

Blue Coat® Systems ProxySG™

Configuration and Management Guide

Volume 1: Introduction

Version SGOS 5.1.3



Contact Information

Blue Coat Systems Inc.

420 North Mary Ave

Sunnyvale, CA 94085-4121

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

bcs.info@bluecoat.com

<http://www.bluecoat.com>

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

Copyright© 1999-2006 Blue Coat Systems, Inc. All rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of Blue Coat Systems, Inc. All right, title and interest in and to the Software and documentation are and shall remain the exclusive property of Blue Coat Systems, Inc. and its licensors. ProxySG™, ProxyAV™, CacheOS™, SGOS™, Spyware Interceptor™, Scope™, RA Connector™, RA Manager™, Remote Access™ are trademarks of Blue Coat Systems, Inc. and CacheFlow®, Blue Coat®, Accelerating The Internet®, WinProxy®, AccessNow®, Ositis®, Powering Internet Management®, The Ultimate Internet Sharing Solution®, Permeo®, Permeo Technologies, Inc.®, and the Permeo logo are registered trademarks of Blue Coat Systems, Inc. All other trademarks contained in this document and in the Software are the property of their respective owners.

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

Document Number: 231-02837

Document Revision: SGOS 5.x 09/2006

Contents

Contact Information

Chapter 1: Volume Organization

Related Blue Coat Documentation.....	7
Document Conventions.....	7

Chapter 2: Master Table of Contents

<i>Volume 2: Getting Started</i>	10
<i>Volume 3: Proxies and Proxy Services</i>	12
<i>Volume 4: Web Communication Proxies</i>	17
<i>Volume 5: Securing the ProxySG</i>	20
<i>Volume 6: Advanced Networking</i>	24
<i>Volume 7: VPM and Advanced Policy</i>	28
<i>Volume 8: Managing Content</i>	36
<i>Volume 9: Access Logging</i>	39
<i>Volume 10: Managing the ProxySG</i>	41
<i>Volume 11: ProxySG Content Policy Language Guide</i>	45
<i>Volume 12: ProxySG Command Line Reference</i>	54

Chapter 3: Customizing the ProxySG

Placing the ProxySG in a Network	59
Initial Setup	60
Simple Policy.....	60
Implementing Policies	60
Managing the ProxySG.....	61
Managing the ProxyAV.....	61
Troubleshooting.....	61
Task Tables	62

Third Party Copyright Notices

Chapter 3: Volume Organization

The documentation suite for the *Blue Coat ProxySG Configuration and Management Guide* is composed of 12 volumes, which includes the *Blue Coat ProxySG Content Policy Language Guide* (Volume 11) and *Blue Coat ProxySG Command Line Reference* (Volume 12).

The *Blue Coat ProxySG Configuration and Management Guide* has been divided into separate volumes to improve accessibility and readability, and to allow like topics to be discussed more thoroughly. For example, the proxies chapter has been converted to *Volume 3: Proxies and Proxy Services*, and each proxy has its own chapter. This allows a solutions-based discussion for each proxy.

Nearly every volume contains a glossary. *Volume 11: ProxySG Content Policy Language Guide* has a separate, CPL-specific glossary. *Volume 12: ProxySG Command Line Reference* has no glossary.

Table 3-1. Volume Organization

Volume Title	Description
<i>Volume 1: Introduction to the ProxySG</i>	Volume 1 contains the table of contents for the entire documentation suite. It also contains a task list of pointers to locations for common tasks.
<i>Volume 2: Getting Started</i>	Contained in this book is everything you need to get started: <ul style="list-style-type: none">• how to log in to the ProxySG CLI and Web-based Management Console• how to change the administrator username, password, and privileged-mode password;• licensing• how to set the ProxySG name and system time, configure the network adapter, load balance, and specify DNS servers.
<i>Volume 3: Proxies and Proxy Services</i>	Volume 3 describes the proxies and proxy services available. Separate chapters describe each of the various kinds of proxies.
<i>Volume 4: Web Communication Proxies</i>	Application proxies, such as IM and streaming, are discussed in this volume.

Table 3-1. Volume Organization (Continued)

Volume Title	Description
<i>Volume 5: Securing the ProxySG</i>	<p>Enabling and maintaining security on the ProxySG is discussed in this volume.</p> <p>Blue Coat supports a number of kinds of authentication, discussed here: LDAP, IWA, RADIUS, Local, Certificate (which allows you to authenticate using certificates), policy substitution, COREid, Netegrity, and Sequence (which allows you to authenticate using multiple authentication servers).</p> <p>Also discussed in this volume is the ProxySG BCAA agent.</p>
<i>Volume 6: Advanced Networking</i>	<p>Topics discussed in this volume are networkings tasks: setting failover, TCP-IP, attack detection, WCCP, and the Routing Information Protocol (RIP). Commands supported for the RIP configuration text file are discussed in the appendix.</p> <p>Health Checks, forwarding, and managing bandwidth are also discussed in this volume.</p>
<i>Volume 7: VPM and Advanced Policy</i>	<p>Discussed in this volume are:</p> <ul style="list-style-type: none"> • Four policy files are used to manage policy: Central, Local, Visual Policy Manager, and Forwarding. T. • Pop-up ad blocking, managing active content, and creating exceptions. • This volume also contains a reference guide and several tutorials for using the Visual Policy Manager.
<i>Volume 8: Managing Content</i>	<p>This volume discusses how to configure and use the ProxySG's content filtering capabilities, as well as configuring and using content filtering vendors to work with the ProxySG.</p> <p>External Services (ICAP and Websense off-box) are also found in this volume.</p>
<i>Volume 9: Access Logging</i>	<p>Log formats, upload clients, upload schedules, and protocols are discussed in this volume.</p> <p>In the Access Log Formats appendix, ELFF, SQUID, NCSA/Common, and custom logs are discussed.</p>
<i>Volume 10: Managing the ProxySG</i>	<p>This volume discusses upgrading the system and configuring event logs, SMNP, STMP, heartbeats, and core images, as well as diagnostics.</p> <p>Health Monitoring, new in this release, is discussed in this volume.</p> <p>The statistics chapter discusses viewing various kinds of statistics—system usage, efficiency, resources, and logs of all kinds.</p>

Table 3-1. Volume Organization (Continued)

Volume Title	Description
<i>Volume 11: ProxySG Content Policy Language Guide</i>	This volume discusses using Content Policy Language (CPL) to create and manage policies on the ProxySG.
<i>Volume 12: ProxySG Command Line Reference</i>	This is a reference, in man-page format, of all the CLI commands supported by SGOS.

Note: The *Blue Coat ProxySG Configuration and Management Guide* suite and the *online help* contain the same information but are not identical. For the latest information, refer to the *Blue Coat ProxySG Configuration and Management Guide* documentation suite.

Related Blue Coat Documentation

- ❑ *Blue Coat 200 Series Installation Guide*
- ❑ *Blue Coat SG 410 Installation Guide*
- ❑ *Blue Coat SG810 Installation Guide*
- ❑ *Blue Coat SG8100 Installation Guide*

Document Conventions

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

Table 3-2. Document Conventions

Conventions	Definition
<i>Italics</i>	The first use of a new or Blue Coat-proprietary term.
Courier font	Command line text that appears on your administrator workstation.
<i>Courier Italics</i>	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 ProxySG 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 4: Master Table of Contents

This chapter contains the table of contents for each of the eleven remaining books in the 12 volume *Blue Coat ProxySG Configuration and Management Guide Suite*. The table of contents for this book, *Volume 1: Introduction to the ProxySG*, is in the front of this book, following the cover.

Volume 2: Getting Started

Contact Information

Chapter 1: About Getting Started

About This Book.....	7
Document Conventions.....	7

Chapter 2: Licensing

About Licensing	9
Licensable Components	9
About the Trial Period.....	10
About License Expiration	11
About the System Serial Number	11
Obtaining a WebPower Account	12
Registering and Licensing the ProxySG Hardware and Software.....	12
Manual License Installation.....	15
Disabling the Components Running in Trial Mode.....	16
Updating a License	17
Automatically Updating a License	17

Chapter 3: Accessing the ProxySG

Before You Begin: Understanding Modes	19
Accessing the ProxySG.....	20
Accessing the CLI.....	20
Accessing the Management Console	20
Accessing the Management Console Home Page	21
Logging On	21
Logging Out.....	21
Changing the Logon Parameters	22
Changing the Username and Password	22
Changing the ProxySG Realm Name.....	24
Changing the ProxySG Timeout.....	25
Viewing the ProxySG Health	25

Chapter 4: Configuring Basic Settings

Configuring the ProxySG Name.....	27
Configuring the Serial Number	27
Configuring the System Time	28
Network Time Protocol.....	29
Configuring HTTP Timeout	30

Chapter 5: Archive Configuration

Sharing Configurations	31
Archiving a Configuration.....	34

Chapter 6: Adapters

About Adapters.....	37
Network Interface States	37
Configuring an Adapter.....	37
Configuring Interface Settings	38
Disabling Transparent Interception	39
Rejecting Inbound Connections.....	40
Using reject-inbound and allow-intercept	40
Manually Configuring Link Settings	41
Setting Up Proxies	41
Detecting Network Adapter Faults	41

Chapter 7: Software and Hardware Bridges

About Bridging.....	43
Traffic Handling.....	44
Bridging Methods	44
About the Pass-Through Adapter	45
Configuring a Software Bridge	45
Customizing the Interface Settings.....	47
Setting Bandwidth Management for Bridging	48
Configuring Failover	48
Setting Up Failover	49
Bridging Loop Detection.....	50
Adding Static Forwarding Table Entries	52
Bypass List Behavior.....	54

Chapter 8: Gateways

About Gateways.....	55
ProxySG Specifics.....	55
Switching to a Secondary Gateway.....	56
Defining Static Routes	57
Installing a Routing Table.....	57

Chapter 9: DNS

ProxySG Specifics.....	59
Configuring Split DNS Support.....	60
Changing the Order of DNS Servers.....	61
Unresolved Hostnames (Name Imputing).....	62
Changing the Order of DNS Name Imputing Suffixes	62
Caching Negative Responses	63

