-log)

### -subcommands-

**option 1:** create {log *log\_name* | format *format\_name*}

**option 2:** cancel-upload {all | log *log\_name*}

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

**option 4:** delete {log *log\_name* | format *format\_name*}

**option 5:** early-upload *megabytes*

**option 6:** edit {log *log\_name*—changes the prompt (see “#(config access-log) edit log *log\_name*” on page 66) | format *format\_name*—changes the prompt (see “#(config access-log) edit format *format\_name*” on page 70)}

**option 7:** exit

**option 8:** max-log-size *megabytes*

**option 9:** no default-logging {icp | ftp | http | im | mms | rtsp | socks | tcp-tunnel}

**option 10:** overflow-policy {delete | stop}

**option 11:** upload {all | log *log\_name*}

**option 12:** view {[log {[brief] | [*log\_name*]}] | [format {[brief] | [*format\_name*]}] | [statistics [*log\_name*]] | [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>	Chooses a default log for ICP.
	ftp <i>log_name</i>	Chooses a default log for FTP.
	http <i>log_name</i>	Chooses a default log for HTTP/HTTPS.
	im <i>log_name</i>	Chooses a default log for IM.
	mms <i>log_name</i>	Chooses a default log for MMS.
	rtsp <i>log_name</i>	Chooses a default log for Real Media/QuickTime.
	socks <i>log_name</i>	Chooses a default log for SOCKS.
delete	log <i>log_name</i>	Deletes an access log.
	format <i>format_name</i>	Deletes an access log format.
early-upload	<i>megabytes</i>	Sets the log size in megabytes that triggers an early upload.

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

edit	log <i>log_name</i>	Changes the prompt. See “# (config access-log) edit log <i>log_name</i> ” on page 66.
	format <i>format_name</i>	changes the prompt. See “# (config access-log) edit format <i>format_name</i> ” on page 70.
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	Deletes the default log for ICP.
	ftp	Deletes the default log for FTP.
	http	Deletes the default log for HTTP/HTTPS.
	im	Deletes the default log for IM.
	mms	Deletes the default log for MMS.
	rtsp	Deletes the default log for Real Media/QuickTime.
	socks	Deletes the default log for SOCKS.
overflow-policy	delete	Deletes the oldest log entries (up to the entire log).
	stop	Stops access logging until logs are uploaded.
upload	all	Uploads all logs.
	log <i>log_name</i>	Uploads a log.
view	[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 access log format configuration.
	[statistics <i>[log_name]</i> ]	Shows access log statistics.
	[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 *kbps*

**option 2:** client-type

sub-option 1: custom

sub-option 2: ftp

sub-option 3: http

sub-option 4: 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: exit
option 10: format-name format_name
option 11: 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 12: 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 13: periodic-upload
sub-option 1: enable
sub-option 2: upload-interval {daily upload_hour (0-23) | hourly hours [minutes] }
```

- option 14:** `remote-size megabytes`
- option 15:** `upload-type {gzip | text}`
- option 16:** `view`
- option 17:** `websense-client`
  - sub-option 1: `alternate hostname [port]`
  - sub-option 2: `primary hostname [port]`

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

<code>bandwidth</code>	<code>kbps</code>	Sets maximum bandwidth in kbps for log uploading.
<code>client-type</code>	<code>custom</code>	Uploads log using the custom client.
	<code>ftp</code>	Uploads log using the FTP client.
	<code>http</code>	Uploads log using the HTTP client.
	<code>websense</code>	Uploads log using the Websense LogServer protocol.
<code>commands</code>	<code>cancel-upload</code>	Cancels a pending access log upload.
	<code>close-connection</code>	Closes a manually opened connection to the remote server.
	<code>delete-logs</code>	Permanently deletes all access logs on the ProxySG.
	<code>open-connection</code>	Manually opens a connection to the remote server.
	<code>rotate-remote-log</code>	Switches to a new remote logfile.
	<code>send-keep-alive</code>	Sends a keep-alive log packet to the remote server.
	<code>test-upload</code>	Tests the upload configuration by uploading a verification file.
	<code>upload-now</code>	Uploads access log now.
<code>connect-wait-time</code>	<code>seconds</code>	Sets time to wait between server connect attempts.
<code>continuous-upload</code>	<code>enable</code>	Uploads access log continuously to remote server.
	<code>keep-alive seconds</code>	Sets the interval between keep-alive log packets.
	<code>lag-time seconds</code>	Sets the maximum time between log packets (text upload only).
	<code>rotate-remote {daily rotation_hour (0-23)   hourly hours [minutes]}</code>	Specifies when to switch to new remote logfile.

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

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.
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.
ftp-client	alternate {encrypted-password <i>encrypted_password</i>   host <i>hostname</i> [ <i>port</i> ]   password <i>password</i>   path <i>path</i>   username <i>username</i> }	Configures the alternate FTP host site.
	filename <i>format</i>	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 <i>encrypted_password</i>   host <i>hostname</i> [ <i>port</i> ]   password <i>password</i>   path <i>path</i>   username <i>username</i> }	Configures the primary FTP host site.
	secure {no   yes}	Selects whether to use secure connections (FTPS). The default is no. If yes, the <i>hostname</i> 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 log *log\_name*) (Continued)

http-client	alternate {encrypted-password <i>encrypted_password</i>   host <i>hostname</i> [ <i>port</i> ]   password <i>password</i>   path <i>path</i>   username <i>username</i> }	Configures the alternate HTTP host site.
	filename <i>format</i>	Configures the remote filename format.
	no {alternate   filename   primary}	Deletes HTTP client parameters.
	primary {encrypted-password <i>encrypted_password</i>   host <i>hostname</i> [ <i>port</i> ]   password <i>password</i>   path <i>path</i>   username <i>username</i> }	Configures the primary HTTP host site.
	secure {no   yes}	Selects whether to use secure connections (HTTPS). The default is no. If yes, the <i>hostname</i> must match the hostname in the certificate presented by the server.
	time-format {local   utc}	Selects the time format to use within upload filename.
periodic-upload	enable	Uploads access log daily/hourly to remote server.
	upload-interval {daily <i>upload_hour</i> (0-23)   hourly <i>hours</i> [ <i>minutes</i> ]}	Specifies access log upload interval.
remote-size	<i>megabytes</i>	Sets maximum size in MB of remote log files.
upload-type	{gzip   text}	Sets upload file type (gzip or text).
view		Shows log settings.
websense-client	alternate <i>hostname</i> [ <i>port</i> ]	Configures the alternate websense server address.
	primary <i>hostname</i> [ <i>port</i> ]	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*.

### 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 prevent 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)
```

**option 1:** client

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

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

```
sub-option 3: connection-limit integer
```

```
sub-option 4: reset-at-connection-limit {yes | no}
```

**option 2:** view

```
sub-option 1: configuration
```

```
sub-option 2: client-table
```

**option 3:** show

**option 4:** exit

Table 3.7: #(config) attack-detection

client	disable	Disables attack-detection mode.
	enable	Enables attack-detection mode.
	connection-limit <i>integer</i>	Limits the number of simultaneous connections from a client. Accepted values are 1-65535. The default is 10.
	reset-at-connection-limit {yes   no}	Defines the behavior when the connection limit is reached: Yes, to reset the connection, or no, to drop the connections over the limit.
exit		Exits configure attack-detection mode and returns to configure mode.
show		Shows the running configuration of the system.

Table 3.7: # (config) attack-detection

view	configuration	Allows you to view attack-detection configuration settings or the number of current connections.
	client-table	Allows you to view attack-detection client-table settings.

*Example*

```

SGOS#(config) attack-detection
SGOS#(config attack-detection) client enable
ok
SGOS#(config attack-detection) view configuration
Attack Detection Configuration
Attack Detection client enabled = true
Number of simultaneous connection from single IP = 5
Reset TCP Connection at connection limit = false
    
```

## #(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

bandwidth-gain

This changes the prompt to:

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

*-subcommands-*

**option 1:** disable

**option 2:** enable

Table 3.8: # (config bandwidth-gain)

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

*Example*

```

SGOS#(config) bandwidth-gain
SGOS#(config bandwidth-gain) enable
ok
SGOS#(config bandwidth-gain) 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 3.9: #(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

### Syntax

bridge

This changes the prompt to:

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

#### -subcommands-

**option 1:** create

**option 2:** delete

**option 3:** edit—changes the prompt (see“(config bridge) edit bridge\_name” on page 76)

**option 4:** exit

Table 3.10: #(config bridge)

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 76.
exit		Exits configure bridge mode and returns to configure mode.

### Example

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

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

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

### 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 3.11: #(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 mode.
failover	<i>failover_group</i>	Associates this bridge to a failover group.

Table 3.11: # (config bridge *bridge\_name*) (Continued)

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 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.
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 test
SGOS#(config bridge test) accept-inbound
    ok
SGOS#(config bridge test) instructions accelerated-pac
    ok
SGOS#(config bridge test) exit
SGOS#(config bridge)

```

**#(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:** viewTable 3.12: #(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</i> <i>port_number</i> mode and returns to configure <i>bridge_name</i> mode.
full-duplex		Configures this port for full duplex.
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 Technical Support at:

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

The central bypass list maintained by Blue Coat contains addresses Blue Coat 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 3.13: `#(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 email 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 email 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 81)

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

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

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

**option 7:** refresh {automatic | bandwidth *kpbs* | no automatic}

**option 8:** view

Table 3.14: #(config caching)

always-verify-source		Specifies the ProxySG to always verify the freshness of an object with the object source.
ftp		Changes the prompt. See“#(config caching) ftp” on page 81.
max-cache-size	<i>megabytes</i>	Specifies the maximum size of the cache to the value indicated by <i>megabytes</i> .
negative-response	<i>minutes</i>	Specifies that negative responses should be cached for the time period identified by <i>minutes</i> .
no	always-verify-source	Specifies that the ProxySG should never verify the freshness of an object with the object source.

Table 3.14: # (config caching)

refresh	automatic	Specifies that the ProxySG should manage the refresh bandwidth.
	bandwidth <i>kbps</i>	Specifies the amount of bandwidth in kilobits to utilize for maintaining object freshness.
	no automatic	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 3.15: #(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 3.16: # (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.
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 3.17: #(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 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:

- Using vendor-based content filtering

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

- SmartFilter™, a provider of Web filtering software used locally on the ProxySG.
- Websense®, a provider of Web filtering software, used either locally on the ProxySG and or remotely on a separate Websense Enterprise Server.
- SurfControl™, a total filtering solution.

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

- Denying access to URLs

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 Policy Language.

