Blue Coat® Systems SG™ Appliance

Volume 1: Getting Started

SGOS Version 5.2.2

Blue Coat

Contact Information

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

http://www.bluecoat.com/support/contact.html

bcs.info@bluecoat.com
http://www.bluecoat.com

For concerns or feedback about the documentation: documentation@bluecoat.com

Document Number: 231-02838
Document Revision: SGOS 5.2.2—09/2007

Third Party Copyright Notices

Blue Coat Systems, Inc. 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 Gillogly.

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.

This work also contains materials derived from public sources.

Additional Information about OpenLDAP can be obtained at:

http://www.openldap.org/

or by sending e-mail to:

info@OpenLDAP.org

Portions Copyright (c) 1992-1996 Regents of the University of Michigan.

All rights reserved.

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided ``as is'' without express or implied warranty.

The OpenLDAP Public License

Version 2.0.1, 21 December 1999

Copyright 1999, The OpenLDAP Foundation, Redwood City, California, USA.

All Rights Reserved.

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. Redistributions must also contain a copy of this document.

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. The name "OpenLDAP" must not be used to endorse or promote products derived from this Software without prior written permission of the OpenLDAP Foundation. For written permission, please contact foundation@openldap.org.

4. Products derived from this Software may not be called "OpenLDAP" nor may "OpenLDAP" appear in their names without prior written permission of the OpenLDAP Foundation. OpenLDAP is a trademark of the OpenLDAP Foundation.

5. Due credit should be given to the OpenLDAP Project

(http://www.openldap.org/.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND 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 OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT,

INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT 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.

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

==========

Copyright (c) 1998-2000 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.

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).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@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 aheared 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).

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 (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the rouines 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)"

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

[end of copyrights and licenses for Novell's LDAP Libraries for C]

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.

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 (eay@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:eay@cryptsoft.com> and Tim J. Hudson <mailto:tjh@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 (eay@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).

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.

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.

The SG Client software is based in part on the work of the Independent JPEG Group

The SG Client software is based in part on the work of the FreeType Project (www.freetype.org)

The SG Client software is based in part on the work of Chris Maunder and info-zip

LEGAL ISSUES
============

In plain English:

1. We don't promise that this software works. (But if you find any bugs, please let us know!)

2. You can use this software for whatever you want. You don't have to pay us.

3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-1998, Thomas G. Lane. All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation. (2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group". (3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software. (Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.) So far as we are aware, there are no patent restrictions on the remaining code.

The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that "The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

The FreeType Project LICENSE

2006-Jan-27

Copyright 1996-2002, 2006 by David Turner, Robert Wilhelm, and Werner Lemberg

Introduction

=========

The FreeType Project is distributed in several archive packages; some of them may contain, in addition to the FreeType font engine, various tools and contributions which rely on, or relate to, the FreeType Project.

This license applies to all files found in such packages, and which do not fall under their own explicit license. The license affects thus the FreeType font engine, the test programs, documentation and makefiles, at the very least.

This license was inspired by the BSD, Artistic, and IJG (Independent JPEG Group) licenses, which all encourage inclusion and use of free software in commercial and freeware products alike. As a consequence, its main points are that:

o We don't promise that this software works. However, we will be interested in any kind of bug reports. (`as is' distribution)

o You can use this software for whatever you want, in parts or full form, without having to pay us. (`royalty-free' usage)

o You may not pretend that you wrote this software. If you use it, or only parts of it, in a program, you must acknowledge somewhere in your documentation that you have used the FreeType code. (`credits')

We specifically permit and encourage the inclusion of this software, with or without modifications, in commercial products. We disclaim all warranties covering The FreeType Project and assume no liability related to The FreeType Project.

Finally, many people asked us for a preferred form for a credit/disclaimer to use in compliance with this license. We thus encourage you to use the following text:

“Portions of this software are copyright (c) 2007The FreeType Project (www.freetype.org). All rights reserved."

Legal Terms

=========

0. Definitions

Throughout this license, the terms `package', `FreeType Project', and `FreeType archive' refer to the set of files originally distributed by the authors (David Turner, Robert Wilhelm, and Werner Lemberg) as the `FreeType Project', be they named as alpha, beta or final release.

`You' refers to the licensee, or person using the project, where `using' is a generic term including compiling the project's source code as well as linking it to form a `program' or `executable'. This program is referred to as `a program using the FreeType engine'.

This license applies to all files distributed in the original FreeType Project, including all source code, binaries and documentation, unless otherwise stated in the file in its original, unmodified form as distributed in the original archive. If you are unsure whether or not a particular file is covered by this license, you must contact us to verify this.

The FreeType Project is copyright (C) 1996-2000 by David Turner, Robert Wilhelm, and Werner Lemberg. All rights reserved except as specified below.

1. No Warranty

THE FREETYPE PROJECT IS PROVIDED `AS IS' WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL ANY OF THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY DAMAGES CAUSED BY THE USE OR THE INABILITY TO USE, OF THE FREETYPE PROJECT.

2. Redistribution

This license grants a worldwide, royalty-free, perpetual and irrevocable right and license to use, execute, perform, compile, display, copy, create derivative works of, distribute and sublicense the FreeType Project (in both source and object code forms) and derivative works thereof for any purpose; and to authorize others to exercise some or all of the rights granted herein, subject to the following conditions:

o Redistribution of source code must retain this license file (`FTL.TXT') unaltered; any additions, deletions or changes to the original files must be clearly indicated in accompanying documentation. The copyright notices of the unaltered, original files must be preserved in all copies of source files.

o Redistribution in binary form must provide a disclaimer that states that the software is based in part of the work of the FreeType Team, in the distribution documentation. We also encourage you to put an URL to the FreeType web page in your documentation, though this isn't mandatory.

These conditions apply to any software derived from or based on the FreeType Project, not just the unmodified files. If you use our work, you must acknowledge us. However, no fee need be paid to us.

3. Advertising

Neither the FreeType authors and contributors nor you shall use the name of the other for commercial, advertising, or promotional purposes without specific prior written permission.

We suggest, but do not require, that you use one or more of the following phrases to refer to this software in your documentation or advertising materials: `FreeType Project', `FreeType Engine', `FreeType library', or `FreeType Distribution'.

As you have not signed this license, you are not required to accept it. However, as the FreeType Project is copyrighted material, only this license, or another one contracted with the authors, grants you the right to use, distribute, and modify it. Therefore, by using, distributing, or modifying the FreeType Project, you indicate that you understand and accept all the terms of this license.

4. Contacts

There are two mailing lists related to FreeType:

o freetype@nongnu.org

Discusses general use and applications of FreeType, as well as future and wanted additions to the library and distribution. If you are looking for support, start in this list if you haven't found anything to help you in the documentation.

o freetype-devel@nongnu.org

Discusses bugs, as well as engine internals, design issues, specific licenses, porting, etc.

Our home page can be found at http://www.freetype.org

=====================

`zip.cpp`—which is used by the Data Collector utility included in the SG Client software—is almost entirely based upon code by info-zip. It has been modified by Lucian Wischik. The modifications were a complete rewrite of the bit of code that generates the layout of the zipfile, and support for zipping tofrom memory or handles or pipes or pagefile or diskfiles, encryption, unicode.

The original code may be found at http:www.info-zip.org. The original copyright text follows.

This is version 1999-Oct-05 of the Info-ZIP copyright and license.

The definitive version of this document should be available at ftp:ftp.cdrom.compubinfoziplicense.html indefinitely.

Copyright (c) 1990-1999 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Christian Spieler, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

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

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

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

Written by Chris Maunder (cmaunder@mail.com) Copyright (c) 1998-2003.

This code may be used in compiled form in any way you desire. This file may be redistributed unmodified by any means PROVIDING it is not sold for profit without the authors written consent, and providing that this notice and the authors name is included. If the source code in this file is used in any commercial application then acknowledgement must be made to the author of this file (in whatever form you wish).

This file is provided "as is" with no expressed or implied warranty. The author accepts no liability for any damage caused through use.

Contents

Chapter 1: About Getting Started

Volume 1: Getting Started describes how to access the Blue Coat SG appliance using the CLI or Management Console, and provides basic configuration information that is required in every environment.

About This Book

This book deals with the following topics:

Document Conventions

The following section lists the typographical and Command Line Interface (CLI) syntax conventions used in this manual.

Table 1-1. Document Conventions

Conventions	Definition
Italics	The first use of a new or Blue Coat-proprietary term.
`Courier font`	Command line text that appears on your administrator workstation.
`Courier Italics`	A command line variable that is to be substituted with a literal name or value pertaining to the appropriate facet of your network system.
`Courier Boldface`	A Blue Coat literal to 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.

Chapter 2: Licensing

This chapter describes the SG appliance licensing behavior.

About Licensing

SGOS 5.x features a global licensing system for the SGOS software. License key files are issued on a per-appliance basis. One license key file includes all of the component licenses for whichever SGOS features you have elected to use.

Note: When your Blue Coat appliance order was completed, you received an e-mail that contained serial numbers for licensable components. Those numbers are required for the procedures in this chapter.

Licensable Components

There are three types of licensable components:

- Required—The **SGOS 5 Base**; these features are required on the SG appliance.
- Included—Additional SGOS 5.x features, which are provided by Blue Coat and that are included in the SGOS 5 base license.
- Optional— Any additional (purchased) features.

When the license key file is created, it contains components of all three types. The following table lists the SG appliance licensable components, categorized by type.

Table 2-1. Licensable Components

Type	Component	Description
Required	SGOS 5 Base	The SG appliance operating system, plus base features: HTTP, FTP, TCP-Tunnel, SOCKS, and DNS proxy.
Included	3rd Party Onbox Content Filtering	Allows use with third-party vendor databases: Intersafe, Optenet, Proventia, SmartFilter, SurfControl, Websense, and Webwasher.
Included	Websense Offbox Content Filtering	For Websense off-box support only.
Included	ICAP Services	External virus and content scanning with ICAP servers.
Included	Bandwidth Management	Allows you to classify, control, and, if required, limit the amount of bandwidth used by different classes of network traffic flowing into or out of the SG appliance.
Included	Windows Media	MMS and RTSP proxy for Windows Media content; content caching and splitting. Full policy control over MMS and RTSP traffic for Windows Media content. When the maximum concurrent streams is reached, all subsequent streams are denied and the client receives a message.

Table 2-1. Licensable Components (Continued)

Type	Component	Description
Included	Real Media	RTSP proxy for Real Media content; content caching and splitting. Full policy control over RTSP traffic for Real Media content. When the maximum concurrent streams is reached, all subsequent streams are denied and the client receives a message.
Included	Apple QuickTime	RTSP proxy for QuickTime content; no caching or splitting; content pass-through. Full policy control over RTSP traffic for QuickTime content.
Included	Netegrity SiteMinder	Allows realm initialization and user authentication to SiteMinder servers.
Included	Oracle COREid	Allows realm initialization and user authentication to COREid servers.
Included	Peer-to-Peer	Allows you to recognize and manage peer-to-peer P2P activity relating to P2P file sharing applications.
Included	HTTP Compression	Allows reduction to file sizes without losing any data.
Optional	SSL (Native SSL Proxy and Reverse HTTPs Proxy, also called SSL Termination)	Native SSL proxy and Reverse HTTPS Proxy (SSL termination) on the SG appliance. You must also purchase an SSL accelerator card to enable SSL termination.
Optional	IM	AOL Instant Messaging: AIM proxy with policy support for AOL Instant Messenger. MSN Instant Messaging: MSN proxy with policy support for MSN Instant Messenger. Yahoo Instant Messaging: Yahoo proxy with policy support for Yahoo Instant Messenger.
Optional	SG Client—Acceleration	Entitles you to support a certain number of SG Clients in your enterprise; however, the license does not limit the number of ADN tunnels to which clients can have access. SG Client licenses are upgradeable so you can support a larger number of users. **Note**: Only the appliance designated as the SG Client Manager requires a license. To use SG Clients in your enterprise, apply the license only to the Client Manager and not to any other appliances in the ADN network.

About the Trial Period

Blue Coat provides a trial period, enabled by default. During initial configuration of new hardware, you can specify an edition of SGOS to run during the trial period. The SG appliance can run either the MACH5 or Proxy Edition of SGOS during the trial period.

Note: If you select Proxy Edition for the trial period but you purchase a MACH5 Edition license, the SG appliance configuration is reset when you install the license. Note also that a few defaults—default proxy policy, trust destination IP address, and tolerating HTTP requests—differ between the two editions.

The initial system boot-up triggers the 60-day trial; during this time you can evaluate the SGOS functionality. For the first 60 days, all licensable components for the trial edition you chose are active and available to use. When a license or demo license is installed during the trial period, components previously available in the trial period, but not part of that license, remain available and active for the remainder of the trial period. However, if the license edition is different than the trial edition you selected, only functionality available in the edition specified in the license remains available for trial.

Each time you navigate to the Management Console License Warning page, you see a text message that identifies the expiration date of your trial period; the **Maintenance > Licensing > View** tab shows the license components with expiration dates. If you require more time to explore the SGOS features, a demo license is available; refer to your reseller or contact Blue Coat Sales.

In the trial period, the Base SGOS user limit is unlimited. When a full license is installed, any user limits imposed by that license are enforced, even if the trial period is still valid.

Disabling the Components Running in Trial Period

You have the option to not let users access features that are currently running in trial period; however, you cannot selectively disable trial period features. You must either enable all of them or disable all of them.

To disable trial period components:

1. On the **View License** tab, select **Disable** in the **Trial Components are enabled** field.
2. Click **Apply**.
3. Click **Refresh Data**. All licenses that are in trial period switch from **Yes** to **No**. Users cannot use these features, and no dialogs warning of license expiration are sent.

Also notice that this option text changes to **Trial Components are disabled: Enabled**. Repeat this process to re-enable trial licenses.

About License Expiration

At the end of the trial or demo period or, subsequently, when any normally licensed component expires, components that have not been licensed do not process requests. A license expiration notification message is logged in the Event Log (refer to the Event log information in *Volume 8: Managing the Blue Coat SG Appliance* for details).

If a license expires, users might not receive notification, depending upon the application they are using. Notifications do occur for the following:

- HTTP (Web browsers)—An HTML page is displayed stating the license has expired.
- SSL—An exception page appears when an HTTPS connection is attempted.
- Instant Messaging clients—Users do not receive a message that the license has expired. Any IM activity is denied, and to the user it appears that the logon connection has failed.

- FTP clients—If the FTP client supports it, a message is displayed stating the license has expired.
- Streaming media clients—If the Windows Media Player, RealPlayer, or QuickTime player version supports it, a message is displayed stating the license has expired.
- SG Client—After the trial license has expired, clients cannot connect to the ADN network.

You can still perform SGOS configuration tasks, CLI, SSH console, serial console, or Telnet connection. Although the component becomes disabled, feature configurations are *not* altered. Also, policy restrictions remain independent of component availability.

About the System Serial Number

Each SG serial number is the appliance identifier used to assign a license key file. The SG appliance contains an EEPROM with the serial number encoded. The appliance recognizes the serial number upon system boot-up.

The serial number is visible by navigating to **Configuration > General > Identification**.

Obtaining a WebPower Account

Before you can register your SG appliance and retrieve the license key, you must have a Blue Coat WebPower user account.

If you do not have a WebPower account or have forgotten your account information, use the following procedure.

To obtain a WebPower account:

1. Select **Maintenance > Licensing > Install**.
2. In the **License Administration** field, click **Register/Manage**. The License Configuration and Management Web page appears (ignore the dialog at this time).
3. Perform one of the following:

   To obtain a new account, click the link for **Need a WebPower User ID**. Enter the information as prompted.

   To obtain your current information for an existing account, click the **Forgot your password** link.

Registering and Licensing Blue Coat Hardware and Software

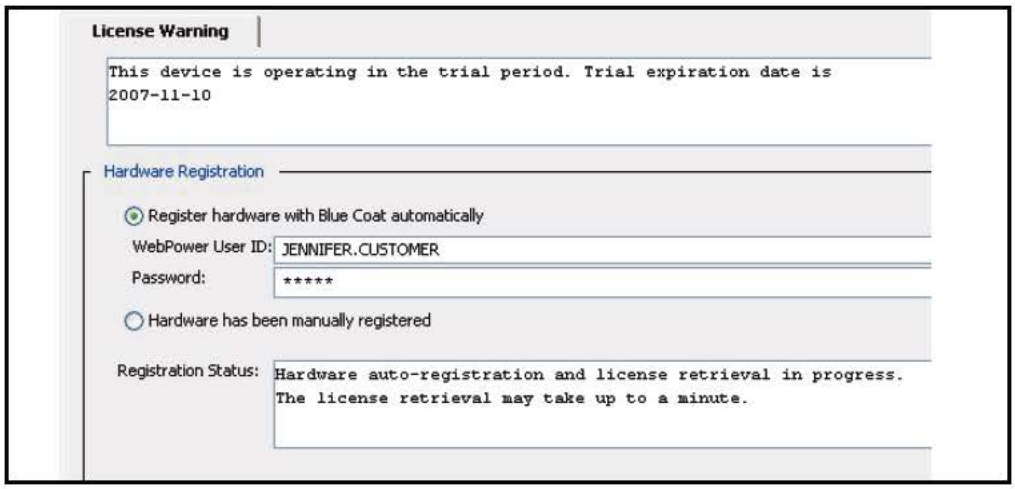
This section describes how to automatically register the hardware and software with Blue Coat.

- If you have not manually registered the hardware, you can automatically register the hardware and install the software license in one step. Continue with "To register the hardware and software" on page 25.
- If you have new hardware (SG210, SG510, SG810, SG 8100) that previously has been registered, the license is already associated with the hardware. Go to **Maintenance > Licensing > Install** and click **Retrieve** to obtain the license. For more information, see "To retrieve the software license:" on page 26.

- If you have older hardware that previously has been registered or if the SG appliance does not have Internet access, you can install the software license under **Maintenance > Licensing > Install**. For more information, see "Manual License Installation" on page 26.

To register the hardware and software

1. Open a browser and ensure pop-up blocking is disabled.
2. Enter the SGOS Management Console URL.
   `https://IP_address:8082`
3. Enter the access credentials specified during initial setup.
4. Click **Management Console**. The license warning/registration page displays.



5. Enter your WebPower credentials and click **Register Now**. It might take up for a minute for the Registration Status field to display the results.

6. Click **Continue**.
7. Select **Maintenance > Licensing > View**.

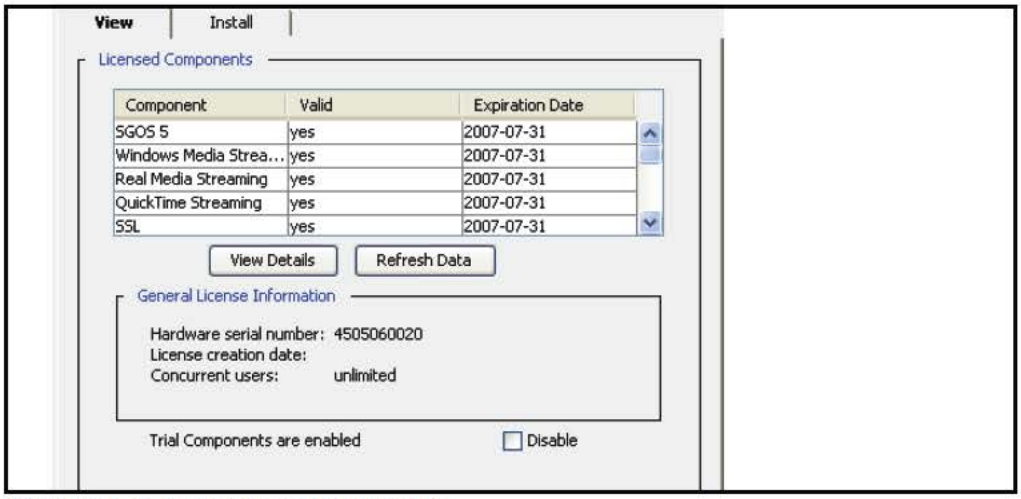


Figure 2-1. Viewing licensed components

Each licensable component is listed, along with its validity and its expiration date.

- To view the most current information, click **Refresh Data**.
- Highlight a license component and click **View Details**. A dialog displays with more detailed information about that component.
- If the trial period is enabled and you click **Maintenance > Licensing > View**, the Management Console displays a check box to disable the trial components. If the trial period is disabled, the Management Console displays a check box to enable the trial components.

Retrieving the License

If the SG appliance is a new system and the hardware has been registered, you can retrieve the associated license by completing the following steps:

To retrieve the software license:

1. Go to **Maintenance > Licensing > Install**.
2. Click **Retrieve**. The Request License Key dialog displays.
3. Enter your WebPower account login information.
4. Click **Send Request**. The Confirm License Install dialog displays.
5. Click **OK**.
6. Click **OK** when the **License Install Succeeded** message displays.
7. Click **Close** to close the Request License Key dialog.