Appendix A: Glossary

Index

Volume 3: Proxies and Proxy Services

Contact Information

Chapter 1: About Proxies and Proxy Services

Creating or Enabling a Proxy Service	9
Configuring Proxies.....	10
About This Book.....	10
Document Conventions.....	10

Chapter 2: About Console Services

About Console Services.....	13
Notes on Managing the HTTP Console	15
Managing the HTTPS Console (Secure Console)	15
Selecting a Keyring	16
Selecting an IP Address.....	16
Enabling the HTTPS Console Service	16
Managing the SSH Console	18
Managing the SSH Host.....	18
Managing SSH Client Keys	18
Notes on Managing the Telnet Console.....	20

Chapter 3: About Proxy Services

Understanding a Proxy Listener	23
Proxy Services.....	23
Understanding Multiple Listeners	26
About Service Attributes	27
Understanding Access Logging with Proxy Services.....	28
Creating or Editing a Proxy Service	28
Viewing the Proxy Services	30
Bypass List.....	30
Adding Static Bypass Entries	30
Using Policy to Configure Dynamic Bypass.....	31

Chapter 4: Managing the CIFS Proxy

About CIFS.....	35
About the Blue Coat CIFS Proxy Solution.....	35
Caching Behavior	36
Authentication.....	36
Policy Support	37

Access Logging.....	37
WCCP Support.....	37
Configuring the ProxySG CIFS Proxy.....	37
About Windows Security Signatures.....	37
Configuring CIFS Proxy Services	39
Configuring the CIFS Proxy	41
Enabling CIFS Access Logging	42
Reviewing CIFS Protocol Statistics.....	43
Reference: Equivalent CIFS Proxy CLI Commands.....	45
Reference: Access Log Fields.....	46
Reference: CPL Triggers, Properties, and Actions	48
Triggers.....	48
Properties and Actions:.....	48

Chapter 5: Managing the DNS Proxy

Creating or Editing a DNS Proxy Service.....	49
Creating a Resolving Name List	51

Chapter 6: Managing the FTP Proxy

Understanding FTP.....	53
Passive Mode Data Connections	53
Understanding IP Reflection for FTP.....	54
Configuring the ProxySG for Native FTP Proxy	55
Creating or Editing the FTP Service.....	55
Configuring the FTP Proxy	57
Configuring FTP Clients	58
Configuring FTP Connection Welcome Banners.....	59

Chapter 7: Managing the Endpoint Mapper and MAPI Proxies

Section A: The Endpoint Mapper Proxy Service

About RPC	62
About the Blue Coat Endpoint Mapper Proxy Solution.....	62
Policy Support	62
Access Logging.....	63
Configuring the ProxySG Endpoint Mapper Service	63
Reviewing Endpoint Mapper Statistics	65
Reference: Equivalent Endpoint Mapper CLI Commands	65
Reference: Access Log Fields.....	65
Reference: CPL Triggers, Properties, and Actions	66
TCP Tunneling Triggers.....	66
Properties and Actions.....	67

Section B: The MAPI Proxy

About MAPI.....	68
About the Blue Coat MAPI Solution	68

Batching.....	69
Keep-Alive	69
Supported Servers.....	70
Access Logging.....	70
More Conceptual Reference	70
Configuring the ProxySG MAPI Proxy.....	70
About the MAPI Service	70
Configuring the MAPI Proxy	70
Reviewing MAPI Statistics	71
Reference: Equivalent MAPI Proxy CLI Commands.....	72
Reference: Access Log Fields.....	72
User Activity.....	72

Chapter 8: Managing the HTTP Proxy

Section A: Creating an HTTP Proxy Service

Section B: Overview: Configuring HTTP Proxy Performance

Understanding Default HTTP Proxy Policy	80
HTTP Proxy Acceleration Profiles.....	80
Byte-Range Support.....	80
Refresh Bandwidth	81
Compression.....	81

Section C: Configuring the HTTP Proxy

Setting Default HTTP Proxy Policy	83
Customizing the HTTP Proxy Profile	85
Using the Normal Profile.....	86
Using the Portal Profile.....	86
Using the Bandwidth Gain Profile	86
Understanding HTTP Proxy Profile Configuration Components	86
Configuring the HTTP Proxy Profile	89
Configuring HTTP for Bandwidth Gain.....	91
Understanding Byte-Range Support.....	91
Understanding Revalidate Pragma-No-Cache	92
Configuring Refresh Bandwidth for the HTTP Proxy	93
Understanding Tolerant HTTP Request Parsing.....	94
Understanding HTTP Object Types	94
Understanding HTTP Compression.....	95
Understand Compression Behavior.....	96
Compression Exceptions.....	97
Configuring Compression	97
Notes	101

Section D: Using Explicit HTTP Proxy with Internet Explorer

Disabling the Proxy-Support Header.....	103
Enabling or Disabling NTLM Authentication for Internet Explorer Clients	104
Using Web FTP	105

Chapter 9: Managing the HTTPS Reverse Proxy

Section A: Configuring the HTTPS Reverse Proxy

Creating a Keyring	108
Deleting an Existing Keyring and Certificate	111
Managing Certificate Signing Requests	111
Creating a CSR	111
Viewing a Certificate Signing Request	112
Managing Server (SSL) Certificates	113
Creating Self-Signed SSL Certificates	113
Importing a Server Certificate.....	115
Using Certificate Revocation Lists	115
Troubleshooting Certificate Problems	117
Creating and Editing an HTTPS Reverse Proxy Service	117

Section B: Configuring HTTP or HTTPS Origination to the Origin Content Server

Creating Policy for HTTP and HTTPS Origination	122
--	-----

Section C: Advanced Configuration

Importing an Existing Keypair and Certificate.....	123
About Certificate Chains.....	125
Importing a CA Certificate	125
Creating CA Certificate Lists.....	126

Chapter 10: Managing Shell Proxies

Customizing Policy Settings for Shell Proxies	129
Conditions	130
Properties	130
Actions.....	130
Boundary Conditions for Shell Proxies	130
Understanding Telnet Shell Proxies.....	131

Chapter 11: Managing a SOCKS Proxy

Creating or Editing a SOCKS Proxy Service	137
Configuring the SOCKS Proxy.....	139
Using Policy to Control the SOCKS Proxy	140

Chapter 12: Managing the SSL Proxy

Understanding the SSL Proxy	141
Determining What HTTPS Traffic to Intercept	142
Managing Decrypted Traffic	142
Intercepting HTTPS Traffic	143

Configuring SSL Rules through Policy	149
Notes	155
Advanced Topics.....	155
Creating an Intermediate CA using OpenSSL	155
Creating an Intermediate CA using Microsoft Server 2003 (Active Directory)	158
 Chapter 13: Managing the SSL Client	
Understanding the SSL Client.....	161
Creating an SSL Client.....	161
Associating a Keyring and Protocol with the SSL Client	161
Changing the Cipher Suites of the SSL Client	162
Troubleshooting Server Certificate Verification.....	165
Setting the SSL Negotiation Timeout.....	165
 Chapter 14: Managing the TCP Tunneling Proxy	
TCP-Tunnel Proxy Services Supported	167
Creating or Editing a TCP-Tunnel Proxy Service.....	167
 Appendix A: Glossary	
 Appendix B: Explicit and Transparent Proxy	
Understanding the Explicit Proxy	179
Understanding the Transparent Proxy	179
Creating an Explicit Proxy Server.....	180
Using the ProxySG as an Explicit Proxy.....	180
Configuring Adapter Proxy Settings	181
Transparent Proxies.....	181
Configuring Transparent Proxy Hardware	181
Configuring IP Forwarding	183
 Appendix C: Understanding SSL	
Public Keys and Private Keys.....	185
Certificates.....	185
Server (SSL) Certificates.....	185
Self-Signed Certificates	186
Keyrings.....	186
Cipher Suites Supported by SGOS	186
Server Gated Cryptography and International Step-Up	187

Index

Volume 4: Web Communication Proxies

Contact Information

Chapter 1: Introduction

Document Conventions.....	7
---------------------------	---

Chapter 2: Managing Instant Messaging Protocols

About the Risks of Instant Messaging	9
About the Blue Coat IM Proxies	9
HTTP Proxy Support.....	9
Instant Messaging Proxy Authentication.....	9
Access Logging.....	10
Managing Skype	10
About Instant Message Network Interactivity	10
Recommended Deployments.....	10
About Instant Messaging Reflection	11
Configuring ProxySG IM Proxies	13
Configuring IM Services	14
Configuring IM DNS Redirection	17
The Default IM Hosts	18
Configuring Instant Messaging HTTP Handoff.....	18
Configuring IM Alerts.....	19
Configuring IM Clients	20
General Configuration	20
AOL Messenger Client Explicit Proxy Configuration.....	20
MSN Messenger Client Explicit Proxy Configuration	21
Yahoo Messenger Client Explicit Proxy Configuration	22
Policy Examples	23
Example 1: File Transfer	24
Example 2: Send an IM Alert Message	26
Reference: Equivalent IM CLI Commands.....	27
Reference: Access Log Fields.....	28
Reference: CPL Triggers, Properties, and Actions	28
Triggers.....	29
Properties and Actions.....	29

Chapter 3: Managing Streaming Media

Section A: Concepts: Streaming Media

About Streaming Media.....	32
Supported Streaming Media Clients and Protocols.....	32
Supported Streaming Media Clients and Servers	32
Supported Streaming Protocols	33