Refer to the *Blue Coat ProxySG Configuration and Management Guide* and the *Blue Coat ProxySG Policy Language Guide and Reference* for complete descriptions of these features.

## Syntax

```
content-filter
```

This changes the prompt to:

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

- *subcommands* -

**option 1:** categories

**option 2:** download {auto| day-of-week {all | friday | monday | none | saturday | sunday | thursday | tuesday | wednesday} | get-now | time-of-day 0-23}

**option 3:** exit

**option 4:** no download {auto | day-of-week {friday | monday | saturday | sunday | thursday | tuesday | wednesday}}

**option 5:** select-provider {none | smartfilter | surfcontrol | websense}

**option 6:** smartfilter—changes the prompt (see “#(config content-filter) smartfilter” on page 86)

**option 7:** surfcontrol—changes the prompt (see “#(config content-filter) surfcontrol” on page 88)

**option 8:** test-url url

**option 9:** websense—changes the prompt (see “#(config content-filter) websense” on page 89)

**option 10:** view

Table 3.18: #(config content-filter)

categories		Shows available categories.
------------	--	-----------------------------

Table 3.18: # (config content-filter) (Continued)

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.
	get-now	Initiates immediate database download.
	time-of-day 0-23	Specifies the time of day for automatic downloads.
exit		Exits configure content filter mode and returns to configure mode.
no download	auto   day-of-week {friday   monday   saturday   sunday   thursday   tuesday   wednesday}	Negates download automatic or day-of-week download commands.
select-provider	none	Specifies that no content filtering is enabled.
	smartfilter	Enables SmartFilter content filtering.
	surfcontrol	Enables SurfControl content filtering.
	websense	Enables Websense content filtering.
smartfilter		Changes the prompt. See “# (config content-filter) smartfilter” on page 86.
surfcontrol		Changes the prompt. See “# (config content-filter) surfcontrol” on page 88.
test-url	url	Displays categories for a URL assigned by the current configuration (selected provider and policy if applicable).
websense		Changes the prompt. See “# (config content-filter) websense” on page 89.

**Example**

```

SGOS#(config) content-filter
SGOS#(config content-filter) select-provider smartfilter

loading database....
ok
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 {encrypted-password *encrypted\_password* | get-now | password *password* | url {standard-list {ftp | http} | premier-list {ftp | http} | url} | username *username*}

**option 3:** exit

**option 4:** no {allow-rdns | download {encrypted-password | password | url | username}}

**option 5:** view

Table 3.19: #(config smartfilter)

allow-rdns		Allow reverse DNS for lookups.
download	encrypted-password <i>encrypted_password</i>	Specifies the encrypted password for the database download server.
	get-now	Initiates immediate database download.
	password <i>password</i>	Specifies the password for the database download server.
	url {standard-list {ftp   http}   premier-list {ftp   http}   url}	Specifies the URL from which to download database.
	username <i>username</i>	Specifies the username for the database download server.
exit		Exits configure smartfilter mode and returns to configure content-filter mode.
no	allow-rdns	Disallows reverse DNS for lookups.
	download {encrypted-password   password   url   username}	Negates download commands.
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 {encrypted-password *encrypted\_password* | get-now | password *password* | url {default | *url*} | username *username*}

**option 2:** exit

**option 3:** no download {encrypted-password | password | url | username}

**option 4:** view

Table 3.20: #(config surfcontrol)

download	encrypted-password <i>encrypted_password</i>	Specifies the encrypted password for the database download server.
	get-now	Initiates immediate database download.
	password <i>password</i>	Specifies the password for the database download server.
	url {default   <i>url</i> }	Specifies the URL from which to download the database.
	username <i>username</i>	Specifies the username for the database download server.
exit		Exits configure surfcontrol mode and returns to configure content-filter mode.
no 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 from which to download the database.
	username	Clears the username for the database download server.
view		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:** download {email-contact *email\_address* | get-now | license *license\_key* | server {*ip\_address* | *hostname*}

**option 2:** exit

**option 3:** no {download {email-contact | license | server} | use-regexes}

**option 4:** open-server {disable | enable | port {default | port}}

**option 5:** use-regexes

**option 6:** view

Table 3.21: #(config websense)

download	email-contact <i>email_address</i>	Specifies an email address that is sent to Websense when downloading the database.
	get-now	Initiates immediate database download.
	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.
exit		Exits configure websense mode and returns to configure content-filter mode.

Table 3.21: # (config websense) (Continued)

no	download {email-contact   license   server}	Clears the download parameters.
	use-regexes	No regular expression filters can be used.
open-server	disable	Disables Websense Open Server service.
	enable	Enables Websense Open Server service.
	port {default   port}	Configures Websense Open Server listening port.
use-regexes		Regular expression filters can be used.
view		Shows the current SurfControl settings.

**Example**

```

SGOS#(config) content-filter
SGOS#(config content-filter) websense
SGOS#(config websense) no use-regexes
    ok
SGOS#(config websense) 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:** exit

**option 2:** heartbeat {disable | enable}

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

**option 4:** send-heartbeat

**option 5:** service-info—changes the prompt (see “#(config diagnostics) service-info” on page 91)

**option 6:** snapshot {create | delete | edit} *snapshot\_name*

**option 7:** view

Table 3.22: # (config diagnostics)

exit		Exits configure diagnostics mode and returns to configure mode.
heartbeat	disable   enable	Enables or disables the ProxySG Heartbeat features.

Table 3.22: # (config diagnostics) (Continued)

monitor	disable   enable	Enables or disables the monitoring feature.
send-heartbeat		Triggers a heartbeat report.
service-info		Changes the prompt. See “# (config diagnostics) service-info” on page 91.
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 92.
view		Displays the current diagnostics 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.

**Syntax**

```
diagnostics
```

This changes the prompt to:

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

```
service-info
```

This changes the prompt to:

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

**- subcommands-**

**option 1:** cancel {all | *one\_or\_more\_from\_view\_status*}

**option 2:** exit

**option 3:** send {*sr\_number* | *one\_or\_more\_commands\_from\_view\_available*}

**option 4:** view {available | status}

Table 3.23: # (config diagnostics service-info)

cancel	all	Cancel all service information being sent to Blue Coat.
	<i>one_or_more_from_view_status</i>	Cancel certain service information being sent to Blue Coat.

Table 3.23: # (config diagnostics service-info) (Continued)

exit		Exits configure diagnostics service-info mode and returns to configure diagnostics mode.
send	<i>sr_num</i>	Sends a specific service request to Blue Coat.
	<i>one_or_more_commands_from_view_available</i>	Sends certain commands to Blue Coat.
view	available	Shows list of service information than can be sent to Blue Coat.
	status	Shows transfer status of service information to Blue Coat.

**Example**

```

SGOS#(config) diagnostics
SGOS#(config diagnostics) service-info
SGOS#(diagnostics service-info) cancel all
ok
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 3.24: #(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	<i>infinite</i>   <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 | resolving
resolved_name | server ip_address}
option 5: dns resolving name [ip_address]
option 6: dns server ip_address
option 7: dns time-to-live seconds

```

Table 3.25: # (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.
	resolving	Sets all entries in the name resolving 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.
	resolving <i>resolved_name</i>	Removes the resolved name identified by <i>resolved_name</i> from the name resolving list.
	server <i>ip_address</i>	Removes the primary DNS server identified by <i>ip_address</i> from the primary DNS server list.
resolving	<i>name</i> [ <i>ip_address</i> ]	Adds the file indicated by <i>name</i> as the name resolving list. Optionally allows the DNS proxy to return any ip address if the DNS request's name matches the domain name suffix string (indicated by <i>name</i> ).
server	<i>ip_address</i>	Adds the new primary domain name server indicated by <i>ip_address</i> to the primary DNS server list.
time-to-live	<i>seconds</i>	Sets the TTL value for matched resolved names.

**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 3.26: #(config) dynamic-bypass

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

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

Table 3.27: #(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.

Table 3.27: #(config event-log) (Continued)

log-size	<i>megabytes</i>	Specifies the maximum size of the event log in megabytes.
mail	add <i>email_address</i>	Specifies an email recipient for the event log output.
	clear	Removes all email recipients from the event log email output distribution list.
	no smtp-gateway	Clears the SMTP gateway used for notifications.
	remove <i>email_address</i>	Removes the email recipient indicated by <i>email_address</i> from the event log email output distribution list.
	smtp-gateway { <i>domain_name</i>   <i>ip_address</i> }	Specifies the SMTP gateway to use for event log email output notifications.
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 { <i>domain_name</i>   <i>ip_address</i> }	Specifies the host domain used for system log notifications.
	no loghost	Clears the loghost setting.
view		Shows current event log settings.
when-full	{ <i>overwrite</i>   <i>stop</i> }	Specifies what should happen to the event log when the maximum size has been reached. <i>overwrite</i> overwrites the oldest information in a FIFO manner; <i>stop</i> disables event logging.

*Note:* You must replace the default Blue Coat SMTP gateway with your gateway. If you do not have access to an SMTP gateway, you can use the Blue Coat gateway to send event messages to Blue Coat (the Blue Coat SMTP gateway will only send mail to Blue Coat; 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 99)

**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 3.28: #(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 [ <i>user-defined.</i> ] <i>exception_id</i> ” on page 99.
exit		Exits configure exceptions mode and returns to configure mode.
inline	{contact   details   format   help   http {contact   details   format   help   summary}   summary} <i>eof_marker</i>	Configures defaults for all exception objects.
load	exceptions	Downloads new exceptions.
no	path	Clears the network path to download exceptions.

Table 3.28: # (config exceptions) (Continued)

path	url	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 3.29: #(config exceptions [user-defined.]exception\_id)

exit		Exits configure exceptions [user-defined] exception_id mode and returns to configure exceptions mode.
------	--	---

Table 3.29: #(config exceptions [user-defined.]exception\_id) (Continued)

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} eof_marker	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 102)

sub-option 2: *service\_group\_name* (see“#(config external-services) edit *service\_group\_name*” on page 103)

sub-option 3: *websense\_service\_name* (see“#(config external-services) edit *websense\_service\_name*” on page 105)

**option 4:** exit

**option 5:** icap-patience {details-inline | header-inline | help-inline | summary-inline} *eof\_marker*

**option 6:** view

**Table 3.30:** #(config external-services)

create	icap <i>icap_service_name</i>	Creates an ICAP service.
	service-group <i>service_group_name</i>	Creates a service group.
	websense <i>websense_service_name</i>	Creates a Websense service
delete	<i>name</i>	Deletes an external service.
edit	<i>icap_service_name</i>	Changes the prompt. See“#(config external-services) edit <i>icap_service_name</i> ” on page 102.
	<i>service_group_name</i>	Changes the prompt. See“#(config external-services) edit <i>service_group_name</i> ” on page 103.
	<i>websense_service_name</i>	Changes the prompt. See“#(config external-services) edit <i>websense_service_name</i> ” on page 105.
exit		Exits configure external-services mode and returns to configure mode.
icap-patience	details-inline <i>eof_marker</i>	Customizes ICAP patience details.
	header-inline <i>eof_marker</i>	Customizes ICAP patience header.
	help-inline <i>eof_marker</i>	Customizes ICAP patience help.
	summary-inline <i>eof_marker</i>	Customizes ICAP patience summary.
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 3.31: #(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.