Manual License Installation

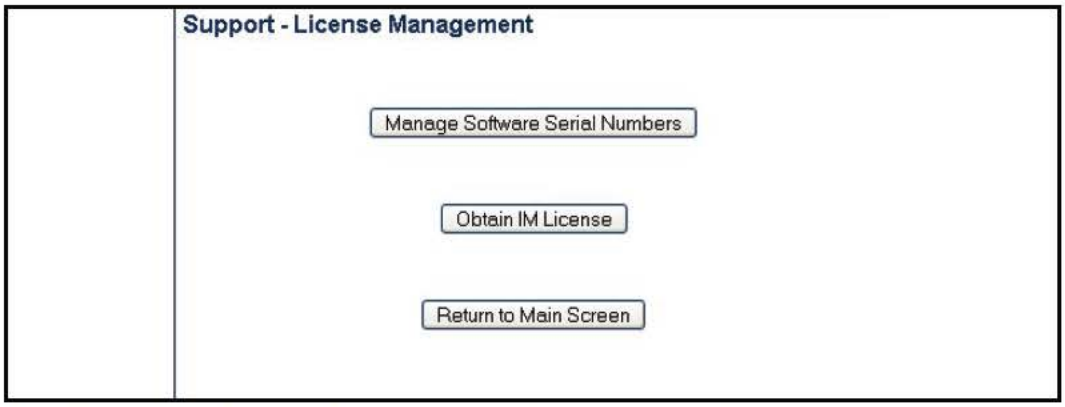
You might need to use manual license installation if:

- The SG appliance serial number is not associated with a software license (you have registered the hardware separately)
- The SG appliance does not have Internet access

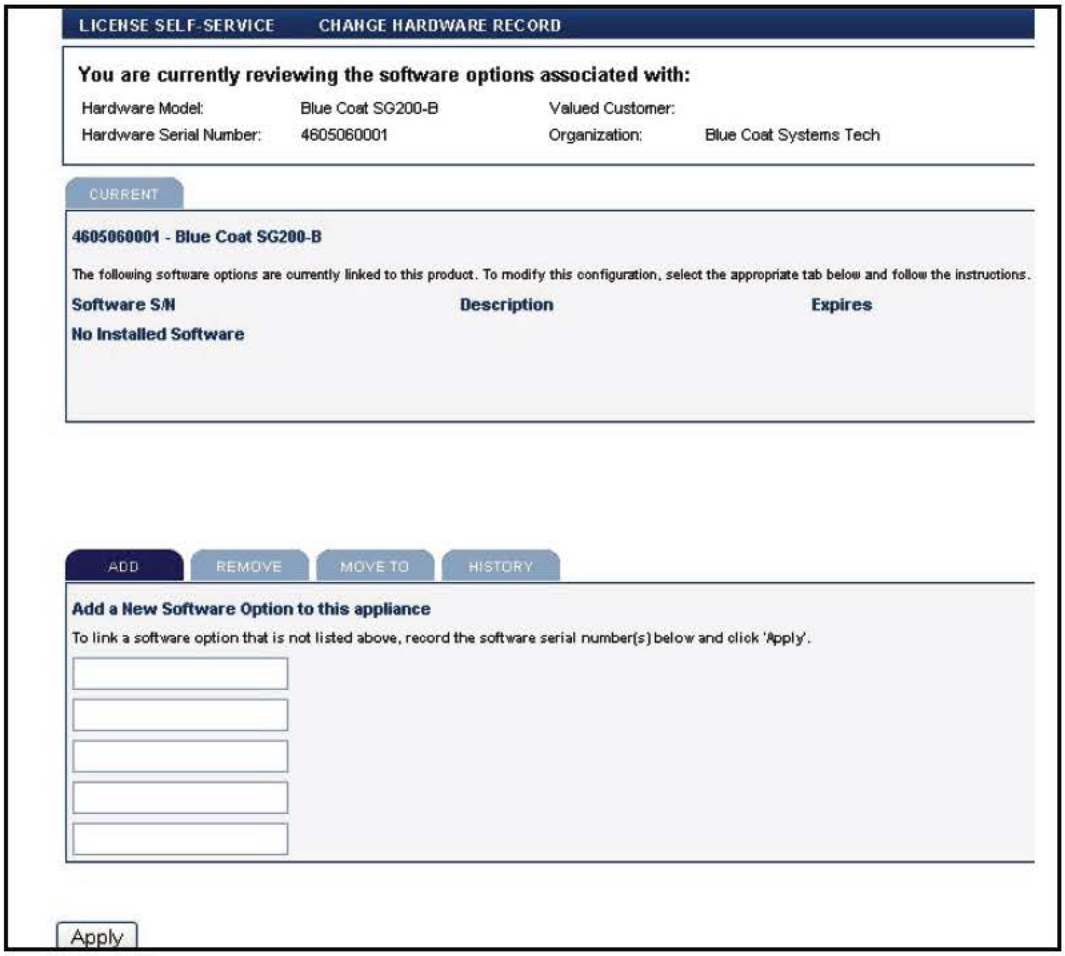
To manually obtain and install the license:

1. Select **Maintenance > Licensing > Install**.
2. Click **Register/Manage**. A new browser window opens and prompts you for your WebPower login information.
3. Enter your WebPower username and password and click **Login**. The **Support - License Management** page displays.

4. Click the serial number of the unit. The **Support - License Management Manage Serial Numbers/Obtain IM License** page displays.



5. Click **Manage Software Serial Numbers**. The **License Self Service Change Hardware Record** displays.



6. The next action depends on whether you have internet access.
   a. If the SG appliance has internet access:
      - Click **Add** to add a software license to the appliance.
      - Using the serial numbers you received when the Blue Coat appliance shipment was delivered, add the serial numbers.
      - Click **Apply** when finished. The software license is now associated with the hardware.
      - From **Management Console > Maintenance > Licensing > Install**, click **Retrieve** and provide the WebPower login information again. For more information on the Retrieve procedure, see "To retrieve the software license:" on page 26.
   b. If the SG appliance does not have internet access:
      - In the **Cust Info > Links** panel, click **Get License.** You are prompted to save a `.bin` file with the license information.
      - Save the `.bin` file.
      - From **Management Console > Maintenance > Licensing > Install**, select one of the following from the **License Key Manual Installation** drop-down list and click **Install**:

Note: A message is written to the event log when you install a license through the SG appliance.

- **Remote URL**—If the file resides on a Web server. The Install License Key dialog displays.

  Enter the URL path and click **Install**. The **Installation Status** field displays relevant information. When installation is complete, click **Results**; examine the results, close the window, and click **OK**. Click **Apply**.

- **Local File**—If the file resides in a local directory. The Upload and Install File window opens.

  Enter a path to the license file or click **Browse** and navigate to the file. Click **Install**. A results window opens. Examine the license installation results; close the window. Click **Close**. Click **Apply**.

The license is now installed. All features that you subscribed to are fully operational.

Manually Updating a License

After the initial license installation, you might decide to use another feature that requires a license. The license must be updated to support the new feature.

To update a license:

1. Select **Maintenance > Licensing > Install**.
2. Click **Register/Manage**.
3. Follow the instructions on the Blue Coat License Self-Service Web page.
4. If using the automatic license installation feature, click **Update**; otherwise, manually install the license as described in "Manual License Installation" on page 26.

Automatically Updating a License

The license automatic update feature allows the SG appliance to contact the Blue Coat licensing Web page 31 days before the license is to expire. If a new license has been purchased and authorized, the license is automatically downloaded. If a new license is not available on the Web site, the SG appliance continues to contact the Web site daily for a new license until the current license expires. Outside the above license expiration window, the SG appliance performs this connection once every 30 days to check for new license authorizations. This feature is enabled by default.

To configure the license auto-update:

1. Select **Maintenance > Licensing > Install**.
2. Select **Use Auto-Update**.
3. Select **Apply** to commit the changes to the SG appliance.

Note: If the automatic license update fails and you receive a Load from Blue Coat error

1. you must log on to your License Management account:
   `https://services.bluecoat.com/eservice_enu/licensing/mgr.cgi.`
2. Click **Update License Key**.

Related CLI Syntax to Manage Licensing

```
SGOS# licensing {disable-trial | enable-trial}
SGOS# licensing request-key [force] user_ID password
SGOS# licensing update-key [force]
SGOS# licensing register-hardware [force] user_ID password
SGOS# licensing mark-registered
```

Chapter 3: Accessing the SG Appliance

The SGOS software uses the Secure Shell (SSH) and HTTPS protocols to securely access the SGOS CLI and Management Console. Both SSHv1 and SSHv2 are enabled by default, and host keys have already been created on the SG appliance.

All data transmitted between the client and the SG appliance using SSH/HTTPS is encrypted.

During initial configuration, you assigned the SG appliance a username and password and a privileged-mode (enabled/configuration) password. These passwords are always stored and displayed hashed.

This chapter discusses:

Important: This chapter assumes that you have completed the first-time setup of the SG appliance using either the front panel or serial console, and that the appliance is running on the network. These steps must be completed before accessing the appliance.

You can manage the SG appliance by logging on to and using one of the following:

- An SSH session to access the CLI.
- The Management Console graphical interface.

You can also use a serial console to access the CLI.

Note: To use a Telnet session, you must use a serial console connection until you configure Telnet for use. (For security reasons Blue Coat does not recommend using Telnet).

Before You Begin: Understanding Modes

SGOS 5.x supports different levels of command security:

- Standard, or unprivileged, mode is read-only. You can see but not change system settings and configurations. This is the level you enter when you first access the CLI.
- Enabled, or privileged, mode is read-write. You can make immediate but not permanent changes to the SG appliance, such as restarting the system. This is the level you enter when you first access the Management Console.
- Configuration is a mode within the Enabled mode. From this level, you can perform permanent changes to the SG appliance configuration.

If you use the Management Console, you are in configuration mode when you log into Enabled mode and type `conf t`.

If you use the CLI, you must enter each level separately:

```
Username: admin
Password:
SGOS> enable
Enable Password:
SGOS# configure terminal
Enter configuration commands, one per line. End with CTRL-Z.
SGOS#(config)
```

For detailed information about the CLI and the CLI commands, refer to *Volume 11: Command Line Interface Reference*.

Note: Although most administrator tasks can be performed using either the Management Console or the CLI, there is the occasional task that can only be done using one of the two: these are specified in the manual.

Accessing the SG Appliance

You can access the SG appliance through either the CLI or the Management Console. By default, SSHv2 (CLI) and HTTPS (Management Console) are used to connect to the appliance.

The SSH and HTTPS ports are configured and enabled. For SSH, you can use either version 1 or version 2 (with password or RSA client key authentication).

Accessing the CLI

If you use the CLI, you can use SSHv2 to access the SG appliance, but you cannot use SSHv1 or Telnet without additional configuration.

Note: Enabling the Telnet-Console introduces a security risk, so it is not recommended.

To use SSHv1, you must first create an SSHv1 host key. For more information on creating SSH host keys, refer to *Volume 2: Proxies and Proxy Services*.

To log on to the CLI, you must have:

- the account name that has been established on the SG appliance
- the IP address of the SG appliance
- the port number (22 is the default port number)

You must log on from your SSH client.

Accessing the Management Console

The Management Console is a graphical Web interface that allows you to manage, configure, monitor, and upgrade the SG appliance from any location.

In the Web browser, enter HTTPS, the SG appliance IP address, and port `8082` (the default management port). For example, if the IP address configured during first-time installation is `10.25.36.47`, enter the URL `https://10.25.36.47:8082` in the Web browser.

The Management Console consists of a set of Web pages stored on the SG appliance. The appliance acts as a Web server on the management port to serve these pages. From the SG home page on the appliance, you can access the configuration, maintenance, and statistics pages, and the documentation. The Management Console is supported with a complete online help facility to assist you in defining the various configuration options.

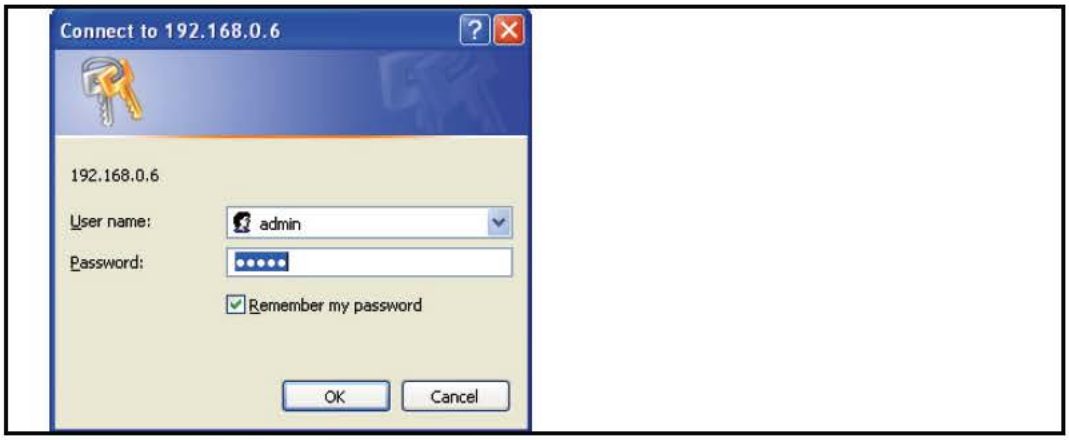
Note: If, when you access the Management Console home page, you get a "host mismatch" or an "invalid certificate" message, you need to recreate the security certificate used by the HTTPS-Console. For information on changing the security certificate, refer to the console services information in *Volume 2: Proxies and Proxy Services*.

Accessing the Management Console Home Page

When you access the Management Console home page (see "Accessing the Management Console" on page 32), you are prompted to log on to the system.

Logging On

Each time you access the Management Console, you must log on.



- The **Site** is the IP address of the SG appliance to which you are logging on.
- The **Realm** is a configurable name that can be anything you choose. The SG appliance IP address is the default. For more information on configuring the realm name, see "Changing the SG Appliance Realm Name" on page 36.
- The **User Name** is the name of the account you are using on this SG appliance. The name must already exist. It cannot be created here.
- The **Password** is the password for the account you are using. It cannot be changed here.

You can change the username and password for the console or the CLI. See "Changing the Logon Parameters" on page 34.

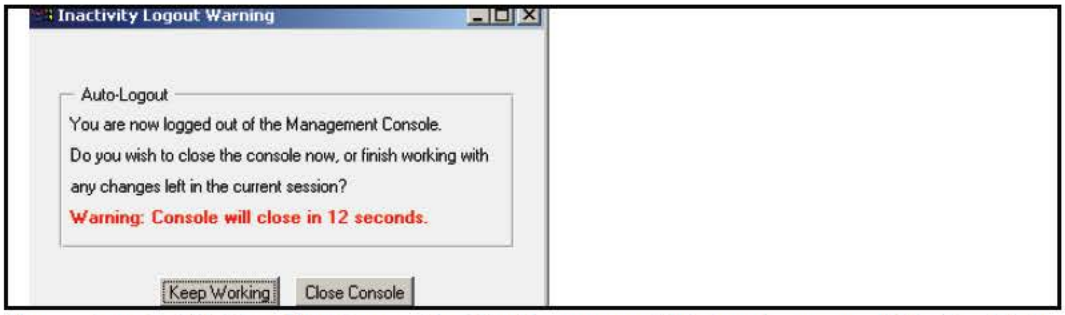
Note: All successful and failed logon attempts are logged to the event log.

Logging Out

Once you have logged on, you do not have to log on again unless you exit the current session or the session times out. The session timeout period, with a default of 900 seconds (15 minutes), is configurable.

Thirty seconds before the session times out, a warning dialog displays. Click the **Keep Working** button or the **X** in the upper-right-corner of the dialog box to keep the session alive.

Note: The **Keep Working** button saves your changes. However, you must log back on to work in other pages.



If you do not click **Keep Working** or the **X** in the upper-right-hand corner within the thirty-second period, you are logged out. You must log back on to access the Management Console.

Click the hyperlink to log back on.

Note: If you are on the Management Console home page when the session times out, you are logged out without seeing the logout warning dialog. You might not be aware that you are logged out until you try to access a Management Console page. You must enter the logon information again.

Changing the Logon Parameters

You can change the console username and password, the console realm name (which displays when you log on to the SG appliance), and the auto-logout timeout (in seconds; the default is 900 seconds.)

The Management Console requires a valid administrator username and password to have full read-write access; you do not need to enter a privileged-mode password as you do when using the CLI. A privileged-mode password, however, must already be set.

Note: To prevent unauthorized access to the SG appliance, only give the console username and password to those who administer the system.

Changing the Username and Password

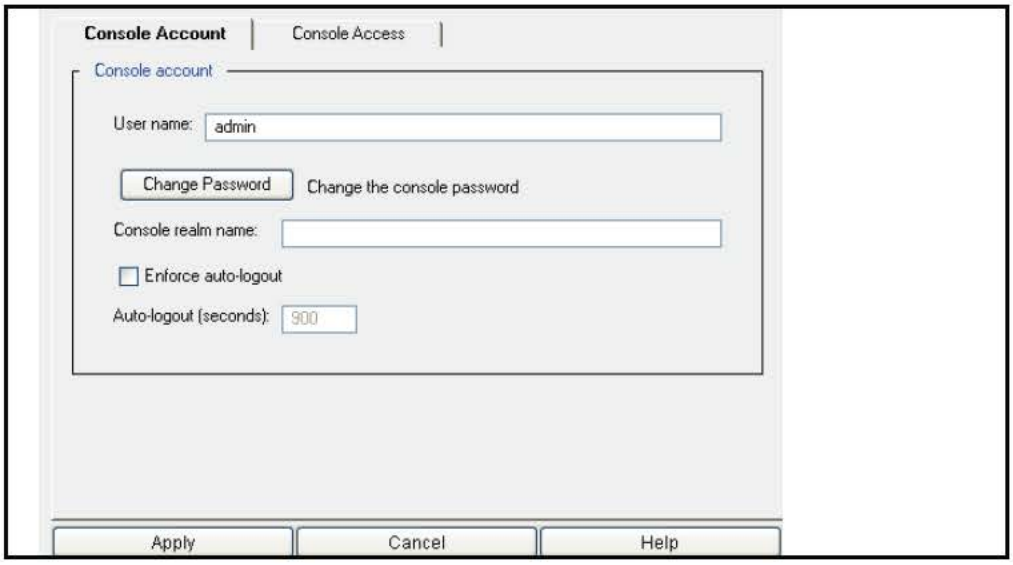
You can change either the username or the password without changing both.

Changing the Username

The console account username was assigned during initial setup of the system. You can change the username at any time.

To change the username:

1. Select **Configuration > Authentication > Console Access > Console Account**.



Note: Changing the Console Account username or password causes the Management Console to refresh and log back on using the new information. Note that each parameter must be changed and individually refreshed. You cannot change both parameters at the same time.

2. Enter the username of the administrator or administrator group who is authorized to view and revise console properties.

   Only one console account exists on the SG appliance. If you change the console account username, that username overwrites the existing console account username.

   The console account username can be changed to anything that is not null and contains no more than 64 characters.

3. Click **Apply**.

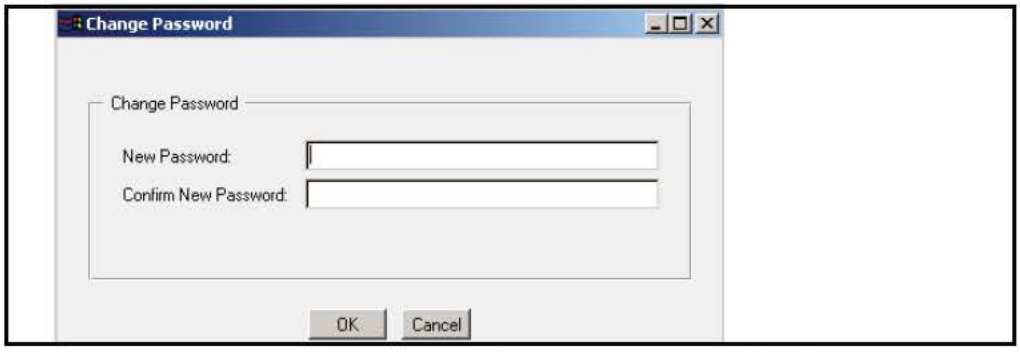
   After clicking **Apply**, an **Unable to Update configuration** error is displayed. The username change was successfully applied, but the configuration could not be fetched from the SG appliance, as the username offered in the fetch request is still the old username.

4. Refresh the screen. You are then challenged for the new username.

To change the password:

The console password and privileged-mode password were defined during initial configuration of the system. The console password can be changed at any time. The privileged-mode, or enabled-mode, password can only be changed through the CLI or the serial console.

1. Select **Configuration > Authentication > Console Access > Console Account**.
2. Click **Change Password**.



3. Enter and re-enter the console password that is used to view and edit configuration information. The password must be from 1 to 64 characters long. As you enter the new password, it is obscured with asterisks. Click **OK**.

Note: This does not change the enabled-mode password. You can only change the enabled-mode password through the CLI.

---

4. Refresh the screen, which forces the SGOS software to re-evaluate current settings. When challenged, enter the new password.
5. (Optional) Restrict access by creating an access control list or by creating a policy file containing `<Admin>` layer rules. For more information, see *Volume 4: Securing the Blue Coat SG Appliance*: Chapter 3: "Controlling Access to the Internet and Intranet".

Related CLI Syntax to Change the Username and Password

Note: Usernames and passwords can each be from 1 to 64 characters in length, but the passwords must be in quotes.

Usernames that contain \ (backward slash), * (asterisk), or ? (question mark) must be escaped when viewing users from the command line interface. The escape character is \.

For example:

- user1* is searched as #(config users) view users user1*
- user1? is searched as #(config users) view users user1\?
- user1\ is searched as #(config users) view users user1\\

```
SGOS#(config) security {username username | password "password" |
front-panel-pin pin}
```

Changing the SG Appliance Realm Name

The realm name displays when you log on to the Management Console. The default realm name is the connection used to access the SG appliance, usually the IP address of the system.

To change the realm name:

1. Select **Configuration > Authentication > Console Access > Console Account**.
2. Enter a new realm name.

The new realm name displays the next time you log on to the Management Console.

3. Select **Apply** to commit the changes to the SG appliance.

Related CLI Syntax to Change the Realm Name

```
SGOS#(config) security management display-realm name
```

The new realm name displays the next time you log on to the Management Console.

Changing the SG Appliance Timeout

The timeout is the length of time a session persists before you are logged out. The default timeout is 900 seconds (15 minutes).

To change the timeout:

1. Select **Configuration > Authentication > Console Access > Console Account**.
2. Either deselect **Enforce auto-logout** (which eliminates auto-logout entirely) or change the auto-logout timeout from its default of **900** seconds (15 minutes) to another value (in seconds). This is the allowable length of time on the SG appliance before the current session times out. Acceptable values are between **300** and **86400** seconds (5 minutes to 24 hours).

   If you change the timeout value, the change takes effect on the next refresh of any Management Console page.
3. Select **Apply** to commit the changes to the SG appliance.