About Processing Streaming Media Content.....	35
Delivery Methods	35
Serving Content: Live Unicast	35
Serving Content: Video-on-Demand Unicast	35
Serving Content: Multicast Streaming.....	36
About HTTP Handoff.....	37
Limiting Bandwidth	37
Caching Behavior: Protocol Specific	38
Caching Behavior: Video on Demand	39
Caching Behavior: Live Splitting	39
Multiple Bit Rate Support.....	39
BitrateThinning	40
Pre-Populating Content	40
About Fast Streaming (Windows Media).....	40
About Streaming Media Authentication	41
Windows Media Server-Side Authentication	41
Windows Media Proxy Authentication.....	41
Real Media Proxy Authentication	42
QuickTime Proxy Authentication	42
Section B: Configuring Streaming Media	
Configuring Streaming Services	43
Configuring Streaming Proxies.....	46
Limiting Bandwidth	47
Configuring Bandwidth Limits—Global.....	47
Configuring Bandwidth Limits—Protocol-Specific.....	48
Configuring Bandwidth Limitation—Fast Start (WM)	48
Configuring the ProxySG Multicast Network	49
Configuring Media Server Authentication Type (Windows Media)	49
Related CLI Syntax to Manage Streaming.....	50
Reference: Access Log Fields.....	50
Reference: CPL Triggers, Properties, and Actions	51
Triggers.....	51
Properties and Actions.....	51
Section C: Additional Configuration Tasks—Windows Media (CLI)	
Managing Multicast Streaming for Windows Media	52
About Multicast Stations	52
About Broadcast Aliases	53
Creating a Multicast Station	53
Monitoring the Multicast Station.....	55
Managing Simulated Live Content (Windows Media)	55
About Simulated Live Content	56
Creating a Broadcast Alias for Simulated Live Content	56
ASX Rewriting (Windows Media).....	57

About ASX Rewrite	57
Section D: Windows Media Player	
Configuring Windows Media Player	61
Windows Media Player Interactivity Notes.....	62
Striding	62
Other Notes.....	62
Section E: RealPlayer	
Configuring RealPlayer.....	64
Section F: QuickTime Player	
Configuring QuickTime Player.....	68
Appendix A: Glossary	
Index	

Volume 5: Securing the ProxySG

Contents

Contact Information

Chapter 1: About Security

Controlling ProxySG Access.....	7
Controlling User Access with Identity-based Access Controls.....	7
SSL Between the ProxySG and the Authentication Server	8
About This Book.....	8
Document Conventions.....	9

Chapter 2: Controlling Access to the ProxySG

Limiting Access to the ProxySG Appliance	11
Requiring a PIN for the Front Panel	11
Limiting Workstation Access	12
Securing the Serial Port.....	12
About Password Security.....	12
Limiting User Access to the ProxySG—Overview	13
Moderate Security: Restricting Management Console Access Through the Console Access Control List (ACL)	15
Maximum Security: Administrative Authentication and Authorization Policy	16
Defining Administrator Authentication and Authorization Policies	16
Defining Policies Using the Visual Policy Manager	17
Defining Policies Directly in Policy Files.....	17
Admin Transactions and <Admin> Layers	17
Example Policy Using CPL Syntax.....	21

Chapter 3: Controlling Access to the Internet and Intranet

Using Authentication and Proxies.....	23
Understanding Authentication Modes	23
Understanding Origin-Style Redirection	25
Selecting an Appropriate Surrogate Credential	26
Configuring Transparent Proxy Authentication.....	26
Using SSL with Authentication and Authorization Services	28
Using SSL Between the Client and the ProxySG.....	28
Creating a Proxy Layer to Manage Proxy Operations.....	29
Using CPL	29

Chapter 4: Certificate Realm Authentication

How Certificate Realm Works	39
-----------------------------------	----

Creating a Certificate Realm.....	40
Defining a Certificate Realm	40
Defining Certificate Realm General Properties	41
Revoking User Certificates	42
Creating the Certificate Authorization Policy	43
Tip.....	43

Chapter 5: Oracle COREid Authentication

Understanding COREid Interaction with Blue Coat	45
Configuring the COREid Access System.....	45
Additional COREid Configuration Notes	46
Configuring the ProxySG Realm	46
Participating in a Single Sign-On (SSO) Scheme	47
Avoiding ProxySG Challenges	47
Creating a COREid Realm	48
Configuring Agents	48
Configuring the COREid Access Server	49
Configuring the General COREid Settings.....	50
Creating the CPL.....	52

Chapter 6: Forms-Based Authentication

Section A: Understanding Authentication Forms

User/Realm CPL Substitutions for Authentication Forms.....	57
Tip.....	58

Section B: Creating and Editing a Form

Section C: Setting Storage Options

Section D: Using CPL with Forms-Based Authentication

Tips.....	64
-----------	----

Chapter 7: IWA Realm Authentication and Authorization

How Blue Coat Works with IWA	65
Creating an IWA Realm	65
IWA Servers	66
Defining IWA Realm General Properties	67
Creating the CPL.....	69
Notes	70

Chapter 8: LDAP Realm Authentication and Authorization

Overview	71
Creating an LDAP Realm	72
LDAP Servers	73
Defining LDAP Base Distinguished Names	74
LDAP Search & Groups Tab (Authorization and Group Information)	76
Customizing LDAP Objectclass Attribute Values.....	78

Defining LDAP General Realm Properties.....	79
Creating the CPL.....	80
Chapter 9: Local Realm Authentication and Authorization	
Creating a Local Realm	83
Changing Local Realm Properties	83
Defining the Local User List	85
Creating a Local User List.....	85
Populating a List using the .htpasswd File	86
Uploading the .htpasswd File	87
Populating a Local User List through the ProxySG.....	87
Enhancing Security Settings for the Local User List.....	89
Creating the CPL.....	90
Chapter 10: Netegrity SiteMinder Authentication	
Understanding SiteMinder Interaction with Blue Coat	93
Configuring the SiteMinder Policy Server	93
Additional SiteMinder Configuration Notes.....	94
Configuring the ProxySG Realm	95
Participating in a Single Sign-On (SSO) Scheme	95
Avoiding ProxySG Challenges	96
Creating a SiteMinder Realm	96
Configuring Agents	96
Configuring SiteMinder Servers	97
Defining SiteMinder Server General Properties.....	98
Configuring General Settings for SiteMinder.....	100
Creating the CPL.....	101
Chapter 11: Policy Substitution Realm Authentication	
How Policy Substitution Realms Work	103
Creating a Policy Substitution Realm	105
Defining a Policy Substitution Realm	105
Defining Policy Substitution Realm General Properties	106
Tips.....	107
Creating the Policy Substitution Policy	108
Notes	108
Chapter 12: RADIUS Realm Authentication and Authorization	
Creating a RADIUS Realm.....	110
Defining RADIUS Realm Properties	110
Defining RADIUS Realm General Properties	111
Creating the Policy.....	113
Fine-Tuning RADIUS Realms.....	113
Creating RADIUS Groups	114
CPL Example	114

Troubleshooting	114
Chapter 13: Sequence Realm Authentication	
Adding Realms to a Sequence Realm.....	117
Creating a Sequence Realm	118
Adding Realms to a Sequence Realm.....	118
Defining Sequence Realm General Properties	119
Tips.....	120
Chapter 14: Windows Single Sign-on Authentication	
Creating a Windows SSO Realm	123
Windows SSO Agents.....	123
Configuring Authorization.....	124
Defining Windows SSO Realm General Properties	125
Modifying the Windows sso.ini File	127
Creating the CPL.....	128
Notes	128
Chapter 15: Managing the Credential Cache	
Tips.....	130
Appendix A: Glossary	
Appendix B: Using the Authentication/Authorization Agent	
Using the BCAA Service	139
Performance Notes	140
Installing the BCAA Service on a Windows System.....	141
Installing the BCAA Service on a Solaris System.....	146
Creating Service Principal Names for IWA Realms.....	146
Troubleshooting Authentication Agent Problems	148
Common BCAA Event Messages	148
Index	

Volume 6: Advanced Networking

Contact Information

Chapter 1: About Advanced Networking

About This Book.....	7
Document Conventions.....	8

Chapter 2: Application Delivery Network Optimization

How ADN Networks are Constructed	10
Using ADN Optimization and other Blue Coat Features to Improve Performance	11
Recommendations.....	11
Configuring ADN Optimization.....	12
Enabling the ADN Manager.....	12
Creating Server Subnets.....	12
Setting Tunneling Parameters.....	13
Setting the Byte-Caching Memory Size	14
Reviewing Byte Caching History Statistics	16
Policy.....	17
Byte Caching.....	17
Compression.....	17
Notes	17

Chapter 3: Attack Detection

Configuring Attack-Detection Mode for the Client	19
Configuring Attack-Detection Mode for a Server or Server Group	23

Chapter 4: Bandwidth Management

Bandwidth Management Overview	25
Allocating Bandwidth	26
Flow Classification.....	29
Configuring Bandwidth Allocation.....	29
Enabling or Disabling Bandwidth Management.....	30
Creating and Editing Bandwidth Classes	30
Bandwidth Management Statistics	33
Current Class Statistics Tab.....	33
Total Class Statistics Tab.....	34
Bandwidth Management Statistics in the CLI	34
Using Policy to Manage Bandwidth.....	35
CPL Support for Bandwidth Management	36
VPM Support for Bandwidth Management.....	36
Bandwidth Allocation and VPM Examples	36
Policy Examples: CPL.....	43

Chapter 5: Configuring Failover

About Failover	45
Configuring Failover	46
Viewing Failover Statistics.....	47

Chapter 6: Configuring the Upstream Networking Environment

Understanding Forwarding.....	49
Understanding Load Balancing	50
Understanding Host Affinity	50
Using Load Balancing and Host Affinity Together	51
Configuring Forwarding.....	51
Creating Forwarding Hosts and Groups.....	51
Editing a Forwarding Host.....	54
Editing a Forwarding Group.....	56
Configuring Load Balancing	57
Configuring Host Affinity	58
Creating a Default Sequence	59
Using Forwarding Directives to Create an Installable List.....	60

Chapter 7: Health Checks

About General Health Checks.....	69
Configuring Service-Specific Health Checks	70
About Global Forwarding and SOCKS Gateway Health Checks	72
Configuring Global Health Checks	73
Pausing or Resuming Global Health Checking	74

Chapter 8: Internet Caching Protocol (ICP) Configuration

Configuring ICP	75
Using ICP Configuration Directives to Create an Installable List.....	75
Naming the IP Hosts	77
Restricting Access	78
Connecting to Other ICP Hosts	79
Creating an ICP Installable List	79
Enabling ICP	80

Chapter 9: Using RIP

Installing RIP Configuration Files	81
Configuring Advertising Default Routes	82
RIP Commands.....	83
net.....	83
host.....	83
RIP Parameters	84
ProxySG-Specific RIP Parameters.....	85
Using Passwords with RIP	86

Chapter 10: Configuring the ProxySG as a Session Monitor

Configuring the Session Monitor.....	87
Configuring the RADIUS Accounting Protocol Parameters	87
Configuring a Session Monitor Cluster	88
Configuring the Session Monitor	89
Creating the CPL.....	90
Notes	90