Table 3.31: # (config icap *icap\_service\_name*) (Continued)

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 104)

**option 3:** exit

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

**option 5:** view

Table 3.32: #(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 <i>service_group_name</i> ) edit <i>entry_name</i> ” on page 104).
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 255Table 3.33: #(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 3.34: #(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 107)

**option 3:** `exit`

**option 4:** `delete group_address`

Table 3.35: #(config failover)

create	<i>group_address</i>	Creates a failover group.
edit	<i>group_address</i>	Changes the prompt. See “#(config failover) edit group_address” on page 107.
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 3.36: # (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.
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	<i>relative_priority</i>	(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	<i>secret</i>	(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

When forwarding content requests, the ProxySG supports the use of default and backup hosts and host groups. 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.

After adding forwarding hosts and groups, you must define which acts as a default and which acts as a backup.

The ProxySG performs health checks with one or more 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 (1) that there is an end-to-end connection and (2) that the host is up and running and will most likely be able to return a response.

With multiple forwarding hosts, health checks are important to the ProxySG. When hosts respond positively to health checks, the ProxySG can forward requests to those hosts, rather than to an unavailable host, and the ProxySG can more quickly fulfill content requests. With a single forwarding host, it is still important for the ProxySG to use health checks to detect whether the host is available.

### 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*] [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 | ssl-session-id}]}

**option 2:** delete {all | group *group\_name* | host *host\_alias*}

**option 3:** download-via-forwarding {disable | enable}

**option 4:** edit {*group\_alias* | *host\_alias*}—changes the prompt (see either “#(config forwarding) edit *group\_alias*” on page 112 or “#(config forwarding) edit *host\_alias*” on page 113)

**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 {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 3.37: # (config forwarding)

create		Creates a forwarding host/group.
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	Disables configuration file downloading using forwarding.
	enable	Enables configuration file downloading using forwarding.
edit	<i>host_or_group_alias</i>	Changes the prompt. See “# (config forwarding) edit <i>host_alias</i> ” on page 113.
exit		Exits configure forwarding mode and returns to configure mode.
failure-mode	closed	Sets the default forwarding failure mode to closed.
	open	Sets the default forwarding failure mode to open.

Table 3.37: # (config forwarding) (Continued)

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, the global default is used.
	ssl-method {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, the global default is used.
	timeout <i>minutes</i>	Sets the timeout in minutes for the host affinity.
integrated-host-timeout	<i>minutes</i>	Sets the timeout for aging out unused integrated hosts.
load-balance	hash {default <i>group_alias</i>   domain [ <i>group_alias</i> ]   url [ <i>group_alias</i> ]   no [ <i>group_alias</i> ]}	Sets if and how load balancing hashes between group members. If a group alias is not specified, the global default is used.
	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, the global default is used.
no path		Negates certain forwarding settings.
path	<i>url</i>	Sets the network path to download forwarding settings.
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 {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 3.38:** #(config forwarding *group\_alias*)

exit		Exits configure forwarding <i>group_alias</i> mode and returns to configure forwarding mode.
------	--	--

Table 3.38: # (config forwarding group\_alias) (Continued)

host-affinity	method {accelerator-cookie   client-ip-address   default}	Changes the host affinity method (non-SSL) for this group.
	ssl-method {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 {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}
- option 11:** proxy
- option 12:** rtsp [*port*]
- option 13:** server
- option 14:** ssl-verify-server
- option 15:** tcp *port*
- option 16:** view

Table 3.39: #(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 {accelerator-cookie   client-ip-address   default}	Changes the host affinity method (non-SSL) for this host.
	ssl-method {client-ip-address   default   ssl-session-id}	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   least-connections   round-robin}	Changes the load balancing method.

Table 3.39: #(config forwarding *host\_alias*) (Continued)

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	Deletes a setting for this host.
proxy		Makes the host a proxy instead of a server; any HTTPS or TCP port will be 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.
ssl-verify-server		Sets SSL to verify server certificates.
tcp	<i>port</i>	Changes the TCP port.
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) 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 stays 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 117)

**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 3.40: #(config health-check)

<code>create</code>	<code>entry_name</code>	Adds a health check entry specified by <code>entry_name</code> .
<code>delete</code>	<code>entry_name</code>	Deletes the specified health check entry.
<code>edit</code>	<code>entry_name</code>	Changes the prompt. See “#(config health-check) edit entry_name” on page 117.
<code>exit</code>		Exits configure health check mode and returns to configure mode.
<code>forwarding</code>	<code>failcount count</code>	Configures the forwarding health check failure count.
	<code>interval seconds</code>	Configures the forwarding health check interval in seconds.
	<code>pause</code>	Pauses the forwarding health checks temporarily (the system remains in <code>pause</code> mode until you use the <code>resume</code> command to end it).
	<code>resume</code>	Resumes the forwarding health checks.
	<code>type {http object   https object   layer-3   layer-4}</code>	Configures the forwarding health check type.

Table 3.40: # (config health-check) (Continued)

socks-gateways	failcount <i>count</i>	Configures the SOCKS gateways health check failure count.
	interval <i>seconds</i>	Configures the SOCKS gateways health check interval in seconds.
	pause	Pauses the SOCKS gateways health checks temporarily (the system remains in <code>pause</code> 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 3.41: # (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 email notification of state changes.

Table 3.41: # (config health-check *entry\_name*) (Continued)

notify		Enables email 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**

Use this command to disable advanced commands. The advanced commands that you can disable include TCP/IP commands. See “#(config) reveal-advanced” on page 140 for information about enabling advanced commands that are disabled.

**Syntax**

```

option 1: hide-advanced all
option 2: hide-advanced expand
option 3: hide-advanced tcp-ip

```

Table 3.42: # (config) hide-advanced

all		Disables all expanded, HTTP, and TCP/IP advanced commands.
expand		Disables all expanded advanced commands.
tcp-ip		Disables all TCP/IP advanced commands.

**Example**

```
SGOS#(config) hide-advanced all
ok
```

**#(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 3.43: # (config) hostname

<i>name</i>		Associates <i>name</i> with the current ProxySG.
-------------	--	--

**Example**

```
SGOS#(config) hostname "Blue Coat 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 | reverse-dns}

**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 | reverse-dns}

sub-option 4: force-ntlm

sub-option 5: parse meta-tag expires

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: www-redirect
sub-option 15: xp-rewrite-redirect
option 7: http parse meta-tag expires
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 upload-with-pasv {disable | enable}
option 19: http version {1.0 | 1.1}
option 20: http www-redirect
option 21: xp-rewrite-redirect

```

Table 3.44: #(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 3.44: # (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.
	reverse-dns	Stores objects under the name of the associated host instead of the IP address.
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 expires		Parses HTML objects for the expires meta-tag.
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 3.44: # (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 Blue Coat's 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."
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 3.45: #(config) icp

no path		Negates the path previously set using the command <code>icp path url</code> .
path	<code>url</code>	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 3.46: # (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 buddy-spoof-message *message\_text*
- option 3:** im exceptions {in-band | out-of-band}
- option 4:** im msn-admin-buddy *buddy*
- option 5:** im yahoo-admin-buddy *buddy*

Table 3.47: # (config) im

aol-admin-buddy	<i>buddy</i>	Set AOL admin buddy name.
buddy-spoof-message	<i>message_text</i>	Set buddy spoof message.
exceptions	in-band	Deliver IM exceptions in band.
	out-of-band	Deliver IM exceptions out of band.
msn-admin-buddy	<i>buddy</i>	Set MSN admin buddy name.
yahoo-admin-buddy	<i>buddy</i>	Set Yahoo admin buddy name.

**Example**

```

SGOS#(config) im exceptions in-band
ok
SGOS#(config) im yahoo-admin-buddy testname
ok

```

**#(config) inline**

There are two ways to create a configuration file for your ProxySG. You can use the SGOS `inline` command or you can create a text file to house the configuration commands.

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

```
SGOS#configure terminal
SGOS#(config) inline wccp token
.
.
.
end
token
```

where `token` marks the end of the inline commands.

If you choose to create a configuration file, 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 bypass-list {central | local} eof_marker`

**option 3:** `inline exceptions`

**option 4:** `inline forwarding eof_marker`

**option 5:** `inline icp-settings eof_marker`

**option 6:** `inline license-key eof_marker`

**option 7:** `inline policy {central | forward | local | vpm-cpl | vpm-xml} eof_marker`

**option 8:** `inline rip-settings eof_marker`

**option 9:** `inline socks-gateways eof_marker`

**option 10:** `inline static-route-table eof_marker`

**option 11:** `inline wccp-settings eof_marker`

Table 3.48: # (config) inline

accelerated-pac	<i>eof_marker</i>	Creates and installs an accelerated PAC file using the console input commands you enter between <code>accelerated-pac eof_marker</code> and the next <i>eof_marker</i> .
bypass-list	{central   local} <i>eof_marker</i>	Creates and installs a bypass list file using the console input commands you enter between <code>bypass-list central</code> or <code>local eof_marker</code> and the next <i>eof_marker</i> .
exceptions		Install exceptions from console input.
forwarding	<i>eof_marker</i>	Creates and installs forwarding configurations using the console input commands you enter between <code>forwarding eof_marker</code> and the next <i>eof_marker</i> .
icp-settings	<i>eof_marker</i>	Creates and installs an ICP settings file using the console input commands you enter between <code>icp-settings eof_marker</code> and the next <i>eof_marker</i> .
license-key	<i>eof_marker</i>	Creates and installs a license key from the console input commands you enter between <code>license-key eof_marker</code> and the next <i>eof_marker</i> .
policy	{central   forward   local   vpm-cpl   xml-cpl} <i>eof_marker</i>	Creates and installs a policy file using the console input commands you enter between <code>policy central</code> , <code>forward</code> , <code>local</code> , <code>vpm-cpl</code> , or <code>vpm-xml eof_marker</code> and the next <i>eof_marker</i> .
rip-settings	<i>eof_marker</i>	Creates and installs a RIP settings file using the console input commands you enter between <code>rip-settings eof_marker</code> and the next <i>eof_marker</i> .
socks-gateways	<i>eof_marker</i>	Creates and installs SOCKS gateway settings from the console input commands you enter between <code>socks-gateways eof_marker</code> and the next <i>eof_marker</i> .
static-route-table	<i>eof_marker</i>	Creates and installs a static route table file using the console input commands you enter between <code>static-route-table eof_marker</code> and the next <i>eof_marker</i> .
wccp-settings	<i>eof_marker</i>	Creates and installs a WCCP settings file using the console input commands you enter between <code>wccp-settings eof_marker</code> and the next <i>eof_marker</i> .