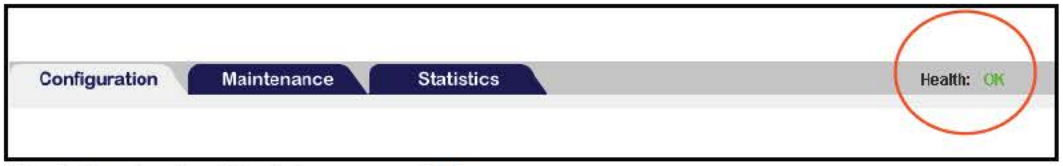
Related CLI Syntax to Change the Timeout

```
SGOS#(config) security management auto-logout-timeout seconds
```

Viewing the Appliance Health

The Management Console displays a visual representation of the overall health state of the SG appliance. The health states are based on the health monitoring metrics, which are described in the Monitoring chapter of *Volume 8: Managing the Blue Coat SG Appliance*.

The health icon is located in the upper right corner of the Management Console.



The following health states are possible:

- **Ok (Green)**
- **Warning (Yellow)**
- **Critical (Red)**

These states are represented by a text string and a color that corresponds to the health of the system (green, yellow or red). The system health changes when one or more of the health metrics reaches a specified threshold or returns to normal.

The Management Console polls the SG appliance every 10 seconds and updates the health state indicator accordingly.

For More Information

To obtain more information about the health state, click the health icon. Clicking the health icon displays the **Statistics > Health** page, which lists the current condition of the system's health monitoring metrics.

Refer to *Volume 8: Managing the Blue Coat SG Appliance* for more information about the health monitoring metrics.

Chapter 4: Configuring Basic Settings

The SG appliance global configurations include: defining the SG appliance name and serial number, setting the time, and configuring NTP for your environment.

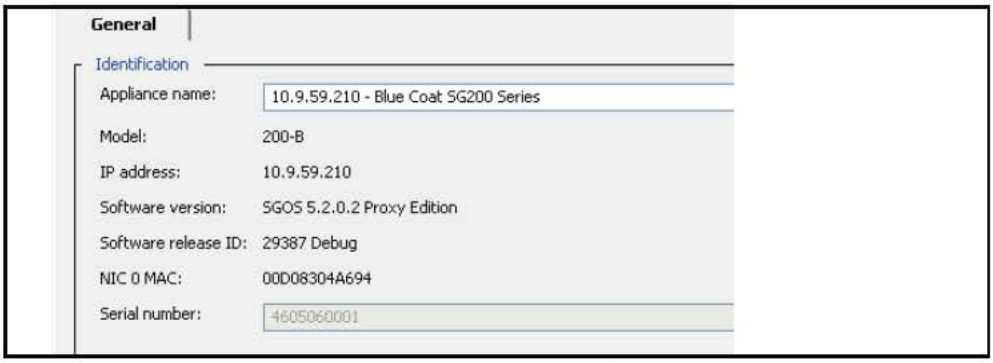
The following topics are discussed in this section:

Configuring the SG Appliance Name

You can assign any name to a SG appliance. A descriptive name helps identify the system.

To set the SG appliance name:

1. Select **Configuration > General > Identification**.



2. In the **Appliance name** field, enter a unique name for the appliance.
3. Select **Apply** to commit the changes to the SG appliance.

Related CLI Syntax for Setting the SG Appliance Name

```
SGOS#(config) hostname name
```

Viewing the Appliance Serial Number

The SG appliance serial number assists Blue Coat Systems Customer Support when analyzing configuration information, including heartbeat reports. This number is found on the SG appliance. The serial number is visible on the Management Console home page.

Configuring the System Time

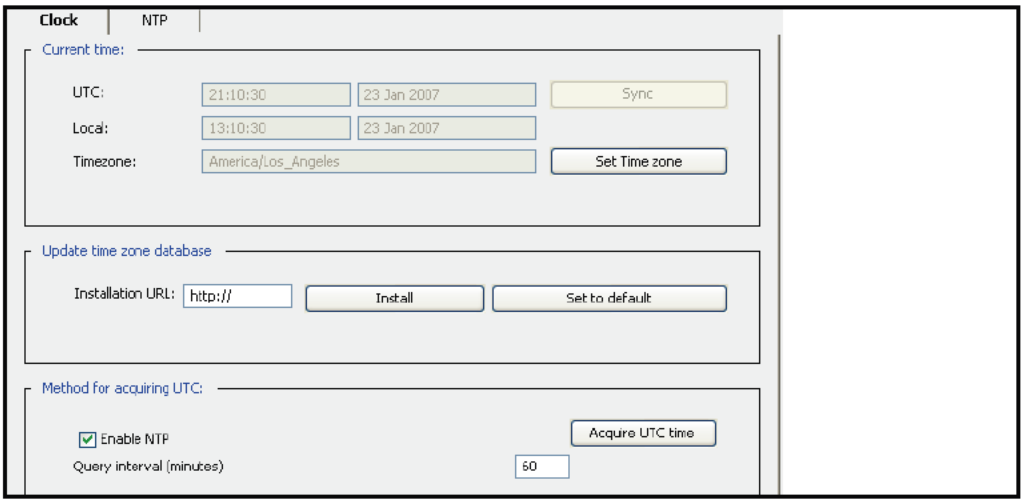
To manage objects, the SG appliance must know the current Coordinated Universal Time (UTC), which is the international time standard and is based on a 24-hour clock. However, time stamps can also record in local time. To do this, local time must also be set based on time zones.

By default, the SG appliance attempts to connect to an NTP server, in the order the servers appear in the NTP server list on the **NTP** tab, to acquire the UTC time. The appliance ships with a list of NTP servers available on the Internet. If the appliance cannot access any of the listed NTP servers, you must manually set the UTC time.

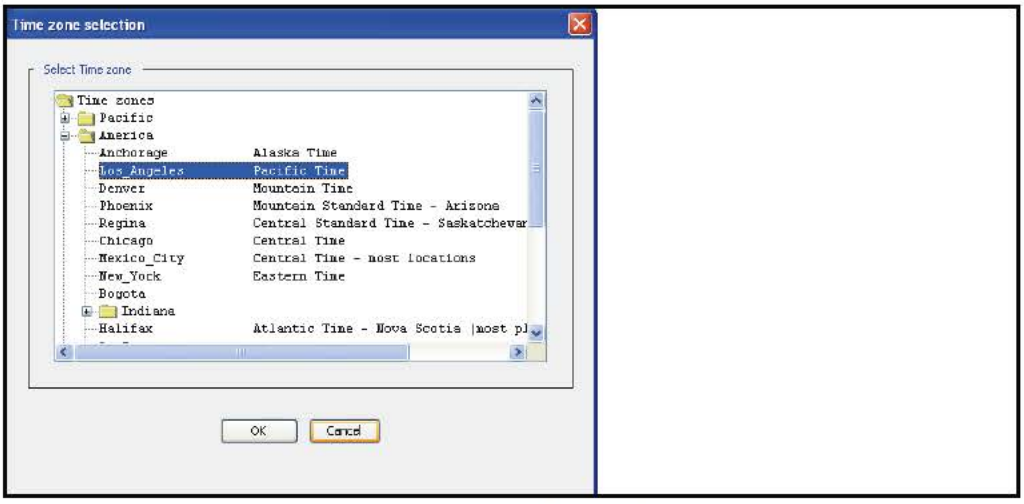
Additionally, the SG appliance ships with a limited list of time zones. If a particular time zone is missing from the included list, the list can be updated at your discretion. Also, the time zone database might need to be updated if the Daylight Savings rules change in your area. The list can be updated by downloading the full time zone database from http://download.bluecoat.com/release/timezones.tar.

To set local time:

1. Select **Configuration > General > Clock > Clock**.



2. Click **Select Time zone**. A popup appears, displaying a list of time zones based on geopolitical regions.



3. Select the time zone that represents your local time. Once the local time zone is selected, event logs record the local time instead of GMT. To add additional time zones to the list, update the appliance's time zone database, as described in the following procedure.

To update the database:

1. Select **Configuration > General > Clock > Clock**.
2. Enter the URL from which the database will be downloaded or click **Set to default**.
3. Click **Install**.

Related CLI Syntax for Adding New Time Zones to the Database:

```
SGOS# (config) timezone database-path [url | default]
SGOS# (config) load timezone-database
```

To acquire the UTC:

1. Ensure that **Enable NTP** is selected.
2. Click **Acquire UTC Time**.

Related CLI Syntax for Acquiring and Setting UTC Time:

```
SGOS# acquire-utc
SGOS#(config) clock [subcommands]
```

Network Time Protocol

The Network Time Protocol (NTP) is used to synchronize the time of a computer client or server to another server or reference time source, such as a radio or satellite receiver or modem. There are more than 230 primary time servers, synchronized by radio, satellite and modem.

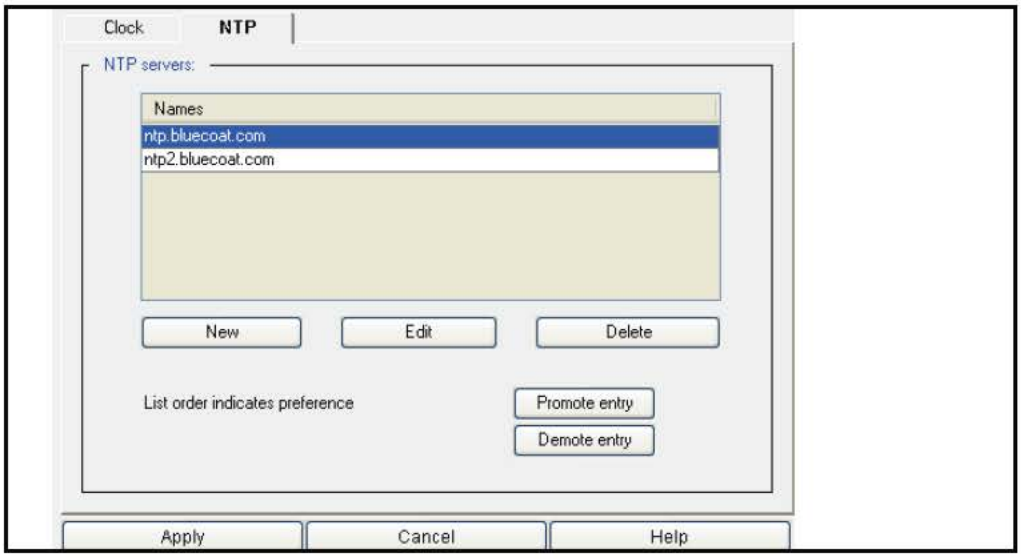
The SG appliance ships with a list of NTP servers available on the Internet, and attempts to connect to them in the order they appear in the NTP server list on the **NTP** tab. You can add others, delete NTP servers, and reorder the NTP server list to give a specific NTP server priority over others.

The SG appliance uses NTP and the Coordinated Universal Time (UTC) to keep the system time accurate.

You can add and reorder the list of NTP servers the SG appliance uses for acquiring the time. The reorder feature is not available.

To add an NTP server:

1. Select **Configuration > General > Clock > NTP**.



2. Click **New** to add a new server to the list.
3. Enter either the domain name or IP address of the NTP server and click **OK**.
4. Select **Apply** to commit the changes to the SG appliance.

Related CLI Syntax for Acquiring and Setting UTC Time:

```
SGOS#(config) ntp [subcommands]
```

To change the access order:

NTP servers are accessed in the order displayed. You can organize the list of servers so the preferred server appears at the top of the list. This feature is not available through the CLI.

1. Select **Configuration > General > Clock > NTP**.
2. Select an NTP server to promote or demote.
3. Click **Promote entry** or **Demote entry** as appropriate.
4. Select **Apply** to commit the changes to the SG appliance.

Configuring HTTP Timeout

You can configure various network receive timeout settings for HTTP transactions. You can also configure the maximum time that the HTTP proxy waits before reusing a client-side or server-side persistent connection. You must use the CLI to configure these settings.

To configure the HTTP receive timeout setting:

At the `(config)` command prompt, enter the following command:

```
SGOS#(config) http receive-timeout {client | refresh | server}
#_seconds
```

where:

`client`	*`#_seconds`*	Sets the receive timeout for client to *`#_seconds`*. The default is 120 seconds.
`refresh`	*`#_seconds`*	Sets receive timeout for refresh to *`#_seconds`*. The default is 90 seconds.
`server`	*`#_seconds`*	Sets receive timeout for server to *`#_seconds`*. The default is 180 seconds.

To configure the HTTP persistent timeout setting:

At the `(config)` command prompt, enter the following command:

```
SGOS#(config) http persistent-timeout {client | server} #_seconds
```

where

`client`	*`#_seconds`*	The maximum amount of time the HTTP proxy waits before closing the persistent client connection if another request is not made. The default is 360 seconds.
`server`	*`#_seconds`*	The maximum amount of time the HTTP proxy waits before closing the persistent server connection if that connection is not re-used for any subsequent request from the proxy. The default is 900 seconds.

Chapter 5: Archive Configuration

Blue Coat allows you to use an existing configuration (modified to include only general parameters, not system-specific settings) to quickly set up a newly-manufactured SG appliance and to save the running configuration off-box for archival purposes.

This section discusses:

Sharing Configurations

You can share configurations between two SG appliances. You can take a *post-setup* configuration file (one that does not include those configuration elements that are established in the setup console) from an already-configured SG appliance and push it to a newly-manufactured system.

Note: Blue Coat Director allows you to push a configuration from one SG appliance to multiple appliances at the same time. For more information on using Director, see *Volume 8: Managing the Blue Coat SG Appliance*.

The new configuration is applied to the existing configuration, changing any existing values. This means, for instance, that if the new configuration creates a realm called *RealmA* and the existing configuration has a realm called *RealmB*, the combined configuration includes two realms, *RealmA* and *RealmB*.

To share configurations, you must

- Change all "encrypted-password" entries to "password" followed by the actual password in quotes.
- Change any "hashed-password" entries to "password" followed by the actual password in quotes.
- Make sure that no services are tied to a specific proxy IP address.
- Download a content filter database, if the configuration includes content filtering.

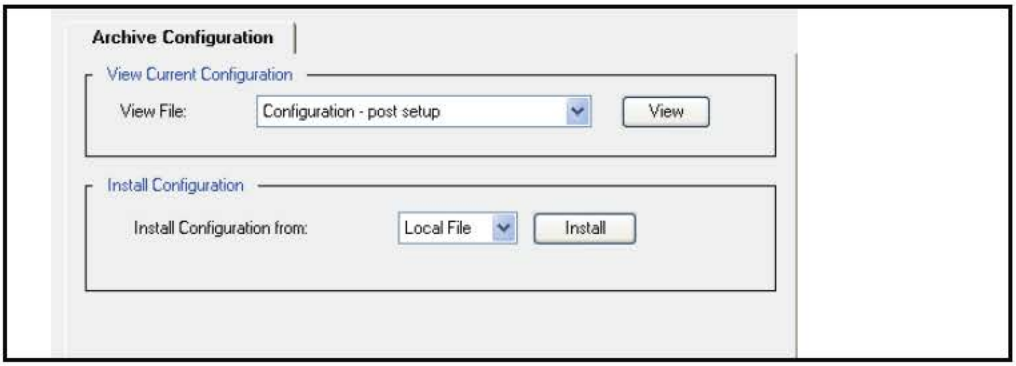
You can use either the Management Console or the CLI to create a post-setup configuration file on one SG appliance and push it to another.

Note: You cannot push configuration settings to a newly manufactured system until you have completed initial setup of the system.

To create and push a configuration to a newly manufactured SG appliance:

From the already configured SG appliance:

1. Select **Configuration > General > Archive.**



2. In the **View Current Configuration** panel, select the configuration from the drop-down list that you want to use for the newly-manufactured machine:
   - **Configuration - post setup**: This displays the configuration on the current system, minus any configurations created through the setup console, such as the hostname and IP address. It also includes the installable lists.
   - **Configuration - brief**: This displays the configuration on the current system, but does not include the installable lists.
   - **Configuration - expanded**: This is the most complete snapshot of the system configuration, but it contains system-specific settings that should not be pushed to a new system.
   - **Results of Configuration Load**: This displays the results of the last configuration pushed to the system.
3. View the configuration you selected by clicking **View**. You can also view the file by selecting **Text Editor** in the **Install Configuration** panel and clicking **Install**.
4. Save the configuration. You can save the file two ways:
   - Save it as a text file on your local system. This is advised if you want to re-use the file.
   - Copy the contents of the configuration. (You will paste the file into the Text Editor on the newly-manufactured system.)

To install the configuration on a newly manufactured SG appliance:

1. Launch the Management Console in a new browser window.
2. Select **Configuration > General > Archive.**
3. The **Archive Configuration** tab displays.
4. In the **Install Configuration** panel, install the configuration using one of the following methods:
   - If you saved the file to your system, browse to the location of the Local File, highlight the file, and click **Install**. The configuration is installed, and the results screen displays.
   - If you copied the contents of the file, paste it into the Text Editor and click **Install**. The configuration is installed, and the results screen displays.

Note: A message is written to the event log when you install a configuration through the SG appliance.

5. Click **Close**.

To create and push a configuration to a newly manufactured SG appliance:

From the already configured SG appliance:

1. From the enable prompt (#), determine which configuration you want to use for the new system. The syntax is:

   ```
   show configuration post-setup | brief | expanded
   ```

   where:

`post-setup`	This displays the configuration on the current system, minus any configurations created through the setup console, such as the hostname and IP address. It also includes the installable lists.
`brief`	This displays the configuration on the current system, but does not include the installable lists.
`expanded`	This is the most complete snapshot of the system configuration, but it contains system-specific settings that should not be pushed to a new system.

2. Save the configuration. You can save the file two ways:
   - Copy the contents of the configuration to the clipboard. (Paste the file into the terminal on the newly-manufactured system.)
   - Save it as a text file on a download FTP server accessible to the SG appliance. This is advised if you want to re-use the file.
3. On the newly-manufactured SG appliance, retrieve the configuration file by doing one of the following:
   - If you saved the configuration to the clipboard, go to the `(config)` prompt and paste the configuration into the terminal.
   - If you saved the configuration on the FTP server:

     At the enable command prompt, enter the following command:

     ```
     SGOS# configure network "url"
     ```

     where *url* must be in quotes and is fully-qualified (including the protocol, server name or IP address, path, and filename of the configuration file). The configuration file is downloaded from the server, and the SG appliance settings are updated.

     Note: If you rename the archived configuration file so that it does not contain any spaces, the quotes surrounding the URL are unnecessary.

     The username and password used to connect to the FTP server can be embedded into the URL. The format of the URL is:

     ```
     ftp://username:password@ftp-server
     ```

where *ftp-server* is either the IP address or the DNS resolvable hostname of the FTP server.

If you do not specify a username and password, the SG appliance assumes that an anonymous FTP is desired and thus sends the following as the credentials to connect to the FTP server:

```
username: anonymous
password: proxy@
```

Archiving a Configuration

In the rare case of a complete system failure, restoring a SG appliance to its previous state is simplified by loading an archived system configuration from an FTP or TFTP server. The archive, taken from the running configuration, contains all system settings differing from system defaults, along with any installable lists configured on the SG appliance.

Archive and restore operations must be done through the CLI.

Note: You can archive a system configuration to an FTP or TFTP server that allows either anonymous logon or requires a specific username and password. Likewise, to restore a system configuration, the server storing the archive can be configured either to allow anonymous logon or to require a username and password.

To prepare to archive a system configuration

1. Obtain write permission to a directory on an FTP server. This is where the archive will be stored.

   The system configuration must be stored using FTP.

2. At the `(config)` command prompt, enter the following commands:

   ```
   SGOS#(config) archive-configuration protocol {ftp | tftp}
   SGOS#(config) archive-configuration host hostname
   ```

   where *hostname* is the IP address of the server.

   Note: TFTP does not require a password, path, or username.

   ```
   SGOS#(config) archive-configuration password password
   -or-
   SGOS#(config) archive-configuration encrypted-password encrypted-
   password
   ```

   where *password* is the password (or encrypted password) used to access the server.

   ```
   SGOS#(config) archive-configuration path path
   ```

   where *path* is the directory on the server where the archive is to be stored, relative to the preset FTP directory.

   ```
   SGOS#(config) archive-configuration filename-prefix filename
   ```

   where *filename* can contain % strings that represent the information in the upload filename. If you do not use the filename command, the SG appliance creates a name with a timestamp and the filename *SG_last-ip-octet_timestamp*. For % string substitutions, see *Volume 8: Access Logging*.

   ```
   SGOS#(config) archive-configuration username username
   ```

   where *user_name* is the username used to access the server.

Example Session

```
SGOS#(config) archive-configuration host 10.25.36.47
  ok
SGOS#(config) archive-configuration password access
 ok
SGOS#(config) archive-configuration username admin1
 ok
SGOS#(config) archive-configuration path ftp://archive.server/stored
 ok
SGOS#(config) archive-configuration protocol ftp
 ok
```

Note: To clear the host, password, or path, type the above commands using empty double-quotes instead of the variable. For example, to clear the path, enter `archive-configuration path “”`.

To archive a system configuration:

At the enable command prompt, enter the following command:

```
SGOS# upload configuration
```

To restore a system configuration:

At the enable command prompt, enter the following command:

```
SGOS# configure network “url”
```

See “Sharing Configurations” on page 45 for more information about formatting the URL for FTP.

Troubleshooting

When pushing a shared configuration or restoring an archived configuration, keep in mind the following issues:

- Encrypted passwords (login, enable, and FTP) cannot be decrypted by a device other than that on which it was encrypted. If you were sharing a configuration, these encrypted passwords were probably already created before the configuration was pushed to the system.
- If the content filtering database has not yet been downloaded, any policy that references categories is not recognized.
- The following passwords must be re-created (if you use the application specified):
  - administrator console passwords (not needed for shared configurations)
  - privileged-mode (enable) passwords (not needed for shared configurations)
  - the front-panel PIN (recommended for limiting physical access to the system)
  - access log FTP client passwords (primary, alternate)
  - archive configuration FTP password
  - RADIUS primary and alternate secret
  - LDAP search password
  - SmartFilter download password
  - WebSense3 download password

- SNMP read, write, and trap community strings
- RADIUS and TACACS+ secrets for splash pages

❒ A full download of the content filtering database must be done.