Chapter 11: SOCKS Gateway Configuration

Using SOCKS Gateways	93
Using the CLI to Create SOCKS Gateways Settings	93
Editing a SOCKS Gateways Host	95
Creating a Default Sequence	95
Using SOCKS Gateways Configuration Directives With Installable Lists	96
Creating a SOCKS Gateway Installable List	98
Tip for SOCKS Configuration	99

Chapter 12: TCP/IP Configuration

RFC-1323.....	101
TCP NewReno	102
ICMP Broadcast Echo Support.....	102
ICMP Timestamp Echo Support	102
TCP Window Size	103
PMTU Discovery	103
TCP Time Wait	103
Viewing the TCP/IP Configuration	104

Chapter 13: Virtual IP Addresses

Chapter 14: WCCP Settings

Appendix A: Glossary

Appendix B: Using Policy to Manage Forwarding

Appendix C: Using WCCP

Overview	123
Using WCCP and Transparent Redirection	123
WCCP Version 1.....	123
WCCP Version 2.....	124
Quick Start.....	125
Configuring a WCCP Version 2 Service on the Router	126
Setting up a Service Group.....	126

Configuring the Internet-Connected Interface	129
Saving and Viewing Changes	131
Creating a ProxySG WCCP Configuration File	132
Understanding Packet Forwarding	132
Understanding Cache Load Balancing	133
Creating a Configuration File	134
Creating a Configuration File using a Text File	138
Examples	139
Displaying the Router's Known Caches	139
Standard HTTP Redirection	139
Standard HTTP Redirection and a Multicast Address	140
Standard HTTP Redirection Using a Security Password	141
Standard Transparent FTP	141
Reverse Proxy Service Group	142
Service Group with Alternate Hashing	142
Troubleshooting: Home Router	143
Identifying a Home Router/Router ID Mismatch	144
Correcting a Home Router Mismatch	146
Tips	146

Index

Volume 7: VPM and Advanced Policy

Contents

Contact Information

Chapter 15: Introduction

Document Conventions.....	7
---------------------------	---

Chapter 16: Managing Policy Files

Creating and Editing Policy Files	11
Using the Management Console.....	11
Using the CLI Inline Command	14
Unloading Policy Files.....	15
Configuring Policy Options.....	15
Policy File Evaluation.....	16
Transaction Settings: Deny and Allow	16
Policy Tracing.....	17
Managing the Central Policy File	18
Configuring Automatic Installation.....	18
Configuring a Custom Central Policy File for Automatic Installation	18
Configuring E-mail Notification.....	18
Configuring the Update Interval.....	19
Checking for an Updated Central Policy File.....	19
Resetting the Policy Files	19
Moving VPM Policy Files from One ProxySG to Another	19
Viewing Policy Files	19
Viewing the Installed Policy.....	20
Viewing Policy Source Files	20
Viewing Policy Statistics.....	20

Chapter 17: The Visual Policy Manager

Section A: About the Visual Policy Manager

Launching the Visual Policy Manager.....	24
About the Visual Policy Manager User Interface.....	25
Menu Bar.....	25
Tool Bar	26
Policy Layer Tabs.....	26

Rules and Objects.....	27
About Code Sharing With the Management Console	27
About VPM Components.....	28
Policy Layers.....	28
Rule Objects	29
Policy Layer/Object Matrix.....	30
The Set Object Dialog	31
The Add/Edit Object Dialog	32
Online Help.....	32
Section B: Policy Layer and Rule Object Reference	
About the Reference Tables	34
Administration Authentication Policy Layer Reference	34
Administration Access Policy Layer Reference	35
DNS Access Policy Layer Reference.....	35
SOCKS Authentication Policy Layer Reference	36
SSL Intercept Layer Reference.....	36
SSL Access Layer Reference	36
Web Authentication Policy Layer Reference	37
Web Access Policy Layer Reference	39
Web Content Policy Layer Reference.....	41
Forwarding Policy Layer Reference	42
Section C: Detailed Object Column Reference	
Source Column Object Reference.....	44
Any	44
Streaming Client.....	44
Client Hostname Unavailable	44
Authenticated User.....	44
Client IP Address/Subnet	44
Client Hostname	45
Proxy IP Address/Port	45
User	45
Group.....	48
Attribute	51
DNS Request Name.....	52
RDNS Request IP Address/Subnet.....	52
DNS Request Opcode.....	52
DNS Request Class	52
DNS Request Type.....	53
DNS Client Transport.....	53
SOCKS Version.....	53
User Agent	53
IM User Agent	54
Request Header	54

Client Certificate	55
IM User	55
P2P Client	55
Client Negotiated Cipher	56
Client Negotiated Cipher Strength	56
Client Negotiated SSL Version	56
Client Connection DSCP Trigger	56
Combined Source Object	57
Source Column/Policy Layer Matrix	58
Destination Column Object Reference	59
Any	59
DNS Response Contains No Data	59
Destination IP Address/Subnet	59
Destination Host/Port	59
Request URL	59
Request URL Category	60
Category	62
Server URL	62
Server Certificate	62
Server Certificate Category	62
Server Negotiated Cipher	62
Server Negotiated Cipher Strength	62
Server Negotiated SSL Version	63
File Extensions	63
HTTP MIME Types	63
Apparent Data Type	63
Response Code	64
Response Header	64
IM Buddy	64
IM Chat Room	65
DNS Response IP Address/Subnet	65
RDNS Response Host	65
DNS Response CNAME	66
DNS Response Code	66
Server Connection DSCP Trigger	66
Combined Destination Objects	67
Destination Column/Policy Layer Matrix	67
Service Column Object Reference	68
Any	68
Using HTTP Transparent Authentication	68
Virus Detected	68
Client Protocol	68

Service Name	68
Protocol Methods	69
SSL Proxy Mode	69
IM File Transfer	70
IM Message Text	70
IM Message Reflection	71
Streaming Content Type	71
ICAP Error Code	71
Combined Service Objects	72
Service Column/Policy Layer Matrix	72
Time Column Object Reference	73
Any	73
Time	73
Combined Time Object	75
Time Column/Policy Layer Matrix	75
Action Column Object Reference	75
Allow	75
Deny	75
Force Deny	75
Allow Read-Only Access	76
Allow Read-Write Access	76
Do Not Authenticate	76
Authenticate	76
Force Authenticate	78
Bypass Cache	78
Do Not Bypass Cache	78
Bypass DNS Cache	78
Do Not Bypass DNS Cache	78
Allow DNS From Upstream Server	78
Serve DNS Only From Cache	78
Enable/Disable DNS Imputing	79
Check/Do Not Check Authorization	79
Always Verify	79
Use Default Verification	79
Block/Do Not Block PopUp Ads	79
Force/Do Not Force IWA for Server Auth	80
Reflect/Do Not Reflect IM Messages	80
Block/Do Not Block IM Encryption	80
Require/Do Not Require Client Certificate	80
Deny	80
Return Exception	80
Return Redirect	81

Set Client Certificate Validation	82
Set Server Certificate Validation.....	82
Set SSL Forward Proxy.....	83
Send IM Alert	85
Modify Access Logging	85
Override Access Log Field.....	86
Rewrite Host.....	87
Reflect IP.....	87
Suppress Header	88
Control Request Header/Control Response Header	89
Notify User.....	90
Strip Active Content	93
HTTP Compression Level.....	95
Set Client HTTP Compression	95
Set Server HTTP Compression.....	96
Manage Bandwidth	96
ADN Server Optimization.....	96
Modify IM Message.....	97
Return ICAP Patience Page	97
Set Dynamic Categorization.....	97
Set External Filter Service	98
Set ICAP Request Service	99
Set ICAP Response Service.....	100
Set FTP Connection.....	100
Set SOCKS Acceleration.....	101
Set Streaming Max Bitrate	101
Set Client Connection DSCP Value	101
Set Server Connection DSCP Value.....	102
Send DNS/RDNS Response Code	102
Send DNS Response	102
Send Reverse DNS Response	103
Do Not Cache	103
Force Cache.....	104
Use Default Caching.....	104
Mark/Do Not Mark As Advertisement	104
Enable/Disable Pipelining	104
Set TTL.....	104
Send Direct.....	104
Integrate/Do Not Integrate New Hosts	104
Allow Content From Origin Server.....	104
Serve Content Only From Cache	104
Select SOCKS Gateway	105

Select Forwarding	105
Server Byte Caching	105
Set IM Transport	105
Set Streaming Transport	105
Authentication Charset	106
Combined Action Objects.....	106
Action Column/Policy Layer Matrix.....	106
Track Object Column Reference	108
Event Log, E-mail, and SNMP	109
Tracing Objects.....	110
Combined Track Object	111
Track Objects/Policy Layer Matrix	111
Comment Object Reference	111
Using Combined Objects	111
Centralized Object Viewing and Managing.....	114
Viewing Objects	114
Managing Objects	116
Creating Categories	117
Refreshing Policy	119
Restricting DNS Lookups	119
About DNS Lookup Restriction.....	119
Creating the DNS Lookup Restriction List	119
Restricting Reverse DNS Lookups	120
About Reverse DNS Lookup Restriction.....	120
Creating the Reverse DNS Lookup Restriction List	120
Setting the Group Log Order.....	120
About the Group Log Order	120
Creating the Group Log Order List.....	121

Section D: Managing Policy Layers, Rules, and Files

How Policy Layers, Rules, and Files Interact.....	122
How VPM Layers Relate to CPL Layers.....	122
Ordering Rules in a Policy Layer.....	123
Using Policy Layers of the Same Type	123
Ordering Policy Layers	124
Installing Policies	125
Managing Policy.....	125
Refreshing Policy	125
Reverting to a Previous Policy	126
Changing Policies	126
Managing Policy Layers.....	126
Managing Policy Rules.....	127
Installing VPM-Created Policy Files	127
Viewing the Policy/Created CPL	129

Section E: Tutorials

Tutorial—Creating a Web Authentication Policy	131
Example 1: Create an Authentication Rule	131
Example 2: Exempt Specific Users from Authentication	135
Tutorial—Creating a Web Access Policy	137
Example 1: Restrict Access to Specific Websites	137
Example 2: Allow Specific Users to Access Specific Websites	141