**Example**

```
SGOS#(config) inline wccp-settings eof
wccp enable
```

```
.
.
.
eof
ok
```

## #(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 3.49: #(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 will be 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 3.50: #(config) interface

<code>fast-ethernet</code>	<code><i>interface_number</i></code>	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 3.51: # (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 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>	
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 3.52: #(config) ip-default-gateway

<code>ip_address</code>	<code>[preference group (1-10)]</code> <code>[weight (1-100)]</code>	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 3.53: #(config) license-key

<code>auto-update</code>	<code>disable   enable</code>	Disables or enables auto-update of the Blue Coat license key.
<code>no path</code>		Negates certain license key settings.
<code>path</code>	<code>url</code>	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 3.54: # (config line-vty)

<code>exit</code>		Exits configure line-vty mode and returns to configure mode.
<code>length</code>	<code>num_lines_on_screen</code>	Specifies the number of lines of code that should appear on the screen at once. Specify 0 to scroll without pausing.
<code>no</code>	<code>length</code>	Disables screen paging.
<code>telnet</code>	<code>no transparent   transparent</code>	Indicates that this is a Telnet protocol-specific configuration. If you specify <code>no transparent</code> , carriage returns are sent to the console as a carriage return plus linefeed. If you specify <code>transparent</code> , carriage returns are sent to the console as a carriage return.
<code>timeout</code>	<code>minutes</code>	Sets the line timeout to the number of minutes indicated by <code>minutes</code> .
<code>view</code>		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

Use this command to load specific configuration or settings files.

## Syntax

**option 1:** load accelerated-pac

**option 2:** load bypass-list {central | local}

**option 3:** load exceptions

**option 4:** load forwarding

**option 5:** load icp-settings

**option 6:** load license-key

**option 7:** load policy {central | local | forward | vpm-cpl | vpm-xml | vpm-software}

**option 8:** load rip-settings

**option 9:** load socks-gateways

**option 10:** load static-route-table

**option 11:** load upgrade

**option 12:** load wccp-settings

Table 3.55: #(config) load

accelerated-pac		Downloads a new accelerated PAC file.
bypass-list	{central   local}	Downloads either a new central or local bypass list file.
exceptions		Downloads new exceptions.
forwarding		Downloads a new forwarding configuration file.
icp-settings		Downloads a new ICP settings file.
license-key		Downloads a new license key.
policy	central	Downloads a new central policy file.
	local	Downloads a new local policy file.
	forward	Downloads a new forward policy file.
	vpm-cpl	Downloads a new VPM CPL policy file.
	vpm-xml	Downloads a new VPM XML policy file.
	vpm-software	Downloads a new VPM software policy file.
rip-settings		Downloads a new RIP settings file.
static-route-table		Downloads a new static route table.
upgrade		Downloads a new system image.
wccp-settings		Downloads a new WCCP configuration file.

### Example

```
SGOS#(config) load bypass-list central
ok
```

## #(config) netbios

Use this command to configure NETBIOS.

### Syntax

```
netbios
```

This changes the prompt to:

```
SGOS#(config netbios)
```

**option 1:** disable

**option 2:** enable

**option 3:** exit

**option 4:** view

Table 3.56: #(config) netbios

disable		Disables NETBIOS services.
enable		Enables NETBIOS services.
exit		Exits configure netbios mode and returns to configure mode.
view		Shows the NETBIOS settings.

### Example

```
SGOS#(config) netbios
SGOS#(config netbios) 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 3.57: # (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).
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 3.58: # (config) ntp

clear		Removes all entries from the NTP server list.
disable		Disables NTP.
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 3.59:** # (config) policy

central-path	<i>url</i>	Specifies the network path (indicated by <i>url</i> ) from which the central policy file may be downloaded.
forward-path	<i>url</i>	Specifies the network path (indicated by <i>url</i> ) from which the forward policy file may be downloaded.
local-path	<i>url</i>	Specifies the network path (indicated by <i>url</i> ) from which the local policy file may be downloaded.
vpm-cpl-path	<i>url</i>	Specifies the network path (indicated by <i>url</i> ) from which the vpm-cpl policy file may be downloaded.
vpm-xml-path	<i>url</i>	Specifies the network path (indicated by <i>url</i> ) from which the vpm-xml policy file may 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 email 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.
	vpm-xml-path	Clears the network path to download VPM XML policy.
notify		Specifies that an email 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 3.59: # (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 3.60: # (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:** core-image {context | full | keep number | none}  
**option 2:** mode {hardware | software}

Table 3.61: # (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 3.62: # (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	Enables return-to-sender versions 1 or 2.

**Example**

```
SGOS#(config) return-to-sender inbound enable
ok
```

**#(config) 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. The advanced commands that you can enable include TCP/IP commands. See “#(config) `hide-advanced`” on page 119 for information about disabling advanced commands that are enabled.

**Syntax**

- option 1:** `reveal-advanced all`
- option 2:** `reveal-advanced expand`
- option 3:** `reveal-advanced tcp-ip`

Table 3.63: # (config) reveal-advanced

all		Reveals all advanced commands.
expand		Enables expanded commands.
tcp-ip		Enables commands for TCP-IP. See “#(config) <code>tcp-ip</code> ” on page 209 for information about TCP-IP commands.

**Example**