❒ SSH certificate keys must be imported.

❒ SSL certificate keys must be imported

In addition, you should make sure the system is functioning whenever you add a feature. For example, make sure the system works after basic configuration; then, after you add authentication, recheck the system.

Chapter 6: Adapters

This chapter describes SG network adapters and the adapter interfaces; the following topics are discussed:

About Adapters

SG appliances ship with one or more network adapters installed on the system, each with one or more interfaces. This chapter describes how to change interface parameters or configure additional adapters or virtual LANs in the appliance. You can also accept or reject inbound connections, change link settings in the event the system did not correctly determine them, and configure the browser for proxy settings.

As you select adapters from the picklist, the **Adapter** panel (**Configuration > Network > Adapters**) displays the state of the configured adapter and its interfaces.

Note: In Blue Coat documentation, the convention for the interface is *adapter*`.`*interface*. For example, `0:0`.

About Virtual LAN Configuration

This section discusses Virtual LAN (VLAN) deployments.

About VLAN Deployments

VLANs are created to group multiple physical network segments into individual broadcast domains. The benefit to this is that clients can be organized logically—for example, based on organization—rather than limited to physical connections to interfaces. Because networks recognize VLANs as they do physical LANs, each VLAN can have an IP prefix assigned to it. This enables IP routing of traffic flow between VLANs, which allows for targeted traffic relaying rather than broadcasting to all connected hosts.

VLAN configuration occurs on the switch. The network administrator specifies which ports belong to which VLANs. The following diagram illustrates a port-based VLAN configuration. Clients on network segments attached to switch ports 1 and 2 belong to VLAN 1, which has the network address `10.0.1.x`; network segments attached to switch ports 14 and 15 belong to VLAN 2, which has the network address `10.0.2.x`.

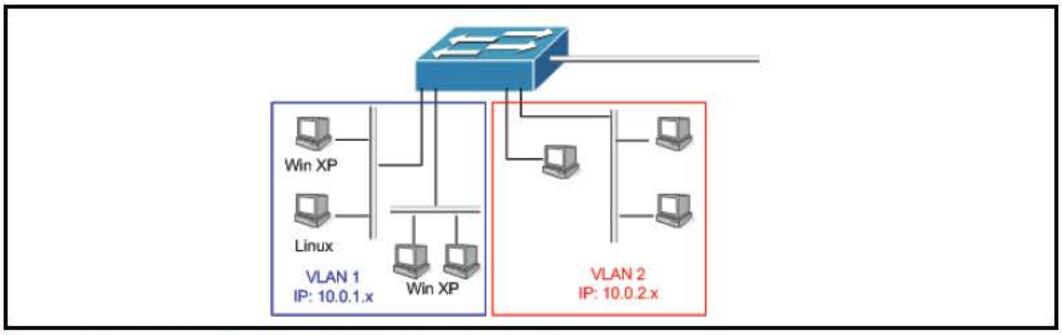


Figure 6-1. Multiple VLANs connected to ports on one switch

As also illustrated in the diagram, clients of different OS types can reside within a VLAN. However, not all clients are able to detect (send or receive) VLAN-tagged packets.

About VLAN Trunking

On the packet level, VLAN identification is achieved by the switch *tagging*, or inserting, the VLAN ID (VID) into the packet header. This allows the next switch inline to know the location of the destination VLAN. When VLANS span multiple switches, a *trunk* data link between switches that carries traffic associated with multiple VLANs is required. The trunk link is attached to a switch port designated for inter-switch communication.

In the following diagram, multiple VLANs are connected by trunk data link between two switches.

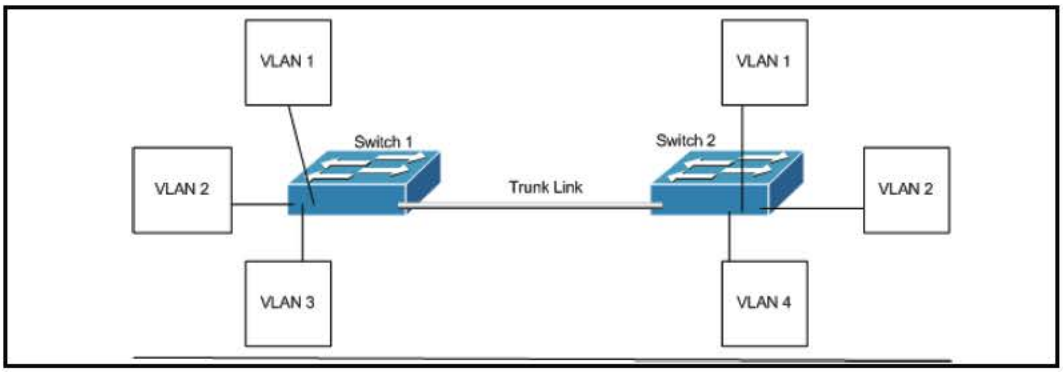


Figure 6-2. Two switches connected by a trunk

About Native VLANs

Each switch port has a designated *native* VLAN. On any given switch, each port might have a different Native VLAN configured on it. While native VLAN connections themselves are not tagged, they can carry both tagged and untagged VLAN traffic. Connections destined to the native VLAN have their packets sent out untagged, and connections destined to non-native VLANs have their packets sent out tagged. The default VID on most switches is 1.

The trunk link carries both the native VLAN (untagged) and all other VLAN (tagged) packets, as illustrated in the following diagram.

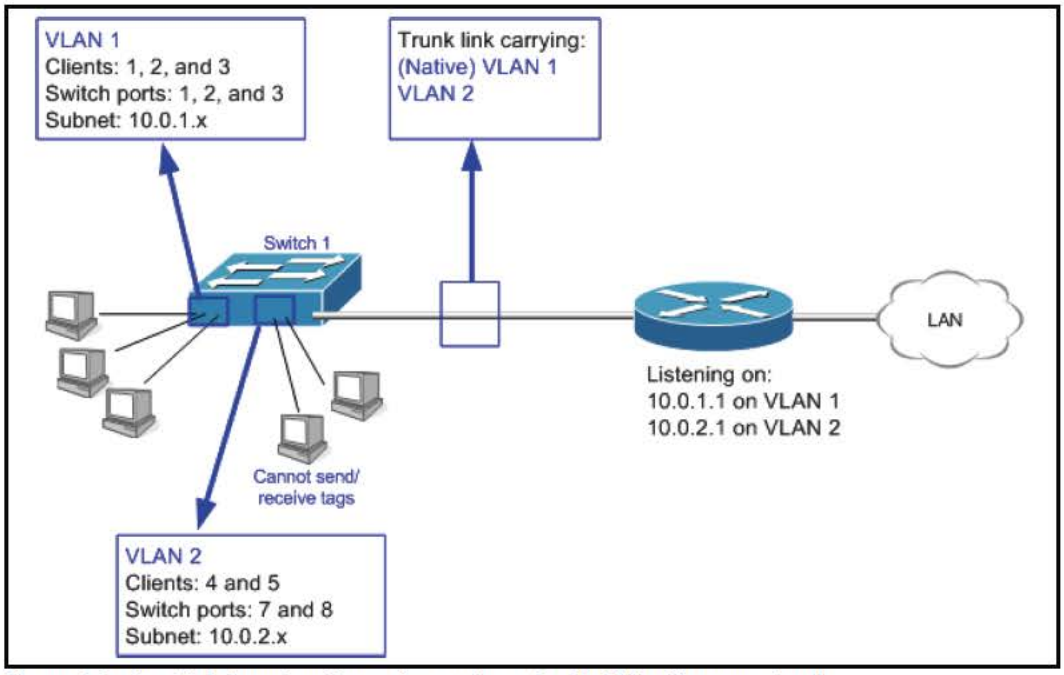


Figure 6-3. A switch broadcasting native and regular VLAN traffic over a trunk

In this example, the client attached to port 7 belongs to VLAN 2. Even though it is part of VLAN2, it does not set tags or receive VLAN-tagged packets. The switch knows the packet belongs to VLAN 2 and tags it accordingly. Conversely, it strips the VLAN 2 tag on the response. The trunk link broadcasts VLAN 1 (the native) and 2 traffic to a router that accepts the subnets of those VLANs.

Deployment complications arise when a device (other than a router) is required between switches. Without VLAN tagging support, any network device deployed in between switches either drops *all* VLAN-tagged traffic or passes it through by a bridging configuration.

This creates a problem if, for example, users located on different floors all belong to VLAN 1, but are separated by proxy that does not recognize VLAN-tagged packets.

Note: In Blue Coat documentation, the convention for VLAN is *adapter*`.`*interface*`.`*VLAN_ID*. For example, `0:0.1` is the native VLAN on adapter `0`, interface `0`.

The Blue Coat Solution

SGOS 5.1.4 and later supports VLAN tagging; therefore, a SG appliance can be deployed inline with switches that are routing VLAN traffic. This allows for uninterrupted VLAN service, plus enables benefits gained with the proxy features.

The Management Console enables you to configure VLAN interfaces the same way you configure physical interfaces. After a VLAN is added, it appears in the list of network interfaces. Properties such as `allow-intercept` and `reject-inbound` are applicable to VLAN interfaces.

The most common deployment is a SG appliance residing between two switches or a switch and a router that is forwarding or bridging traffic; in these cases, preserving tagged packets is essential to your network.

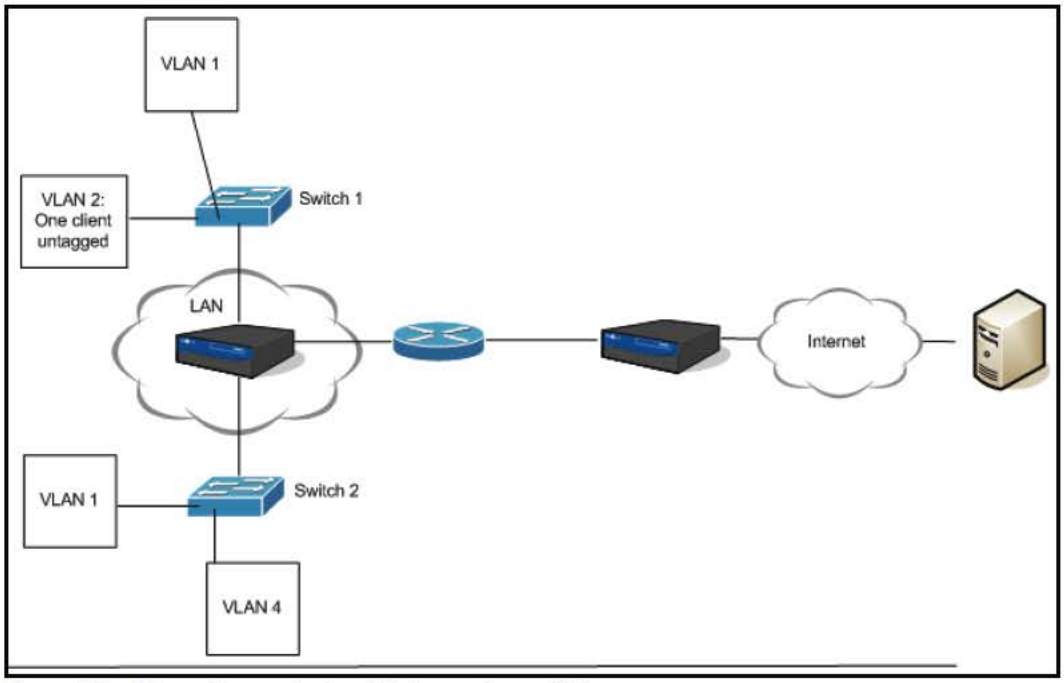


Figure 6-4. SG appliance deployed between two switches

As the SG appliance strips outgoing native VLAN tags, trunking on both interfaces is required to both recognize and preserve the tagged packets.

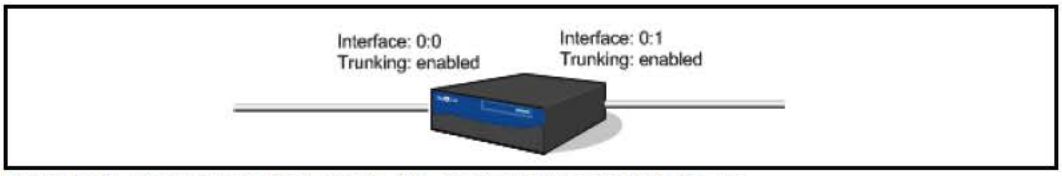


Figure 6-5. Trunking enabled on two SG appliance physical interfaces

Based on this deployment:

- The SG appliance accepts all packets, regardless of their tag, and, if configuration and policy allows, passes them from one interface to the other with the original VLAN tagged preserved.
- If a packet arrives on one interface on VLAN 2, it remains on VLAN 2 when it is forwarded out another interface. If a packet arrives untagged and the destination interface has a different native VLAN configured, the SG appliance adds a tag to ensure the VLAN is preserved. Similarly, if a tagged packet arrives and the VLAN ID matches the native VLAN of the destination interface, the SG appliance removes the tag before forwarding the packet.

Note: Bridge groups *cannot* be based on VLANs.

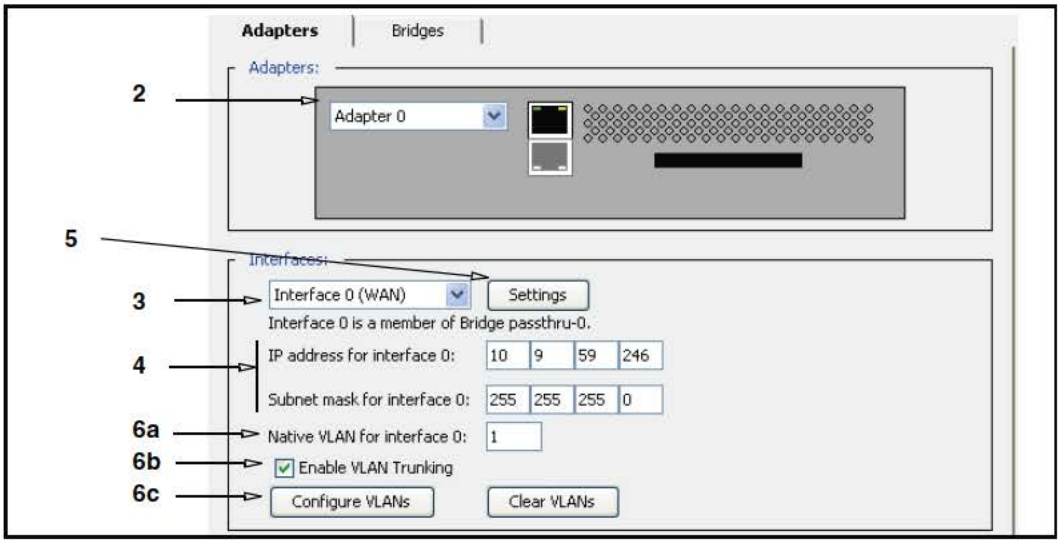
Configuring an Adapter

The following procedure describes how to configure an adapter. Repeat the process if the system has additional adapters.

To configure a network adapter:

1. Select **Configuration > Network > Adapters > Adapters**.

> **Note:** Different SG appliance models have different adapter configurations, and the appearance of the **Adapters** tab varies accordingly.



2. Select an adapter from the **Adapter** drop-down list.

   Notice that in the **Interfaces** field, a message displays stating whether the interface belongs to a bridge. For more information about network bridging, see Chapter 7: "Software and Hardware Bridges" on page 61.

3. (Optional) If you have a multiple-interface adapter, select an interface from the drop-down list.

4. Enter the IP address and subnet mask for the interface into the **IP address for interface x** and **Subnet mask for interface x** fields (where **interface x** refers to the interface selected in the **Interfaces** drop-down list.)

5. (Optional) To configure link settings, restrict inbound connections, or set up browser proxy behavior for the adapter, select the interface and click **Settings**. Enter any changes and click **OK** to close the Settings dialog.

   See "Configuring Interface Settings" on page 57 for more information about configuring adapter settings.

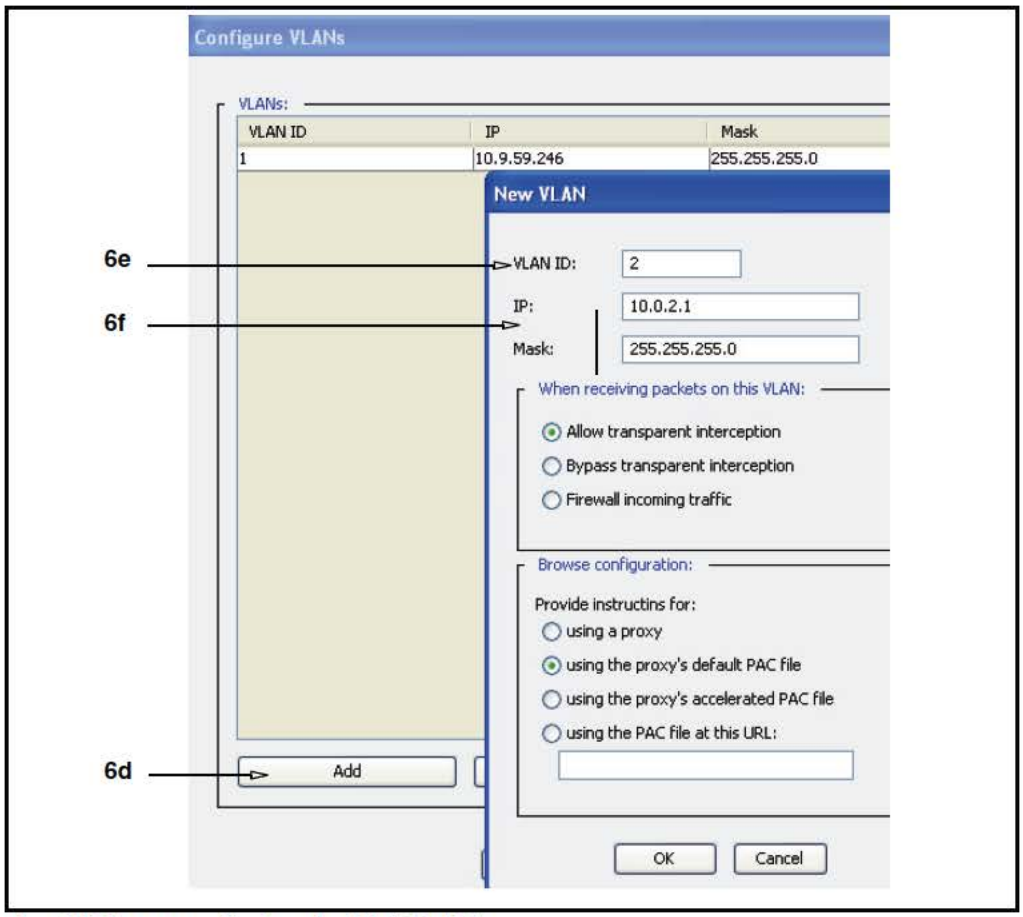
> **Note:** The default is to permit all inbound connections. You should always manually configure link settings to avoid problems. The browser default is to use the proxy's default PAC file. (See "Configuring Interface Settings" on page 57 below for more information on link settings and inbound connections.)

6. If applicable, configure Virtual LAN (VLAN) options (see "About Virtual LAN Configuration" on page 51):

a. By default, the native VID for any SG appliance interface is **1**, as most switches by default are configured to have their native VIDs as **1**. Only change this value if the native VID of the switch connected to this interface is a value other than **1**; match that value here.

b. If this SG appliance is inline to forward or bridge traffic, select enable trunking to make the link to this interface a data link from the router that recognizes VLAN-tagged packets from multiple-VLAN sources.

c. To add more VLANs (not the native VLAN) to the interface, click **Configure > VLANs**.



d. Click **Add** to display the VLAN dialog.

e. Specify the **VLAN ID** (VID) number of the VLAN accepted on this interface.

f. Specify the VLAN IP address and subnet mask.

g. The receiving packet and browser behavior is the same as for physical interfaces. See "Configuring Interface Settings" on page 57".

h. Click **OK** in both dialogs.

7. Click **Apply**.

Related CLI Syntax to Configure an Adapter/Native VLAN

- To enter configuration mode:

```
SGOS#(config) interface fast-ethernet adapter:interface
SGOS#(config) interface adapter:interface
```

- The following VLAN subcommands are available:

```
SGOS#(config interface adapter:interface) native-vlan #
SGOS#(config interface adapter:interface.vlan_id) vlan-trunk {enable |
disable}
```

Configuring Interface Settings

The **Settings** button in the **Interfaces** field allows you to restrict inbound connections on the selected adapter, and to select manual or automatic configuration of the adapter link settings.

The default for Inbound connections is to permit all incoming connections. Although link settings can be automatically configured, Blue Coat recommends manually setting them.

Note: Rejecting inbound connections improperly or manually configuring link settings improperly might cause the SG appliance to malfunction. Ensure that you know the correct settings before attempting either of these. If the SG fails to operate properly after changing these settings, contact Blue Coat Support.

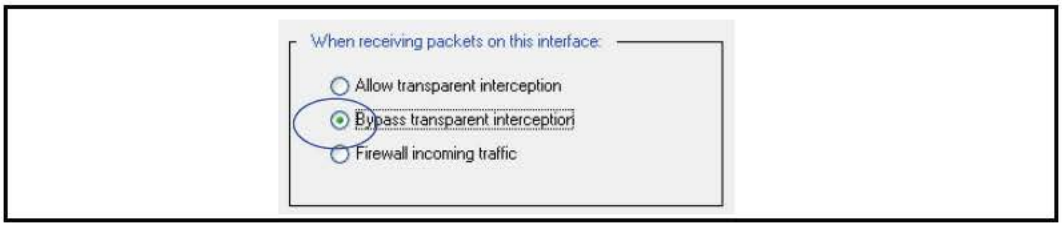
Disabling Transparent Interception

This feature enables the administrator to specify the interfaces that will intercept traffic. By default, the SG appliance intercepts connections in both directions. Using this feature, the administrator can configure it to intercept the connection in only one direction.

Note: To use this feature, `reject-inbound` must be disabled.

To bypass transparent interception:

1. Select **Configuration > Network > Adapters > Adapters**.
2. Select an adapter from the **Adapter** drop-down list.
3. Click **Settings**.



4. Select **Bypass Transparent Interception**.
5. Click **OK** to close the Settings dialog.
6. Click **Apply**.

Related CLI Syntax to Disable Transparent Interception

- To enter configuration mode for standard interfaces:

```
SGOS#(config interface adapter:interface) allow-intercept {enable |
disable}
```

- To enter configuration mode for VLAN interfaces:

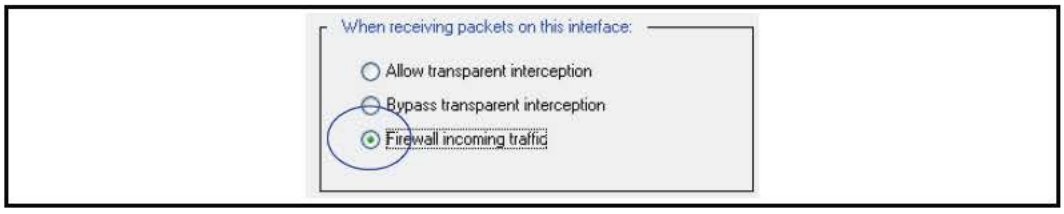
```
SGOS#(config interface adapter:interface.vlan_id) allow-intercept
{enable | disable}
```

Rejecting Inbound Connections

This feature enables the administrator to reject all inbound traffic. If enabled, all inbound traffic is silently dropped—except for console access traffic. The default setting is disabled; the SG appliance allows inbound connections on all network adapters.

To reject inbound connections:

1. Select **Configuration > Network > Adapters > Adapters**.
2. Select an adapter from the **Adapter** drop-down list.
3. Click **Settings**.



4. Select **Firewall Incoming Traffic**.
5. Click **OK** to close the Settings dialog.
6. Click **Apply**.

Related CLI Syntax for Rejecting Inbound Connections

- To enter configuration mode for standard interfaces:

```
SGOS#(config interface adapter:interface) reject-inbound {enable |
disable}
```

- To enter configuration mode for VLAN interfaces:

```
SGOS#(config interface adapter:interface.vlan_id) reject-inbound
{enable | disable}
```

Using reject-inbound and allow-intercept

The `allow-intercept` and `reject-inbound` commands are interface-level configurations and are not bridge-specific. The `reject-inbound` command always has precedence.

The following table describes how traffic is handled for the three possible settings of these options.

Table 6-1. Command Interaction for Reject-Inbound and Allow-Intercept

reject-inbound	allow-intercept	Non-proxy ports (mgmt-console, ssh, etc)	Explicit proxy ports	Transparent proxy ports	Other ports
Disabled	Enabled	Terminated	Terminated	Terminated	Forwarded
Disabled	Disabled	Terminated	Terminated	Forwarded	Forwarded
Enabled	Enabled/ Disabled	Silently dropped	Silently dropped	Silently dropped	Silently dropped

Manually Configuring Link Settings

By default, the SGOS software automatically determines the link settings for all network adapters. However, Blue Coat strongly recommends manually setting the link settings to avoid problems.

To manually configure link settings:

1. Select **Configuration > Network > Adapters > Adapters.**
2. Select an adapter from the **Adapters** drop-down list.
3. Click **Settings**.
4. Select **Manually configure link settings**.
5. Select **Half** or **Full** duplex.
6. Select the correct network speed.
7. Click **OK** to close the Advanced Settings dialog.
8. Click **Apply**.

Related CLI Syntax to Manually Configure Link Settings

- To enter configuration mode for standard interfaces:

```
SGOS#(config interface adapter:interface) {full-duplex | half-duplex}
```

Configuring Proxies

To configure proxies, refer to *Volume 2: Proxies and Proxy Services*.

Detecting Network Adapter Faults

The SG appliance can detect whether the network adapters in an appliance are functioning properly. If the appliance finds that an adapter is faulty, it stops using it. When the fault is remedied, the SG appliance detects the functioning adapter and uses it normally.

To determine whether an adapter is functioning properly:

1. Check whether the link is active (that is, a cable is connected and both sides are up).
2. Check the ratio of error packets to good packets: both sent and received.
3. Check if packets have been sent without any packets received.

If an adapter fault is detected and the adapter has an IP address assigned to it, the SG appliance logs a severe event. When an adapter does not have an IP address, the appliance does not log an entry.

Chapter 7: Software and Hardware Bridges

This chapter describes the SGOS hardware and software bridging capabilities. Network bridging through the SG appliance provides transparent proxy pass-through and failover support.

The following topics are discussed:

About Bridging

Bridging functionality allows SG appliances to be easily deployed as transparent redirection devices, without requiring the additional expense and maintenance of L4 switches or WCCP-capable routers. Bridging is especially useful in smaller deployments in which explicit proxies or L4 switches are not feasible options.

Bridges are used to segment Ethernet collision domains, thus reducing frame collisions. Unlike a hub, a bridge uses a frame's destination MAC address to make delivery decisions. Because these decisions are based on MAC addressing, bridges are known as Layer 2 devices.

To make efficient delivery decisions, the bridge must discover the identity of systems on each collision domain, and then store this information in its bridging table. After learning the identity of the systems on each collision domain, the bridge uses the source MAC address of frames to determine from which interface a given system can be reached.

A branch office that would take advantage of a bridging configuration is likely to be small; for example, it might have only one router and one firewall in the network, as shown below.

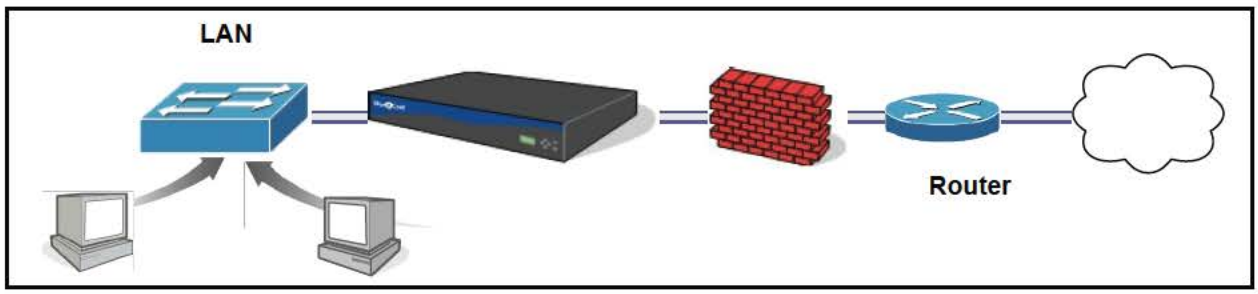


Figure 7-1. A Bridged Configuration

To ensure redundancy, the SG appliance supports both serial and parallel failover modes. See " Configuring Failover" for more information about serial and parallel failover configurations.

About Traffic Handling

Because the bridge intercepts all traffic, you can take advantage of the powerful proxy services and policies built into the SG appliance to control how that traffic is handled. If the SG appliance recognizes the intercepted traffic, you can apply policy to it. Unrecognized traffic is forwarded out. This traffic handling flow is shown in the following figure.

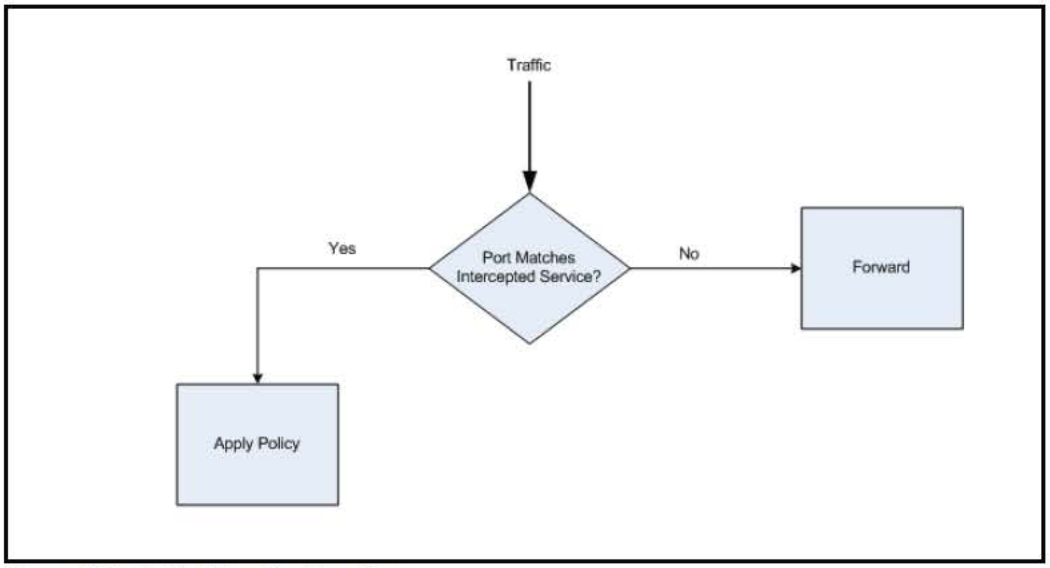


Figure 7-2. Traffic Flow Decision Tree

Because policy can be applied only to recognized protocols, it is important to specify port ranges that will capture all traffic, even that operating on lesser-known ports.

About Bridging Methods

The SG appliance provides bridging functionality by two methods:

- Software—A software, or *dynamic*, bridge is constructed using a set of installed interfaces. Within each logical bridge, interfaces can be assigned or removed.

  See "Configuring Programmable Pass-Through/NIC Adapters" on page 65 for more information.

- Hardware—A hardware, or *pass-through*, bridge uses a 10/100 dual interface Ethernet adapter. This type of bridge provides pass-through support.

  See " About the Pass-Through Adapter" for more information.

Note: If you want to use an L4 switch or an explicit proxy instead of bridging, you must disable the bridging pass-thru card.

About the Pass-Through Adapter

A pass-through adapter is a 10/100 dual interface Ethernet adapter designed by Blue Coat to provide an efficient fault-tolerant bridging solution. If this adapter is installed on an SG appliance, SGOS detects the adapter upon system bootup and automatically creates a bridge—the two Ethernet interfaces serve as the bridge ports. If the SG appliance is powered down or loses power for any reason, the bridge fails open; that is, Web traffic passes from one Ethernet interface to the other. Therefore, Web traffic is uninterrupted, but does not route through the appliance.

Important: This scenario creates a security vulnerability.

Once power is restored to the SG appliance, the bridge comes back online and Web traffic is routed to the appliance and thus is subject to that appliance's configured features, policies, content scanning, and redirection instructions. Note that bridging supports only failover; it does not support load balancing.

Note: The adapter state is displayed on **Configuration > Network > Adapters**.

Reflecting Link Errors

When the SG appliance is deployed transparently with bridging enabled, link errors that occur on one interface can be reflected to the other bridge interface. This allows a router connected to the SG appliance on the healthy link to detect this failure and recompute a path around this failed segment. When the interface with the original link error is brought back up, the other interface is automatically restarted as part of the health check process.

Reflecting link errors requires that two interfaces be available and connected in a bridging configuration; it also requires that the `propagation-failure` option is enabled. By default, `propagation-failure` is disabled.

Note: This feature is only applicable to a two-interface hardware or software bridge. The `propagation-failure` option sets itself to disabled in any other scenario.

If the link goes down while `propagation-failure` is disabled, the previous link state is immediately reflected to the other interface if `propagation-failure` is enabled during this time.

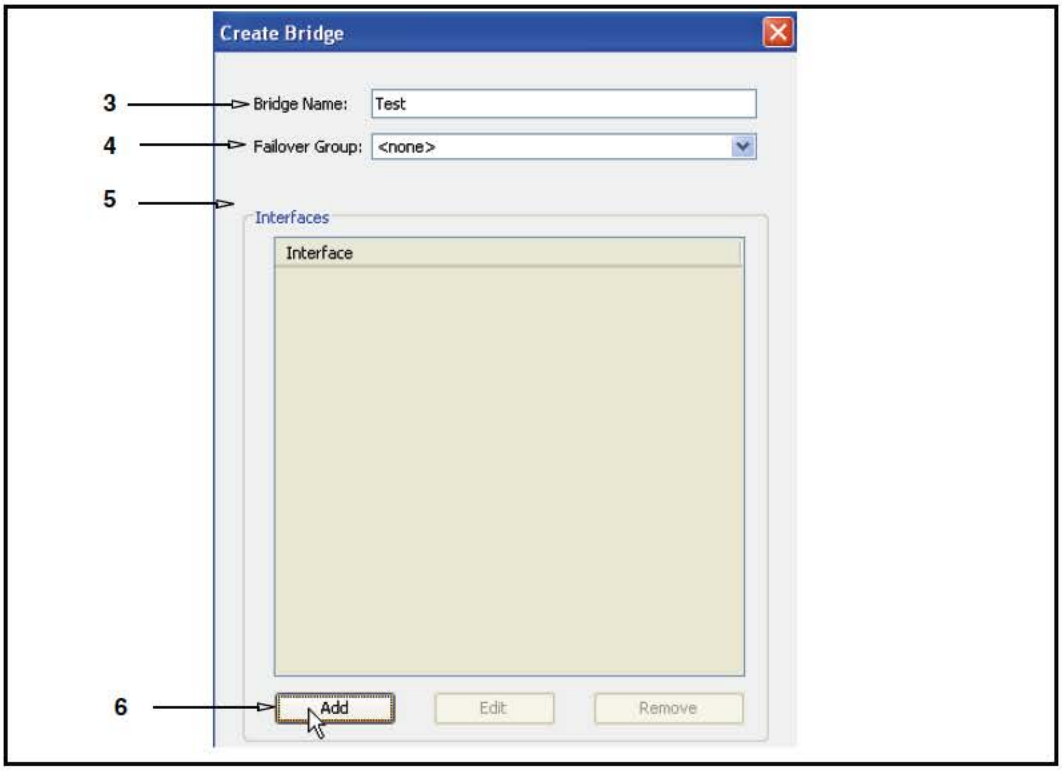
Configuring a Software Bridge

This section describes how to use the Management Console or the CLI to link adapters and interfaces to create a network bridge.

Before configuring a software bridge, ensure that your adapters are of the same type. Although the software does not restrict you from configuring bridges with adapters of different speeds (10/100 or GIGE, for example), the resulting behavior is unpredictable.

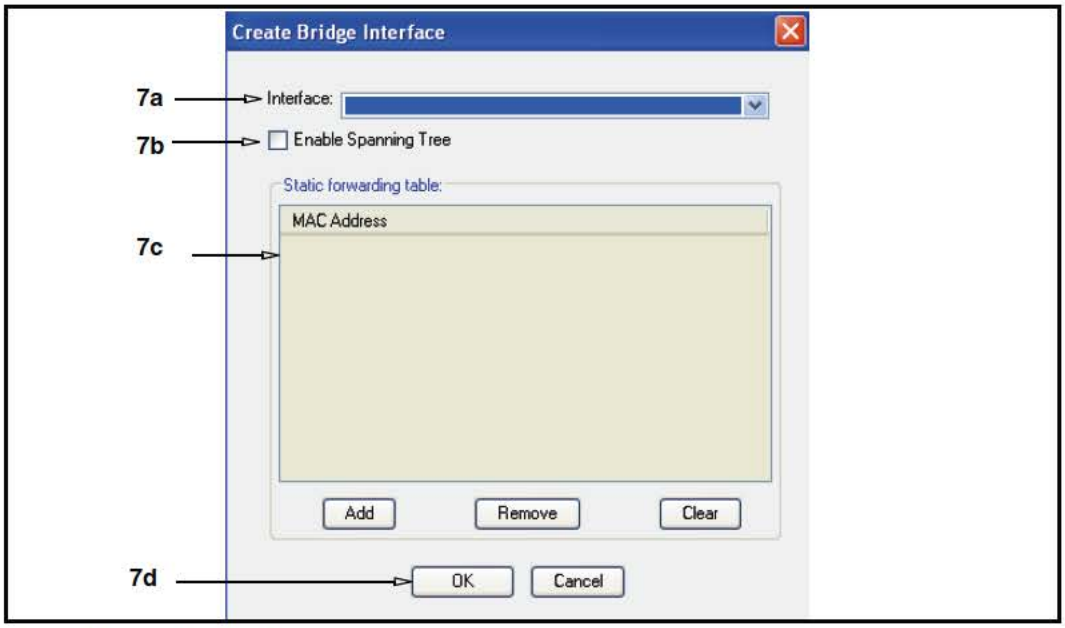
To create and configure a software bridge:

1. Select **Configuration > Network > Adapters > Bridges**.
2. Click **New**.



3. In the **New Bridge Name** field, enter a name for the bridge—up to 16 characters. The bridge name is case insensitive, that is, you cannot name one bridge "ABC" and another bridge "abc".
4. (Optional) If you want to assign the bridge to a failover group select it from the **Failover Group** drop-down list.

   See "Configuring Failover" on page 68 for more information about configuring failover.
5. If you have a two-interface bridge and want to enable link error propagation, select the **Propagation Failure** check box.
6. Click **Add**. The **Add Bridge Interface** dialog displays.



7. Configure the bridge interface options:
   a. From the **Interface** drop-down menu, select an interface.
   b. (Optional) To enable bridging loop avoidance, select **Enable Spanning Tree**. See "Bridging Loop Detection" on page 69 for more information about the Spanning Tree Protocol.
   c. If you are using firewall configurations that require the use of static forwarding table entries, add a static forwarding table entry that defines the next hop gateway that is on the correct side of the bridge. For more information on static forwarding table entries, see"Adding Static Forwarding Table Entries" on page 71.
   d. Click **OK**.
   e. Repeat Step 7 for each interface you want to attach to the bridge.
8. Click **OK** to close the **Create Bridge Interface** and **Create Bridge** dialogs.
9. Select **Apply** to commit the changes to the SG appliance.

Related CLI Syntax to Configure a Software Bridge

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

Configuring Programmable Pass-Through/NIC Adapters

Some Blue Coat appliances ship with a network adapter card that can be used as a pass-through adapter or as a Network Interface Card (NIC), depending on the configured mode. If the network adapter mode is set to disabled, the adapter interfaces can be used as NICs or as part of a software bridge.

If your appliance includes a programmable adapter card, the Edit Bridge dialog displays a **Mode** option that allows you to specify the card behavior. The following programmable adapter modes are available:

- **Disabled**—Disables the bridge and allows the adapter interfaces to be reused as NICs or as part of another bridge.

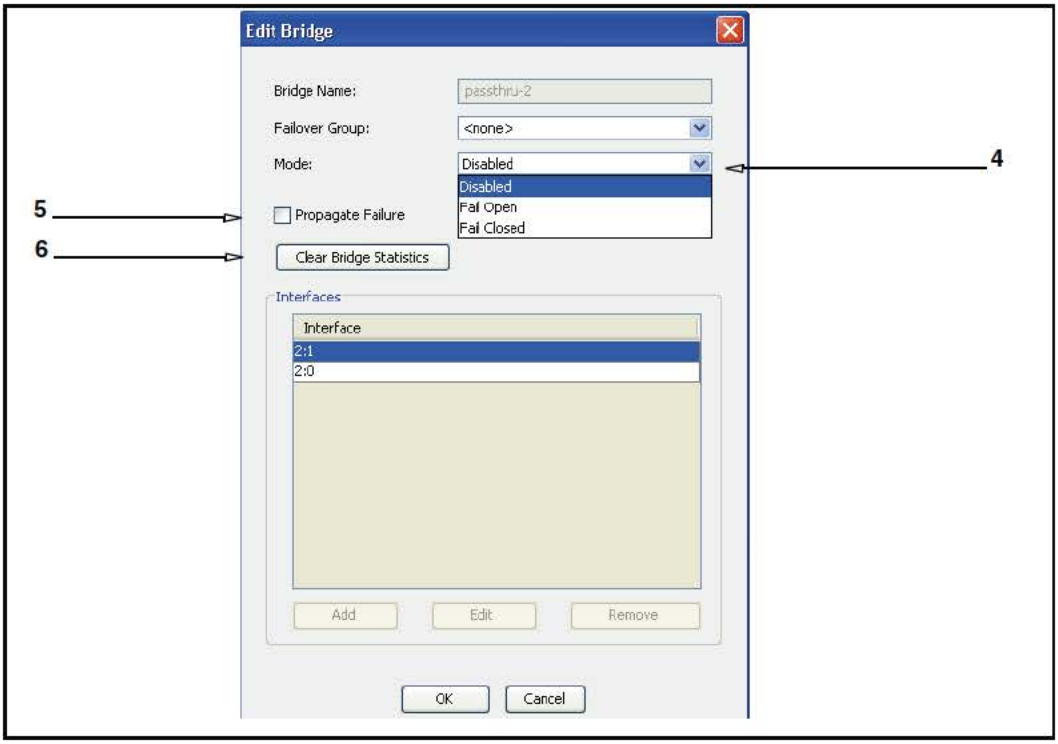
- **Fail Open**—If the SG appliance fails, all traffic passes through the bridge so clients can still receive data.
- **Fail Closed**—If the SG appliance fails, all traffic is blocked and service is interrupted. This mode provides the same functionality as a user-configured software bridge.

Note: If you create a software bridge, the programmable bridge card mode is implicitly Fail Closed (if the appliance fails, the software bridge is non-functional).

The following procedure describes programmable adapter configuration.

To configure the function of the programmable adapter:

1. Select **Configuration** > **Network** > **Adapters** > **Bridges**.
2. In the Bridges section, select the bridge you want to configure.
3. Click **Edit**. The Edit Bridge dialog displays.



4. Select the desired mode from the **Mode** drop-down list.
5. If you have a two-interface bridge and want to enable link error propagation, select the **Propagation Failure** check box.
6. (Optional) Use **Clear Bridge Statistics** to reset the traffic history of the bridge, which includes packet and byte counts, to 0.
7. Click **OK** to save your changes and close the Edit Bridge dialog.
8. Click **Apply** to commit the changes to the SG appliance.

Related CLI Syntax to Configure a Programmable Adapter Card

```
SGOS#(config) bridge
SGOS#(config bridge) edit bridge_name
SGOS#(config bridge bridge_name) mode fail-open
SGOS#(config bridge bridge_name) mode fail-closed
SGOS#(config bridge bridge_name) mode disable
```

Note: If the bridge adapters are not programmable, the `mode` commands are not visible.

Customizing the Interface Settings

To further customize the bridge, edit the interface settings.

Editing the interface settings allows you to

- Allow transparent interception. It is bypassed by default. You must configure the WAN interface to allow transparent interception.

Note: If you have a MACH5 license, a programmable bridge card, and labeled WAN/LAN interfaces, the WAN interface allows transparent interception by default.

- Firewall incoming traffic. Firewalls must be specifically configured.

See "Configuring Interface Settings" on page 57 for more information.

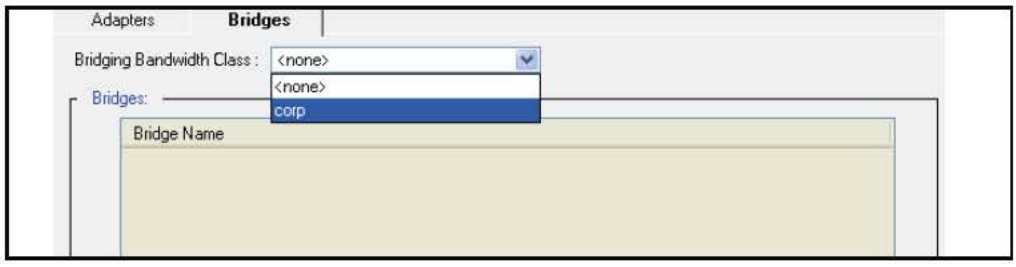
The **Bridge Settings** options allow you to clear bridge forwarding table and clear bridge statistics.

Setting Bandwidth Management for Bridging

After you have created and configured a bandwidth management class for bridging, you can manage the bandwidth used by all bridges. Refer to *Volume 5: Advanced Networking* for more information on bandwidth management.

To configure bandwidth management for bridging:

1. Select **Configuration > Network > Adapters > Bridges**.



2. In the **Bridging Bandwidth Class** drop-down menu, select a bandwidth management class to manage the bandwidth for bridging, or select **<none>** to disable bandwidth management for bridging.
3. Select **Apply** to commit the changes to the SG appliance.

Related CLI Syntax to Set a Bridging Bandwidth Class

```
SGOS#(config bridge) bandwidth-class bridge_name
```

```
SGOS#(config) bandwidth-management
SGOS#(config bandwidth-management) [subcommands]
```

Configuring Failover

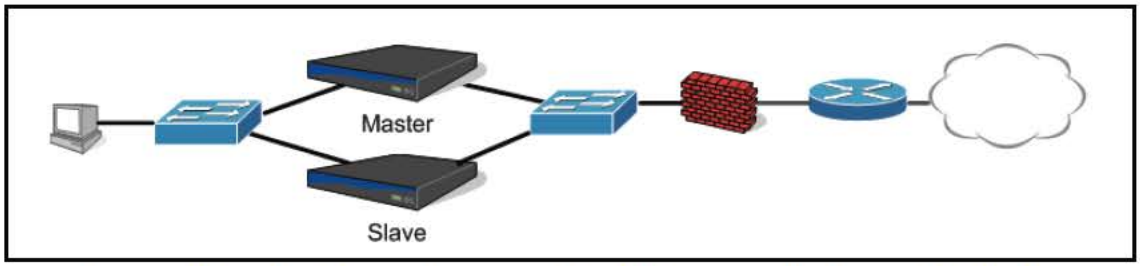
In failover mode, two appliances are deployed, a master and a slave. The master sends keepalive messages (*advertisements*) to the slaves. If the slaves do not receive advertisements at the specified interval, the slave takes over for the master. When the master comes back online, the master takes over from the slave again.

The SGOS bridging feature allows two different types of failover modes, *parallel* and *serial*. Hardware and software bridges allow different failover modes:

- Software bridges allow serial or parallel failover. However, note that if the SG appliance fails, serial failover also fails.
- Hardware bridges allow serial failover only.

Parallel Failover

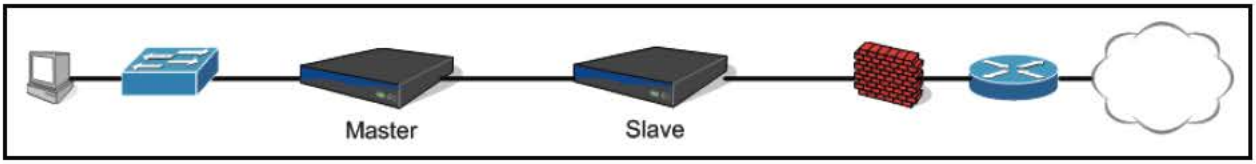
In parallel failover mode, two systems are deployed side by side on redundant paths. In parallel failover, the slave does not actively bridge any packets unless the master fails. If the master fails, the slave takes over the master IP address and begins bridging. A parallel failover configuration is shown in the following figure.



Because of the redundant paths, you must enable Spanning Tree to avoid bridge loops. See "Bridging Loop Detection" on page 69 for more information about STP.

Serial Failover

In serial failover mode, the slave is inline and continuously bridges packets, but does not perform any other operations to the bridged traffic unless the master fails. If the master fails, the slave takes over the master IP address and applies policy, etc. A serial configuration is shown in the following figure.



Setting Up Failover

Failover is accomplished by doing the following:

- Creating virtual IP addresses on each proxy.
- Creating a failover group.
- Attaching the bridge configuration.

- Selecting a failover mode (parallel or serial).

Both proxies can have the same priority (for example, the default priority). In that case, priority is determined by the local IP address—the SG appliance with the highest local IP will assume the role of master.

Example

The following example creates a bridging configuration with one bridge on standby.

Note: This deployment requires a hub on both sides of the bridge or a switch capable of interface mirroring.

- SG A—software bridge IP address: `10.0.0.2`. Create a virtual IP address and a failover group, and designate this group the *master*.

```
SG_A#(config) virtual-ip address 10.0.0.4
SG_A#(config) failover
SG_A#(config failover) create 10.0.0.4
SG_A#(config failover) edit 10.0.0.4
SG_A#(config failover 10.0.0.4) master
SG_A#(config failover 10.0.0.4) enable
```

  The preceding commands create a failover group called `10.0.0.4`. The priority is automatically set to `254` and the failover interval is set to `40`.

- SG B—software bridge IP address: `10.0.0.3`. Create a virtual IP address and a failover group.

```
SG_B#(config) virtual-ip address 10.0.0.4
SG_B#(config) failover
SG_B#(config failover) create 10.0.0.4
SG_B#(config failover) edit 10.0.0.4
SG_B#(config failover 10.0.0.4) enable
```

  In the bridge configuration on *each* SG appliance, attach the bridge configuration to the failover group:

```
SG_A#(config bridge bridge_name) failover group 10.0.0.4
SG_B#(config bridge bridge_name) failover group 10.0.0.4
```

- Specify the failover mode:

```
SG_A#(config bridge bridge_name) failover mode serial
SG_B#(config bridge bridge_name) failover mode serial
```

Bridging Loop Detection

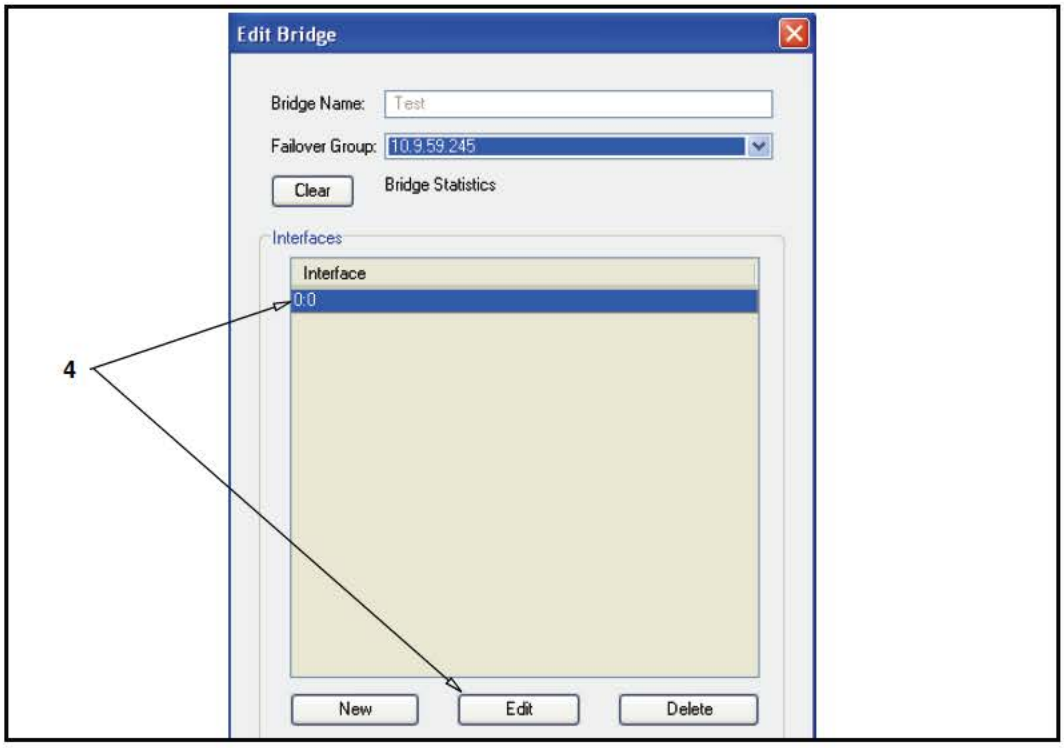
Bridging now supports the Spanning Tree Protocol (STP). STP is a link management protocol that prevents bridge loops in a network that has redundant paths that can cause packets to be bridged infinitely without ever being removed from the network.

STP ensures that a bridge, when faced with multiple paths, uses a path that is loop-free. If that path fails, the algorithm recalculates the network and finds another loop-free path.

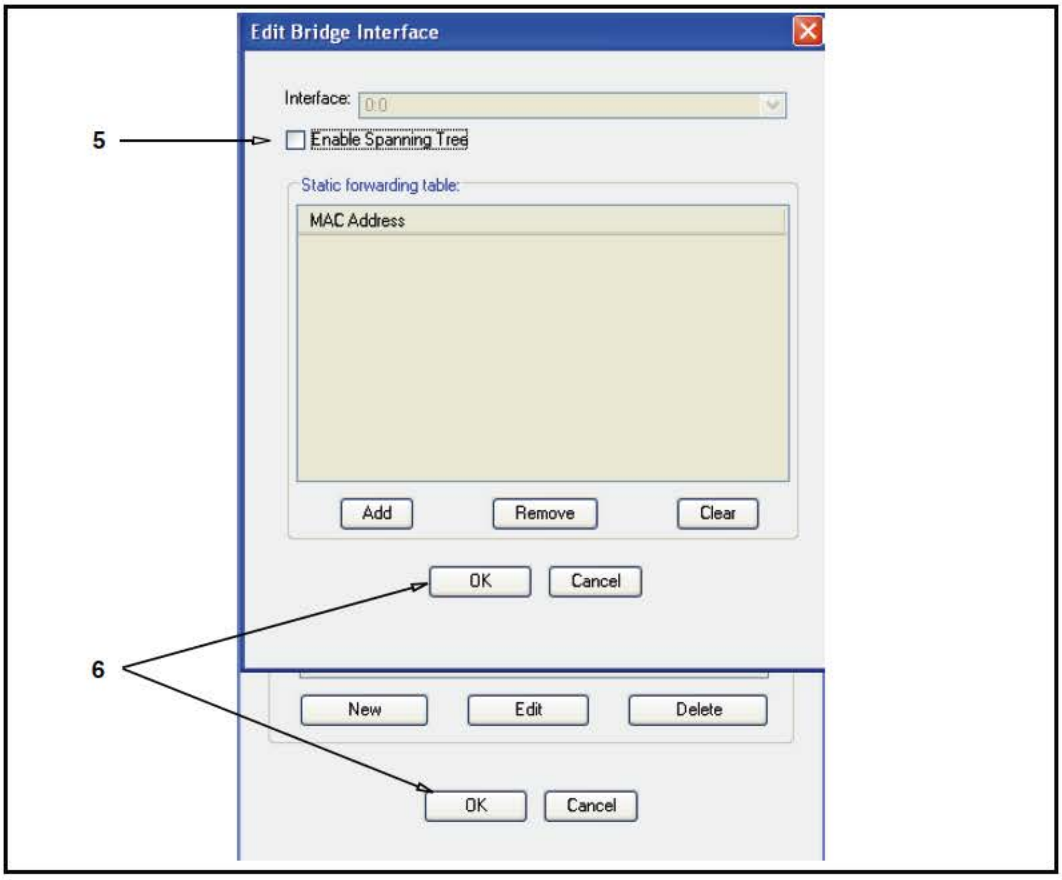
The administrator can enable or disable spanning tree participation for the interface.

Enable spanning tree participation:

1. Select **Configuration > Network > Adapters > Bridges**.
2. Select the desired bridge.
3. Click **Edit**.



4. In the **Edit Bridge** window, highlight the interface you want to configure and click **Edit**. The **Edit Bridge Interface** dialog displays.



5. Click **Enable Spanning Tree**.
6. Click **OK** to close the **Edit Bridge Interface** and **Edit Bridge** windows.
7. Select **Apply** to commit the changes to the SG appliance.

Related CLI Syntax to Enable Spanning Tree Participation:

```
SGOS#(config bridge bridge_name) spanning-tree adapter#:interface#
{enable | disable}
```

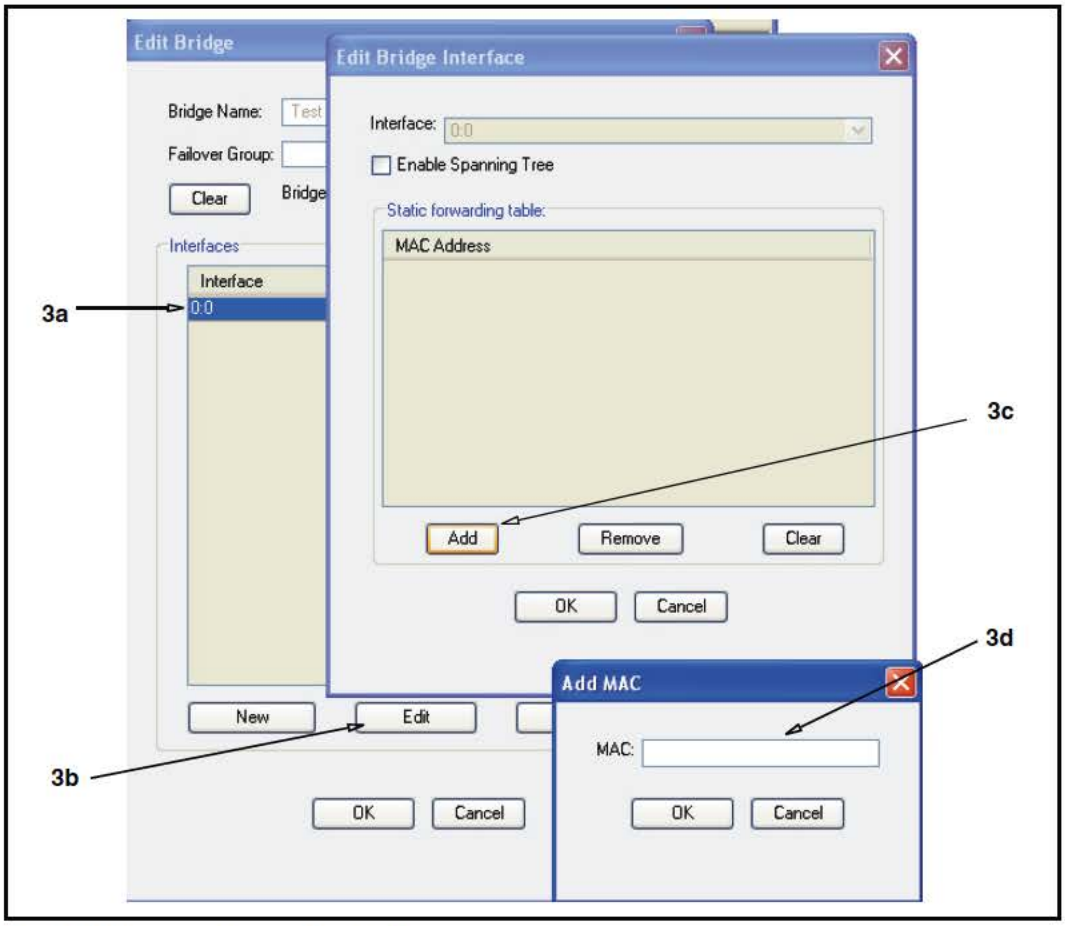
Adding Static Forwarding Table Entries

Certain firewall configurations require the use of static forwarding table entries. Failover configurations use virtual IP (VIP) addresses and virtual MAC (VMAC) addresses. When a client sends an ARP request to the firewall VIP, the firewall replies with a VMAC (which can be an Ethernet multicast address); however, when the firewall sends a packet, it uses a physical MAC address, not the VMAC.

The solution is to create a static forwarding table entry that defines the next hop gateway that is on the correct side of the bridge.

To create a static forwarding table:

1. Select **Configuration > Network > Adapters > Bridges**.
2. Select the bridge you want to edit and click **Edit**. The **Edit Bridge Interface** dialog displays.



3. Add the static forwarding table entry.
   a. In the **Edit Bridge** window, select the interface on which to create the static forwarding table entry.
   b. Click **Edit**.
   c. In the **Edit Bridge Interfaces** window, click **Add**.
   d. In the **Add Mac** window, add the MAC address of the next hop gateway and click **OK**.
4. Click OK to close the **Edit Bridge Interface** and **Edit Bridge** windows.
5. Select **Apply** to commit the changes to the SG appliance.

Related CLI Syntax to Create a Static Forwarding Table Entry

```
SGOS#(config bridge bridge_name) static-fwtable-entry
adapter#:interface# mac-address
```

Bypass List Behavior

The dynamic bypass list is handled differently, depending on the OS version. In SGOS 4.x, packets matching the dynamic bypass list are forwarded in the IP layer. In SGOS 5.x, the packets are forwarded in the bridge layer, which is more appropriate and efficient. For more information on using bypass lists in SGOS 5.x, refer to *Volume 2: Proxies and Proxy Services*.

The behavior of the static bypass list stays the same. The packets are forwarded in IP layer.

Chapter 8: Gateways

A key feature of the SGOS software is the ability to distribute traffic originating at the appliance through multiple gateways. You can also fine tune how the traffic is distributed to different gateways. This feature works with any routing protocol (such as static routes or RIP).

Note: Load balancing through multiple gateways is independent from the per-interface load balancing the SG appliance automatically does when more than one network interface is installed.

This chapter discusses:

- "About Gateways"
- "SG Appliance Specifics" on page 73
- "Switching to a Secondary Gateway" on page 74
- "Routing" on page 74

About Gateways

During the initial setup of the SG appliance, you optionally defined a *gateway* (a device that serves as entrance and exit into a communications network) for the SG appliance.

By using multiple gateways, an administrator can assign a number of available gateways into a preference group and configure the load distribution to the gateways within the group. Multiple preference groups are supported.

The gateway specified applies to all network adapters in the system.

SG Appliance Specifics

Which gateway the SG appliance chooses to use at a given time is determined by how the administrator configures the assignment of preference groups to default gateways. You can define multiple gateways within the same preference group. A SG appliance can have from 1 to 10 preference groups. If you have only one gateway, it automatically has a weight of 100.

Initially, all gateways in the lowest preference group are considered to be the active gateways. If a gateway becomes unreachable, it is dropped from the active gateway list, but the remaining gateways within the group continue to be used until they all become unreachable, or until an unreachable gateway in a lower preference group becomes reachable again. If all gateways in the lowest preference group become unreachable, the gateways in the next lowest preference group become the active gateways.

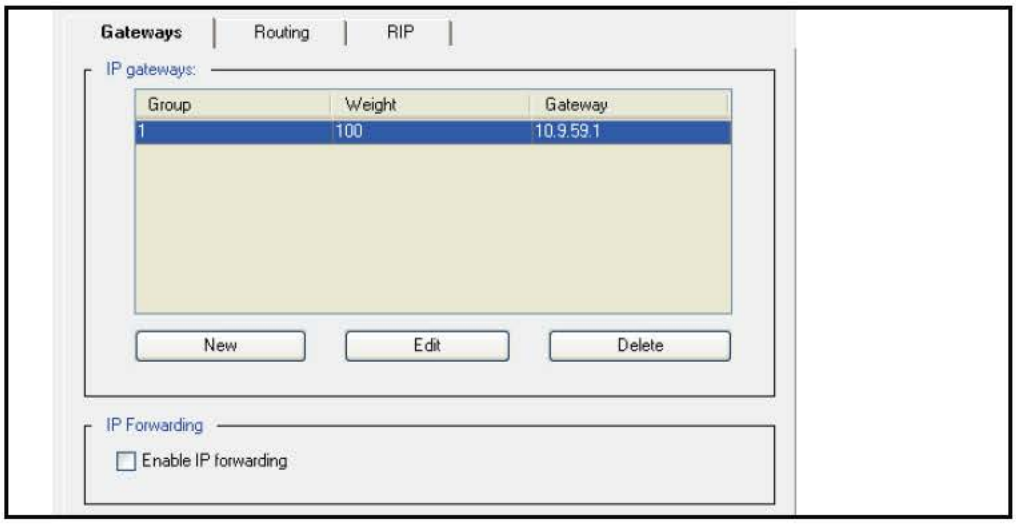
In addition to a preference group, each gateway within a group can be assigned a relative weight value from 1 to 100. The weight value determines how much bandwidth a gateway is given relative to the other gateways in the same group. For example, in a group with two gateways, assigning both gateways the same weight value, whether 1 or 100, results in the same traffic distribution pattern. In a group with two gateways, assigning one gateway a value of 10 and the other gateway a value of 20 results in the SG appliance sending approximately twice the traffic to the gateway with a weight value of 20.

Switching to a Secondary Gateway

When a gateway goes down, the networking code detects the unreachable gateway in 20 seconds, and the switch over takes place immediately if a secondary gateway is configured. All configured gateways are affected, not just default gateways, as was the case in earlier releases.

To configure multiple gateway load balancing:

1. Select **Configuration > Network > Routing > Gateways**.



2. Click **New**.
3. Enter the IP address, group, and weight for the gateway into the Add list item dialog that appears.
4. Click **OK**.
5. Repeat steps 2 to 4 until IP addresses, groups, and weights have been defined for all of your gateways.
6. Select **Apply** to commit the changes to the SG appliance.

Related CLI Syntax to Configure Multiple Gateway Load Balancing

```
SGOS#(config) ip-default-gateway ip_address preference_group weight
```

Routing

By default, routing is done transparently if the SG appliance can verify (trust) the destination IP addresses provided by the client. If the destination IP addresses cannot be trusted, the SG appliance uses static routes.

Note: If your environment uses explicit proxy or Layer-4 redirection, or if the destination IP addresses cannot be verified by the SG appliance, static routes must be configured.

Hardware or software bridges can be transparently routed if the destination IP address/hostname can be verified. If the client-provided destination IP address is not in the list of resolved IP addresses for the particular host, then the SG appliance uses static routes instead. For hostname-less protocols such as CIFS and FTP, the IP address can always be trusted. For other protocols, such as HTTP, RTSP, and MMS, which have a hostname that must be resolved, verification can be an issue. URL rewrites that modify the hostname also can cause verification to fail.

Transparent ADN connections that are handed off to an application proxy (HTTP or MAPI, for example) can utilize L2/L3 transparency. Also, transparent ADN connections that are tunneled but not handed off can utilize the functionality.

Note: IM is not supported with trust client addressing. In order to login and chat, the default router must have Internet access. Other IM features require direct connections, so static routes are required.

This feature is not user-configurable.

Using Static Routes

If you use an explicit proxy or layer-4 redirection deployment, or a Blue Coat feature such as forwarding where the destination IP cannot be verified by the SG appliance, you can use static routes.

A static route is a manually-configured route that specifies the transmission path a packet must follow, based on the packet's destination address. A static route specifies a transmission path to another network, and a default static route already exists.

Situations in which static routes are used include:

- DNS load balancing. Sites that use DNS load balancing and return a single IP address cause a mismatch between the IP address provided by the client and the IP address resolved by the SG appliance.
- Anywhere that appropriate client-side routing information is unavailable, such as for forwarding hosts, dynamic categorization, and ADN peers.

Note: For bridged deployments, transparent routing, in most cases, overrides any static route lookups.

The routing table is a text file containing a list of IP addresses, subnet masks, and gateways. You are limited to 10,000 entries in the static routes table. The following is a sample router table:

```
10.25.36.0   255.255.255.0   10.25.36.1
10.25.37.0   255.255.255.0   10.25.37.1
10.25.38.0   255.255.255.0   10.25.38.1
```

When a routing table is installed, all requested URLs are compared to the list and routed based on the best match.

You can install the routing table several ways.

- Using the Text Editor, which allows you to enter settings (or copy and paste the contents of an already-created file) directly onto the appliance.
- Creating a local file on your local system; the SG appliance can browse to the file and install it.
- Using a remote URL, where you place an already-created file on an FTP or HTTP server to be downloaded to the SG appliance.
- Using the CLI `inline static-route-table` command, which allows you to paste a static route table into the SG appliance.
- Using the CLI `static-routes` command, which requires that you place an already-created file on an FTP or HTTP server and enter the URL into the SG appliance.

Note: If you upgrade to SGOS 5.x from SGOS 4.x, entries from the central and local bypass lists are converted to static route entries in the static route table. The converted static route entries are appended after the existing static route entries. Duplicate static route entries are silently ignored.

All traffic leaving the SG appliance is affected by the static route entries created from the SGOS 4.x bypass lists.

Installing a Routing Table

To install a routing table:

1. Select **Configuration > Network > Routing > Routing**.
2. From the drop-down list, select the method used to install the routing table; click **Install**.
   - Remote URL:

     Enter the fully-qualified URL, including the filename, where the routing table is located. To view the file before installing it, click **View**. Click **Install**. To view the installation results, click **Results**; close the window when you are finished. Click **OK**.
   - Local File:

     Click **Browse** to bring up the Local File Browse window. Browse for the file on the local system. Open it and click **Install**. When the installation is complete, a results window opens. View the results and close the window.
   - Text Editor:

     The current configuration is displayed in installable list format. You can customize it or delete it and create your own. Click **Install**. When the installation is complete, a results window opens. View the results, close this window, and click **Close**.
3. Click **Apply** to commit the changes to the SG appliance.

Related CLI Syntax to Install a Routing Table

To install a routing table, you can use the `inline` command to install the table directly, or enter a path to a remote URL that has an already-created text file ready to download.

- To paste a static route table directly into the CLI:

```
SGOS#(config) inline static-route-table end-of-file_marker
paste static routing table
eof
  ok
```

- To enter the static route table manually:

```
SGOS#(config) inline static-route-table end-of-file_marker
10.25.36.0   255.255.255.0   10.25.46.57
10.25.37.0   255.255.255.0   10.25.46.58
10.25.38.0   255.255.255.0   10.25.46.59
eof
  ok
```

- To enter a path to a remote URL:

```
SGOS#(config) static-routes path url
SGOS#(config) load static-route-table
```

Notes

- Any deployment that causes traffic to traverse the link from the SG appliance to the home router twice is not supported. Some WCCP configurations might not work as expected.
- If you use URL host rewrite functionality in your policies, mismatches can occur between the client-provided IP address and the resolved, rewritten hostname. In these cases, static routing is used.

Chapter 9: DNS

During first-time installation of the SG appliance, you configured the IP address of a single primary Domain Name Service (DNS) server. Using the **Configuration > Network > DNS** tab, you can change this primary DNS server at any time, and you can also define additional primary DNS servers and one or more alternate DNS servers.

This chapter discusses:

SG Appliance Specifics

If you have defined more than one DNS server, the SGOS software uses the following logic to determine which servers are used to resolve a DNS host name and when to return an error to the client:

- SGOS first sends requests to DNS servers in the primary DNS server list.
- Servers are always contacted in the order in which they appear in a list.
- The next server in a list is only contacted if the SG appliance does not receive a response from the current server.
- If none of the servers in a list returns a response, the SG appliance returns an error to the client.
- The SG appliance only sends requests to servers in the alternate DNS server list if a server in the primary list indicates that a DNS host name cannot be resolved.

  If a DNS server returns any other error (other than an indication that a DNS host name could not be resolved), the SG appliance returns the error to the client.

  If a server in both the primary and alternate DNS server lists are unable to resolve a DNS host name, an error is returned to the client.

The SG appliance always attempts to contact the first server in the primary DNS server. If a response is received from this server, no attempts are made to contact any other DNS servers in the primary list.

If the response from the first primary DNS server indicates a name error, the SG appliance sends a DNS request to the first alternate DNS server, if one is defined. If no alternate DNS servers have been defined, an error is returned to the client indicating a name error. If the first alternate DNS server is unable to resolve the IP address, a name error is returned to the client, and no attempt is made to contact any other DNS servers in either the primary or alternate DNS server lists.

If a response is not received from any DNS server in a particular DNS server list, the SG appliance sends a DNS request to the next server in the list. The SG appliance returns a name error to the client if none of the servers in a DNS server list responds to the DNS request.

Note: The alternate DNS server is not used as a failover DNS server. It is only used when DNS resolution of primary DNS server returns name error. If a timeout occurs when looking up the primary DNS server, no alternate DNS server is contacted.

If the SG appliance receives a negative DNS response (a response with an error code set to Name Error), it caches that negative response. You can configure the SG appliance's negative response time-to-live value. (A value of zero disables negative caching.) If the SG appliance is not configured (the default), the SG appliance caches the negative response and uses the TTL value from the DNS response to determine how long it should be cached.

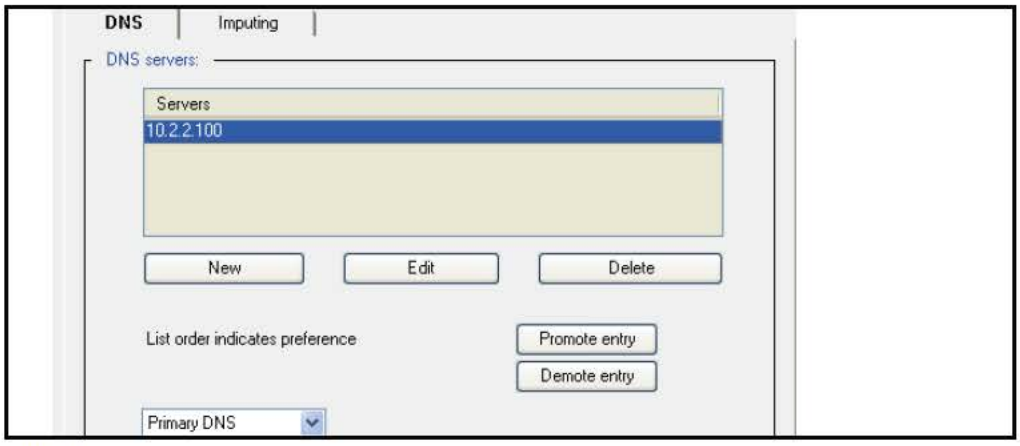
Configuring Split DNS Support

Customers with split DNS server configuration (for example, environments that maintain private internal DNS servers and external DNS servers) might choose to populate an Alternate DNS server list as well as the Primary DNS server list. In the SG appliance, the internal DNS servers are placed in the Primary list, while external DNS servers (with the Internet information) populate the Alternate list.

Complete the following procedures to configure primary and alternate DNS servers.

To add a primary DNS server:

1. Select **Configuration > Network > DNS > DNS**.



2. Click **New**.
3. Enter the IP address of the DNS server in the dialog that appears and click **OK**.
4. Select **Apply** to commit the changes to the SG appliance.

Related CLI Syntax to Add a DNS Server

To add a primary DNS server:

```
SGOS#(config) dns server ip_address
```

To Add an Alternate DNS Server

1. Select **Configuration > Network > DNS > DNS**.

   The DNS tab displays.
2. Select **Alternate DNS** in the drop-down list.
3. Click **New**.
4. Enter the IP address of the DNS server in the dialog that appears and click **OK**.
5. Select **Apply** to commit the changes to the SG appliance.

Related CLI Syntax to Adding an Alternate DNS Server

To add an alternate DNS server:

```
SGOS#(config) dns alternate ip_address
```

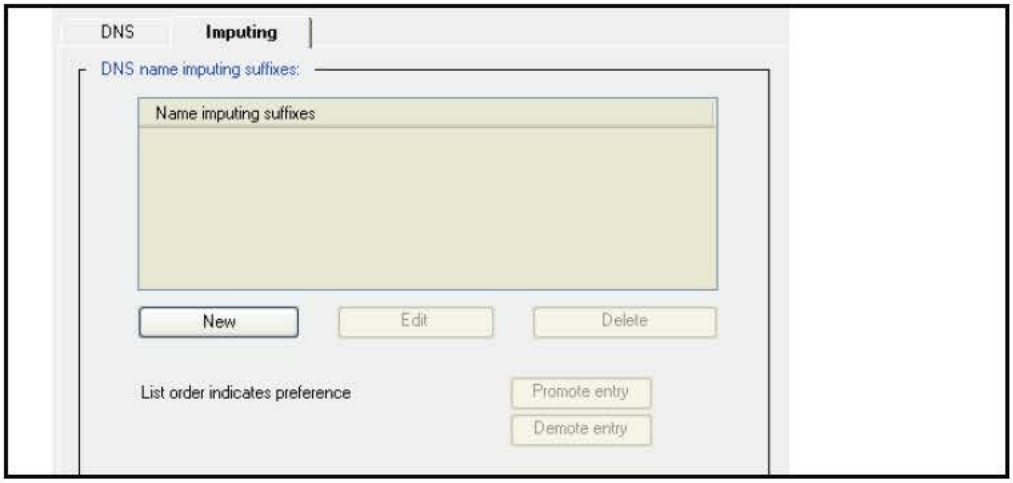
Repeat until alternate DNS servers have been defined.

Changing the Order of DNS Servers

The SG appliance uses DNS servers in the order displayed. You can organize the list of servers so that the preferred servers appear at the top of the list. This functionality is not available through the CLI.

To change the order of DNS servers:

1. Select **Configuration > Network > DNS > Imputing**.



2. Select the DNS server to promote or demote.
3. Click **Promote entry** or **Demote entry** as appropriate.
4. Select **Apply** to commit the changes to the SG appliance.

Unresolved Hostnames (Name Imputing)

Name imputing allows the SG appliance to resolve host names based on a partial name specification. When the SG appliance submits a host name to the DNS server, the DNS server resolves the name to an IP address. The SG appliance queries the original hostname before checking imputing entries unless there is no period in the host name, in which case imputing is applied first. The SG appliance tries each entry in the name-imputing list until the name is resolved or it comes to the end of the list. If by the end of the list the name is not resolved, the SG appliance returns a DNS failure.

For example, if the name-imputing list contains the entries `company.com` and `com`, and a user submits the URL `http://www.eedept`, the SG appliance resolves the host names in the following order.

```
http://www.eedept
http://www.eedept.company.com
http://www.eedept.com
```

To add names to the imputing list:

1. Select **Configuration > Network > DNS > Imputing**.

   The Imputing tab displays.

2. Click **New** to add a new name to the imputing list.
3. Enter the name in the dialog that appears and click **OK**.
4. Select **Apply** to commit the changes to the SG appliance.

Related CLI Syntax to Add Names to the Imputing List

To add names to the imputing list:

```
SGOS#(config) dns imputing suffix
```

For example, to use `company.com` as the imputing suffix, enter `dns-imputing company.com`.

Repeat until all imputing suffixes have been entered.

Changing the Order of DNS Name Imputing Suffixes

The SG appliance uses imputing suffixes in the order displayed. You can organize the list of suffixes so the preferred suffix appears at the top of the list. This functionality is only available through the Management Console. You cannot configure it through the CLI.

To change the order of DNS name imputing suffixes:

1. Select **Configuration > Network > DNS > Imputing**.

   The Imputing tab displays.

2. Select the imputing suffix to promote or demote.
3. Click **Promote entry** or **Demote entry** as appropriate.
4. Select **Apply** to commit the changes to the SG appliance.

Caching Negative Responses

By default, the SG appliance caches negative DNS responses sent by a DNS server. You can configure the SG appliance to set the time-to-live (TTL) value for a negative DNS response to be cached. You can also disable negative DNS response caching.

Note: The SG appliance generates more DNS requests when negative caching is disabled.

The SG appliance supports caching of both type A and type PTR DNS negative responses.

This functionality is only available through the CLI. You cannot configure DNS negative caching through the Management Console.

To configure negative caching TTL values:

From the `(config)` prompt:

```
SGOS#(config) dns negative-cache-ttl-override seconds
```

where *seconds* is any integer between 0 and 600.

Setting the TTL value to 0 seconds disables negative DNS caching; setting the TTL setting to a non-zero value overrides the TTL value from the DNS response.

To restore negative caching defaults:

From the `(config)` prompt):

```
SGOS#(config) dns no negative-cache-ttl-override
```

Appendix A: Glossary

A

access control list	Allows or denies specific IP addresses access to a server.
access log	A list of all the requests sent to an appliance. You can read an access log using any of the popular log-reporting programs. When a client uses HTTP streaming, the streaming entry goes to the same access log.
account	A named entity that has purchased the appliance or the Entitlements from Blue Coat.
activation code	A string of approximately 10 characters that is generated and mailed to customers when they purchase the appliance.
active content stripping	Provides a way to identify potentially dangerous mobile or active content and scripts, and strip them out of a response.
active content types	Used in the Visual Policy Manager. Referring to Web Access policies, you can create and name lists of active content types to be stripped from Web pages. You have the additional option of specifying a customized message to be displayed to the user
administration access policy	A policy layer that determines who can access the SG appliance to perform administrative tasks.
administration authentication policy	A policy layer that determines how administrators accessing the SG appliance must authenticate.
Application Delivery Network (ADN)	A WAN that has been optimized for acceleration and compression by Blue Coat. This network can also be secured through the use of appliance certificates. An ADN network is composed of an ADN manager and backup ADN manager, ADN nodes, and a network configuration that matches the environment.
ADN backup manager	Takes over for the ADN manager in the event it becomes unavailable. See *ADN manager.*
ADN manager	Responsible for publishing the routing table to SG Clients (and to other SG appliances).
ADN optimize attribute	Controls whether to optimize bandwidth usage when connecting upstream using an ADN tunnel.
asx rewrite	Allows you to rewrite URLs and then direct a client's subsequent request to the new URL. One of the main applications of ASX file rewrites is to provide explicit proxy-like support for Windows Media Player 6.4, which cannot set explicit proxy mode for protocols other than HTTP.
audit	A log that provides a record of who accessed what and how.

authenticate-401 attribute	All transparent and explicit requests received on the port always use transparent authentication (cookie or IP, depending on the configuration). This is especially useful to force transparent proxy authentication in some proxy-chaining scenarios
authenticated content	Cached content that requires authentication at the origin content server (OCS). Supported authentication types for cached data include basic authentication and IWA (or NTLM).
authentication	Allows you to verify the identity of a user. In its simplest form, this is done through usernames and passwords. Much more stringent authentication can be employed using digital certificates that have been issued and verified by a Certificate Authority. *See also* basic authentication, proxy authentication, and SSL authentication.
authentication realm	Authenticates and authorizes users to access SG services using either explicit proxy or transparent proxy mode. These realms integrate third-party vendors, such as LDAP, Windows, and Novell, with the Blue Coat operating system.
authorization	The permissions given to an authenticated user.

B

bandwidth class	A defined unit of bandwidth allocation.
bandwidth class hierarchy	Bandwidth classes can be grouped together in a class hierarchy, which is a tree structure that specifies the relationship among different classes. You create a hierarchy by creating at least one parent class and assigning other classes to be its children.
bandwidth management	Classify, control, and, if needed, limit the amount of bandwidth used by network traffic flowing in or out of an SG appliance.
basic authentication	The standard authentication for communicating with the target as identified in the URL.
BCAAA	Blue Coat Authentication and Authorization Agent. Allows SGOS 5.x to manage authentication and authorization for IWA, CA eTrust SiteMinder realms, Oracle COREid, Novell, and Windows realms. The agent is installed and configured separately from SGOS 5.x and is available from the Blue Coat Web site.
BCLP	Blue Coat Licensing Portal.
byte-range support	The ability of the SG appliance to respond to byte-range requests (requests with a `Range:` HTTP header).

C

cache	An "object store," either hardware or software, that stores information (objects) for later retrieval. The first time the object is requested, it is stored, making subsequent requests for the same information much faster. A cache helps reduce the response time and network bandwidth consumption on future, equivalent requests. The SG appliance serves as a cache by storing content from many users to minimize response time and prevent extraneous network traffic.
cache control	Allows you to configure which content the SG appliance stores.

cache efficiency	A tab found on the Statistics pages of the Management Console that shows the percent of objects served from cache, the percent loaded from the network, and the percent that were non-cacheable.
cache hit	Occurs when the SG appliance receives a request for an object and can serve the request from the cache without a trip to the origin server.
cache miss	Occurs when the appliance receives a request for an object that is not in the cache. The appliance must then fetch the requested object from the origin server. .
cache object	Cache contents includes all objects currently stored by the SG appliance. Cache objects are not cleared when the SG appliance is powered off.
Certificate Authority (CA)	A trusted, third-party organization or company that issues digital certificates used to create digital signatures and public key/private key pairs. The role of the CA is to guarantee that the individuals or company representatives who are granted a unique certificate are who they claim to be.
child class (bandwidth gain)	The child of a parent class is dependent upon that parent class for available bandwidth (they share the bandwidth in proportion to their minimum/maximum bandwidth values and priority levels). A child class with siblings (classes with the same parent class) shares bandwidth with those siblings in the same manner.
client consent certificates	A certificate that indicates acceptance or denial of consent to decrypt an end user's HTTPS request.
client-side transparency	A way of replacing the appliance IP address with the Web server IP address for all port 80 traffic destined to go to the client. This effectively conceals the SG appliance address from the client and conceals the identity of the client from the Web server.
concentrator	An SG appliance, usually located in a data center, that provides access to data center resources, such as file servers.
content filtering	A way of controlling which content is delivered to certain users. SG appliances can filter content based on content categories (such as gambling, games, and so on), type (such as http, ftp, streaming, and mime type), identity (user, group, network), or network conditions. You can filter content using vendor-based filtering or by allowing or denying access to URLs.

D

default boot system	The system that was successfully started last time. If a system fails to boot, the next most recent system that booted successfully becomes the default boot system.
default proxy listener	*See* proxy service (d efault).
denial of service (DoS)	A method that hackers use to prevent or deny legitimate users access to a computer, such as a Web server. DoS attacks typically send many request packets to a targeted Internet server, flooding the server's resources and making the system unusable. Any system connected to the Internet and equipped with TCP-based network services is vulnerable to a DoS attack. The SG appliance resists DoS attacks launched by many common DoS tools. With a hardened TCP/IP stack, SG appliance resists common network attacks, including traffic flooding.

destination objects	Used in Visual Policy Manager. These are the objects that define the target location of an entry type.
detect protocol attribute	Detects the protocol being used. Protocols that can be detected include: HTTP, P2P (eDonkey, BitTorrent, FastTrack, Gnutella), SSL, and Endpoint Mapper.
diagnostic reporting	Found in the Statistics pane, the Diagnostics tab allows you to control whether Daily Heartbeats and/or Blue Coat Monitoring are enabled or disabled.
directives	Commands used in installable lists to configure forwarding and SOCKS gateway.
DNS access	A policy layer that determines how the SG appliance processes DNS requests.
domain name system (DNS)	An Internet service that translates domain names into IP addresses. *See also* private DNS or public DNS.
dynamic bypass	Provides a maintenance-free method for improving performance of the SG appliance by automatically compiling a list of requested URLs that return various kinds of errors.
dynamic real-time rating (DRTR)	Used in conjunction with the Blue Coat Web Filter (BCWF), DRTR (also known as *dynamic categorization*) provides real-time analysis and content categorization of requested Web pages to solve the problem of new and previously unknown uncategorized URLs—those not in the database. When a user requests a URL that has not already been categorized by the BCWF database (for example, a brand new Web site), the SG appliance dynamic categorization service analyzes elements of the requested content and assigns a category or categories. The dynamic service is consulted *only* when the installed BCWF database does not contain category information for an object.

E

early intercept attribute	Controls whether the proxy responds to client TCP connection requests before connecting to the upstream server. When early intercept is disabled, the proxy delays responding to the client until after it has attempted to contact the server.
ELFF-compatible format	A log type defined by the W3C that is general enough to be used with any protocol.
emulated certificates	Certificates that are presented to the user by SG appliance when intercepting HTTPS requests. Blue Coat emulates the certificate from the server and signs it, copying the subjectName and expiration. The original certificate is used between the SG appliance and the server.
encrypted log	A log is encrypted using an external certificate associated with a private key. Encrypted logs can only be decrypted by someone with access to the private key. The private key is not accessible to the SG appliance.
EULA	End user license agreement.
event logging	Allows you to specify the types of system events logged, the size of the event log, and to configure Syslog monitoring. The appliance can also notify you by email if an event is logged. *See also* access logging.

explicit proxy	A configuration in which the browser is explicitly configured to communicate with the proxy server for access to content. This is the default for the SG appliance, and requires configuration for both browser and the interface card.
extended log file format (ELFF)	A variant of the common log file format, which has two additional fields at the end of the line—the referer and the user agent fields.

F

fail open/closed	Failing open or closed applies to forwarding hosts and groups and SOCKS gateways. Fail open or closed applies when health checks are showing sick for each forwarding or SOCKS gateway target in the applicable fail-over sequence. If no systems are healthy, the SG appliance fails open or closed, depending on the configuration. If closed, the connection attempt simply fails. If open, an attempt is made to connect without using any forwarding target (or SOCKS gateway). Fail open is usually a security risk; fail closed is the default if no setting is specified.
filtering	*See* content filtering.
forward proxy	A proxy server deployed close to the clients and used to access many servers. A forward proxy can be explicit or transparent.
FTP	*See* Native FTP; Web FTP.

G

gateway	A device that serves as entrance and exit into a communications network.

H

hardware serial number	A string that uniquely identifies the appliance; it is assigned to each unit in manufacturing.
health check tests	The method of determining network connectivity, target responsiveness, and basic functionality. The following tests are supported: • ICMP • TCP • SSL • HTTP • HTTPS • Group • Composite and reference to a composite result • ICAP • Websense • DRTR rating service

health check type	The kind of device or service the specific health check tests. The following types are supported: • Forwarding host and forwarding group • SOCKS gateway and SOCKS gateway group • CAP service and ICAP service group • Websense off-box service and Websense off-box service group • DRTR rating service • User-defined host and a user-defined composite
heartbeat	Messages sent once every 24 hours that contain the statistical and configuration data for the SG appliance, indicating its health. Heartbeats are commonly sent to system administrators and to Blue Coat. Heartbeats contain no private information, only aggregate statistics useful for pre-emptively diagnosing support issues. The SG appliance sends emergency heartbeats whenever it is rebooted. Emergency heartbeats contain core dump and restart flags in addition to daily heartbeat information.
host affinity	The attempt to direct multiple connections by a single user to the same group member. Host affinity is closely tied to load balancing behavior; both should be configured if load balancing is important.
host affinity timeout	The host affinity timeout determines how long a user remains idle before the connection is closed. The timeout value checks the user's IP address, SSL ID, or cookie in the host affinity table.

I

inbound traffic (bandwidth gain)	Network packets flowing into the SG appliance. Inbound traffic mainly consists of the following: • Server inbound: Packets originating at the origin content server (OCS) and sent to the SG appliance to load a Web object. • Client inbound: Packets originating at the client and sent to the SG appliance for Web requests.
installable lists	Installable lists, comprised of directives, can be placed onto the SG appliance in one of the following ways: • Creating the list using the SG text editor • Placing the list at an accessible URL • Downloading the directives file from the local system
integrated host timeout	An integrated host is an origin content server (OCS) that has been added to the health check list. The host, added through the `integrate_new_hosts` property, ages out of the integrated host table after being idle for the specified time. The default is 60 minutes.
intervals	Time period from the completion of one health check to the start of the next health check.
IP reflection	Determines how the client IP address is presented to the origin server for explicitly proxied requests. All proxy services contain a reflect-ip attribute, which enables or disables sending of client's IP address instead of the SG's IP address.

issuer keyring	The keyring used by the SG appliance to sign emulated certificates. The keyring is configured on the appliance and managed through policy.

L

licensable component (LC)	(Software) A subcomponent of a license; it is an option that enables or disables a specific feature.
license	Provides both the right and the ability to use certain software functions within an AV (or SG) appliance. The license key defines and controls the license, which is owned by an account.
listener	The service that is listening on a specific port. A listener can be identified by any destination IP/subnet and port range. Multiple listeners can be added to each service.
live content	Also called live broadcast. Used in streaming, it indicates that the content is being delivered fresh.
LKF	License key file.
load balancing	A way to share traffic requests among multiple upstream systems or multiple IP addresses on a single host.
local bypass list	A list you create and maintain on your network. You can use a local bypass list alone or in conjunction with a central bypass list. *See* bypass list.
local policy file	Written by enterprises (as opposed to the central policy file written by Blue Coat); used to create company- and department-specific advanced policies written in the Blue Coat Policy Language (CPL).
log facility	A separate log that contains a single logical file and supports a single log format. It also contains the file's configuration and upload schedule information as well as other configurable information such as how often to rotate (switch to a new log) the logs at the destination, any passwords needed, and the point at which the facility can be uploaded.
log format	The type of log that is used: NCSA/Common, SQUID, ELFF, SurfControl, or Websense. The proprietary log types each have a corresponding pre-defined log format that has been set up to produce exactly that type of log (these logs cannot be edited). In addition, a number of other ELFF type log formats are also pre-defined (im, main, p2p, ssl, streaming). These can be edited, but they start out with a useful set of log fields for logging particular protocols understood by the SG appliance. It is also possible to create new log formats of type ELFF or Custom which can contain any desired combination of log fields.
log tail	The access log tail shows the log entries as they get logged. With high traffic on the SG appliance, not all access log entries are necessarily displayed. However, you can view all access log information after uploading the log.

M

MACH5	SGOS 5 MACH5 Edition.

Management Console	A graphical Web interface that lets you to manage, configure, monitor, and upgrade the SG appliance from any location. The Management Console consists of a set of Web pages and Java applets stored on the SG appliance. The appliance acts as a Web server on the management port to serve these pages and applets.
management information base (MIB)	Defines the statistics that management systems can collect. A managed device (gateway) has one or more MIBs as well as one or more SNMP agents, which implements the information and management functionality defined by a specific MIB.
maximum object size	The maximum object size stored in the SG appliance. All objects retrieved that are greater than the maximum size are delivered to the client but are not stored in the SG appliance.
MIME/FILE type filtering	Allows organizations to implement Internet policies for both uploaded and downloaded content by MIME or FILE type.
multi-bit rate	The capability of a single stream to deliver multiple bit rates to clients requesting content from appliances from within varying levels of network conditions (such as different connecting bandwidths and traffic).
multicast	Used in streaming; the ability for hundreds or thousands of users to play a single stream.
multicast aliases	Used in streaming; a streaming command that specifies an alias for a multicast URL to receive an .nsc file. The .nsc files allows the multicast session to obtain the information in the control channel
multicast station	Used in streaming; a defined location on the proxy where the Windows Media player can retrieve streams. A multicast station enables multicast transmission of Windows Media content from the cache. The source of the multicast-delivered content can be a unicast-live source, a multicast (live) source, and simulated live (video-on-demand content converted to scheduled live content).
multimedia content services	Used in streaming; multimedia support includes Real Networks, Microsoft Windows Media, Apple QuickTime, MP3, and Flash.

N

name inputing	Allows an SG appliance to resolve host names based on a partial name specification. When a host name is submitted to the DNS server, the DNS server resolves the name to an IP address. If the host name cannot be resolved, Blue Coat adds the first entry in the name-inputing list to the end of the host name and resubmits it to the DNS server
native FTP	Native FTP involves the client connecting (either explicitly or transparently) using the FTP protocol; the SG appliance then connects upstream through FTP (if necessary).
NCSA common log format	Blue Coat products are compatible with this log type, which contains only basic HTTP access information.
network address translation (NAT)	The process of translating private network (such as intranet) IP addresses to Internet IP addresses and vice versa. This methodology makes it possible to match private IP addresses to Internet IP addresses even when the number of private addresses outnumbers the pool of available Internet addresses.

non-cacheable objects	A number of objects are not cached by the Blue Coat appliance because they are considered non-cacheable. You can add or delete the kinds of objects that the appliance considers non-cacheable. Some of the non-cacheable request types are: • Pragma no-cache, requests that specify non-cached objects, such as when you click refresh in the Web browser. • Password provided, requests that include a client password. • Data in request that include additional client data. • Not a GET request.
.nsc file	Created from the multicast station definition and saved through the browser as a text file encoded in a Microsoft proprietary format. Without an .nsc file, the multicast station definition does not work.
NTP	To manage objects in an appliance, an SG appliance must know the current Universal Time Coordinates (UTC) time. By default, the SG appliance attempts to connect to a Network Time Protocol (NTP) server to acquire the UTC time. SG appliance 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.

O

object (used in caching)	An object is the item that is stored in an appliance. These objects can be frequently accessed content, content that has been placed there by content publishers, or Web pages, among other things.
object (used in Visual Policy Manager)	An object (sometimes referred to as a condition) is any collection or combination of entry types you can create individually (user, group, IP address/subnet, and attribute). To be included in an object, an item must already be created as an individual entry.
object pipelining	This patented algorithm opens as many simultaneous TCP connections as the origin server will allow and retrieves objects in parallel. The objects are then delivered from the appliance straight to the user's desktop as fast as the browser can request them.
origin content server (OCS)	Also called origin server. This is the original source of the content that is being requested. An appliance needs the OCS to acquire data the first time, to check that the content being served is still fresh, and to authenticate users.
outbound traffic (bandwidth gain)	Network packets flowing out of the SG appliance. Outbound traffic mainly consists of the following: • Client outbound: Packets sent to the client in response to a Web request. • Server outbound: Packets sent to an OCS or upstream proxy to request a service.

P

PAC (Proxy AutoConfiguration) scripts	Originally created by Netscape, PACs are a way to avoid requiring proxy hosts and port numbers to be entered for every protocol. You need only enter the URL. A PAC can be created with the needed information and the local browser can be directed to the PAC for information about proxy hosts and port numbers.
packet capture (PCAP)	Allows filtering on various attributes of the Ethernet frame to limit the amount of data collected. You can capture packets of Ethernet frames going into or leaving an SG appliance.

parent class (bandwidth gain)	A class with at least one child. The parent class must share its bandwidth with its child classes in proportion to the minimum/maximum bandwidth values or priority levels.
passive mode data connections (PASV)	Data connections initiated by an FTP client to an FTP server.
pipelining	*See* object pipelining.
policies	Groups of rules that let you manage Web access specific to the needs of an enterprise. Policies enhance SG appliance feature areas such as authentication and virus scanning, and let you control end-user Web access in your existing infrastructure. *See also* refresh policies.
policy-based bypass list	Used in policy. Allows a bypass based on the properties of the client, unlike static and dynamic bypass lists, which allow traffic to bypass the appliance based on destination IP address. *See also* bypass lists and dynamic bypass.
policy layer	A collection of rules created using Blue Coat CPL or with the VPM.
pragma: no cache (PNC)	A metatag in the header of a request that requires the appliance to forward a request to the origin server. This allows clients to always obtain a fresh copy *(of the request?).*
proxy	Caches content, filters traffic, monitors Internet and intranet resource usage, blocks specific Internet and intranet resources for individuals or groups, and enhances the quality of Internet or intranet user experiences. A proxy can also serve as an intermediary between a Web client and a Web server and can require authentication to allow identity based policy and logging for the client. The rules used to authenticate a client are based on the policies you create on the SG appliance, which can reference an existing security infrastructure—LDAP, RADIUS, IWA, and the like.
Proxy Edition	SGOS 5 Proxy Edition.
proxy service	The proxy service defines the ports, as well as other attributes. that are used by the proxies associated with the service.
proxy service (default)	The default proxy service is a service that intercepts all traffic not otherwise intercepted by other listeners. It only has one listener whose action can be set to bypass or intercept. No new listeners can be added to the default proxy service, and the default listener and service cannot be deleted. Service attributes can be changed.
public key certificate	An electronic document that encapsulates the public key of the certificate sender, identifies this sender, and aids the certificate receiver to verify the identity of the certificate sender. A certificate is often considered valid if it has been digitally signed by a well-known entity, which is called a Certificate Authority (such as VeriSign).
public virtual IP (VIP)	Maps multiple servers to one IP address and then propagates that information to the public DNS servers. Typically, there is a public VIP known to the public Internet that routes the packets internally to the private VIP. This enables you to “hide” your servers from the Internet.

R

real-time streaming protocol (RTSP)	A standard method of transferring audio and video and other time-based media over Internet-technology based networks. The protocol is used to stream clips to any RTP-based client.
reflect client IP attribute	Enables the sending of the client's IP address instead of the SG's IP address to the upstream server. If you are using an application delivery network (ADN), this setting is enforced on the concentrator proxy through the **Configuration > App. Delivery Network > Tunneling** tab.
registration	An event that binds the appliance to an account, that is, it creates the Serial#, Account association.
remote authentication dial-in user service (RADIUS)	Authenticates user identity via passwords for network access.
reverse proxy	A proxy that acts as a front-end to a small number of pre-defined servers, typically to improve performance. Many clients can use it to access the small number of predefined servers.
routing information protocol (RIP)	Designed to select the fastest route to a destination. RIP support is built into Blue Coat appliances.
router hops	The number of jumps a packet takes when traversing the Internet.

S

secure shell (SSH)	Also known as Secure Socket Shell. SSH is an interface and protocol that provides strong authentication and enables you to securely access a remote computer. Three utilities—login, ssh, and scp—comprise SSH. Security via SSH is accomplished using a digital certificate and password encryption. Remember that the Blue Coat SG appliance requires SSH1. An SG appliance supports a combined maximum of 16 Telnet and SSH sessions.
serial console	A third-party device that can be connected to one or more Blue Coat appliances. Once connected, you can access and configure the appliance through the serial console, even when you cannot access the appliance directly.
server certificate categories	The hostname in a server certificate can be categorized by BCWF or another content filtering vendor to fit into categories such as banking, finance, sports.
server portals	Doorways that provide controlled access to a Web server or a collection of Web servers. You can configure Blue Coat SG appliances to be server portals by mapping a set of external URLs onto a set of internal URLs.
server-side transparency	The ability for the server to see client IP addresses, which enables accurate client-access records to be kept. When server-side transparency is enabled, the appliance retains client IP addresses for all port 80 traffic to and from the SG appliance. In this scheme, the client IP address is always revealed to the server.
service attributes	Define the parameters, such as explicit or transparent, cipher suite, and certificate verification, that the SG appliance uses for a particular service. .

SG appliance	A Blue Coat security and cache box that can help manage security and content on a network.
sibling class (bandwidth gain)	A bandwidth class with the same parent class as another class.
simple network management protocol (SNMP)	The standard operations and maintenance protocol for the Internet. It uses MIBs, created or customized by Blue Coat, to handle *(needs completion).*
simulated live	Used in streaming. Defines playback of one or more video-on-demand files as a scheduled live event, which begins at a specified time. The content can be looped multiple times, or scheduled to start at multiple start times throughout the day.
SmartReporter log type	A proprietary ELFF log type that is compatible with the SmartFilter SmartReporter tool.
SOCKS	A proxy protocol for TCP/IP-based networking applications that allows users transparent access across the firewall. If you are using a SOCKS server for the primary or alternate forwarding gateway, you must specify the appliance's ID for the identification protocol used by the SOCKS gateway. The machine ID should be configured to be the same as the appliance's name.
SOCKS proxy	A generic way to proxy TCP and UDP protocols. The SG appliance supports both SOCKSv4/4a and SOCKSv5; however, because of increased username and password authentication capabilities and compression support, Blue Coat recommends that you use SOCKS v5.
splash page	Custom message page that displays the first time you start the client browser.
split proxy	Employs co-operative processing at the branch and the core to implement functionality that is not possible in a standalone proxy. Examples of split proxies include: • Mapi Proxy • SSL Proxy
SQUID-compatible format	A log type that was designed for cache statistics and is compatible with Blue Coat products.
squid-native log format	The Squid-compatible format contains one line for each request.
SSL authentication	Ensures that communication is with "trusted" sites only. Requires a certificate issued by a trusted third party (Certificate Authority).
SSL interception	Decrypting SSL connections.
SSL proxy	A proxy that can be used for any SSL traffic (HTTPS or not), in either forward or reverse proxy mode.
static route	A manually-configured route that specifies the transmission path a packet must follow, based on the packet's destination address. A static route specifies a transmission path to another network.

statistics	Every Blue Coat appliance keeps statistics of the appliance hardware and the objects it stores. You can review the general summary, the volume, resources allocated, cache efficiency, cached contents, and custom URLs generated by the appliance for various kinds of logs. You can also check the event viewer for every event that occurred since the appliance booted.
stream	A flow of a single type of data, measured in kilobits per second (Kbps). A stream could be the sound track to a music video, for example.
SurfControl log type	A proprietary log type that is compatible with the SurfControl reporter tool. The SurfControl log format includes fully-qualified usernames when an NTLM realm provides authentication. The simple name is used for all other realm types.
syslog	An event-monitoring scheme that is especially popular in Unix environments. Most clients using Syslog have multiple devices sending messages to a single Syslog daemon. This allows viewing a single chronological event log of all of the devices assigned to the Syslog daemon. The Syslog format is: "Date Time Hostname Event."
system cache	The software cache on the appliance. When you clear the cache, all objects in the cache are set to expired. The objects are not immediately removed from memory or disk, but a subsequent request for any object requested is retrieved from the origin content server before it is served.

T

time-to-live (TTL) value	Used in any situation where an expiration time is needed. For example, you do not want authentication to last beyond the current session and also want a failed command to time out instead of hanging the box forever.
traffic flow (bandwidth gain)	Also referred to as *flow.* A set of packets belonging to the same TCP/UDP connection that terminate at, originate at, or flow through the SG appliance. A single request from a client involves two separate connections. One of them is from the client to the SG appliance, and the other is from the SG appliance to the OCS. Within each of these connections, traffic flows in two directions—in one direction, packets flow out of the SG appliance (outbound traffic), and in the other direction, packets flow into the SG (inbound traffic). Connections can come from the client or the server. Thus, traffic can be classified into one of four types: • Server inbound • Server outbound • Client inbound • Client outbound These four traffic flows represent each of the four combinations described above. Each flow represents a single direction from a single connection.
transmission control protocol (TCP)	TCP, when used in conjunction with IP (Internet Protocol) enables users to send data, in the form of message units called packets, between computers over the Internet. TCP is responsible for tracking and handling, and reassembly of the packets; IP is responsible for packet delivery.
transparent proxy	A configuration in which traffic is redirected to the SG appliance without the knowledge of the client browser. No configuration is required on the browser, but network configuration, such as an L4 switch or a WCCP-compliant router, is required.

trial period	Starting with the first boot, the trial period provides 60 days of free operation. All features are enabled during this time.

U

unicast alias	Defines an name on the appliance for a streaming URL. When a client requests the alias content on the appliance, the appliance uses the URL specified in the unicast-alias command to request the content from the origin streaming server.
universal time coordinates (UTC)	An SG appliance must know the current UTC time. By default, the appliance attempts to connect to a Network Time Protocol (NTP) server to acquire the UTC time. If the SG appliance cannot access any NTP servers, you must manually set the UTC time.
URL filtering	*See* content filtering.
URL rewrite rules	Rewrite the URLs of client requests to acquire the streaming content using the new URL. For example, when a client tries to access content on www.mycompany.com, the appliance is actually receiving the content from the server on 10.253.123.123. The client is unaware that mycompany.com is not serving the content; however, the appliance access logs indicate the actual server that provides the content.

W

WCCP	Web Cache Communication Protocol. Allows you to establish redirection of the traffic that flows through routers.
Web FTP	Web FTP is used when a client connects in explicit mode using HTTP and accesses an ftp:// URL. The SG appliance translates the HTTP request into an FTP request for the OCS (if the content is not already cached), and then translates the FTP response with the file contents into an HTTP response for the client.
Websense log type	A Blue Coat proprietary log type that is compatible with the Websense reporter tool.

X

XML responder	HTTP XML service that runs on an external server.
XML requestor	XML realm.

Index