Chapter 18: Advanced Policy Tasks

Section A: Blocking Pop Up Windows

About Pop Up Blocking	152
Interactivity Notes	152
Recommendations.....	152

Section B: Stripping or Replacing Active Content

About Active Content.....	154
About Active Content Types	154
Script Tags.....	154
JavaScript Entities	155
JavaScript Strings	155
JavaScript Events.....	155
Embed Tags	155
Object Tags.....	156

Section C: Modifying Headers

Section D: Defining Exceptions

Built-in Exceptions	158
User-Defined Exceptions	162
About Exception Definitions	162
About the Exceptions Hierarchy.....	164
About the Exceptions Installable List.....	164
Creating or Editing Exceptions	166
Creating and Installing an Exceptions List.....	167
Viewing Exceptions	169

Section E: Managing Peer-to-Peer Services

About Peer-to-Peer Communications	171
The Blue Coat Solution.....	171
Supported Services	171
Deployment	171
Policy Control	172
VPM Support	172
CPL Support	172
Policy Example	173
Proxy Authentication	173
Access Logging.....	173

Section F: Managing QoS Traffic

- About Type of Service Information..... 174
- The Blue Coat Solution..... 174
- About DSCP Values..... 174
- About QoS Policy Tasks..... 175
 - Test Incoming QoS..... 175
 - Preserve a Connection QoS Value..... 176
 - Change the DSCP Value 176
- Policy Components..... 177
 - VPM Objects 177
 - VPM Example..... 177
 - CPL Components 178
- Access Logging..... 179

Appendix D: Glossary

Appendix A:

Volume 8: Managing Content

Chapter 1: Introduction

Document Conventions.....	7
---------------------------	---

Chapter 2: Content Filtering

Section A: About Content Filtering

Content Filtering Databases	10
Content Filtering Categories	10
On-box vs. Off-box Solutions	10
The ProxySG Content Filtering Solutions	10
The Blue Coat Web Filter Solution	11
About Blue Coat Web Filter	11
About Dynamic Categorization	12

Section B: Configuring Blue Coat Web Filter

Selecting Blue Coat Web Filter and Downloading the Database	14
Scheduling Automatic Downloads for Blue Coat Web Filter	18
Configuring Dynamic Categorization	18
Disabling Dynamic Categorization	19
Diagnostics	20

Section C: Configuring a Local Database

Selecting the Local Database and Downloading the Database	21
Scheduling Automatic Downloads for a Local Database	24
Diagnostics	24

Section D: Configuring Internet Watch Foundation

Selecting the IWF Database	26
Scheduling Automatic Downloads for IWF	28
Diagnostics	29

Section E: Configuring Third-Party Vendor Content Filtering

Selecting the Provider and Downloading the Database	30
Scheduling Automatic Downloads for a Third-Party Database	37
Diagnostics	38

Section F: Applying Policy

Applying Policy to Categorized URLs	40
Using Content Filtering Vendors with ProxySG Policies	42
Defining Custom Categories in Policy	43
Notes	45

Section G: Configuring Websense Off-box Content Filtering

Chapter 3: ICAP

Section A: About Content Scanning

Supported ICAP Servers	52
------------------------------	----

Determining Which Files to Scan.....	52
About Response Modification.....	53
About Request Modification	54
Returning the Object to the ProxySG	55
Caching and Serving the Object.....	55
ICAP v1.0 Features.....	55
Sense Settings	56
ISTags.....	56
Persistent Connections.....	56
Section B: Configuring ProxySG ICAP Communications	
Configuration Tasks	57
Installing the ICAP Server	57
Creating an ICAP Service	57
Deleting an ICAP Service.....	61
Customizing ICAP Patience Text	61
HTTP Patience Text	61
FTP Patience Text.....	64
Section C: Creating ICAP Policy	
VPM Objects.....	66
Example ICAP Policy	66
Exempting HTTP Live Streams From Response Modification	70
Streaming Media Request Modification Note	70
CPL Notes	70
Section D: Managing Virus Scanning	
Advanced Configurations.....	72
Using Object-Specific Scan Levels.....	72
Improving Virus Scanning Performance.....	72
Updating the ICAP Server	72
Replacing the ICAP Server	72
Access Logging.....	73
Symantec AntiVirus Scan Engine 4.0.....	73
Finjan SurfinGate 7.0	73
Chapter 4: Configuring Service Groups	
About Weighted Load Balancing.....	75
Creating a Service Group	76
Deleting a Service Group or Group Entry	79
Displaying External Service and Group Information	79

Appendix B: Glossary

Appendix A:

Index

Volume 9: Access Logging

Contact Information

Chapter 1: About Access Logging

Overview	5
Understanding Facilities	5
Understanding Protocols and Formats	6
Enabling or Disabling Access Logging	7
Document Conventions.....	8

Chapter 2: Creating and Editing Log Formats

Creating a Custom or ELFF Log Format	11
--	----

Chapter 3: Creating and Editing Access Log Facility

Editing an Existing Log Facility	16
Associating a Log Facility with a Protocol	17
Disabling Access Logging for a Particular Protocol	18
Configuring Global Settings	19

Chapter 4: Configuring the Upload Client

Encrypting the Access Log	22
Importing an External Certificate	22
Deleting an External Certificate	23
Digitally Signing Access Logs	23
Disabling Log Uploads.....	25
Decrypting an Encrypted Access Log.....	26
Verifying a Digital Signature.....	26
Editing Upload Clients.....	26
Editing the FTP Client	26
Editing the HTTP Client	28
Editing the Custom Client	29
Editing the Custom SurfControl Client	30
Editing the Websense Client	31

Chapter 5: Configuring the Upload Schedule

Testing Access Log Uploading.....	35
Viewing Access-Log Statistics.....	35
Viewing the Access Log Tail	36
Viewing the Log File Size	36
Viewing Access Logging Status.....	37
Viewing Access-Log Statistics.....	38
Example: Using VPM to Prevent Logging of Entries Matching a Source IP	40

Appendix B: Glossary

Appendix C:

Appendix D: Access Log Formats

Custom or W3C ELFF Format..... 51

 Example Access Log Formats..... 54

SQUID-Compatible Format..... 54

 Action Field Values..... 54

NCSA Common Access Log Format..... 56

 Access Log Filename Formats..... 57

Fields Available for Creating Access Log Formats 58

Index

Volume 10: Managing the ProxySG

Contact Information.....	ii
Chapter 1: About Managing the ProxySG	
Document Conventions.....	7
Chapter 2: Monitoring the ProxySG	
Using Director to Manage ProxySG Systems.....	9
Setting up Director and ProxySG Communication	9
Setting Director as a Trap Recipient.....	10
Setting Up Event Logging and Notification.....	11
Configuring Which Events to Log.....	11
Setting Event Log Size.....	11
Enabling Event Notification	12
Syslog Event Monitoring	13
Viewing Event Log Configuration and Content	14
Configuring SNMP	16
Enabling SNMP	16
Configuring SNMP Community Strings	17
Configuring SNMP Traps.....	18
Configuring Health Monitoring.....	19
Health Monitoring Requirements	19
About Hardware/Environmental Metrics (Sensors).....	20
About System Resource Metrics	21
About Health Monitoring Thresholds	22
About Health Monitoring Notification.....	24
Changing Threshold and Notification Properties.....	24
Getting A Quick View of the ProxySG Health	25
Viewing Health Monitoring Statistics.....	26
Troubleshooting	27
Chapter 3: Maintaining the ProxySG	
Restarting the ProxySG	29
Hardware and Software Restart Options	29
Restoring System Defaults.....	30
Restore-Defaults	30
Factory-Defaults.....	31
Keep-Console.....	31
Clearing the DNS Cache	33
Clearing the Object Cache.....	33
Clearing the Byte Cache	34
Troubleshooting Tip	34
Upgrading the ProxySG.....	34
The ProxySG 5.x Version Upgrade.....	34

Managing ProxySG Systems	36
Setting the Default Boot System	38
Locking and Unlocking ProxySG Systems.....	38
Replacing a ProxySG System	39
Deleting a ProxySG System	39
Disk Reinitialization	39
Multi-Disk ProxySG	39
Single-Disk ProxySG	40
Deleting Objects from the ProxySG.....	40

Chapter 4: Diagnostics

Diagnostic Reporting (Service Information)	42
Sending Service Information Automatically.....	42
Managing the Bandwidth for Service Information	43
Configure Service Information Settings	44
Creating and Editing Snapshot Jobs	46
Packet Capturing (the Job Utility)	48
PCAP File Name Format.....	48
Common PCAP Filter Expressions	48
Configuring Packet Capturing.....	49
Core Image Restart Options	53
Diagnostic Reporting (Heartbeats)	54
Diagnostic Reporting (CPU Monitoring).....	55

Chapter 5: Statistics

Selecting the Graph Scale.....	57
General Statistics	57
System Summary	57
Viewing the System Summary	58
Viewing SSL Accelerator Cards.....	58
Viewing System Environment Sensors.....	59
Viewing Disk Status	59
System Usage Statistics	60
Viewing CPU Utilization	60
Viewing Bandwidth Gain	61
Viewing Cache Freshness	62
Viewing Refresh Bandwidth Statistics.....	63
Active Sessions	64
Viewing Active Sessions	64
What is not Displayed	69
Filtering the Display	70
Obtaining HTML and XML Views of Active Sessions Data.....	71
HTTP/FTP History Statistics	71
Viewing the Number of HTTP/FTP Objects Served	71