```
SGOS#(config) reveal-advanced expand
ok
SGOS#(config) reveal-advanced tcp-ip
ok
SGOS#(config) reveal-advanced all
ok
```

**#(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 3.64: `#(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
- LDAP – Lightweight Directory Access Protocol
- Local – Users and groups stored locally on the ProxySG
- NTLM – Windows NT Challenge Response
- RADIUS – Remote Authentication for Dialup Users

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 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 may 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 ProxySG Configuration and Management Guide*.

## Syntax

**option 1:** security allowed-access {add | remove} source\_ip [ip\_mask]

**option 2:** 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 147)

sub-option 4: view [realm\_name]

**option 3:** security default-authenticate-mode {auto | sg2}

**option 4:** security destroy-old-password [force]

**option 5:** security enable-password password

**option 6:** security enforce-acl {disable | enable}

**option 7:** security flush-credentials

sub-option 1: [on-policy-change {disable | enable}]

sub-option 2: [realm realm]

**option 8:** security hashed-enable-password hashed\_password

**option 9:** security hashed-password hashed\_password

**option 10:** 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 149)

sub-option 4: view [realm\_name]

**option 11:** 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 152)

sub-option 4: view [*realm\_name*]

**option 12:** 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 153)

**option 13:** 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 14:** 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 155)

sub-option 4: view [*realm\_name*]

**option 15:** security password *password*

**option 16:** security password-display {encrypted | keyring *keyring* | none | view}

**option 17:** 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 156)

sub-option 5: view [*realm\_name*]

**option 18:** 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 159)

sub-option 4: view [*realm\_sequence\_name*]

**option 19:** 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 20:** `security username user_name`

**Table 3.65:** `#(config) security`

allowed-access	<code>add source_IP [mask]</code>	Adds the specified IP to the access control list.
	<code>remove source_IP [mask]</code>	Removes the specified IP from the access control list.
certificate	<code>create-realm realm_name</code>	Creates a new certificate realm with the name specified. The maximum number of certificate realms is 40.
	<code>delete-realm realm_name</code>	Deletes the specified certificate realm.
	<code>edit-realm realm_name</code>	Changes the prompt. See “ <code>#(config) security certificate edit-realm realm_name</code> ” on page 147.
	<code>view [realm_name]</code>	Displays the configuration of all certificate realms or just the configuration for <code>realm_name</code> if specified.
default-authenticate-mode	auto	Sets the default <code>authenticate.mode</code> to auto.
	sg2	Sets the default <code>authenticate.mode</code> to sg2.
destroy-old-passwords	[force]	Destroys recoverable passwords in configuration used by previous versions. Do not use this command if you intend to downgrade as the old passwords will be destroyed. Specify “force” to destroy the passwords without a prompt for confirmation.
enable-password	<code>password password</code>	Sets the console enable password to the password specified. 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.
hashed-enable-password	<code>hashed_password</code>	Specifies the console enable password in hashed format.

Table 3.65: # (config) security (Continued)

hashed-password	<i>hashed_password</i>	Specifies the console password in hashed format.
ldap	create-realm {ad   iplanet   nds   other} <i>realm_name</i> [ <i>base_DN</i> ] <i>primary_host</i> [ <i>primary_port</i> ]	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 <i>realm_name</i>	Deletes the specified LDAP realm.
	edit-realm	Changes the prompt. See “# (config) security ldap edit-realm <i>realm_name</i> ” on page 149.
	view [ <i>realm_name</i> ]	Displays the configuration of all LDAP realms or just the configuration for <i>realm_name</i> if specified.
local	create-realm <i>realm_name</i>	Creates a new Local realm with the name specified. The maximum number of Local realms is 40.
	delete-realm <i>realm_name</i>	Deletes the specified Local realm.
	edit-realm	Changes the prompt. See “# (config) security local edit-realm <i>realm_name</i> ” on page 152.
	view [ <i>realm_name</i> ]	Displays the configuration of all Local realms or just the configuration for <i>realm_name</i> if specified.
local-user-list	clear [force]	Clears all local user lists. Lists referenced by Local realms and the default local user list will be recreated but empty. Specify “force” to clear realms without a prompt for confirmation.
	create <i>local_user_list</i>	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 <i>local_user_list</i>	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 <i>local_user_list</i> [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 <i>local_user_list</i> ” on page 153.

Table 3.65: # (config) security (Continued)

management	auto-logout-timeout <i>seconds</i>	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 <i>name</i>	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 <i>realm_name</i> <i>primary_server_host</i> [ <i>primary_server_port</i> ]	Creates a new NTLM realm with the name, primary server host and port specified. The maximum number of NTLM realms is 40.
	delete-realm <i>realm_name</i>	Deletes the specified NTLM realm.
	edit-realm	Changes the prompt. See “# (config) security ntlm edit-realm <i>realm_name</i> ” on page 155.
	view [ <i>realm_name</i> ]	Displays the configuration of all NTLM realms or just the configuration for <i>realm_name</i> if specified.
password	password	Specifies the console password.
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.
radius	create-realm <i>realm_name</i> <i>secret</i> <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> <i>encrypted-secret</i> <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 156.
	view [ <i>realm_name</i> ]	Displays the configuration of all RADIUS realms or just the configuration for <i>realm_name</i> if specified.

Table 3.65: # (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 159.
	view [ <i>realm_name</i> ]	Displays the configuration of all realm sequences 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 that requests requiring authentication will be redirected to.
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 3.66: # (config certificate *realm\_name*)

authorization	<code>append-base-dn {disable   dn <i>DN_to_append</i>   enable}</code>	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 will be used. Applies to LDAP authorization realms only.
	<code>container-attr-list <i>list_of_attribute_names</i></code>	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.
	<code>no {container-attr-list   realm-name}</code>	Clears the container attribute list or the authorization realm.
	<code>realm-name <i>authorization_realm_name</i></code>	Specifies the authorization realm to use. Only LDAP and Local realms are valid authorization realms.
	<code>username-attribute <i>username_attribute</i></code>	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 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:** display-name *display\_name*

**option 5:** distinguished-name

sub-option 1: user-attribute-type *user\_attribute\_type*

sub-option 2: base-dn {add | demote | promote | remove} *base\_dn* | clear

**option 6:** exit

**option 7:** membership-attribute *attribute\_name*

**option 8:** membership-type {group | user}

**option 9:** membership-username {full | relative}

**option 10:** no {alternate-server | membership-attribute}

**option 11:** 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 12:** primary-server *host* [*port*]

**option 13:** protocol-version {2 | 3}

**option 14:** referrals-follow {disable | enable}

**option 15:** rename *new\_realm\_name*

**option 16:** 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 17:** server-type {ad | iplanet | nds | other}

**option 18:** spoof-authentication {disable | enable}

**option 19:** ssl {disable | enable}

**option 20:** ssl-verify-server {disable | enable}

**option 21:** `timeout seconds`

**option 22:** `view`

**option 23:** `virtual-url url`

**Table 3.67:** `#(config ldap 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>case-sensitive</code>	<code>disable   enable</code>	Specifies whether or not the LDAP server is case-sensitive.
<code>display-name</code>	<code>display-name</code>	Specifies the display name for this realm.
<code>distinguished-name</code>	<code>user-attribute-type</code> <code>user_attribute_type</code>	Specifies the attribute type that defines the relative user name.
	<code>base-dn {add   demote   promote   remove} base_dn</code>	Adds/demotes/promotes/removes a base DN from the base DN list, or clears the base DN list.
<code>exit</code>		Exits configure security ldap mode and returns to configure mode.
<code>membership-attribute</code>	<code>attribute_name</code>	Specifies the attribute that defines group membership.
<code>membership-type</code>	<code>group   user</code>	Specifies the membership type. Specify <code>group</code> if user memberships are specified in groups. Specify <code>user</code> if memberships are specified in users.
<code>membership-username</code>	<code>full   relative</code>	Specifies the username type to use during membership lookups. The <code>full</code> option specifies that the user's FQDN will be used during membership lookups, and <code>relative</code> option specifies that the user's relative username will be used during membership lookups. Only one can be selected at a time.
<code>no</code>	<code>alternate-server   membership-attribute</code>	Clears the alternate-server or membership-attribute values.

Table 3.67: #(config ldap realm\_name) (Continued)

objectclass	container {add   remove} container_objectclass   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} group_objectclass   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} user_objectclass   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	host [port]	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	new_realm_name	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 encrypted_password	Specifies the password to bind with during searches in encrypted format.
	password password	Specifies the password to bind with during searches.
	user-dn user_dn	Specifies the user DN to bind with during searches.
server-type	{ad   iplanet   nds   other}	Specifies the LDAP server type for this realm.
spoof-authentication	disable   enable	Disables/enables the forwarding of user credentials from the credential cache to the OCS. This will only work if the ProxySG and the OCS expect the same user credential combinations.

Table 3.67: #(config ldap *realm\_name*) (Continued)

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	<i>seconds</i>	Specifies the LDAP server's timeout.
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 ldap edit-realm testldap
SGOS#(config ldap testldap) server-type iplanet
ok
SGOS#(config ldap testldap) spoof-authentication enable
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:** display-name *display\_name*

**option 3:** exit

**option 4:** local-user-list *local\_user\_list\_name*

**option 5:** rename *new\_realm\_name*

**option 6:** spoof-authentication {disable | enable}

**option 7:** view

**option 8:** virtual-url *url*

Table 3.68: #(config local *realm\_name*)

cache-duration	seconds	Specifies the length of time to cache credentials for this realm.
display-name	<i>display_name</i>	Specifies the display name for this realm.

Table 3.68: #(config local *realm\_name*) (Continued)

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.
rename	<i>new_realm_name</i>	Renames this realm to <i>new_realm_name</i> .
spooof-authentication	disable   enable	Disables/enables the forwarding of user credentials from the credential cache to the OCS. This will only work if the ProxySG and the OCS expect the same user credential combinations.
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 local edit-realm testlocal
SGOS#(config local testlocal) cache-duration 1500
ok
SGOS#(config local testlocal) spooof-authentication disable
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:** exit

**option 2:** group

sub-option 1: create *group\_name*

sub-option 2: delete *group\_name* [force]

**option 3:** user

sub-option 1: create *user\_name*

sub-option 2: delete *user\_name* [force]

sub-option 3: 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 4: view

```

**Table 3.69:** #(config local-user-list *local\_user\_list*)

exit		Exits configure local-user-list mode and returns to configure mode.
group	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.
user	create <i>user_name</i>	Creates the specified user in the local user list.
	delete <i>user_name</i>	Deletes the specified user in the local user list.
	edit <i>user_name</i>	Edits the specified user in the local user list. Changes the prompt to #(config local-user-list <i>local_user_list</i> <i>user_name</i> ).
	disable   enable	Disables/enables the user account.
	exit	Exits configure local-user-list <i>user_list</i> mode and returns to configure local-user-list mode.
	group add   remove <i>group_name</i>	Adds/removes the specified group from the user.
	hashed-password <i>hashed_password</i>	Specifies the user's password in hashed format.
password <i>password</i>	Specifies the user's password.	
view	view	Displays the user account.
view		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 3.70: #(config ntlm *realm\_name*)

alternate-server	<i>host</i> [ <i>port</i> ]	Specifies the alternate server host and port.
cache-duration	<i>seconds</i>	Specifies the length of time to cache credentials for this realm.
credentials-basic	disable   enable	Disables/enables support for Basic credentials in this realm. At least one of Basic or NTLM credentials must be supported.
credentials-ntlm	disable   enable	Disables/enables support for NTLM credentials in this realm. At least one of Basic or NTLM credentials must be supported.

Table 3.70: #(config ntlm realm\_name) (Continued)

display-name	<i>display_name</i>	Specifies the display name for this realm.
exit		Exits configure ntlm-realm mode and returns to configure mode.
no alternate-server		Clears the alternate-server.
primary-server	<i>host [port]</i>	Specifies the primary server host and port.
rename	<i>new_realm_name</i>	Renames this realm to <i>new_realm_name</i> .
timeout	<i>seconds</i>	Specifies the NTLM request timeout.
ssl	disable   enable	Disables/enables SSL communication between the ProxySG and CAASNT.
ssl-verify-server	disable   enable	Specifies whether or not to verify the CAASNT certificate.
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 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 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:** 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 8:** rename *new\_realm\_name*  
**option 9:** timeout *seconds*  
**option 10:** server-retry *count*  
**option 11:** spoof-authentication {disable | enable}  
**option 12:** view  
**option 13:** virtual-url *url*

Table 3.71: #(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>	<i>type</i> stands for the service type, which can be one of the following: <ol style="list-style-type: none"> <li>1. Login</li> <li>2. Framed</li> <li>3. Callback Login</li> <li>4. Callback Framed</li> <li>5. Outbound</li> <li>6. Administrative</li> <li>7. NAS Prompt</li> <li>8. Authenticate Only</li> <li>9. Callback NAS Prompt</li> <li>10. Call Check</li> <li>11. Callback Administrative</li> </ol> If the user record contains Check-list ServiceType attributes, then at least one of the ServiceType values must match the service-type of the RADIUS server as configured on the ProxySG.
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.

Table 3.71: #(config radius realm\_name) (Continued)

exit		Exits configure radius-realm mode and returns to configure mode.
no alternate-server		Clears the alternate-server.
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	<p>type stands for the service type, which can be one of the following:</p> <ol style="list-style-type: none"> <li>1. Login</li> <li>2. Framed</li> <li>3. Callback Login</li> <li>4. Callback Framed</li> <li>5. Outbound</li> <li>6. Administrative</li> <li>7. NAS Prompt</li> <li>8. Authenticate Only</li> <li>9. Callback NAS Prompt</li> <li>10. Call Check</li> <li>11. Callback Administrative</li> </ol> <p>If the user record contains Check-list ServiceType attributes, then at least one of the ServiceType values must match the service-type of the RADIUS server as configured on the ProxySG.</p>
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.
spooof-authentication	disable   enable	Disables/enables the forwarding of user credentials from the credential cache to the OCS. This will only work if the ProxySG and the OCS expect the same user credential combinations.
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) spooof-authentication enable

```

```

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 3.72: #(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) serial-number

This command configures the ProxySG serial number.

### Syntax

**option 1:** serial-number *serial\_number*

Table 3.73: #(config) serial-number

<i>serial_number</i>	Configures the ProxySG serial number.
----------------------	---------------------------------------

### Example

```
SGOS#(config) serial-number 123
ok
```

## #(config) services

Use this command to configure DNS, 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 162)

**option 2:** dns—changes the prompt (see“(config services) dns” on page 163)

**option 3:** exit

**option 4:** ftp—changes the prompt (see“(config services) ftp” on page 164)

**option 5:** http—changes the prompt (see“(config services) http” on page 165)

**option 6:** https—changes the prompt (see“(config services) https” on page 167)

**option 7:** http-console—changes the prompt (see“(config services) http-console” on page 169)

**option 8:** https-console—changes the prompt (see“(config services) https-console” on page 170)

**option 9:** mms—changes the prompt (see“(config services) mms” on page 171)

**option 10:** msn-im—changes the prompt (see“(config services) msn-im” on page 172)

**option 11:** rtsp—changes the prompt (see“(config services) rtsp” on page 173)

**option 12:** socks—changes the prompt (see“(config services) socks” on page 174)

- option 13:** `ssh-console`—changes the prompt (see “#(config services) `ssh-console`” on page 176)
- option 14:** `tcp-tunnel`—changes the prompt (see “#(config services) `tcp-tunnel`” on page 178)
- option 15:** `telnet-console`—changes the prompt (see “#(config services) `telnet-console`” on page 179)
- option 16:** `view`
- option 17:** `yahoo-im`—changes the prompt (see “#(config services) `yahoo-im`” on page 180)

Table 3.74: #(config services)

<code>aol-im</code>		Configures AOL IM services. See “#(config services) <code>aol-im</code> ” on page 162.
<code>dns</code>		Configures DNS services. See “#(config services) <code>dns</code> ” on page 163.
<code>exit</code>		Exits the <code>config services</code> mode and returns to the <code>config</code> prompt.
<code>ftp</code>		Configures transparent or explicit FTP services. See “#(config services) <code>ftp</code> ” on page 164.
<code>http</code>		Configures HTTP services. See “#(config services) <code>http</code> ” on page 165.
<code>https</code>		Configures HTTPS services. See “#(config services) <code>https</code> ” on page 167.
<code>http-console</code>		Configures HTTP Console services. See “#(config services) <code>http-console</code> ” on page 169.
<code>https-console</code>		Configures HTTPS Console services. See “#(config services) <code>https-console</code> ” on page 170.
<code>mms</code>		Configures MMS services. See “#(config services) <code>mms</code> ” on page 171.
<code>msn-im</code>		Configures MSN IM services. See “#(config services) <code>msn-im</code> ” on page 172.
<code>rtsp</code>		Configures RTSP services. See “#(config services) <code>rtsp</code> ” on page 173.
<code>socks</code>		Configures SOCKS services. See “#(config services) <code>socks</code> ” on page 174.
<code>ssh-console</code>		Configures SSH services. See “#(config services) <code>ssh-console</code> ” on page 176.
<code>tcp-tunnel</code>		Configures TCP-tunneling services. See “#(config services) <code>tcp-tunnel</code> ” on page 178.

Table 3.74: #(config services) (Continued)

telnet-console		Configures Telnet Console services. See “#(config services) telnet-console” on page 179.
view		Displays all services-related configuration information.
yahoo-im		Configures Yahoo IM services. See “#(config services) yahoo-im” on page 180.

**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 {transparent {disable | enable} [ip:]port | send-client-ip {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 3.75: #(config services aol-im)

attribute send-client-ip	disable [ip:]port	Disables spoof attribute for listener.
	enable [ip:]port	Enables spoof attribute for listener.
create	[ip:]port	Creates an AOL-IM services listener.
delete	[ip:]port	Deletes an AOL-IM services listener.
disable	[ip:]port	Disables an AOL-IM services listener. This is the default setting.
enable	[ip:]port	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 3.76: #(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) 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 3.77: #(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 3.78: #(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
```

```
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 {sslv2 | sslv3 | tlsv1 | sslv2v3 | sslv2tlsv1 |  
sslv3tlsv1 | sslv2v3tlsv1} 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 3.79: # (config services https)

attribute	cipher-suite <i>ip:port</i>	Specifies the cipher suite to use.
	ccl <i>ip:port</i>	Sets CA Certificate List to use for verifying certificates.
	forward-client-cert {disable   enable} <i>ip:port</i> }	Enables or disables client certificate forwarding
	send-client-ip {disable   enable} <i>ip:port</i> }	Enables or disables sending client's IP as source IP address.
	ssl-protocol-version {sslv2   sslv3   tlsv1   sslv2v3  sslv2tlsv1   sslv3tlsv1   sslv2v3tlsv1} <i>ip:port</i>	Specifies the SSL protocol version.
	verify-client {disable   enable} <i>ip:port</i> }	Enables or disables client verification.
create	<i>ip:port</i> <i>keyring id</i>	Creates an HTTPS services listener port.
delete	attribute ccl <i>ip:port</i>   <i>ip:port</i>	Deletes the HTTPS services settings.
disable	<i>ip:port</i>	Disables the HTTPS services listener port.
enable	<i>ip:port</i>	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 3.80: #(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 cypher-suite [*ip:port*]

**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 3.81: #(config services https-console)

attribute cypher-suite	[ <i>ip:port</i> ]	Configures HTTPS Console services cypher suite.
create	[ <i>ip:port</i> ] [ <i>keyring_id</i> ]	Creates an HTTPS Console services listener.
delete	[ <i>ip:port</i> ]	Deletes an HTTPS Console services listener.
disable	[ <i>ip:port</i> ]	Disables an HTTPS Console services listener.
enable	[ <i>ip:port</i> ]	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 3.82: #(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} [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 3.83: # (config services msn-im)

attribute send-client-ip	{disable   enable} <i>[ip:]port</i>	Disables or enables spoof attribute for listener.
create	<i>[ip:]port</i>	Creates an MSN IM services listener port.
delete	<i>[ip:]port</i>	Deletes the specified MSN IM services listener port.
disable	<i>[ip:]port</i>	Disables the MSN IM services on the specified port. This is the default setting.
enable	<i>[ip:]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 3.84: #(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 3.85: #(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. To use SSHv1, you must create and enable 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 3.86: # (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 SSHv2—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 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.
exit	[ip]:port	Deletes the SSH-console at the port specified.
		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.
view	client-key [ <i>username</i> ]	Displays the client key associated with the indicated <i>username</i> or the legacy client key fingerprints.
	director-client-key [ <i>key_id</i> ]	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
M1vQT9uyenKymwZE1DNe/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 3.87: #(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.

Table 3.87: #(config services tcp-tunnel) (Continued)

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-console**

Use this command to enable and configure Telnet services.