Viewing the Number of HTTP/HTTPS/FTP Bytes Served	72
Viewing Active Client Connections	72
Viewing HTTP/FTP Client and Server Compression Gain Statistics	73
IM History Statistics	74
IM Connection Data Tab	74
IM Activity Data Tab	75
IM Clients Tab	76
P2P History Statistics	77
P2P Data	77
P2P Clients	78
P2P Bytes	79
SSL History Statistics	80
Unintercepted SSL Data	80
Unintercepted SSL Clients	80
Unintercepted SSL Bytes	81
Streaming History Statistics	82
Viewing Windows Media Statistics	82
Viewing Real Media Statistics	82
Viewing QuickTime Statistics	83
Viewing Current and Total Streaming Data Statistics	84
SOCKS History Statistics	85
Viewing SOCKS Clients	85
Viewing SOCKS Connections	85
Viewing SOCKS Client and Server Compression Gain Statistics	86
Shell History Statistics	87
Resources Statistics	88
Viewing Disk Use Statistics	88
Viewing Memory Use Statistics	88
Viewing Data Allocation Statistics in RAM and on Disk	89
Efficiency Statistics	90
Viewing the Cache Efficiency Summary	90
Viewing a Breakdown of Non-Cacheable Data	91
Viewing the Cache Data Access Pattern	92
Viewing Totals for Bytes Served	92
Contents Statistics	93
Viewing Cached Objects by Size	93
Viewing the Number of Objects Served by Size	94
Event Logging	94
Viewing the Event Log	94
Advanced Statistics	95
Using the CLI show Command to View Statistics	96

Appendix E: Glossary

Index

Volume 11: ProxySG Content Policy Language Guide

Contact Information

Preface: Introducing the Content Policy Language

About the Document Organization.....	xiii
Supported Browsers	xiv
Related Blue Coat Documentation	xiv
Document Conventions.....	xiv

Chapter 1: Overview of Content Policy Language

Concepts	15
Transactions	15
Policy Model	16
Role of CPL	17
CPL Language Basics.....	17
Comments	17
Rules.....	17
Notes	18
Quoting.....	19
Layers.....	20
Sections	21
Definitions.....	22
Referential Integrity.....	23
Substitutions	23
Writing Policy Using CPL.....	23
Authentication and Denial	24
Installing Policy.....	25
CPL General Use Characters and Formatting	25
Troubleshooting Policy	26
Upgrade/Downgrade Issues.....	27
CPL Syntax Deprecations	27
Conditional Compilation	27

Chapter 2: Managing Content Policy Language

Understanding Transactions and Timing.....	29
<Admin> Transactions	29
<Proxy> Transactions.....	30
<DNS-Proxy> Transactions.....	31
<Cache> Transactions	32
<Exception> Transaction	32
<Forwarding> Transactions	32
<SSL> Transactions	32

Timing.....	33
Understanding Layers.....	34
<Admin> Layers.....	34
<Cache> Layers.....	35
<Exception> Layers.....	36
<Forward> Layers.....	37
<Proxy> Layers.....	37
<DNS-Proxy> Layers.....	38
<SSL-Intercept> Layers.....	38
<SSL> Layers.....	39
Layer Guards.....	39
Timing.....	40
Understanding Sections.....	40
[Rule].....	41
[url].....	42
[url.domain].....	42
[url.regex].....	42
[server_url.domain].....	42
Section Guards.....	43
Defining Policies.....	43
Blacklists and Whitelists.....	44
General Rules and Exceptions to a General Rule.....	44
Best Practices.....	47

Chapter 3: Condition Reference

Condition Syntax.....	49
Pattern Types.....	50
Unavailable Conditions.....	51
Layer Type Restrictions.....	51
Global Restrictions.....	51
Condition Reference.....	51
admin.access=.....	52
attribute.name=.....	53
authenticated=.....	55
bitrate=.....	56
category=.....	58
client.address=.....	59
client.connection.dscp=.....	60
client.connection.negotiated_cipher=.....	61
client.connection.negotiated_cipher.strength=.....	62
client.connection.negotiated_ssl_version=.....	63
client.host=.....	64
client.host.has_name=.....	65
client.protocol=.....	66
condition=.....	67

console_access=	69
content_admin=	70
content_management	71
date[.utc]=	72
day=	73
dns.client_transport=	74
dns.request.address=	75
dns.request.category=	76
dns.request.class=	77
dns.request.name=	78
dns.request.opcode=	79
dns.request.type=	80
dns.response.a=	81
dns.response.cname=	82
dns.response.code=	83
dns.response.nodata=	84
dns.response.ptr=	85
exception.id=	86
ftp.method=	88
group=	89
has_attribute.name=	91
has_client=	92
hour=	93
http.connect=	95
http.method=	96
http.method.custom=	97
http.method.regex=	98
http.request_line.regex=	99
http.request.version=	100
http.response.apparent_data_type=	101
http.response.code=	102
http.response.data=	103
http.response.version=	104
http.transparent_authentication=	105
http.x_method=	106
icap_error_code=	107
im.buddy_id=	108
im.chat_room.conference=	109
im.chat_room.id=	110
im.chat_room.invite_only=	111
im.chat_room.type=	112
im.chat_room.member=	113
im.chat_room.voice_enabled=	114
im.client=	115
im.file.extension=	116
im.file.name=	117
im.file.path=	118
im.file.size=	119
im.message.opcode=	120

im.message.reflected=	121
im.message.route=	122
im.message.size=	123
im.message.text=	124
im.message.type=	125
im.method=	126
im.user_agent=	127
im.user_id=	128
live=	129
minute=	130
month=	131
proxy.address=	132
proxy.card=	133
proxy.port=	134
p2p.client=	135
raw_url.regex=	136
raw_url.host.regex=	137
raw_url.path.regex=	138
raw_url.pathquery.regex=	139
raw_url.port.regex=	140
raw_url.query.regex=	141
realm=	142
release.id=	144
release.version=	145
request.header.header_name=	146
request.header.header_name.address=	147
request.header.header_name.count=	148
request.header.header_name.length=	149
request.header.Referer.url=	150
request.header.Referer.url.category=	153
request.raw_headers.count=	154
request.raw_headers.length=	155
request.raw_headers.regex=	156
request.x_header.header_name=	157
request.x_header.header_name.address=	158
request.x_header.header_name.count=	159
request.x_header.header_name.length=	160
response.header.header_name=	161
response.raw_headers.count=	162
response.raw_headers.length=	163
response.raw_headers.regex=	164
response.x_header.header_name=	165
server.certificate.hostname.category=	166
server.connection.dscp=	167
server_url=	168
socks=	171
socks.accelerated=	172
socks.method=	173
socks.version=	174

ssl.proxy_mode=	175
streaming.client=	176
streaming.content=	177
time=	178
tunneled=	180
url=	181
url.category=	188
user=	189
user.domain=	191
user.x509.issuer=	192
user.x509.serialNumber=	193
user.x509.subject=	194
virus_detected=	195
weekday=	196
year=	197

Chapter 4: Property Reference

Property Reference	199
access_log()	200
access_server()	201
action()	202
adn.server.optimize()	203
adn.server.optimize.inbound()	204
adn.server.optimize.outbound()	205
advertisement()	206
allow	207
always_verify()	208
authenticate()	209
authenticate.charset()	210
authenticate.force()	211
authenticate.form()	212
authenticate.mode()	213
authenticate.new_pin_form()	215
authenticate.query_form()	216
authenticate.redirect_stored_requests()	217
authenticate.use_url_cookie()	218
bypass_cache()	219
cache()	220
category.dynamic.mode()	222
check_authorization()	223
client.certificate.require()	224
client.certificate.validate()	225
client.certificate.validate.check_revocation()	226
client.connection.dscp()	227
cookie_sensitive()	228
delete_on_abandonment()	229
deny()	230
deny.unauthorized()	231
detect_protocol()	232

direct()	233
dns.respond()	234
dns.respond.a()	235
dns.respond.ptr()	236
dynamic_bypass()	237
exception()	238
exception.autopad()	239
force_cache()	240
force_deny()	241
force_exception()	242
force_patience_page()	243
force_protocol()	244
forward()	245
forward.fail_open()	246
ftp.match_client_data_ip()	247
ftp.match_server_data_ip()	248
ftp.server_connection()	249
ftp.server_data()	250
ftp.transport()	251
ftp.welcome_banner()	252
http.allow_compression()	253
http.allow_decompression()	254
http.client.allow_encoding()	255
http.client.persistence()	256
http.client.recv.timeout()	257
http.compression_level()	258
http.force_ntlm_for_server_auth()	259
http.refresh.recv.timeout()	261
http.request.version()	262
http.response.parse_meta_tag.Cache-Control()	263
http.response.parse_meta_tag.Expires()	264
http.response.parse_meta_tag.pragma-no-cache()	265
http.response.version()	266
http.server.accept_encoding()	267
http.server.accept_encoding.allow_unknown()	268
http.server.connect_attempts()	269
http.server.persistence()	270
http.server.recv.timeout()	271
icp()	272
im.block_encryption()	273
im.reflect()	274
im.strip_attachments()	275
im.transport()	276
integrate_new_hosts()	277
limit_bandwidth()	278
log.rewrite.field-id()	279
log.suppress.field-id()	280
max_bitrate()	281
never_refresh_before_expiry()	282

never_serve_after_expiry()	283
patience_page()	284
pipeline()	285
reflect_ip()	286
refresh()	287
remove_IMS_from_GET()	288
remove_PNC_from_GET()	289
remove_reload_from_IE_GET()	290
request.filter_service()	291
request.icap_service()	293
response.icap_service()	294
response.raw_headers.max_count()	295
response.raw_headers.max_length()	296
response.raw_headers.tolerate()	297
server.certificate.validate()	298
server.certificate.validate.check_revocation()	299
server.certificate.validate.ignore()	300
server.connection.dscp()	301
shell.prompt()	302
shell.realm_banner()	303
shell.welcome_banner()	304
socks.accelerate()	305
socks.allow_compression()	306
socks.authenticate()	307
socks.authenticate.force()	308
socks_gateway()	309
socks_gateway.fail_open()	310
socks_gateway.request_compression()	311
ssl.forward_proxy()	312
ssl.forward_proxy.hostname()	313
ssl.forward_proxy.issuer_keyring()	314
ssl.forward_proxy.server_keyring()	315
ssl.forward_proxy.splash_text()	316
ssl.forward_proxy.splash_url()	317
streaming.transport()	318
terminate_connection()	319
trace.destination()	320
trace.request()	321
trace.rules()	322
ttl()	323
ua_sensitive()	324

Chapter 5: Action Reference

Argument Syntax	325
Action Reference	325
append()	326
delete()	327
delete_matching()	328
im.alert()	329

log_message()	330
notify_email()	331
notify_snmp()	332
redirect()	333
rewrite()	335
set()	338
transform	340