**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 3.88:** #(config services telnet-console)

create	[ip:]port	Creates a Telnet services port indicated by [ip:]port.
delete	[ip:]port	Deletes the Telnet services port indicated by [ip:]port.
disable	[ip:]port	Disables the Telnet services port.
enable	[ip:]port	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-console
SGOS#(config services telnet-console) view
Port:      23   Type: telnet
Properties: enabled, explicit
Port:      9002  Type: telnet
Properties: enabled, explicit
Port:      9003  Type: telnet
Properties: enabled, explicit
Port:      30   Type: telnet
Properties: enabled, explicit
SGOS#(config services telnet-console) delete 9003
ok
SGOS#(config services telnet-console) create 25
ok
SGOS#(config services telnet-console) disable 9003
ok
SGOS#(config services telnet-console) exit
SGOS#(config services) exit
SGOS#(config)

```

**#(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} [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 yahoo-im)

attribute	send-client-ip {disable [ip:]port   enable [ip:]port}	Disables or enables spoof attribute for listener.
create	[ip:]port	Creates a Yahoo IM services listener port.
delete	[ip:]port	Deletes the specified Yahoo IM services listener port.
disable	[ip:]port	Disables the Yahoo IM services on the specified port.
enable	[ip:]port	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) show**

Use this command to display specific configuration settings or options.

**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 archive-configuration

**option 4:** show arp-table

**option 5:** show bandwidth-gain

**option 6:** show bridge

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

sub-option 2: fwtable *bridge\_name*

sub-option 3: statistics *bridge\_name*

**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 configuration

sub-option 1: [brief]

sub-option 2: [expanded]

sub-option 3: [noprompts]

**option 12:** show content

sub-option 1: outstanding-requests {[deletes] | [revalidates] | [priority]}

sub-option 2: priority {[regex regex] | [url url]}

sub-option 3: statistics

sub-option 4: url *url*

**option 13:** show content-distribution

**option 14:** show content-filter

sub-option 1: smartfilter

sub-option 2: surfcontrol

sub-option 3: status

sub-option 4: websense

**option 15:** show cpu

**option 16:** show diagnostics

sub-option 1: service-info

sub-option 2: snapshot *snapshot\_name*

sub-option 3: status

**option 17:** show disk

sub-option 1: *disk\_number*

sub-option 2: all

**option 18:** show dns

**option 19:** show download-paths

**option 20:** show dynamic-bypass

**option 21:** show efficiency

**option 22:** show environmental

**option 23:** show event-log

**option 24:** show exceptions  
sub-option 1: built-in [*id*]  
sub-option 2: user-defined [*id*]

**option 25:** show external-services [*statistics*]

**option 26:** show failover  
sub-option 1: configuration [*group\_address*]  
sub-option 2: statistics

**option 27:** show forwarding

**option 28:** show health-checks

**option 29:** show hostname

**option 30:** show http

**option 31:** show http-stats

**option 32:** show icp-settings

**option 33:** show identd

**option 34:** show im  
sub-option 1: aol-statistics  
sub-option 2: configuration  
sub-option 3: msn-statistics  
sub-option 4: yahoo-statistics

**option 35:** show installed-systems

**option 36:** show interface  
sub-option 1: all  
sub-option 2: *interface\_number*

**option 37:** show ip-default-gateway

**option 38:** show ip-route-table

**option 39:** show ip-rts-table

**option 40:** 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 41:** show licenses

**option 42:** show netbios

**option 43:** show ntp

**option 44:** show policy

sub-option 1: [listing]

sub-option 2: [order]

sub-option 3: [proxy-default]

**option 45:** show profile

**option 46:** show realms

**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 security

sub-option 1: [local-user-list [*local\_user\_list\_name*]

sub-option 2: [local-user-list-group *local\_user\_list\_name group\_name*]

sub-option 3: [local-user-list-user *local\_user\_list\_name user\_name*]

**option 52:** 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 53:** show sessions

**option 54:** show snmp

**option 55:** show socks-gateways

**option 56:** show socks-machine-id

**option 57:** show socks-proxy

**option 58:** 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 59:** show splash-generator

**option 60:** show ssl

- sub-option 1: ccl [*list\_name*]
- sub-option 2: ssl-client [*ssl\_client*]

**option 61:** show static-routes

**option 62:** show status

**option 63:** 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 64:** show tcp-rtt

**option 65:** show telnet-management

**option 66:** show terminal

**option 67:** show timezones

**option 68:** show user-authentication

**option 69:** show version

**option 70:** show virtual-ip

**option 71:** show wccp

- sub-option 1: configuration
- sub-option 2: statistics

Table 3.90: # (config) show

accelerated-pac		Displays the current accelerated PAC settings.
access-log	[default-logging]	Displays the current access log settings.
	[format {[brief]   [format_name]}]	Displays access log default policy.
	[log {[brief]   [log_name]}]	Displays access log configuration.
	[statistics [log_name]]	Displays access log statistics.
archive-configuration		Displays archive configuration settings.
arp-table		Displays ARP information.
bandwidth-gain		Displays the current bandwidth-gain commands.
bridge	configuration [bridge_name]	Displays bridge configuration.
	fwtable bridge_name	Displays bridge forward table.
	statistics bridge_name	Displays bridge statistics.
bypass-list		Displays the current bypass list.
caching		Displays the current caching settings.
clock		Displays the current ProxySG time setting.
commands	[delimited {[all]   [privileged]}]	Displays commands in a format for parsing.
	[formatted {[all]   [privileged]}]	Displays commands in a format for viewing.
configuration	[brief]	Displays configuration without inline expansion.
	[expanded]	Displays configuration with inline expansion.
	[noprompts]	Displays configuration without "--More--" prompts.
content	outstanding-requests {[deletes]   [revalidates]   [priority]}	Displays outstanding distribution and revalidation requests, priority deletion policies, content management statistics, or cached object information.
	priority {[regex regex]   [url url]}	
	statistics	
	url url	
content-distribution		Displays the sizes of objects in the cache.
content-filter	smartfilter   surfcontrol   status   websense	Displays the current content filter settings.
cpu		Displays CPU usage.
diagnostics	service-info   status   snapshot snapshot_name	Displays the remote diagnostics commands.

Table 3.90: # (config) show (Continued)

disk	<i>disk_number</i>   all	Displays disk status and information.
dns		Displays DNS servers and name imputing settings.
download-paths		Displays the current downloaded configuration paths.
dynamic-bypass		Displays the current dynamic bypass configuration settings.
efficiency		Displays efficiency statistics.
environmental		Displays environmental information.
event-log		Displays the current event log settings.
exceptions	[ <i>exception_id</i> ]   [ <i>user_defined_exception_id</i> ] ]	Displays exception definitions.
external-services	[ <i>statistics</i> ]	Displays external services or external services statistics information.
failover	configuration [ <i>group_address</i> ]   statistics	Displays failover settings.
forwarding		Displays the current forwarding settings.
health-checks		Displays health check information.
hostname		Displays the current hostname.
http		Displays HTTP settings.
http-stats		Displays HTTP statistics.
icp-settings		Displays ICP settings.
identd		Displays IDENTD service settings.
im	aol-statistics   configuration   msn-statistics   yahoo-statistics	Displays IM information.
installed-systems		Displays SGOS versions available on the ProxySG.
interface	all   <i>interface_number</i>	Displays interface status and configuration information.
ip-default-gateway		Displays the IP address of the default gateway.
ip-route-table		Displays route table information.
ip-rts-table		Displays return-to-sender route table information.

Table 3.90: # (config) show (Continued)

ip-stats	all	Displays all TCP/IP statistics.
	e#	Displays TCP/IP statistics for ethernet interface 0 - 7.
	ip	Displays IP specific statistics.
	memory	Displays TCP/IP memory statistics.
	summary	Displays TCP/IP summary statistics.
	tcp	Displays TCP specific statistics.
	udp	Displays UDP specific statistics.
licenses		Displays produce license information.
netbios		Displays NETBIOS settings.
ntp		Displays NTP servers and information.
policy	[listing]	Displays the results of the policy load.
	[order]	Displays the policy evaluation order.
	[proxy-default]	Displays the proxy default policy.
profile		Displays the system profile.
realms		Displays current authentication realms.
resources		Displays allocation of system resources.
restart		Displays system restart settings.
return-to-sender		Displays "return to sender" settings.
rip	parameters   routes   statistics	Displays RIP settings.
security	[local-user-list local_user_list_name]	Displays security settings.
	[local-user-list-group local_user_list_name group_name]	
	[local-user-list-user local_user_list_name user_name]	
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 services settings.
sessions		Displays information about Telnet connections.
snmp		Displays SNMP statistics.
socks-gateways		Displays SOCKS gateway settings.
socks-machine-id		Displays the SOCKS machine ID.
socks-proxy		Displays SOCKS proxy settings.

Table 3.90: # (config) show (Continued)

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.
splash-generator		Displays splash generator commands.
ssl	ccl [ <i>list_name</i> ]	Displays information regarding CA certificate lists.
	ssl-client [ <i>ssl_client</i> ]	Displays information regarding the SSL-client.
static-routes		Displays static route table information.
status		Displays current system status.
streaming	configuration	Displays streaming configuration.
	quicktime {configuration   statistics}	Displays QuickTime streaming.
	real-media {configuration   statistics}	Displays Real Media streaming.
	statistics	Displays streaming statistics.
	windows-media {configuration   statistics}	Displays Windows Media streaming.
tcp-rtt		Displays default TCP Round Trip Time.
telnet-management		Displays Telnet management status.
terminal		Displays terminal configuration parameters and subcommands.
timezones		Displays timezones used.
user-authentication		Displays user authentication information.
version		Displays system hardware and software status.
virtual-ip		Displays the current virtual IP settings.
wccp	configuration   statistics	Displays the current WCCP configuration.

**Example**

```
SGOS# (config) show bypass-list
TCP/IP Bypass List Information
Destination  Mask  Source  Mask  Gateway  Interface  Life(secs)  UseCount
```

**#(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 3.91: #(config snmp)

authorize-traps		Enables SNMP authorize traps.
disable		Disables SNMP for the ProxySG.
enable		Enables SNMP for the ProxySG.
encrypted-read-community	<i>encrypted_password</i>	Specifies encrypted read community string.
encrypted-trap-community	<i>encrypted_password</i>	Specifies encrypted trap community string.

Table 3.91: # (config snmp) (Continued)

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\_domain SOCKS\_port* [version=(4|5 [user=*user\_name* password=*password*])]
- option 2:** delete {all | gateway *gateway\_alias*}
- option 3:** edit *gateway\_alias*—changes the prompt (see“#(config socks-gateways) edit *gateway\_alias*” on page 193)
- 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 3.92: #(config socks-gateways)

create	<i>gateway_alias gateway_domain SOCKS_port</i> [version=(4 5 [user= <i>user_name</i> password= <i>password</i> ])]	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 193.
exit		Exits configure socks-gateways mode and returns to configure mode.
failure-mode	closed   open	Sets the failure mode to open or closed.
no path		Clears network path to download SOCKS gateway settings.
path	<i>url</i>	Specifies the network path to download SOCKS gateway settings.

Table 3.92: # (config socks-gateways) (Continued)

sequence	add <i>gateway_alias</i>	Adds an alias to the end of the default failover sequence.
	clear	Clears the default failover sequence.
	demote <i>gateway_alias</i>	Demotes an alias one place towards the end of the default failover sequence.
	promote <i>gateway_alias</i>	Promotes an alias one place towards the start of the default failover sequence.
	remove <i>gateway_alias</i>	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:** user

**option 7:** version

**option 8:** view

Table 3.93: # (config socks-gateways gateway\_alias)

exit		Exits configure socks-gateways <i>gateway_alias</i> mode and returns to configure socks-gateways mode.
host	<i>gateway_host</i>	Changes the host name.
no	password   user	Optional, and only if you use version 5. Deletes the version 5 password or username.
password	<i>password</i>	Optional, and only if you use version 5. Changes the version 5 password.
port	<i>socks_port</i>	Changes the SOCKS port.
user	<i>user_name</i>	Optional, and only if you use version 5. Changes the version 5 username.
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**

**option 1:** socks-machine-id *machine\_id*

Table 3.94: # (config) socks-machine-id

<i>machine_id</i>		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, 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-proxyaccept-timeout *seconds*

**option 2:** socks-proxyconnect-timeout *seconds*

**option 3:** socks-proxymax-connections *num\_connections*

**option 4:** socks-proxymax-idle-timeout *seconds*

**option 5:** socks-proxymin-idle-timeout *seconds*

Table 3.95: #(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>	Sets maximum SOCKS client idle time threshold.
min-idle-timeout	<i>seconds</i>	Sets minimum SOCKS client idle time threshold.

### Example

```
SGOS#(config) socks-proxy accept-timeout 120
ok
```

## #(config) splash-generator

Use this command to display a custom message page, or *splash page*, to a user the first time he or she starts the client browser. Subsequent URL requests from the client then provide the user with the requested content.

### Syntax

```
splash-generator
```

This changes the prompt to:

SGOS#(config splash-generator)

**- subcommands-**

**option 1:** cluster

- sub-option 1: disable
- sub-option 2: enable
- sub-option 3: peer-ip 1 - 5 ip\_address
- sub-option 4: sdp-port port

**option 2:** disable

**option 3:** enable

**option 4:** exit

**option 5:** protocol {tacacs | radius}

**option 6:** radius

- sub-option 1: acct-listen-port port
- sub-option 2: auth-listen-port port
- sub-option 3: encrypted-secret-key key
- sub-option 4: forwarding {disable | ip-spoof | proxy-state}
- sub-option 5: no secret-key
- sub-option 6: secret-key key

**option 7:** tacacs

- sub-option 1: encrypted-secret-key key
- sub-option 2: forwarding {disable | enable}
- sub-option 3: listen-port port
- sub-option 4: multi-session {disable | enable}
- sub-option 5: no {all-servers | one-server IP\_address [port] | secret-key}
- sub-option 6: server IP\_address [port]
- sub-option 7: secret-key key

**option 8:** timeout seconds

**option 9:** view

Table 3.96: #(config splash-generator)

cluster	disable	Disables splash-generator cluster support.
	enable	Enables splash-generator cluster support.
	peer-ip {1 - 5 ip_address}	Indicates the cluster peer address.
	sdp-port port	Indicates the Session Distributor Protocol port.
disable		Disables the splash generator.
enable		Enables the splash generator.
exit		Exits configure splash generator mode and returns to configure mode.

Table 3.96: # (config splash-generator) (Continued)

protocol	tacacs	Indicates that the TACACS+ protocol should be used.
	radius	Indicates that the RADIUS protocol should be used.
radius	acct-listen-port <i>port</i>	Listens for incoming RADIUS accounting requests on the port indicated by <i>port</i> .
	auth-listen-port <i>port</i>	Listens for incoming RADIUS authorization requests on the port indicated by <i>port</i> .
	encrypted-secret-key <i>encrypted-key</i>	Sets the encrypted secret key to <i>encrypted-key</i> .
	forwarding {disable   ip-spoof   proxy-state}	Disables forwarding of RADIUS requests, or enables forwarding of RADIUS packets using IP spoofing, or enables forwarding of RADIUS packets using proxy state.
	no secret key	Sets the MD5 secret key to an empty string.
	secret-key <i>key</i>	Sets the MD5 secret key to <i>key</i> .
tacacs	encrypted-secret-key <i>encrypted-key</i>	Sets the encrypted secret key to <i>encrypted-key</i> .
	forwarding {disable   enable}	Disables or enables forwarding of TACACS+ requests.
	listen-port <i>port</i>	Listens for incoming TACACS+ requests on the port indicated by <i>port</i> .
	multi-session {disable   enable}	Disables or enables multiple TACACS+ sessions capability.
	no all-servers	Removes all TACACS+ server entries.
	no one-server <i>ip_address</i> [ <i>port</i> ]	Removes the TACACS+ server entry indicated by <i>IP_address</i> .
	no secret-key	Sets the secret key to an empty string.
	server <i>ip_address</i> [ <i>port</i> ]	Adds the server indicated by <i>IP_address</i> to the TACACS+ server list.
	secret-key <i>key</i>	Sets the secret key to <i>key</i> .
timeout	<i>seconds</i>	Indicates the splash timeout in seconds.

**Example**

```

SGOS#(config) splash-generator
SGOS#(config splash-generator) enable
ok
SGOS#(config splash-generator) protocol radius
ok
SGOS#(config splash-generator) exit
SGOS#(config)

```

## #(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 {no-show | 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: keyring *keyring\_id*

sub-option 5: signing-request *keyring\_id*

sub-option 6: 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 200)

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 201)

**option 4:** exit

**option 5:** import

sub-option 1: ca-certificate *name*

sub-option 2: certificate *keyring\_id*

sub-option 3: keyring {no-show | show} *keyring\_id*

```

sub-option 4: signing-request keyring_id
option 6: show ssl
sub-option 1: ccl [list_name]
sub-option 2: ssl-client [ssl_client]
option 7: ssl-nego-timeout seconds
option 8: view
sub-option 1: ca-certificate name
sub-option 2: ccl
sub-option 3: certificate keyring_id
sub-option 4: keypair {des | des3 | unencrypted} keyring_id | keyring_id
sub-option 5: keyring [keyring_id]
sub-option 6: signing-request keyring_id
sub-option 7: ssl-client
sub-option 8: ssl-nego-timeout
sub-option 9: summary ca-certificate [name]

```

Table 3.97: #(config ssl)

create	ccl <i>list_name</i>	Creates a list to contain CA certificates.
	certificate <i>keyring_id</i>	Creates a certificate. Certificates can be associated with a keyring.
	keyring {no-show   show} <i>keyring_id</i> [ <i>key_length</i> ]	Creates a keyring, with a keypair. The show   no-show option indicates whether the keypair is viewable.
	signing-request <i>keyring_id</i>	Creates a certificate signing request. The request must be associated with a keyring.
	ssl-client <i>ssl_client_name</i>	Associates the SSL client with a keyring. Only the default is permitted.
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.
	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 the SSL client.
edit	ccl <i>list_name</i>	Changes the prompt. See“#(config ssl) edit ccl <i>list_name</i> ”on page 200.
	ssl-client <i>ssl_client_name</i>	Changes the prompt. See“#(config ssl) edit ssl-client <i>ssl_client_name</i> ”on page 201.
exit		Exits configure ssl mode and returns to configure mode.

Table 3.97: # (config ssl) (Continued)

import	ca-certificate <i>name</i>	Imports CA certificates.
	certificate <i>keyring_id</i>	Imports certificates.
	keyring {no-show   show} <i>keyring_id</i>	Imports keyrings.
	signing-request <i>keyring_id</i>	Imports signing requests.
show ssl	ccl [ <i>list_name</i> ]	Shows running system information about CA certificate lists.
	ssl-client [ <i>ssl_client</i> ]	Shows running system information about ssl clients.
ssl-nego-timeout	<i>seconds</i>	Configures SSL negotiation timeout period.
view	ca-certificate <i>name</i>	Displays Certificate Authority certificate.
	ccl	Displays CA certificate lists.
	certificate <i>keyring_id</i>	Displays certificate.
	keypair {des   des3   unencrypted} <i>keyring_id</i>   <i>keyring_id</i>	Displays keypair.
	keyring [ <i>keyring_id</i> ]	Displays keyring.
	signing-request <i>keyring_id</i>	Displays certificate signing request.
	ssl-client	Displays summary information of SSL clients.
	ssl-nego-timeout	Displays SSL negotiation timeout period status summary.
	summary ca-certificate [ <i>name</i> ]	Displays summary certificate commands.

**Examples:**

```

SGOS#(config) ssl
SGOS#(config ssl) create keyring show | no-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 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:** exit

**option 3:** remove *ca\_certificate\_name*

**option 4:** view

Table 3.98: #(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.)
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:** ciphersuite

**option 2:** exit

**option 3:** keyring-id *keyring\_id*

**option 4:** protocol *ssl2* | *ssl3* | *tlsv1* | *ssl2v3* | *ssl2tlsv1* | *ssl3tlsv1* | *ssl2v3tlsv1*

**option 5:** view

**Table 3.99:** #(config ssl *ssl\_default\_client\_name*)

ciphersuite		Configures SSL client cipher suites.
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>ssl2</i>   <i>ssl3</i>   <i>tlsv1</i>   <i>ssl2v3</i>   <i>ssl2tlsv1</i>   <i>ssl3tlsv1</i>   <i>ssl2v3tlsv1</i>	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) ciphersuite
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:

```
10.63.0.0255.255.0.010.63.158.213
10.64.0.0255.255.0.010.63.158.213
10.65.0.0255.255.0.010.63.158.226
```

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 3.100: `#(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 *kpbs*  
 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 3.101:** #(config) streaming

max-client-bandwidth	<i>kbps</i>	Sets the maximum client bandwidth permitted to <i>kbps</i> .
max-gateway-bandwidth	<i>kbps</i>	Sets the maximum gateway bandwidth permitted to <i>kbps</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.

Table 3.101: #(config) streaming (Continued)

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>kbps</i>	Sets the maximum connections allowed.
	max-connections <i>number</i>	Sets the maximum client bandwidth allowed.
	max-gateway-bandwidth <i>kbps</i>	Sets the maximum gateway bandwidth allowed.
	no {max-client-bandwidth   max-connections   max-gateway-bandwidth}	Negates QuickTime parameters.
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 3.101: #(config) streaming (Continued)

windows-media	<code>asx-rewrite <i>number in_addr</i> <i>cache_proto cache_addr</i> [<i>cache_port</i>]</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 3.101: #(config) streaming (Continued)

windows-media, continued	broadcast-alias <i>alias url</i> <i>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: <i>yyyy-mm-dd</i> <i>today</i> <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: <i>hh:mm</i> <i>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.</i>
	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.
	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> .
	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> .

Table 3.101: #(config) streaming (Continued)

windows-media, continued	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   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} <i>cache_ip_address</i>	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.
	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 <code>unicast-alias</code> command to request the content from the origin streaming server.

Table 3.101: #(config) streaming (Continued)

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 <code>mmst</code> , <code>mmsu</code> , or <code>http</code> . If the protocol is <code>mms</code> , 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. Because TCP-IP is an advanced command, you might need to use the `(config) reveal-advanced tcp-ip` command in order to access the TCP-IP commands. See "`#(config) reveal-advanced`" on page 140 for more information.

## Syntax

**option 1:** `tcp-ip icmp-bcast-echo`

**option 2:** `tcp-ip icmp-tstamp-echo`

**option 3:** `tcp-ip ip-forwarding {disable | enable}`

**option 4:** `tcp-ip no {icmp-bcast-echo | icmp-tstamp-echo | rfc-1323 | tcp-newreno}`

**option 5:** `tcp-ip rfc-1323`

**option 6:** `tcp-ip tcp-newreno`

**option 7:** `tcp-ip window-size window_size`

Table 3.102: #(config) tcp-ip

<code>icmp-bcast-echo</code>		Enables ICMP broadcast echo responses.
<code>icmp-tstamp-echo</code>		Enables ICMP timestamp echo responses.
<code>ip-forwarding</code>	<code>disable   enable</code>	Enables or disables IP-forwarding.
<code>no</code>	<code>icmp-bcast-echo   icmp-tstamp-echo   rfc-1323   tcp-newreno</code>	Disables specified TCP-IP settings.
<code>rfc-1323</code>		Enables RFC-1323 support (satellite communications).
<code>tcp-newreno</code>		Enables NewReno support (improved fast recovery).
<code>window-size</code>	<code><i>window_size</i></code>	Specifies TCP window size for satellite communications.

### Example

```
SGOS#(config) tcp-ip ip-forwarding enable
ok
SGOS#(config) tcp-ip rfc-1323
ok
SGOS#(config) tcp-ip no icmp-bcast-echo
ok
```

## #(config) tcp-rtt

Use this command to configure the number of TCP round trip time ticks.

### Syntax

`tcp-rtt num_500ms_ticks`

Table 3.103: #(config) tcp-rtt

<code><i>num_500ms_ticks</i></code>		Indicates the default TCP Round Trip Time in ticks.
-------------------------------------	--	---

*Example*

```
SGOS#(config) tcp-rtt 500
ok
```

 **#(config) telnet-management**

Enables or disables the ability to configure SSHD through Telnet.

**Syntax**

**option 1:** telnet-management allow-sshd-config

**option 2:** telnet-management deny-sshd-config

Table 3.104: #(config) telnet-management

allow-sshd-config		Enables configuring of SSHD through Telnet.
deny-sshd-config		Disables configuring of SSHD through Telnet.

*Example*

```
SGOS#(config) telnet allow-sshd-config
ok
```

 **#(config) timezone**

Use this command to set the local time zone on the ProxySG.

**Syntax**

```
timezone timezone_num
```

Table 3.105: #(config) timezone

timezone_num		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 3.106: #(config) upgrade-path

<code>url</code>		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 3.107: #(config) virtual-ip

<code>address</code>	<code>ip_address</code>	Specifies the virtual IP to add.
<code>clear</code>		Removes all virtual IP addresses.
<code>no address</code>	<code>ip_address</code>	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 ProxySG 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 3.108: # (config) wccp

disable		Disables WCCP.
enable		Enables WCCP.
no path		Negates certain WCCP settings.
path	<i>url</i>	Specifies the network path from which to download WCCP settings.

**Example**

```
SGOS#(config) wccp path 10.25.36.47/files/wccp.txt  
ok
```