Chapter 6: Definition Reference

Definition Names	343
define action.....	344
define active_content.....	346
define category	348
define condition.....	350
define javascript	352
define policy.....	354
define server_url.domain condition.....	355
define string	357
define subnet.....	358
define url condition	359
define url.domain condition	361
define url_rewrite.....	363
restrict dns.....	365
restrict rdns	366
transform active_content	367
transform url_rewrite	368

Appendix A: Glossary

Appendix B: Testing and Troubleshooting

Enabling Rule Tracing.....	373
Enabling Request Tracing.....	374
Using Trace Information to Improve Policies.....	375

Appendix C: Recognized HTTP Headers

Appendix D: CPL Substitutions

Available Substitutions	383
Access Log Fields	384
Substitution Modifiers.....	419
Timestamp Modifiers	419
String Modifiers	421
Host Modifiers.....	421

Appendix E: Using Regular Expressions

Regular Expression Syntax	424
---------------------------------	-----

Regular Expression Details.....	425
Backslash	426
Circumflex and Dollar.....	427
Period (Dot)	428
Square Brackets	428
Vertical Bar.....	429
Lowercase-Sensitivity.....	429
Subpatterns	430
Repetition	431
Back References	433
Assertions.....	433
Once-Only Subpatterns.....	435
Conditional Subpatterns	435
Comments	436
Performance	436
Regular Expression Engine Differences From Perl	436

Volume 12: ProxySG Command Line Reference

Contact Information

Chapter 1: Introduction

Audience for this Document	9
Organization of this Document	9
Related Blue Coat Documentation	9
Document Conventions	10
SSH and Script Considerations	10
Standard and Privileged Modes	10
Accessing Quick Command Line Help	11

Chapter 2: Standard and Privileged Mode Commands

Standard Mode Commands	13
> display	15
> enable	16
> exit	17
> help	18
> ping	19
> show	20
> show access-log	25
> show bandwidth-management	26
> show bridge	27
> show commands	28
> show diagnostics	29
> show disk	30
> show exceptions	31
> show im	33
> show ip-stats	34
> show sources	35
> show ssl	36
> show streaming	37
> traceroute	38
Privileged Mode Commands	39
# acquire-utc	40
# bridge	41
# cancel-upload	42
# clear-arp	43
# clear-cache	44
# clear-statistics	45
# configure	46
# disable	47
# disk	48
# display	49
# exit	50
# help	51

# hide-advanced	52
# inline	53
# kill	55
# licensing	56
# load	57
# pcap	59
# pcap filter	60
# pcap start	62
# ping	64
# policy	65
# purge-dns-cache	66
# restart	67
# restore-sgos4-config	68
# restore-defaults	69
# reveal-advanced	70
# show	71
# show adn	73
# show attack-detection	74
# show configuration	75
# show content	76
# show proxy-services	77
# show security	78
# show ssh	79
# show ssl	80
# temporary-route	82
# test	83
# traceroute	84
# upload	85

Chapter 3: Privileged Mode Configure Commands

Configure Commands	87
#(config) accelerated-pac	88
#(config) access-log	89
#(config log <i>log_name</i>)	92
#(config format <i>format_name</i>)	96
#(config) adn	97
#(config) alert	101
#(config) archive-configuration	105
#(config) attack-detection	106
#(config client)	108
#(config server)	111
#(config) bandwidth-gain	113
#(config) bandwidth-management	114
#(config bandwidth-management <i>class_name</i>)	115
#(config) banner	117
#(config) bridge	118
#(config bridge <i>bridge_name</i>)	119
#(config) caching	121
#(config caching ftp)	123

#(config) clock	125
#(config) console-services	126
#(config http-console)	127
#(config https-console)	128
#(config ssh-console)	130
#(config telnet-console)	131
#(config) content	132
#(config) content-filter	133
#(config bluecoat)	136
#(config i-filter)	138
#(config intersafe)	140
#(config iwf)	142
#(config local)	144
#(config optenet)	146
#(config proventia)	148
#(config smartfilter)	150
#(config surfcontrol)	152
#(config websense)	154
#(config webwasher)	156
#(config) diagnostics	158
#(config service-info)	160
#(config snapshot snapshot_name)	162
#(config) dns	163
#(config) event-log	165
#(config) exceptions	167
#(config exceptions [user-defined.]exception_id)	168
#(config) exit	169
#(config) external-services	170
#(config icap icap_service_name)	172
#(config service-group service_group_name)	174
#(config websense websense_service_name)	176
#(config) failover	178
#(config) forwarding	180
#(config forwarding group_alias)	183
#(config forwarding host_alias)	184
#(config) front-panel	186
#(config) ftp	187
#(config) health-check	188
#(config health-check entry_name)	190
#(config) hide-advanced	192
#(config) hostname	193
#(config) http	194
#(config) icp	196
#(config) identd	197
#(config) im	198
#(config) inline	200
#(config) installed-systems	201
#(config) interface	202
#(config interface interface_number)	203

#(config) ip-default-gateway	205
#(config) license-key	206
#(config) line-vty	207
#(config) load	208
#(config) mapi	209
#(config) netbios	210
#(config) no	211
#(config) ntp	212
#(config) policy	213
#(config) profile	215
#(config) proxy-services	216
#(config dynamic-bypass)	218
#(config static-bypass)	220
#(config aol-im)	221
#(config cifs)	222
#(config dns)	223
#(config endpoint-mapper)	224
#(config ftp)	225
#(config http)	226
#(config https-reverse-proxy)	228
#(config mms)	230
#(config msn-im)	231
#(config rtsp)	232
#(config socks)	233
#(config ssl)	234
#(config tcp-tunnel)	235
#(config telnet)	237
#(config yahoo-im)	238
#(config) restart	239
#(config) return-to-sender	240
#(config) reveal-advanced	241
#(config) rip	242
#(config) security	243
#(config security allowed-access)	246
#(config security authentication-forms)	247
#(config security certificate)	249
#(config security coreid)	251
#(config security default-authenticate-mode)	254
#(config security destroy-old-password)	255
#(config security enable-password and hashed-enable-password)	256
#(config security enforce-acl)	257
#(config security flush-credentials)	258
#(config security front-panel-pin and hashed-front-panel-pin)	259
#(config security iwa)	260
#(config security ldap)	262
#(config) security local	266
#(config security local-user-list)	268
#(config security management)	270
#(config) security password and hashed_password	271

#(config) security password-display	272
#(config security policy-substitution)	273
#(config security radius)	275
#(config security request-storage)	278
#(config security sequence)	279
#(config security siteminder)	281
#(config windows-sso)	285
#(config) security transparent-proxy-auth	287
#(config) security username	288
#(config) session-monitor	289
#(config) shell	291
#(config) show	292
#(config) snmp	293
#(config) socks-gateways	295
#(config socks-gateways gateway_alias)	297
#(config) socks-machine-id	298
#(config) socks-proxy	299
#(config) ssh-console	300
#(config) ssl	301
#(config ssl ccl list_name)	305
#(config ssl <i>crl_list_name</i>)	306
#(config ssl ssl__default_client_name)	307
#(config) static-routes	308
#(config) streaming	309
#(config) tcp-ip	313
#(config) tcp-rtt	314
#(config) tcp-rtt-use	315
#(config) timezone	316
#(config) upgrade-path	317
#(config) virtual-ip	318
#(config) wccp	319

Chapter 5: Customizing the ProxySG

The top-level tasks you need to carry out to customize the ProxySG to your environment are:

- ❑ “Placing the ProxySG in a Network” on page 59
- ❑ “Initial Setup” on page 60
- ❑ “Simple Policy” on page 60
- ❑ “Implementing Policies” on page 60
- ❑ “Managing the ProxySG” on page 61
- ❑ “Managing the ProxyAV” on page 61
- ❑ “Troubleshooting” on page 61

This chapter also includes a task list that provides pointers in the documentation.

Placing the ProxySG in a Network

To install a ProxySG into a network, the network must be set up to present the ProxySG with traffic to control.

- ❑ Explicit Proxy: All the ProxySG needs is IP address connectivity to the network; browsers must be configured to point to the ProxySG through a PAC file.
- ❑ Transparent Proxy: The majority of networks use transparent proxy. Transparent proxying occurs when the ProxySG receives traffic destined for Origin Content Servers (OCS) and terminates the traffic, then initiates the same request to the OCS.
 - Bridging: With this configuration, you do not have to make router or L4 switch configuration changes. The ProxySG is placed inline on a segment of the network where all outgoing traffic flows; one Ethernet interface is connected to the internal network, the other Ethernet interface is connected to the Internet. The ProxySG terminates all traffic on the service ports in which the proxy has been configured and sends the request to the outside OCS. All other traffic is bridged between the two Ethernet interfaces.

Note that this configuration, without using policy controls, can lead to an *open* proxy. An open proxy results when traffic is allowed on the outside (Internet) interface because users are accessing internal Web servers behind the proxy.

- WCCP: If the site has Cisco routers, WCCP can be used to direct certain TCP/IP connections to the ProxySG. TCP/IP ports to forward to the ProxySG are communicated between ProxySG appliances and the Cisco routers. Typically, this is enforced on the outgoing interface on the Cisco router.
- L4 switching: Similar to WCCP, the L4 switch is configured to forward traffic for specific TCP/IP ports to the attached ProxySG.

Initial Setup

The ProxySG must be initially configured before it operates on a network. This can be done through the front panel (if applicable) or the serial console. The initial setup sets not only the IP address, but enable and console passwords. Once completed, the ProxySG can be managed through the serial console, SSH, or HTTPS at port 8082. Information on setting up the ProxySG is in the Quick Start Guide and Installation Guide for your platform.

Simple Policy

The default policy on new ProxySG appliances is to deny everything. To test initial setup, you can create a policy of ALLOW, along with changing access logging to log to the default logs. If the ProxySG is correctly set up, Web browsers can surf the Internet and all transactions are logged. Once the ProxySG setup is verified, the policy should again be set to DENY, unless otherwise required.

If the policy is set to allow everything and a bridged configuration is used, clients can send a connection request for any port, including e-mail, using the proxy to send spam. This is called an *open proxy* and usually results in performance slowdowns (among other things).

To prevent the ProxySG from becoming an open proxy in a bridged configuration if you must use an ALLOW configuration, add the following policy to the end of the local policy:

```
define subnet Trusted_Clients
    10.0.0.0/8
end subnet

define subnet Trusted_Servers
    216.52.23.0/24
end subnet

<Proxy>
    client.address = Trusted_Clients OK ; Policy below applies
    proxy.address = Trusted_Servers OK ; Policy below applies
    FORCE_DENY ; Force a denial for everything else

<Proxy>
    ; Add other allow or deny rules here
    ; Example: Allow all traffic not denied above
    ALLOW
```

Implementing Policies

Once the basic system is set up, you need to decide which controls—policies—to put in place. Typically, the following are configured on the system:

- ❑ Proxy caching (HTTP, FTP, Streaming)
- ❑ Authentication/single sign-on
- ❑ Access control policy
- ❑ Content filtering
- ❑ Web anti-virus

Implementing policies is a two-step process:

- ❑ Configure the feature; for example, choose Blue Coat Web Filter (BCWF) or another content filtering vendor, enable it, and schedule downloads of the database.

- ❑ Create policy through the graphical Visual Policy Manager (VPM) or through the Content Policy Language (CPL).

Managing the ProxySG

Once the configuration and policy on the ProxySG are set, you should know how to evaluate the current operating state. This can include reviewing event log messages, utilizing SNMP, or diagnostics such as CPU utilization.

- ❑ Archive a configuration file: *Volume 2: Getting Started*
- ❑ Upgrade the system: *Volume 10: Managing the ProxySG*
- ❑ Set up event logging: *Volume 10: Managing the ProxySG*
- ❑ Configure SNMP: *Volume 10: Managing the ProxySG*
- ❑ Understand Diagnostics: *Volume 10: Managing the ProxySG*

Managing the ProxyAV

The ProxySG with ProxyAV™ integration is a high-performance Web anti-virus (AV) solution. For most enterprises, Web applications and traffic are mission-critical, representing 90% of the total Internet traffic.

By deploying the ProxySG/ProxyAV solution, you gain performance and scalability (up to 250+ Mbps HTTP throughput), along with Web content control.

For information on managing the ProxyAV, refer to the *Blue Coat ProxyAV Configuration and Management Guide*.

Troubleshooting

Use the access logs, event logs, and packet captures to check connections and view traffic passing through the ProxySG. Use policy tracing to troubleshoot policy. Note that policy tracing is global; that is, it records every policy-related event in every layer. Turning on policy tracing of any kind is expensive in terms of system resource usage and slows down the ProxySG's ability to handle traffic.

- ❑ Policy tracing: For information on using policy tracing, refer to *Volume 7: VPM and Advanced Policy*.
- ❑ Access Logs: For information on configuring and using access logs, refer to *Volume 9: Access Logging*.
- ❑ Event logs: For information on using event logs, refer to *Volume 10: Managing the ProxySG*.
- ❑ Packet capture: For information on using the PCAP utility, refer to *Volume 10: Managing the ProxySG*.

Task Tables

The tables below refer to the sections in the manuals that describe the top-level tasks to customize the ProxySG to your environment. The tables are listed in alphabetical order (for example, *access logging*, *authentication*, *bridging*, *caching*, and so on).

Table 5.1: Access Logging

Task	Reference
Configure access logging with <ul style="list-style-type: none">• Blue Coat Reporter• SurfControl Reporter• Websense Reporter	<ul style="list-style-type: none">• Blue Coat Reporter: Chapter 3, “Creating the First Profile,” <i>Blue Coat Reporter Configuration and Management Guide</i>• SurfControl Reporter: <i>Volume 8: Managing Content</i>• Websense Reporter: <i>Volume 8: Managing Content</i>

Table 5.2: Anti-Virus

Task	Reference
Block Web viruses using ProxyAV	<i>Volume 8: Managing Content</i>
Set up anti-virus filtering	<i>Blue Coat ProxyAV Configuration and Management Guide</i>

Table 5.3: Authentication

Task	Reference
Achieve single sign-on with IWA (formerly NTLM)	<i>Volume 5: Securing the ProxySG</i>
Select the right authentication mode	<i>Volume 5: Securing the ProxySG</i>
Install the Blue Coat authentication/authorization agent to work with IWA (formerly NTLM)	<i>Volume 5: Securing the ProxySG</i>
Configure authentication to work with an existing authentication service	<i>Volume 5: Securing the ProxySG</i>
Set up authentication schemes and use them in policy	<i>Volume 5: Securing the ProxySG</i>

Table 5.4: Bridging

Task	Reference
Configure bridging (hardware or software)	<i>Volume 2: Getting Started</i>
Allow those from outside a bridged deployment to get to internal servers	<i>Volume 3: Proxies and Proxy Services</i>

Table 5.5: Caching

Task	Reference
Disable caching	<i>Volume 3: Proxies and Proxy Services</i>

Table 5.6: HTTP

Task	Reference
Redirect HTTP with WCCP	<i>Volume 3: Proxies and Proxy Services</i>

Table 5.7: HTTPS

Task	Reference
Create a transparent HTTPS service	<i>Volume 3: Proxies and Proxy Services</i>

Table 5.8: Instant Messaging

Task	Reference
Allow, block, and control the supported Instant Messaging clients	<i>Volume 4: Web Communication Proxies</i>

Table 5.9: Management

Task	Reference
Get the Management Console to work	<i>Volume 2: Getting Started</i>
Manage the System: <ul style="list-style-type: none">• License the system• Back up the configuration• View statistics<ul style="list-style-type: none">• Resources• Efficiency• SNMP monitoring	<ul style="list-style-type: none">• <i>Volume 2: Getting Started</i>• <i>Volume 2: Getting Started</i>• <i>Volume 10: Managing the ProxySG</i>• <i>Volume 10: Managing the ProxySG</i>• <i>Volume 10: Managing the ProxySG</i>• <i>Volume 10: Managing the ProxySG</i>

Table 5.10: Policy

Task	Reference
Set up authentication schemes and use them in policy	<i>Volume 5: Securing the ProxySG</i>
Limit network access and configuring compliance pages	<i>Volume 5: Securing the ProxySG</i>
Block unwanted content	<i>Volume 5: Securing the ProxySG</i>

Table 5.10: Policy

Change policy default	<i>Volume 7: VPM and Advanced Policy</i>
Write policy using the Visual Policy Manager (VPM)	<i>Volume 7: VPM and Advanced Policy</i>
Write policy using the Content Policy Language (CPL)	<i>Blue Coat ProxySG Content Policy Language Guide</i>

Table 5.11: Proxies

Task	Reference
Determine the best type of proxy for the environment	<i>Volume 3: Proxies and Proxy Services</i>
Set up HTTPS Reverse Proxy	<i>Volume 3: Proxies and Proxy Services</i>
Get traffic to the proxy	<i>Volume 3: Proxies and Proxy Services</i>

Table 5.12: Reporter, Blue Coat

Task	Reference
Make Blue Coat Reporter work with access logging	Blue Coat Reporter: Chapter 3, "Creating the First Profile," <i>Blue Coat Reporter Configuration and Management Guide</i>
Use Scheduler to set up report generation	Chapter 3, "Using Scheduler," in the <i>Blue Coat Reporter Configuration and Management Guide</i>
Generate specific reports for specific people	<i>Blue Coat Reporter Configuration and Management Guide</i>

Table 5.13: Reporter, SurfControl

Task	Reference
Configure SurfControl Reporter	<i>Volume 8: Managing Content</i>

Table 5.14: Reporter, Websense

Task	Reference
Configure Websense Reporter	<i>Volume 8: Managing Content</i>

Table 5.15: Services

Task	Reference
Create a port service	<i>Volume 3: Proxies and Proxy Services</i>

Table 5.16: Streaming

Task	Reference
Control streaming protocols	<i>Volume 4: Web Communication Proxies</i>

Table 5.17: WCCP

Task	Reference
Configure WCCP for multiple ports	<i>Volume 6: Advanced Networking</i>
Redirect HTTP with WCCP	<i>Volume 6: Advanced Networking</i>
Configure the home-router IP	<i>Volume 6: Advanced Networking</i>
Configure multiple home-routers	<i>Volume 6: Advanced Networking</i>
Configure a multicast address as the proxy's home router	<i>Volume 6: Advanced Networking</i>

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.

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

MD5

RSA Data Security, Inc. MD5 Message-Digest Algorithm

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

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

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

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

THE BEER-WARE LICENSE" (Revision 42):

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

Microsoft Windows Media Streaming

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

OpenLDAP

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

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

The OpenLDAP Public License Version 2.7, 7 September 2001

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

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

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

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

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

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

OpenSSH

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

This file is part of the OpenSSH software.

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

OpenSSH contains no GPL code.

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

[Tatu continues]

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

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

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

[The licence continues]

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

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

NO WARRANTY

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

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

Cryptographic attack detector for ssh - source code

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

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

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

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

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

@version 3.0 (December 2000)

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

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

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

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

This code is hereby placed in the public domain.

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

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

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

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

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

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

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

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

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

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

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

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

OpenSSL

Copyright (c) 1995-1998 Eric Young (eyay@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>](mailto:eay@cryptsoft.com) and [Tim J. Hudson <mailto:tjh@cryptsoft.com>](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.
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 routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

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

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

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

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

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

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

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

PCRE

Copyright (c) 1997-2001 University of Cambridge

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

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

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

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

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

PHAOS SSLava and SSLavaThin

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

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

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

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

RealSystem

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

SNMP

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

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

Restricted Rights Legend:

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

PROPRIETARY NOTICE

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

STLport

Copyright (c) 1999, 2000 Boris Fomitchev

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

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

The code has been modified.

Copyright (c) 1994 Hewlett-Packard Company

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

Copyright (c) 1997 Moscow Center for SPARC Technology

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

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

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

SmartFilter

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

SurfControl

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

Symantec AntiVirus Scan Engine

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

TCPIP

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

Their copyright header follows:

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

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

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

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

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

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

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR

CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Trend Micro

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

zlib

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

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

ICU License - ICU 1.8.1 and later
COPYRIGHT AND PERMISSION NOTICE
Copyright (c) 1995-2003 International Business Machines Corporation and others
All rights reserved.
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, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation. 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 OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE. Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder