

# BLUE COAT

## *Blue Coat SGOS 5.5.x Release Notes*

*Version: SGOS 5.5.11.7*

*BCAAA Protocol Version: See "Important Notes about SGOS 5.5.x" on page 5*

*Release Date: 08/4/2014*

*Document Revision: 08/08/2014*

### Release Note Directory

These release notes present information by each release in the SGOS 5.5.x software line. Each section provides feature descriptions, fixes and known issues.

- ❑ [Section A: "SGOS 5.5.x Reference Information"](#) on page 5—If you are a new user to SGOS 5.5.x, Blue Coat strongly recommends that you read this section in its entirety. The section identifies topics such as supported platforms, important upgrade information, and additional requirements specific to SGOS 5.5.x version information.
- ❑ [Section B: "SGOS 5.5.11.7, build 145725"](#) on page 10
- ❑ [Section C: "SGOS 5.5.11.5, build 125595"](#) on page 11
- ❑ [Section D: "SGOS 5.5.11.3, build 114227"](#) on page 13
- ❑ [Section E: "SGOS 5.5.11.1, build 110885"](#) on page 14
- ❑ [Section F: "SGOS 5.5.10.1, build 92100"](#) on page 20
- ❑ [Section G: "SGOS 5.5.9.1, build 81874"](#) on page 25
- ❑ [Section H: "SGOS 5.5.8.1, build 78310"](#) on page 31
- ❑ [Section I: "SGOS 5.5.7.1 , build 77648"](#) on page 34
- ❑ [Section J: "SGOS 5.5.6.2, build 71837"](#) on page 41
- ❑ [Section K: "SGOS 5.5.6.1, build 70899"](#) on page 42
- ❑ [Section L: "SGOS 5.5.5.1, build 63141"](#) on page 45
- ❑ [Section M: "SGOS 5.5.4.1, build 53805"](#) on page 51
- ❑ [Section N: "SGOS 5.5.3.31, build 51877"](#) on page 62
- ❑ [Section O: "SGOS 5.5.3.1, build 46382"](#) on page 63

- ❑ [Section P: "SGOS 5.5.2.1, build 45055"](#) on page 68
- ❑ [Section Q: "SGOS 5.5.1.1, build 43412"](#) on page 75
- ❑ [Section R: "Limitations in SGOS 5.5.x"](#) on page 89
- ❑ [Section S: "SGOS 5.5.x — Support Files and Support for Other Products"](#) on page 92—List of all supported clients, browsers, and products that work together with a ProxySG running SGOS 5.5.x.

## SGOS 5.5.x Feature Matrix

The following table lists the features and enhancements introduced in the SGOS 5.5.x release line, with cross-reference links to feature descriptions.

This table only lists releases with new features.

Table 1–1 SGOS 5.5.x Feature Matrix

| Component         | Feature Introduction/<br>Enhancement                                        | 5.5.1 | 5.5.2 | 5.5.3 | 5.5.4 |
|-------------------|-----------------------------------------------------------------------------|-------|-------|-------|-------|
| Access Logging    | "Copy Existing Log Schema to a New Custom Schema" on page 83                | X     |       |       |       |
|                   | "Logging the Proxy Source Port When Connecting to a Remote Site" on page 83 | X     |       |       |       |
| ADN               | "Fast Transparent Tunnels" on page 75                                       | X     |       |       |       |
|                   | "Adaptive Compression" on page 76                                           | X     |       |       |       |
|                   | "Peer Deletion" on page 76                                                  | X     |       |       |       |
|                   | "Port Consolidation" on page 76                                             | X     |       |       |       |
|                   | "MAPI" on page 76                                                           | X     |       |       |       |
| Authentication    | "Session-Monitor Support Enhancements" on page 68                           |       | X     |       |       |
| CIFS Proxy        | "Pre-Population CLI Commands" on page 80                                    | X     |       |       |       |
|                   | "SMB Signing" on page 80                                                    | X     |       |       |       |
| Content Filtering | "Content Filtering Redesign" on page 77                                     | X     |       |       |       |
|                   | "Support for SmartFilter Category Map 4" on page 51                         |       |       |       | X     |
| DNS Proxy         | "DNS Proxy" on page 83                                                      | X     |       |       |       |
| Event Logging     | "Log when Syslog is Enabled or Disabled" on page 83                         | X     |       |       |       |
|                   | "Multiple Syslog Servers" on page 84                                        | X     |       |       |       |
| Hardware          | "Support for the SG300 and SG600 Appliances" on page 62                     |       |       | X     |       |
| Health Checks     | "Email Alerts Subject Line" on page 84                                      | X     |       |       |       |

Table 1–1 SGOS 5.5.x Feature Matrix

| Component         | Feature Introduction/<br>Enhancement                                      | 5.5.1 | 5.5.2 | 5.5.3 | 5.5.4 |
|-------------------|---------------------------------------------------------------------------|-------|-------|-------|-------|
| HTTP Proxy        | "HTTP Network Error Transparency" on page 81                              | X     |       |       |       |
|                   | "Tunnel on Protocol Error" on page 81                                     | X     |       |       |       |
|                   | "Trust Destination IP for Client-less Connections" on page 82             | X     |       |       |       |
|                   | "Limiting Client-less Connections" on page 82                             | X     |       |       |       |
| IPv6              | "IPv6 Support" on page 75                                                 | X     |       |       |       |
|                   | "IPv6 Support in RTSP Proxy" on page 69                                   |       | X     |       |       |
| Malware Scanning  | "Threat Protection" on page 79                                            | X     |       |       |       |
| Network           | "Nameable Interfaces" on page 83                                          | X     |       |       |       |
|                   | "WCCP Router Affinity" on page 79                                         | X     |       |       |       |
|                   | "WCCP Service Groups" on page 79                                          | X     |       |       |       |
| Services          | "Redesign" on page 77                                                     | X     |       |       |       |
|                   | "Listen on Source IP Address" on page 77                                  | X     |       |       |       |
| SNMP              | "SNMP Support for Multiple CPU Cores" on page 51                          |       |       |       | X     |
| SSL Proxy         | "SSL Connection Bypassing for Client Certificates" on page 82             | X     |       |       |       |
| Virtual Appliance | "Support for ProxySG VA" on page 69                                       |       | X     |       |       |
| VPM               | "CPL Layer" on page 78                                                    | X     |       |       |       |
|                   | "File Extension Object" on page 78                                        | X     |       |       |       |
|                   | "Return Redirect Object: Support for 301 and 307 Return Codes" on page 78 | X     |       |       |       |
|                   | "Usability Enhancements" on page 78                                       | X     |       |       |       |

## Section A: SGOS 5.5.x Reference Information

This section applies to all SGOS 5.5.x releases.

### Important Notes about SGOS 5.5.x

Before beginning the upgrade process, please read the following information:

- ❑ If you are using the Blue Coat Authentication and Authorization Agent (BCAAA), use the version(s) recommended on the [SW Download](#) pages. Even if you are already running BCAA, you might want to upgrade to the latest BCAA version because it may contain important fixes.

Do *not* upgrade SGOS unless you have first installed the compatible BCAA version. Refer to the following documents for more information:

- The [BCAAA Service Requirements](#) for BCAA directory services support and sizing requirements.
- The [SGOS Upgrade/Downgrade Quick Reference](#) and the [SGOS Upgrade/Downgrade Guide](#) for instructions to upgrade or downgrade BCAA.
- ❑ If you are upgrading from SGOS 4.x and the appliance has previously run SGOS 5.x, the 5.x configuration is applied during upgrade. You must restore the SGOS 4.x configuration settings. The [SGOS Upgrade/Downgrade Guide](#) contains this procedure, but continue reading these Release Notes for further upgrade information.
- ❑ The JRE version required to run the Management Console has changed. JRE 1.4.x is no longer supported. For SGOS 5.5.x, the earliest supported JRE is 1.5.0\_15. See "[Java Runtime Environment \(JRE\) Information](#)" on page 9.

To proceed with the upgrade, go to "[Upgrading to this Release](#)" on page 6.

### Product Documentation

Access the SGOS 5.5.x product documentation on BlueTouch Online:

<https://bto.bluecoat.com/documentation/pubs/view/SGOS 5.5.x>

## Support

Frequently asked questions and more information about this release can be found in the Knowledge Base:

<https://kb.bluecoat.com>

Direct support questions regarding this release to:

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

For questions or comments related directly to these Release Notes, send an e-mail to: [documentation.inbox@bluecoat.com](mailto:documentation.inbox@bluecoat.com)

## Upgrading to this Release

All SGOS upgrade information is now located in a single BTO location:

<https://bto.bluecoat.com/documentation/pubs/view/Upgrading%20and%20Migrating%20SGOS>

The release-specific upgrade/downgrade guides have been removed. You should refer instead to these documents:

- ❑ [\*SGOS Upgrade/Downgrade Quick Reference\*](#)

This document contains the upgrade path intended to be used for all SGOS releases and also provides the high-level upgrade steps.

- ❑ [\*SGOS Upgrade/Downgrade Guide\*](#)

This document provides the detailed steps required for upgrading to this release, including BCAA upgrade procedures. It also contains feature change information.

Blue Coat also recommends reading the [\*SGOS 5.5.x Feature Change Reference\*](#). This document includes two sections: one for SGOS 5.5.x-specific features, and one with legacy information that is important for upgrades from pre-SGOS 5.4.x, including SGOS 4.x.

---

**Important:** Schedule your upgrade during off-peak hours. If you have ADN configured, upgrade the ADN Managers—Primary manager and Backup Manager—before upgrading the ADN nodes.

---

## Upgrade Prerequisites

To upgrade to this release, you must first determine if your hardware platform is supported, and whether you can upgrade directly or must upgrade through an interim release. You must also familiarize yourself with potential upgrade/downgrade issues.

Before installing or upgrading to SGOS 5.5.x, perform the following:

1. Determine if SGOS 5.5.x is supported on your hardware platform. See ["Supported ProxySG Platforms"](#) on page 7.
2. Determine your upgrade path. Refer to the [SGOS Upgrade/Downgrade Quick Reference](#).
3. Understand the BCAA upgrade/downgrade process. Refer to the [BCAA Service Requirements](#) and the [SGOS Upgrade/Downgrade Guide](#).
4. Read the upgrade notes in ["Upgrade/Downgrade Notes"](#) on page 8.
5. Ensure that your browser has the correct JRE installed. See ["Java Runtime Environment \(JRE\) Information"](#) on page 9.
6. Recommended—Learn about the changes and fixes in the SGOS version you are upgrading to. See ["SGOS 5.5.10.1, build 92100"](#) on page 20.
7. Recommended—Learn about third-party product support. See [Section S: "SGOS 5.5.x — Support Files and Support for Other Products"](#) on page 92.
8. When you are ready to upgrade a ProxySG, follow the steps in the [SGOS Upgrade/Downgrade Guide](#).

## Supported ProxySG Platforms

All SGOS 5.x versions, including 5.5.x, require a minimum of 512 MB of memory. SGOS 5.5.x contains significant new functionality and upgrading might impact CPU usage; therefore, proper sizing is critical. If the peak CPU utilization on your system exceeds 65 percent on an SG810 and lower models, or 70 percent on an SG8100 models running SGOS 4.2.8.6, contact your Blue Coat sales representative or Blue Coat reseller agent before upgrading to SGOS 5.5.x

Hardware: The following ProxySG models can be upgraded to SGOS 5.5.x:

- ❑ SG200-B
- ❑ SG200-C
- ❑ SG210
- ❑ SG300 (requires SGOS 5.5.3.31 or higher)
- ❑ SG510
- ❑ SG600 (requires SGOS 5.5.3.31 or higher)
- ❑ SG810
- ❑ SG8100
- ❑ SG900 (requires SGOS 5.5.6.2 or higher)
- ❑ SG9000 (except 9000-30 and 9000-40)

Older ProxySG models cannot be upgraded to this release. In addition, 256 MB RAM systems, like the SG200-A, cannot be upgraded to SGOS 5.5.x. To upgrade the hardware to a newer model, contact your Blue Coat sales representative or Blue Coat reseller agent.

## Supported Upgrade/Downgrade Paths

Refer to the [SGOS Upgrade/Downgrade Quick Reference](#).

## Upgrade/Downgrade Notes

This section provides important information involved in upgrading and downgrading Blue Coat SGOS.

---

**Note:** For feature-specific impacts, see the [SGOS 5.5.x Feature Change Reference](#).

---

### Upgrading Licenses

The ProxySG automatically checks for license updates upon reboot or once daily for a month before the currently installed license expires. By default, automatic license check is enabled, that is the **Use Auto-Update** button is selected in the **Maintenance > Licensing > Install** tab.

Perform the steps below to upgrade your license — from SGOS 4.x to 5.x license or from the MACH5 edition license to the Proxy edition license, as applicable.

#### To upgrade the license:

In the Management Console, select **Maintenance > Licensing > Install**. In the **License Key Automatic Installation** field perform one of the following:

- If you previously used the Management Console to retrieve an SGOS license and the **Use Auto-Update** button is enabled, click **Update**.
- If you did not previously use the Management Console to retrieve an SGOS license and you have a valid WebPower/BlueTouch account login (for the appliance to be upgraded), click **Retrieve**. The Request License Key dialog displays. Enter your BlueTouch credentials and click **Send Request**.

The Blue Coat license server:

- Receives the request;
- Automatically upgrades the SGOS 4.x license to the SGOS 5.x license; and
- Returns the new license to the ProxySG.

To verify the SGOS 5.x license has been loaded, click the **View** tab and look for SGOS 5.x components.

### Alternate Methods

If you cannot directly access the Internet, contact Blue Coat Support Services for assistance. You are asked to provide the hardware serial numbers of the appliances to be upgraded and account details, such as contact name, e-mail address, and BlueTouch Online account name. If you do not have a BlueTouch Online account or if you have lost the password, see "[Upgrade/Downgrade Notes](#)" on page 8 for details.



## Java Runtime Environment (JRE) Information

To run the SGOS 5.5.x Management Console, you must install the [Sun Java JRE](#) version 1.5.0\_15 or later, including 1.6 (except for 1.6\_05, which causes VPM on-line help problems).

JRE 1.4.x is no longer supported. For SGOS 5.5.x, the earliest supported JRE is 1.5.0\_15.

You have the following options:

- ❑ Get a supported JRE from [Sun](#) and install it yourself.
- ❑ When you start the ProxySG Management Console for the first time after upgrading to SGOS 5.4 or later and your currently installed JRE is earlier than 1.5.0\_15, your Web browser attempts to download a more current JRE.

Following are details about Internet Explorer and Firefox:

- (Recommended.) Use Internet Explorer because it attempts to download JRE 1.5.0\_15. Follow the prompts on your screen to download and install this JRE.
- Firefox attempts to install the latest JRE, which might not be compatible with the Management Console.

---

**Note:** If you upgrade JRE from a lower version, clear the browser's cache.

---

## Downgrading your ProxySG Appliance with Increased Object Store Capacity to SGOS 5.5.x

The SG900 appliances are multi-disk systems that were manufactured with SGOS 6.2, and have increased object limits enabled by default. All other multi-disk systems can get this extra capacity by initiating the `disk increase-object-limit` command after upgrading to 6.2. The disks are re-initialized in a format that is not compatible with SGOS releases prior to 6.2.

Hence, if your disks have the increased object capacity, you must use the `disk decrease-object-limit` command before downgrading to a pre-6.2 release. This command preserves the configuration, registry settings, policy, licensing files, and the appliance birth certificate; it does not retain cache contents, access logs, event log, and sysinfo snapshots.

**WARNING! If you fail to use the `disk decrease-object-limit` command before downgrading to a pre-6.2 release, all data and settings will be lost after the downgrade. For details refer to FAQ1429: <https://kbbluecoat.com/index?page=content&id=FAQ1429>.**

## Section B: SGOS 5.5.11.7, build 145725

*Release Date: 08/4/2014, build 145725*

*BCAAA Protocol Version: "Important Notes about SGOS 5.5.x" on page 5*

*Compatible with: SGME 5.5.x and 6.x, Reporter 8.x and 9.x, ProxyAV 3.x, and ProxyClient 3.1.x, 3.2.x, 3.3.x, and 3.4.x*

### SGOS 5.5.11.7 Contents

The following issues have been fixed in SGOS 5.5.11.7.

### Security Fixes in 5.5.11.7

This section lists security fixes that have been resolved in SGOS 5.5.11.7.

- ❑ Old passwords could be used to login via SSH and Serial console CLI indefinitely until either logging in via web, logging in with the new password, or logging in with the wrong password. Please see <https://kb.bluecoat.com/index?page=content&id=SA77> for more information. (B#198396)

### Fixes in SGOS 5.5.11.7

This section lists issues reported in previous versions that have been resolved in SGOS 5.5.11.7.

#### *Hardware Drivers*

- ❑ Error when reading SPD memory from DIMM 1 on ProxySG 510 A/B appliances has been resolved. (B#204226)

#### *Licensing*

- ❑ An **unsupported configuration** message was present on ProxySG 510-A appliances after installing the license. (B#205153)

#### *Storage*

- ❑ Advanced URL /Diagnostics/Hardware/Info incorrectly displayed an **unsupported configuration** message for a correct configuration. (B#205155)

#### *System Statistics*

- ❑ A CMOS +3V battery voltage sensor was added to the list of hardware environment sensors. (B#200555)

#### *TCP/IP and General Networking*

- ❑ The ProxySG experienced a hardware reset at 0xE in process `tcipip` in `tcipip.dll` when WCCP was enabled. (B#191086, SR2-938418552)

## Section C: SGOS 5.5.11.5, build 125595

---

### Section C: SGOS 5.5.11.5, build 125595

*Release Date: 02/18/2014, build 125595*

*BCAAA Protocol Version: "Important Notes about SGOS 5.5.x" on page 5*

*Compatible with: SGME 5.5.x and 6.x, Reporter 8.x and 9.x, ProxyAV 3.x, and ProxyClient 3.1.x, 3.2.x, 3.3.x, and 3.4.x*

### SGOS 5.5.11.5 Contents

The following issues have been fixed in SGOS 5.5.11.5.

### Fixes in SGOS 5.5.11.5

This section lists issues reported in previous versions that have been resolved in SGOS 5.5.11.5.

#### *Authentication*

- ❑ An SAP client received an error because the authorization header was stripped off after the certificate authentication. (B#189352; SR 2-582756412)

#### *Build*

- ❑ The Management Console (MC) falsely reported that the Java certificate, presented by the ProxySG management console, expired on August 2013. (B#192624; SR 2-634441472)

#### *CIFS\_Proxy*

- ❑ The ProxySG experienced high memory pressure in CIFS Proxy that triggered a software restart at 0x5b0006 in process Threshold\_Monitor in kernel\_shim.dll. (B#185929; SR-550916322, 2-592683722, 2-598967242)
- ❑ The ProxySG experienced high memory pressure in CIFS Proxy when a very large directory was read. (B#189948; SR 2-595519876, 2-596398052, 2-605964402)

#### *HTTP\_Proxy*

- ❑ The ProxySG appliance experienced memory pressure when there were unlimited HTTP RW pipeline prefetch requests. (B#177408; SR 2-476653002, 2-544155192, 2-549758412, 2-581176522, 2-583710379, 2-583968147, 2-604871612, 2-604871662, 2-657137491)
- ❑ The ProxySG experienced a software restart at 0x810002 in process HTTP CW xxx when URLs contained numeric IP addresses and a default port (for example, <http://10.168.0.1:80/>...) were present in the HTTP response and transformation was applied. (B#189102)

## Section C: SGOS 5.5.11.5, build 125595

---

### MC\_Legacy

- ❑ When the Management Console made CLI inline commands, sometimes it used `EOF` and sometimes it used `eofNNNN` where `NNNN` was a timestamp. This was a problem because some Base64 encoded certificates contain the string `EOF`. (B#190784; SR 2-583733942)

### Services

- ❑ Users were unable to view the SNMP service from the CLI if the ProxySG was upgraded or had a new installation of the SGOS 5.5.x release. The problem occurred when the fix for B#88912 was not present in the release and the SNMP service was not re initialized. (B#187617; SR 2-570064643)

### SSL/TLS\_and\_PKI

- ❑ Users received an `ssl_server_cert_untrusted_issuer` exception page after upgrading. (B#188929; SR 2-583083032)
- ❑ The ProxySG experienced a hardware restart at `0x810002` in process `HTTP_CW_xxx` after removing almost all of the SSL certificates from the browser-trusted CCL. (B#189557; SR 2-574928642)

### Storage

- ❑ A compact flash file system error occurred that may have resulted in a **no bootable image** error after an upgrade. (B#188719)
- ❑ The ProxySG experienced a software restart at `0x10005` in process group `PG_UNKNOWN` in process `ATA_Clock` under load. (B#194543; SR 2-650117242)

### TCP/IP\_and\_General\_Networking

- ❑ The interface link DOWN event was missing from the syslog, but could be seen in the event log. (B#183536; SR 2-517558071)
- ❑ Memory utilization increased when SGRP (failover) was enabled. The rate of the increase was dependent on the number of SGRP groups configured, the frequency of SGRP advertisements, the number of interfaces on the box, and the amount of memory available. (B#191410)
- ❑ If a local category database contained an IPv4 address, DNS lookup from the ProxySG was always IPv4 even when it matched a IPv6 policy. (B#191724; SR 2-621471742)

### URL\_Filtering

- ❑ The ProxySG experienced a hardware restart at `0xE` in process group `PG_POLICY_HTTP` in process `HTTP_CW` when there was intermittent communication with a DRTR server. (B#173517; SR 2-439910172, 2-501845072, 2-592705522, 2-594134712)

## Section D: SGOS 5.5.11.3, build 114227

---

### Section D: SGOS 5.5.11.3, build 114227

*Release Date: 07/17/2013, build 114227*

*BCAAA Protocol Version: "Important Notes about SGOS 5.5.x" on page 5*

*Compatible with: SGME 5.5.x and 6.x, Reporter 8.x and 9.x, ProxyAV 3.x, and ProxyClient 3.1.x, 3.2.x, 3.3.x, and 3.4.x*

### SGOS 5.5.11.3 Contents

The following issues have been fixed in SGOS 5.5.11.3.

### Fixes in SGOS 5.5.11.3

This section lists issues reported in previous versions that have been resolved in SGOS 5.5.11.3.

#### *Authentication*

- ❑ An SAP client received an error because the authorization header was stripped off after the certificate authentication. (B#189352; SR2-582756412)

#### *IPv6 Stack and IPv6 Proxies*

- ❑ On the ProxySG8100 appliance (cobra card) ndp output shows `ioctlsocket` errors. (B#131388; SR 2-585750302)

#### *Storage*

- ❑ Support has been added for a 1TB drive, model Toshiba MG03SCA100, for the 900 and 9000 platforms. (B#188968)

#### *TCP/IP and General Networking*

- ❑ During SGRP failover to a backup proxy, any inbound ADN connection to the backup Proxy, with a VIP as a destination, would fail and time-out. (B#189607)

## Section E: SGOS 5.5.11.1, build 110885

---

### Section E: SGOS 5.5.11.1, build 110885

*Release Date: 05/02/2013, build 110885*

*BCAAA Protocol Version: ["Important Notes about SGOS 5.5.x" on page 5](#)*

*Compatible with: SGME 5.5.x and 6.x, Reporter 8.x and 9.x, ProxyAV 3.x, and ProxyClient 3.1.x, 3.2.x, 3.3.x, and 3.4.x*

### SGOS 5.5.11.1 Contents

See the following sections for information on this release.

- ❑ ["SGOS 5.5.11.1 - Security" on page 14](#)
- ❑ ["Fixes in SGOS 5.5.11.1" on page 14](#)
- ❑ ["Known Issues in SGOS 5.5.11.1" on page 19](#)

For a list of limitations, see ["Limitations in SGOS 5.5.x" on page 89](#).

### SGOS 5.5.11.1 - Security

SGOS 5.5.11.1 includes the following security improvements.

- ❑ The SSL 3.0 implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly initialize data structures for block cipher padding, which might allow remote attackers to obtain sensitive information by decrypting the padding data sent by an SSL peer. This OpenSSL vulnerability has been fixed in this release (B#173630). See [CVE-2011-4576](#).
- ❑ The ProxySG appliance is no longer vulnerable to denial-of-service (DoS) attacks via Server Gated Cryptography (SGC) renegotiation (B#174186). ([CVE-2011-4619](#))
- ❑ Fixed OpenSSL ASN1 BIO vulnerability (B#176491) ([CVE-2012-2110](#) and [CVE-2012-2131](#))

### Fixes in SGOS 5.5.11.1

This section lists issues reported in previous versions that have been resolved in SGOS 5.5.11.1.

#### ADN

- ❑ A new ADN CLI command, previously available in 6.x releases, is available to select transparent mode for edge peers. This functionality allows SGOS 5.5 to initiate connections to concentrators running SGOS 5.4 using regular acceleration. The `connect-transparent` command controls transparent tunnels as follows:
  - `connect-transparent enable`  
Allows transparent tunnel initiation, and defaults to fast mode.
  - `connect-transparent enable fast`  
Allows transparent tunnel initiation, and defaults to fast mode.

## Section E: SGOS 5.5.11.1, build 110885

---

- `connect-transparent enable regular`  
Allows transparent tunnel initiation, and defaults to regular mode.

The preceding settings are persistent, even after a reboot. Fast Transparent Tunnel (FFT) mode is the default mode for transparent tunnels where supported. (B#186308)

### Authentication

- ❑ Fixed an issue in which the appliance intermittently redirected a few of the clients to a virtual URL in a loop. (B#171963)
- ❑ When BCAA could not find a Domain Controller (DC) in DNS, subsequent queries in Windows SSO would not be performed. (B#177099, SR-2-465952782)
- ❑ BCAA missed some Windows logon sessions for Windows Single Sign-On (SSO). (B#180556)
- ❑ Kerberos Constrained Delegation caused authentication to fail for users who were not in the same domain as the BCAA server. (B#182032, SR-2-507995556)
- ❑ Successful authentication on the second order/preference in sequence realm did not honor surrogate refresh time when the subsequent request was HTTPS (no SSL interception). The problem only happened with a sequence realm and HTTPS websites, not with LDAP or RADIUS realms. (B#183758, SR-2-519589002)
- ❑ The ProxySG appliance experienced a hardware restart at 0xE in process `tcpip` in `tcpip.dll` during RADIUS operations. (B#184222, SR-2-535662252)
- ❑ The ProxySG appliance experienced a hardware restart at 0x00000058 in process `LDAP Authorization Refresh Worker` in `authenticator.dll` when a LDAP realm was deactivated. (B#186283, SR-2-553289942)

### Cache Engine

- ❑ RAM usage statistics were incorrectly displayed on the diagnostic page. (B#175956, SR-2-463708992)
- ❑ The ProxySG appliance restarted when a disk or file system was corrupted during a read operation. Error handling was added to prevent a crash under similar circumstances. (B#182297, SR-2-509498222)
- ❑ The ProxySG appliance experienced a hardware restart at 0x40 in process `HTTP CW C329CEC0` in `ce_admin.dll` due to an internal error. (B#183763, SR-2-531893442)

### CIFS Proxy

- ❑ Certain CIFS applications did not save cached files correctly, which resulted in an error message that was displayed when the file was accessed. (B#175312, SR-2-429251582)

## Section E: SGOS 5.5.11.1, build 110885

---

- ❑ A shared mode Excel2007 worksheet was corrupted when the client accessed the file via ADN and local. (B#177034, SR-2-473079682)
- ❑ When a MacOS client attempted to access an Excel file on network share with CIFS Proxy over ADN, it received a `File cannot be accessed` error message. This occurred when the appliance was in a transparent ADN inline setup and did not occur when the user accessed the same file from a Windows client. (B#181562, SR-2-483175913)
- ❑ Some Windows XP clients were unable to print from remote branches after upgrading SGOS. When this fix is installed on both the concentrator and edge ProxySG appliances, users can print from Windows XP clients. (B#186986)

### Client Manager

- ❑ ProxyClient download links now work with clients running Microsoft Security Update KB2585542. (B#176150, SR-2-438141662)

### FTP Proxy

- ❑ Memory usage by the FTP proxy was high when FTP objects were ICAP scanned and cached. (B#171317, SR-2-422651927, 2-487799532)

### Health Checks

- ❑ DRTR server did not fail over, even though the DRTR service sent back a non-OK response, for example, 403 or 503. (B#184426)

### HTTP Proxy

- ❑ The ProxySG now closes the client connection when the server connection cannot be persisted. Previously, when the server wasn't the one that closed the connection, the ProxySG didn't implement the client persistence policy. As a result, the client connection stayed open, and then caused the ProxySG appliance to re-use the connection it just closed with the server. (B#177618)
- ❑ When two consecutive requests on the same persistent connection were resolved to different HTTPS servers, the handshake to the second server failed with a `SSL Certificate Hostname Mismatch (ssl_domain_invalid)` error. (B#167020)
- ❑ HTTP proxy responded incorrectly when an invalid URL was in the request. It returned an `Appliance Error` instead of a `Request Error`. (B#174711, SR-2-450579168)
- ❑ URLs starting with encoded forward slashes are no longer treated as relative URLs when transforming HTML pages. This caused 500 server errors to be sent back when transforming HTML pages. (B#178317, SR-2-493370842)
- ❑ Cacheable YouTube videos could not be downloaded on an iPhone going through the appliance unless HTTP Client Persistence for youtube.com was disabled, **Delete On Abandonment** was configured, and byte-ranges were disabled. (B#179612, SR-2-488577951)



## Section E: SGOS 5.5.11.1, build 110885

---

- ❑ An HTTP 500 internal server error was returned when going to certain sites. This happened when the Pipelining/Prefetching subsystem stored non-cacheable objects as "serve-once" and the actual request for it came after it had expired. (B#180288, SR-2-497496414)
- ❑ The ProxySG appliance experienced a hardware restart at 0x5d92e000, in Process HTTP CW BF26DEC0 in `shared_dll.dll`. The problem occurred when encoded characters were in different segments of a message. (B#180704)
- ❑ The ProxySG experienced a software restart at 0x810002 in process HTTP CW 81EE9B50 when there was an SSL connection error upstream, HTTPS **Intercept on Exception** was enabled (on by default), and the request header size was greater than 8K. The restart did not occur if the appliance was not intercepting SSL connections using HTTPS proxy and **Intercept on Exception** was disabled. (B#181503, SRs-2-506572632,2-514571922)
- ❑ HTTP 412 Precondition Failed response code was erroneously returned to the client when the OCS responded with a HTTP 401 Unauthorized error code. This occurred when the ProxySG appliance was configured for **Cache Bypass** mode on a client IP. (B#181528, SR-2-500957787)

### MAPI Proxy

- ❑ Logging into a Windows domain took a long time when EPMapper was enabled. (B#184850, SR-2-540581559)

### Policy

- ❑ The transformation of relative URLs starting with "../" did not perform correctly. (B#181309)

### Proxy Forwarding

- ❑ When configuring a forwarding host, the ProxySG appliance incorrectly stored the result for the `default-sequence add` command in the archived configuration. The user was then unable to install the configuration from backup. (B#183217, 2-524953062)

### SSL/TLS and PKI

- ❑ Fixed an issue in which the browser could have received a certificate error for certain SSL websites due to a missing "Thawte\_Premium\_Server\_CA" certificate. (B#175163, SRs 2-476980862, 2-477341292, 2-480765572, 2-481269722)

### SOCKS Proxy

- ❑ SOCKS application returned port unreachable, therefore unable to connect to a server, when the ProxySG's LAN interface was connected to a private network and the WAN interface was connected to a public network where the default gateway was in a public network. (B#170781, SRs-2-416900694,2-454376092)

## Section E: SGOS 5.5.11.1, build 110885

---

### TCP/IP and General Networking

- ❑ The value of `tcp-keepalive-timeout` was not included in the Configuration Archive. The problem was seen when the user displayed `show config (tcp-ip tcp-keepalive-timeout` was not displayed). (B#156690, SR-2-430445092)
- ❑ On multi-processor platforms, the Packet Capture Time was off from the system clock. (B#175128)
- ❑ Software bridge failover took a very long time. The issue happened due to TCN not aging the bridge forwarding table. If the spanning tree was enabled on the ProxySG appliance and a topology change was detected (for example, receipt of the TCN, or bstp make blocking, or forward delay timer expired), then these bridge associated hash table entries were not removed from the table. (B#175656, SR-2-480685922)
- ❑ The number of TCP connections in `established` or `close_wait` states (SNMP OID "1.3.6.1.2.1.6.9") is reported incorrectly after long, continuous usage of the ProxySG appliance. (B#176434)
- ❑ The Proxy SG appliance exhibited a slow memory leak caused by RIP route deletion. (B#183369, SR-2-523883530)
- ❑ The ProxySG appliance experienced a software restart when the CLI command `traceroute6 -w IP_addr | host_name` was issued. (B#184243, SR-2-526788032)
- ❑ The ProxySG appliance returned SYN-ACK packets through the wrong VLAN interface when the incoming SYN packet had a non-zero VLAN priority. (B#186235, SR-2-556792732)
- ❑ The ProxySG appliance experienced a software restart at 0x30000 in process `tcpip` in `Kernel.dll` during RIP operations. (B#173268, SR-2-436416797)

### URL Filtering

- ❑ Fixed an issue in which an object in URL Category was not denied due to DRTR. The issue occurred when a WebPulse request was made from the ProxySG appliance with an extracted query which was subsequently determined to be invalid. (B#173268, SR 2-436416797)

Section E: SGOS 5.5.11.1, build 110885

---

## Known Issues in SGOS 5.5.11.1

This section describes known issues in SGOS 5.5.11.1 that might impact your environment. See also the known issues in earlier 5.5.x versions.

### CIFS Proxy

- ❑ When using configuration archives to restore/copy a configuration, the SMB signing configuration will be missing (the commands actually fail). The workaround is to use the correct syntax and re-configure the SMB signing configuration manually after restoring configuration from archive. (B#182879)

### Event Logging

- ❑ The interface link DOWN event is missing from the syslog, but can be seen in the event log, when the SNMP Trap is enabled. (B#183536, SR-2-517558071)

## Section F: SGOS 5.5.10.1, build 92100

---

### Section F: SGOS 5.5.10.1, build 92100

*Release Date: 09/06/2012, build 92100*

*BCAAA Protocol Version: ["Important Notes about SGOS 5.5.x" on page 5](#)*

*Compatible with: SGME 5.5.x, Reporter 8.x and 9.x, ProxyAV 3.x, and ProxyClient 3.1.x, 3.2.x, 3.3.x, and 3.4.x*

### SGOS 5.5.10.1 Contents

See the following sections for information on this release.

- ❑ ["Fixes in SGOS 5.5.10.1" on page 20](#)
- ❑ ["Known Issues in SGOS 5.5.10.1" on page 23](#)

For a list of limitations, see ["Limitations in SGOS 5.5.x" on page 89](#).

### Changes in SGOS 5.5.10.1

SGOS 5.5.10.1 and higher releases contain the updated licensing subsystem referenced in Technical Field Alert 109. This important upgrade includes the new licensing validation certificate and is required for future seamless operation of the ProxySG appliance. (B#176727)

For more information, see:

- ❑ Technical Field Alert  
<https://kb.bluecoat.com/index?page=content&id=TFA109>
- ❑ Knowledge Base Article  
<https://kb.bluecoat.com/index?page=content&id=FAQ2197>

### Fixes in SGOS 5.5.10.1

This section lists issues reported in previous versions that have been resolved in SGOS 5.5.10.1.

#### **Authentication**

- ❑ Fixed a format error in the base64-encoded basic username (X-Authenticated-User) header. This occurred in the NetBIOS-style username (IE: domain\username) within the policy substitution realm. This problem does not happen for NetBIOS-style names from the IWA realm. (B#171171, SR-2-423586401)
- ❑ Fixed an issue in which Windows SSO sometimes stopped the domain controller query when a DC could not be found through the DNS service. (B#177099, SR-2-465952782)

## CIFS Proxy

- ❑ Fixed the software restart in process `Threshold_Monitor` in `kernel_shim.dll`, caused by memory depletion in systems with large CIFS directories. The problem occurred when the CIFS proxy was caching directories with over 16K files. (B#177932, SR-2-475201929, 2-477539060, 2-478735932)
- ❑ Microsoft Word documents could not be saved in CIFS proxy installation. (B#167399, SR-2-400817662, 2-429251582)

## Cache Engine

- ❑ Increased the performance of the 9000-20B. (B#172338)
- ❑ Fixed a software restart in process `Cache Administrator` in `kernel_shim.dll`. Without this fix, it is necessary to reinitialize the drives to get back to a clean state. (B#177209, SR-2-397613262, 2-454421927, 2-482947091)
- ❑ Fixed a restart in `Cache Administrator` in `ce_admin.dll` due to watchdog timer alarm. The problem occurred during a copy of a large file from file server to client. This fix forces the maximum cacheable object size for SG300 to be 10GB. (B#175054, SR-2-454992522)

## CLI Console

- ❑ Fixed a page fault at `0xc3401000` in process `CLI_Worker_2` in `con_agent.dll` when viewing service info in the Management Console. (**Maintenance > Service Info > Send info-> Send service info > view progress**). The problem occurred when there were no transactions to be viewed. (B#150893, SR-2-331898832, 2-456351610, 2-489396388)

## HTTP Proxy

- ❑ Fixed a page fault at `0x4` in process `HTTP_CW_C9199D10` in `libhttp.exe.so`. The fault occurred when creating the host affinity `set_cookie` header for the response. (B#176129, SR-2-467157562)
- ❑ Fixed a problem in which intercepted HTTPS connections failed. The problem occurred when the Detect Protocol feature was disabled and when policy used `http.response (data|apparent_data_type)` conditions. (B#175858, SR-2-465428362, 2-471571442, 2-478448213)
- ❑ Fixed an issue in which the URLs within the HTML conditional comments were not rewritten properly. The problem occurred when attempting to rewrite Internet Explorer conditional comments. (B#170610, SR-2-409713042)
- ❑ Fixed an issue in which SSL did not set the URL for the transaction. The problem occurred under client handshake error during SSL control handoff to HTTP. (B#169520, SR-2-411852002)
- ❑ Fixed a problem in which the ProxySG intermittently returned a `403 Policy denied` exception when a redirect response was interpreted as a policy denied error. (B#164655, SR-2-470467172)

## MAPI Proxy

- ❑ Fixed a page fault at 0x3c in process `EPM Tunnel Acceptor` in `services.dll`. The problem occurred due to unresolved integrity of internal objects. (B#178099, SR-2-482131052)

## Policy

- ❑ Fixed an issue when the ProxySG presented an exception page with category `unavailable`. The problem occurred in transparent deployments, when `Intercept on exception` was triggered for a request, and a custom exception page was to be served. The category variable was not displayed in the exception page to the client. (B#175211, SR-2-450957492)

## SSL Proxy

- ❑ Fixed a memory leak in the SSL proxy when extracting the URL from the certificate. The problem occurred when the OCSP on the ProxySG was configured to fetch the URL from the certificate. There is no workaround except for disabling OCSP. (B#174507, SR-2-450822961)
- ❑ Fixed an issue in which the SSL certificate cache did not remove expired certificates when continually accessed. This issue occurred when the OCS updated its expired certificate to a new, valid one and the ProxySG did not refresh its certificate cache with the new certificate—unless the server was not accessed for a period of 2 hours (internal cache timeout value). Workaround available: Execute the following CLI command: `(config ssl)clear-certificate-cache`. (B#170116, SR-2-409700084, 2-429076173, 2-429395682)

## Storage

- ❑ Fixed a hardware restart in process `ATA_clock` in `ata.dll`. The problem occurred under traffic load and can be reproduced by forcing `restart regular`, `restart upgrade`, `restart upgrade keep-sgos5-config` (B#175016, SR-2-454456212, 2-476107352)

## TCP/IP and General Networking

- ❑ Fixed an issue in which the ProxySG restarted because of a page fault at 0x4 in process `rip` in `rip.dll` under the following conditions:
  - RIP was enabled and there were RIP routes existing in the RIP routing table
  - There was a host route (with netmask 255.255.255.255) configured on the ProxySG and there were many occurrences of TCP retransmission on this host route (due to packet loss, latency, and so on). (B#176020, SR-2-466164384)

## Known Issues in SGOS 5.5.10.1

### Cache Engine

- ❑ Software restart at 0x40021 in process Cache Administrator in kernel\_shim.dll at .text+0xcdc. There is no workaround for the problem. (B#176032, SR-2-466261042, 2-476048532, 2-482667542)
- ❑ RAM usage statistics are incorrectly displayed on the diagnostic page. There is no workaround for this issue. (B#175956, SR-2-463708992)

### CIFS Proxy

- ❑ Shared mode Excel2007 worksheet is corrupted while the client is accessing the file via ADN and local. Workaround: Use policy to disable caching for CIFS or ensure that all access to the Excel file is through the proxy. (B#177034, SR-2-473079682)
- ❑ Certain CIFS applications do not save cached files correctly. There is no workaround for the issue. (B#175312, SR-2-429251582)
- ❑ File copy can abort when copying large amount of data in Windows XP. There is no workaround for the issue. (B#174379, SR-2-449524981)

### HTTP Proxy

- ❑ The ProxySG sends 500 server error when it is transforming HTML pages. The ProxySG no longer treats URLs starting with encoded forward slashes as relative URLs. There is no workaround for this issue. (B#178317, SR-2-493370842)
- ❑ The HTTP proxy responds incorrectly when an invalid URL is in the request. The appliance returns Appliance Error instead of Request Error. There is no workaround for the issue. (B#174711, SR-2-450579168)

### SOCKS Proxy

- ❑ The SOCKS application returns port unreachable (and is therefore unable to connect to a server) when the ProxySG appliance's LAN interface is connected to a private network, the WAN interface is connected to public network, and the default gateway is in the public network. There is no workaround for this problem. (B#170781, SR-2-416900694, 2-454376092)

### SSL/TLS

- ❑ The browser might receive a certificate error for certain SSL websites due to missing certificates. As a workaround, the customer may add the following certificates: Thawte Premium Server CA. (B#175163, SR-2-476980862, 2-477341292, 2-480765572, 2-481269722)

## **TCP/IP and General Networking**

- ❑ The fix for this SGOS 5.5.9.1 issue introduced the CLI command `tcp_keepalive_timeout`. The use of underscores does not conform to CLI style and will be fixed in a future release. The command should be `tcp-keepalive-timeout` instead of `tcp_keepalive_timeout`. There is no workaround for the problem. (B#156690, SR-2-430445092)

## **URL Filtering**

- ❑ The object in URL Category is not being denied due to DRTR. The issue will occur if a WebPulse request is made from the ProxySG with an extracted query that is subsequently determined as invalid. The response for such query is none. There is no workaround for the issue unless the customer upgrades to version 6.x (B#173268, SR-2-436416797)



## Section G: SGOS 5.5.9.1, build 81874

*Release Date: 03/09/2012, build 81874*

*BCAAA Protocol Version: "Important Notes about SGOS 5.5.x" on page 5*

*Compatible with: SGME 5.5.x, Reporter 8.x and 9.x, ProxyAV 3.x, and ProxyClient 3.1.x and 3.2.x*

### SGOS 5.5.9.1 Contents

See the following sections for information on this release.

- ❑ ["Fixes in SGOS 5.5.9.1" on page 25](#)
- ❑ ["Known Issues in SGOS 5.5.9.1" on page 29](#)

For a list of limitations, see ["Limitations in SGOS 5.5.x" on page 89](#).

### Fixes in SGOS 5.5.9.1

This section lists issues reported in previous versions that have been resolved in SGOS 5.5.9.1.

#### Authentication

- ❑ Fixed the issue that caused RADIUS authentication requests to fail on SGOS 5.5.3.4 through SGOS 5.5.8.1. (B#174363, SR 2-432796702)
- ❑ Fixed the issue with the way SGOS/BCAAA handled null sessions that resulted in failed login attempts or an inability to access information. (B#143614, SR 2-306578362) This issue manifested itself in the following ways:
  - On Active Directory under Windows 2008, BCAA would perform a successful user lookup for a null session and provide the ProxySG with the credentials NT AUTHORITY\anonymous logon, and the login attempt would fail.
  - On IWA authentication, if the ProxySG was configured with surrogate credential caching, the user would be denied Internet access for the duration of the caching interval, as the credentials belonging to that user would not match those already cached by the ProxySG.
- ❑ Fixed the issue with policy substitution on LDAP search and RADIUS accounting/session monitor failures that were caused because the proxy-state attribute in RADIUS packets were ignored. (B#172552, SR 2-433277333)
- ❑ Fixed the restart in Process "PDW t=56823484 for=303EFC0" in "authenticator.dll" that was triggered when defining a large authentication policy. (B#172739)

#### Cache Engine

- ❑ Fixed the issue that caused a software restart when a byte-range request for an object was larger than the maximum cache size. (B#174250, SR 2-434672152)

- ❑ Fixed the software restart at 0x20108 in "kernel\_shim.dll" that was caused by disk errors. (B#168944, SR 2-429846092, 2-430599742, 2-430629517, 2-430835712, 2-434889562, 2-441576552)
- ❑ Fixed the issue where the ProxySG stopped accepting connections and forwarding requests when the disks were in regulation. (B#174063, SR 2-444946902)
- ❑ Fixed the issue that placed the system in regulation and occasionally caused connectivity issues when a disk-read error triggered the HTTP worker limit on the appliance. (B# 174674)

### CIFS Proxy

- ❑ Fixed a restart in process "Threshold\_Monitor" in "kernel\_shim.dll" at .text+0xcdc when the ProxySG was under memory regulation. With this fix, when the ProxySG is in memory regulation, directory pre-fetch is automatically disabled to save memory, and automatically re-enabled after regulation is disengaged. (B#171612, SR 2-426760363)

### CLI

- ❑ Fixed the issue with invalid base64 output for the `show adv <url> base64` command. The command now generates valid base64 output. (B#172809)
- ❑ Fixed the memory issue that blocked the display of access log information using the `tail-f` advanced URL command. (B#167820, SR 2-405919012 2-410351092 2-425511482)

### Content Filtering

- ❑ Fixed the failure with incremental updates to the SmartFilter database. This fix resolves the problem that started after 3/20/2012, where each SmartFilter database update resulted in a full database download. (B# 175149, SR 2-457400982)

### Flash Proxy

- ❑ Fixed the restart issue that occasionally occurred when access logging was enabled and the format being logged contained the `s-ip` field. (B#172359)

### Front Panel

- ❑ Fixed the SG510 restart at 0x1 (ck\_not\_reply\_blocked) in "FPAdmin" when using the front panel. (B#173485, SR 2-439562061)

### HTTP Proxy

- ❑ Fixed the issue that caused a failure to prefetch an HTTP pipeline request and HTTP pipeline redirect request. (B#165946, SR 2-397594002)
- ❑ Fixed the issue that caused a system restart at 0x11 (software watchdog expired) in "kernel.ex" due to a race condition accessing an unlocked data structure. (B# 174427, SR 2-420063869)

- ❑ Fixed the issue with the mismatch between the `http persistent-timeout server` setting on the ProxySG and the firewall or upstream device that caused the firewall or upstream device to silently drop idle connections when the session idle timeout was reached on the firewall. (B# 173860, SR 2-432673732)
- ❑ Fixed a restart at 0x40 in Process "HTTP SW B8098EC0 for B80DFEC0" in "ce\_admin.dll" that occurred when ICAP was enabled. (B#174032)
- ❑ When using the `http.response.apparent_data_type condition` if a remote server incorrectly reports the content-encoding scheme on a file, a content-encoding exception would be displayed to the client regardless of whether or not the condition was evaluated. This issue is now fixed, and the exception page only displays if the `http.response.apparent_data_type condition` is evaluated and the ProxySG appliance cannot decode the file. (B#173169)

### MAPI Proxy

- ❑ Fixed the issue where Outlook users experienced performance degradations when sending large attachments with high compression rate or multiple attachment files with Outlook 2010. (B# 171228, SR 2-400546642)

### Policy/VPM

- ❑ The Web Access Layer in the VPM on the ProxySG Management Console, now supports the following server/client certificate conditions and actions that were until now available only in the SSL Access layer:

#### Conditions

- **Add Server Certificate** hostname and subject in the **Destination** column.
- **Add Client Certificate** common name and subject in the **Source** column.

#### Actions

- **Add Server Certificate Validation Object** and its variants

The VPM GUI does not support the `server.certificate.validate(auto)` option that the CPL supports.

- **Add Client Certificate Validate Object** and its variants

This change should reduce the interference between how the SSL-allow policy works with other policy such as the user-notification policy) By providing these actions and conditions in the Web Access Layer, a more intelligent SSL-Allow policy can be crafted. The SSL-Allow policy no longer needs to constantly rewrite the URL, and thereby interfere with any policy in the system. (B#172806, SR 2-355204627)

- ❑ Fixed the issue with high memory usage when evaluating HTTP policy. (B#168955, SR 2-411533902)
- ❑ Fixed the issue on multiprocessor ProxySG models that caused a restart owing to a high volume of SNMP traps generated when evaluating HTTP policy. (B#171298)

- ❑ Fixed the issue that caused corruption of VPM policy when you created a custom object with the same name as a factory static object. For example, creating a URL destination object with the name 'Any'.

This fix prevents you from creating a VPM condition or action with the names "Allow" "Deny" "Deny (Content Filter)" or "Any". If used, an error message now displays to inform you that the object name is already in use. (B#174146, SR 2-445366182)

- ❑ Updated the list of browser versions used when adding a custom user agent in the Web Access Layer. List of supported user agents is:
  - Firefox 4.x, 5.x, 6.x, 7.x
  - IE 8.x, 9.x
  - Opera 10.x, 11.x
  - Chrome 12 and lower, 13.x, 14.x, 15.x
  - Safari 4.x, 5.x
  - Phone, iPad, iPod, Blackberry, Android, Windows Mobile
  - Wget 1.x(B#169989)

### Quicktime Proxy

- ❑ Fixed the issue that caused the ProxySG appliance to relay network credentials to the OCS in an RTSP SETUP request. Because quicktime players send the `Authorization:` header for non-describe requests during an HTTP/RTSP exchange, the proxy returned an HTTP 401 error instead of an HTTP 407 error for proxy authentication. As a result, the login/password of users was sent to the streaming server in an RTSP SETUP request. (B#171863, SR 2-428932622)

### SSL/PKI

- ❑ Fixed the issue where a change in the configuration of your SSL version did not save the corresponding cipher-suite changes to the registry. Cipher-Suite changes are now persistent across an appliance restart. (B#168486, SR 2-408770702)
- ❑ Fixed the OCSP response validation error, where the ProxySG incorrectly returned an error when validating the certificate chain for the OCSP responder. As a work around you had to explicitly import and trust the certificate of the CA that signed the OCSP responder's certificate. The explicit trust is no longer needed if the CA that signed the OCSP responder's certificate is a CA in the certificate chain for the server certificate being validated. (B#172850)

## Storage

- ❑ Fixed the write failure on disk 2 of the SG510, SG300, and SG600 appliances. The disk-write failure occurred when the disks were reset to factory defaults using the `restore-defaults factory-defaults` CLI command; the error was logged in the ProxySG event log. (B#174801, SR 2-453029222)

## TCP/IP and General Networking

- ❑ Fixed the issue with the TCP idle slow-start mechanism, which caused users to experience delays when a connection to an OCS was idle for more than the current retransmit value. This fix replaces RFC 2414 with RFC 3390 which is a standard for TCP to increase the permitted initial window from one or two segments to roughly 4KB. Now data can be sent with a larger initial window, and this change helps reduce delays. (B#171660, SR 2-423898499)
- ❑ Fixed the issue with filters when taking a packet capture. You can now use the `ip host <name>` or `ip host <ip>` filters and successfully record the flow of traffic between the ProxySG and the client machine. (B# 169898, SR 2-415075902)
- ❑ Fixed the ProxySG configuration archive to now include the value of the `tcp-keepalive-timeout`. (B#156690, SR 2-430445092)
- ❑ Fixed the issue with the reboot loop that occurred when you upgrade the ProxySG from 4.x to 5.x. This issue occurred if the 4.x configuration had a hardware bridge with a port whose speed was explicitly set to 1GB. (B#174084, SR 2-443742892)
- ❑ Fixed the issue that caused timeouts on CIFS sessions when bypassed remote clients were accessing Netapp file servers. (B#168055, SR 2-402522403)

## Known Issues in SGOS 5.5.9.1

### Active Sessions

- ❑ When the ProxySG is handling a very large number of sessions, the list of proxied active sessions sometimes does not display in the Management Console and the Management Console may become unresponsive.

**Workaround:** To avoid this issue, set a limit in the **Display the most recent connections** field. (B#136362)

### Authentication

- ❑ The ProxySG redirects some clients to a virtual URL that intermittently causes an authentication loop. (B#171963)

### Health Checks

- ❑ Occasionally the health of a composite health check is affected by a change in the health state of a host that is not a member of the composite group. (B#161309)

## Health Monitoring

- ❑ If you are upgrading from SGOS 4.x and have configured the **alert notification sensor** configuration, the settings are not ported over to SGOS 5.x. (B#163187)

## HTTP Proxy

- ❑ When using Firefox for an SSL connection to a server that presents an untrusted certificate, the access-log field `x-exception-id` is populated with the string 'internal\_error'. (B#169520, SR 2-411852002)
- ❑ The URL transform rule converts the XML Name Space contents to lowercase, and breaks the W3C recommendations on naming convention. (B#149572)
- ❑ When two consecutive requests on the same persistent connection are resolved to different HTTPS servers, the handshake to the second server fails with an error: `SSL Certificate Hostname Mismatch (ssl_domain_invalid)`. (B#167020)
- ❑ The ProxySG appliance intermittently returns an HTTP 403 response with a Policy denied exception when a redirect response is interpreted as a policy denied error. (B#164655)

## Management Console

- ❑ If you use the well known WCCP service group name `web-cache`, the Management Console defaults the **Assignment-type** to **Source-IP**. This results in a configuration compilation error because service flags are not supported for the well known service group `web-cache`. (B#167036)

## MAPI Proxy

- ❑ Endpoint mapper does not restrict interception of MAPI connections by source IP, when two listeners are created where one is set to bypass and the other set to intercept all source IP addresses. (B#154100)

## SNMP

- ❑ When the appliance name is modified, an SNMP GET for host name returns the old name instead of the new name. (B#163728)

## SSL/PKI

- ❑ When going to an invalid domain using SSL, the browser may hang for a while before returning a page not found error. This issue occurs when the OCS doesn't exist or the SSL service is down and the ProxySG appliance is deployed as a transparent proxy. (B#170345, SR 2-409135452)

## Section H: SGOS 5.5.8.1, build 78310

*Release Date: 12/19/2011, build 78310*

*BCAAA Protocol Version: "Important Notes about SGOS 5.5.x" on page 5*

*Compatible with: SGME 5.5.x, Reporter 8.x and 9.x, ProxyAV 3.x, and ProxyClient 3.1.x and 3.2.x*

### SGOS 5.5.8.1 Contents

See the following sections for information on this release.

- ❑ ["Fixes in SGOS 5.5.8.1" on page 31](#)
- ❑ ["Known Issues in SGOS 5.5.8.1" on page 32](#)

### Fixes in SGOS 5.5.8.1

This section lists issues reported in previous versions that have been resolved in SGOS 5.5.8.1.

#### *Cache Engine*

- ❑ Fixed the issue where the hanging refresh bandwidth allocation from the CLI disabled automatic bandwidth management until it was re-enabled or the machine was restarted. (B#165763, SR 2-397022650)
- ❑ Fixed the issue that caused a software restart in process `Cache Administrator` in `ce_admin.dll` at `.text+0x128be`. (B#168544, SR 2-409081022)

#### *HTTP Proxy*

- ❑ Fixed the issue that caused software restart in process `HTTP CW BB9F0EC0` in `transactions.dll` at `.text+0x2a014`. (B#166582, SR 2-399604322)
- ❑ Fixed the issue that caused software restart in process `HTTP Admin` in `http.dll` at `.text+0x5406d` due to improper memory handling. (B#167938, SR 2-406218312)
- ❑ Fixed the issue that caused software restart in process `HTTP CW B904CEC0` in `kernel_shim.dll` at `.text+0xcfc`. (B#169849, SR 2-415601652)

#### *Health Monitor*

- ❑ Fixed the issue where the health monitoring status was not displayed correctly in GUI unless the ProxySG was restarted. (B#169175, SR 2-407967842)

#### *IPV6*

- ❑ Fixed the issue where the IPv6 DNS servers did not appear in the **show configuration** command output. (B#170955, SR 2-421781832)

## *MAPI Proxy*

- ❑ Fixed the issue that caused the ProxySG appliance to restart unexpectedly when `keepalive` was enabled. (B#170975, SR 2-422738332)

## *Real Media Proxy*

- ❑ Fixed issue that caused the ProxySG appliance to restart when the cacheable audio or video was played continuously for more than 4 hours with frequent pause and play combination. (B#170738, SR 2-396256592)

## *TCP/IP and General Networking*

- ❑ Fixed the issue where the RIP table constantly flipped next default routes due to RIP advertisements. (B#164029, SR 2-382685942)
- ❑ Fixed the issue with UDP response traffic sent through incorrect routing path when a static route was expanded. (B#170327, SR 2-410201602)

## *URL Filtering*

- ❑ Fixed the issue where the old URL categorization persisted even after a successful DB purge. (B#168711, SR 2-408098742)

## *Windows Media Proxy*

- ❑ Fixed the issue where the media streams failed to play and caused an unexpected software restart in process `RTSP_WM_Dispatcher` in `kernel_shim.dll`. (B#165751)

## **Known Issues in SGOS 5.5.8.1**

This section describes known issues in SGOS 5.5.8.1 that might impact your environment. See also the known issues in earlier 5.5.x versions.

### *Access Logging*

- ❑ Non UTF8 characters appear in access log. (B#170934, SR 2-409051632)

### *Active Sessions*

- ❑ When the ProxySG is handling a large number of sessions, the list of **Proxied Sessions**, under **Statistics>Sessions>Active Sessions** occasionally does not show up in the Management Console and the MC becomes unresponsive. A workaround for this issue is to set a limit in the **Display the most recent connections** field. (B#136362)

## *HTTP Proxy*

- ❑ ProxySG appliance is not caching the response and not including the "Age" header in the response, subsequent requests are served from the origin content server, not from the appliance's cache. (B#150152)



## MAPI Proxy

- ❑ When two MAPI listeners are created and one of them is set to bypass and the other set to intercept all source IP addresses, in some cases, the ProxySG Endpoint Mapper does not restrict interception of MAPI connections by source IP address. (B#154100)

## OCSP

- ❑ The ProxySG appliance incorrectly returns an error when validating the certificate chain for the OCSP responder.  
Work around: Explicitly import and trust the certificate of the CA that signed the OCSP responder's certificate. The explicit trust is no longer needed if the CA that signed the OCSP responder's certificate is a CA in the certificate chain for the server certificate being validated. (B#158946)

## Services

- ❑ CIFS intercepts may be set incorrectly after upgrading from SGOS 5.4.x to 5.5.x and then restoring to default settings. (B#131303)

## SSL Proxy

- ❑ Software restart process in HTTP SW 619D9F20 for 6197CF20 in shared\_dll.dll at .text+0x4cd4 (Fast\_hybrid\_heap::malloc). (B#169272, SR 2-413207371, 2-414368812)

## TCP/IP and General Networking

- ❑ ProxySG causes timeouts on CIFS sessions when bypassed remote clients are accessing Netapp file servers. (B#168055, SR 2-402522403)

## User Documentation

- ❑ The **webpulse.notify.malware (yes | no)** policy setting for the malware notification feature needs to be updated in the CPL Reference Guide. (B#140633 )
- ❑ The SSL Proxy guide needs to be updated with information about forcing a redirect when encountering a bad OCS certificate. (B#160172)

## Section I: SGOS 5.5.7.1 , build 77648

*Release Date: 06/16/2011, build 77648*

*BCAAA Protocol Version: "Important Notes about SGOS 5.5.x" on page 5*

*Compatible with: SGME 5.5.x, Reporter 8.x and 9.x, ProxyAV 3.x, and ProxyClient 3.1.x and 3.2.x*

### SGOS 5.5.7.1 Contents

See the following sections for information on this release.

- ❑ ["Changes in SGOS 5.5.71" on page 34](#)
- ❑ ["Fixes in SGOS 5.5.7.1" on page 34](#)
- ❑ ["Known Issues in SGOS 5.5.7.1" on page 38](#)

### Changes in SGOS 5.5.71

This section describes important changes in SGOS 5.5.7.1.

- ❑ Added support for the Seagate 500GB HDD SST500NM0001 for the ProxySG 9000-5/10/20 and ProxySG 900-10 appliances.
- ❑ Added support for 1TB HDD Seagate ST100NM0001 and Toshiba MK1001TRKB drives for the ProxySG 900-10B/20/30/45 and ProxySG 9000-20B appliances. Please note that running a system with 1TB drives on an SGOS 5.5 release *prior* to SGOS 5.5.6.5 will cause the system to restart.

### Fixes in SGOS 5.5.7.1

This section lists issues reported in previous versions that have been resolved in SGOS 5.5.7.1.

#### *ADN*

- ❑ Fixed the issue where an incoming ADN session does not contain client IP addresses in the active sessions incoming ADN sessions tab on core Proxy SG appliance, which is running SGOS 5.5.5.1. (B#159229, SR 2-369667028)
- ❑ Fixed the issue where the ADN peers were not appearing in the GUI on edge proxy. (B#164281, SR 2-387414632)

#### *Authentication*

- ❑ Fixed issue where the WinSSO DC query failed on Windows 2008 machines due to disabled Computer Browser service. (SR 2-373961092, 2-375230242, 2-384513265, 2-385140130)
- ❑ Fixed the issue where the ProxySG appliance does not detect addition of a new group to an LDAP realm until a reboot or manual forced realm refresh. (B# 160468, SR 2-376143201)

- ❑ Fixed the issue where an LDAP authorization with nested group fails when invalid group DN is present in the policy. (B#161112, SR 2-373446205, 2-378025464)
- ❑ Fixed the issue where session monitor occasionally failed after the ProxySG appliance was restarted. (B#162856, 2-378435962, 2-398157211)

## *Cache Engine*

- ❑ Fixed the issue where the hanging refresh bandwidth allocation from the CLI disabled automatic bandwidth management until it was re-enabled or the machine was restarted. (B#165763, SR 2-397022650)

## *CIFS Proxy*

- ❑ Fixed the issue where the Synology NAS devices could not be connected through the ProxySG appliance using the hostname of the NAS. However, using the IP address for connecting to the Synology NAS devices works as expected. (B#157411, SR 2-335186972)
- ❑ Fixed the issue where the Proxy SG appliance restarts if the server closes the connection at a particular stage in the setup of a signed connection. (B#164459, SR 2-390668771)

## *CLI Console*

- ❑ Fixed the issue with the on-screen display of the enable password when the tab and backspace keys were used after entering the password. (B#161520, SR 2-378934782)
- ❑ Fixed the issue where upgrading from 5.4 to 5.5 adds command that cannot be deleted in Mach5 edition. (B#161449, SR 2-373467092)

## *IPV6*

- ❑ Fixed the issue where the ProxySG appliance restarts on traceroute6 for non-reachable host names. (B#161610, SR 2-379595212)

## *ICAP*

- ❑ Fixed the issue where the ICAP statistics was not removed from GUI and SYSINFO when trend statistics cleared or ICAP service was deleted. (B#160442, SR 2-375847292)

## *Kernel*

- ❑ Fixed the issue where the ProxySG appliance restarted in the restart mode set to Hardware, an old RTC record was used to update the RTC. The system time was turned off on the next boot. (B#161233)

## *MAPI Proxy*

- ❑ Fixed the issue where the active MAPI connections were not being decremented on the branch in the case of BDC failure. Statistic counter is available in sysinfo mapi:client-volume or Management Console Statistics/Protocol details/MAPI History. (B#162286, SR 2-377985667)
- ❑ Fixed the issue where the server client throttling was not supported during attachment download optimization. You may experience Outlook reconnects or software restart of the ProxySG appliance. (B#169049, SR 2-412371442)
- ❑ Fixed the issue with Microsoft Outlook cache mode data does not synch with Microsoft Exchange. The issue occurs when the Exchange server rejects a client request during attachment upload protocol optimization, due to overload. (B#167473, SR 2-400546642)

## *Object store*

- ❑ When the system is under high load a watchdog may occur while scanning for objects to delete. (B#169774, SR 2-415295402)

## *Persistent Configuration Infrastructure*

- ❑ Fixed the issue where the ProxySG appliance becomes unresponsive due to a registry deadlock while reading the internal configuration. (B#164937, SR 2-392653219, 2-393955131)

## *Policy*

- ❑ Fixed the Policy evaluation issue for CPL with http.response.code statements that were sometimes wrongly matched with the ProxySG's response to the client rather than with the OCS's response code. (B#162024, SR 2-365914932)

## *SGRP*

- ❑ Fixed the issue where the boundary condition check was missing while accepting SGRP Secret. Maximum supported length of secret is 32 characters. A longer secret was causing corruption in SGRP data. The fix ensures that characters beyond 32 are discarded. (B#163112, SR 2-384566972)

## *Sky UI*

- ❑ Fixed the issue where the Sky UI incorrectly reported zero ADN peers in an active ADN session. (B#155937, SR 2-385498662)

## *SNMP*

- ❑ Fixed the issue where the OIDs for the IP address table of IP-MIB having ipv6 address-related parts were presented incorrectly. (B#164632, SR 2-384488382)
- ❑ Private MIB files are not compliant with the RFC. (B#165663, SR 2-370327962)

## SSL Proxy

- ❑ Fixed the issue where event logs contained Failed to get the peer certificate errors. (B#159481, SR 2-359961302)
- ❑ Fixed the issue with creating a ccl whose name was exactly same as an existing ccl, but differed only in case where either of the ccl could not be deleted unless both the ccls were empty. (B#168986, SR 2-410593782)
- ❑ Fixed the issue where the watchdog timer expires while generating 2K keys. (B#165965)
- ❑ Fixed the issue where Proxy crashed while terminating an upload attachment optimization. This occurred due to useless connections where Proxy does not have an identified user. (B#166398, SR 2-403209993)

## Storage

- ❑ Fixed the issue where the ProxySG appliance becomes unresponsive due to timeout of disk I/O requests when bus/host resets are failing. (B#161564, SR 2-379237352)

## TCP/IP and General Networking

- ❑ Fixed the issue where software restart was caused in process libnet\_admin in util.dll at .text+0x1020.
- ❑ Fixed the issue with double entries creation in CCM table for a single connection. The connection had to be consistently cleared off after the traffic stopped. (B#157331, SR 2-388345420)
- ❑ Fixed the issue where the ProxySG appliance reported Bridge\_Looped detected and one of the bridge interfaces was on mute causing network outage. (B#158053, SR 2-364197992)
- ❑ Fixed the issue where the ADN transparent tunnel load balancing broke after rebooting the ProxySG appliance in the cluster. (B#159056, SR 2-367481083)
- ❑ Fixed the issue where software restart was caused in process tcpip in tcpip.dll at .text+0x168dde (ip\_output). (B#162420, SR 2-383420741, 2-404879152)
- ❑ Fixed the issue where an interface base host route used by WCCP for an offnet home router IP can be permanently marked as down if ARP resolution for that IP is not successful after several attempts. (B#164040, SR 2-389073511)
- ❑ Fixed the issue where the ProxySG appliance sends TCP retransmissions for non-acknowledged packets even after it has finished the connection. (B#163063, SR 2-378717772)
- ❑ Fixed the issue with the WCCP settings lost after reboot when config file size gets larger. (B#164377, SR 2-387650773)
- ❑ Fixed the issue where SNMP does not work if response passes through bridge ports, due to the dynamic rules created while bypassing the redirect packet. (B#165815, SR 2-392801292, 2-403139501)

- ❑ Fixed the issue where software restart was caused in process `tcipip_admin` in at `.text+0x0` due to fragmented syn packet with the TCP option (or part of) on the second fragment. (B#168119, SR 2-406125179)
- ❑ Fixed the issue where SNMP did not work if the response passed through bridge ports, due to the dynamic rules created while bypassing the redirect packet. (B# 165815, SR 2-392801292, 2-403139501)

### *Timezones and NTP*

- ❑ Fixed the issue with updated timezones to reflect Egypt no longer observing daylight savings. (B#163310)

### *URL Filtering*

- ❑ Fixed the issue where the memory fragmentation causes the ProxySG appliance to become unstable during Smartfilter update. (B#161324)
- ❑ Added an advanced url to dump the license information from content filtering, content filter, and license. This prints out the websense user limits from the registry, as well as the list of IP addresses that are being counted for the day. It also contains the last reset time, and the expiry times for all the databases, including drtr. (B#161478)
- ❑ Fixed the issue with Smartfilter not matching domains with `.xxx dot Triplex` domains. (B#167629, SR 2-404309765)
- ❑ The build and look-up functionality have been updated in the RTU database. (B#165084, SR 2-415864814)

### *User Documentation*

- ❑ The Proxy SSL guide demonstrated a method to allow a user to decide whether to proceed to the origin content server when the server has a bad certificate. The example policy did not take into account that other policy, which evaluates response data, can override the redirect action. (B#159591, SR 2-355204627, 2-391479385)
- ❑ The user manual was updated with information on password imports from archive. (B#159868, SR 2-367838972)

### *Windows Media Proxy*

- ❑ Fixed the Memory Regulation issue that occurred due to high number of TCP Connections established via loopback address. (B#161113, SR 2-376143201)
- ❑ Fixed the issue with media streams failing to play via Microsoft Silverlight plug-in. (B#165665)

## **Known Issues in SGOS 5.5.7.1**

This section describes known issues in SGOS 5.5.7.1 that might impact your environment. See also the known issues in earlier 5.5.x versions.

## Access Logging

ProxySG appliance restarts in Process "ALOGAdmin:main" in "kernel.dll" at .text+0xbcf6 due to attempt to pass stale socket by ALOGAdmin. This happens when the Access Log is being populated with the Proxy's IP address from a connection that no longer exists. (B#160458, SR 2-376057088)

## Active Sessions

- ❑ When the ProxySG is handling a large number of sessions, the list of **Proxied Sessions**, under **Statistics>Sessions>Active Sessions** occasionally does not show up in the Management Console and the MC becomes unresponsive. A workaround for this issue is to set a limit in the **Display the most recent connections** field. (B# 136362)

## Health Monitoring

- ❑ GUI does not display the correct health monitoring status until the ProxySG appliance is restarted. (B#169175, SR 2-407967842)

## HTTP Proxy

- ❑ ProxySG appliance is not caching the response and not including the "Age" header in the response, subsequent requests are served from the OCS (Origin Content Server), not from the appliance's cache. (B#150152)
- ❑ Software restart in process HTTP Admin in http.dll at .text+0x5406d due to improper memory handling. (B#167938, SR 2-406218312)

## MAPI Proxy

- ❑ When two MAPI listeners are created and one of them is set to bypass and the other set to intercept all source IP addresses, in some cases, the ProxySG Endpoint Mapper does not restrict interception of MAPI connections by source IP address. (B#154100)

## OCSP

- ❑ Fixed the OCSP response validation error. The ProxySG appliance incorrectly returned an error when validating the certificate chain for the OCSP responder. The error was that the OCSP responder's certificate could not be validated.  
Work around: Explicitly import and trust the certificate of the CA that signed the OCSP responder's certificate. The explicit trust is no longer needed if the CA that signed the OCSP responder's certificate is a CA in the certificate chain for the server certificate being validated.

## Services

- ❑ CIFS intercepts may be set incorrectly after upgrading from SGOS 5.4.x to 5.5.x and then restoring to default settings. (B#131303)

## SSL

- ❑ The SSL certificate cache does not remove old and/or expired certificates when the server is continually accessed. The old and/or expired certificates are removed when the server is not accessed for a 2-hour interval. (B#170116, SR 2-409700084)

## TCP/IP and General Networking

- ❑ When the ProxySG appliance receives fragmented packets (from a router) and reflect-client IP is set, the SG does not rebuild the fragment prior to forwarding them to the client. This may result in failing to access a site. (B#150796, SR 2-336431112)  
Workaround: Use a forward rule on the edge proxies and disable reflect-client-IP for this domain only.)

## URL Filtering

- ❑ Old URL categorization still persists even after a successful DB purge. (B#168711, SR 2-408098742)



## Section J: SGOS 5.5.6.2, build 71837

*Release Date: 06/30/2011, build 71837*

*BCAAA Protocol Version: "Important Notes about SGOS 5.5.x" on page 5*

*Compatible with: SGME 5.5.x, Reporter 8.x and 9.x, ProxyAV 3.x, and ProxyClient 3.1.x and 3.2.x*

### SGOS 5.5.6.2 Contents

See the following sections for information on this release.

- ["Changes in SGOS 5.5.6.2"](#) on page 41

### Changes in SGOS 5.5.6.2

This section lists important changes in SGOS 5.5.6.2.

#### *Support for the SG 900 Appliance*

- SGOS 5.5.6.2 is the first release to support the new SG900 Series appliances.

---

**Note:** SG900 appliance support is included only in SGOS 5.5.6.2 or later.  
Do not downgrade the SG900 to a SGOS version earlier than SGOS 5.5.6.2.

---

## Section K: SGOS 5.5.6.1, build 70899

*Release Date: 06/16/2011, build 70899*

*BCAAA Protocol Version: "Important Notes about SGOS 5.5.x" on page 5*

*Compatible with: SGME 5.5.x, Reporter 8.x and 9.x, ProxyAV 3.x, and ProxyClient 3.1.x and 3.2.x*

### SGOS 5.5.6.1 Contents

See the following sections for information on this release.

- ❑ "Fixes in SGOS 5.5.6.1" on page 42
- ❑ "Known Issues in SGOS 5.5.6.1" on page 43
- ❑ "Limitations in SGOS 5.5.x" on page 89

### Fixes in SGOS 5.5.6.1

This section lists issues reported in previous versions that have been resolved in SGOS 5.5.6.1.

#### *ADN*

- ❑ Fixed issue where the ProxySG Appliance caused the ProjectWise application to fail with a decompression error, while streaming through a policy that does compression and byte caching. (B# 152542, SR 2-346175542)

#### *Authentication*

- ❑ The ProxySG appliance with Netegrity's SiteMinder Agent will now check to see if a form login URL contains a query string. If it does, it will append the "&" character to it's query string, instead of the wrong character "?". (B#158968, SR 2-366018232)
- ❑ Fixed issue where a cross-forest trust exists between two forests, a SSO/LDAP authorization failed because BCAA failed to get a proper DN for the user from the domain in the other trusted forest. (B#157958, SR 2-359738262)

#### *CIFS Proxy*

- ❑ Fixed issue where the ProxySG appliance stopped accepting connections due to improper memory handling in the CIFS component. (B# 151850, SR 2-336393882)
- ❑ Resolved issue where a picture file, on the network, intermittently got deleted when a user rotated it using Windows Picture and Fax Viewer, when using a MACH5 edition. (B#151078, SR 2-335186972)

## HTTP Proxy

- ❑ Fixed issue where incorrect VLAN tags set by the ProxySG appliance caused packet drops in the firewall.  
This happened in a transparent mode, with the setting of **trust destination IP** set to **disabled**. The Retrieval Worker (RW) was sending the SYN packets to the wrong VLAN.  
(B#153542, SR 2-348239943)

## IPv6

- ❑ Resolved issue where the ProxySG appliance caused a connection failure in a transparent DNS Proxy setup on IPv6 over TCP. (B#158487, SR 2-367287322)

## TCP/IP and General Networking

- ❑ Enabled a configurable CLI option to disable SWS (Silly Window Syndrome) avoidance.  

```
# silly-window-syndrome avoidance "enable"(default)
# silly-window-syndrome avoidance "disable".
```

Note: Using the above command with the "enable" and "disable" options should be used with caution. It may lead to additional network congestion, depending on your network deployment. (B#131063, SR 2-366993774)

## Known Issues in SGOS 5.5.6.1

This section describes known issues in SGOS 5.5.6.1 that might impact your environment. See also the known issues in earlier 5.5.x versions.

### Access Logging

- ❑ ProxySG appliance restarts in Process "ALOGAdmin:main" in "kernel.dll" at .text+0xbcf6 due to attempt to pass stale socket by ALOGAdmin. This happens when the Access Log is being populated with the Proxy's IP address from a connection that no longer exists. (B#160458, SR 2-376057088)

### Active Sessions

- ❑ When the ProxySG is handling a large number of sessions, the list of **Proxied Sessions**, under **Statistics>Sessions>Active Sessions** occasionally does not show up in the Management Console and the MC becomes unresponsive.  
A workaround for this issue is to set a limit in the **Display the most recent connections** field. (B# 136362)

### ADN

- ❑ Client's IP address is not displaying in incoming ADN sessions, in the Management Console (under **Statistics>Sessions>Active Sessions**, in the **ADN Inbound Connections** tab). (B#159229, SR 2-369667028)

- ❑ ProxySG appliance restarts due to Page Fault in `bdc.factory.nbwpl` in `"bdc.dll"` at `.text+0xa48d` (B# 160317, SR 2-373446515)

## *HTTP Proxy*

- ❑ ProxySG appliance is not caching the response and not including the "Age" header in the response, subsequent requests are served from the OCS (Origin Content Server), not from the appliance's cache. (B#150152)

## *MAPI Proxy*

- ❑ When two MAPI listeners are created and one of them is set to bypass and the other set to intercept all source IP addresses, in some cases, the ProxySG Endpoint Mapper does not restrict interception of MAPI connections by source IP address. (B#154100)

## *Services*

- ❑ CIFS intercepts may be set incorrectly after upgrading from SGOS 5.4.x to 5.5.x and then restoring to default settings. For example, one of the ports on the CIFS service may be set to intercept and the other to bypass. The workaround is to manually edit the intercept/bypass settings for the CIFS service. (B#131303)

## *TCP/IP and General Networking*

- ❑ When the ProxySG appliance receives fragmented packets (from a router) and Reflect-Client IP is enabled, the appliance is not rebuilding the fragmented packets prior to forwarding them to the client. The outcome of this scenario is failure to access the requested site.  
The current workaround is to use a forward rule on the edge Proxies and disable Reflect-Client IP for this domain only. (B#150796, SR 2-336431112)
- ❑ HTTP pipelining does not work as intended when Reflect-Client IP is enabled. This issue is seen in a multiple gateway deployment.  
The current workaround is to disable HTTP pipelining. (B#152099, SR 2-284636164)

## Section L: SGOS 5.5.5.1, build 63141

*Release Date: 04/21/2011, build 63141*

*BCAAA Protocol Version: "Important Notes about SGOS 5.5.x" on page 5*

*Compatible with: SGME 5.5.x, Reporter 8.x and 9.x, ProxyAV 3.x, and ProxyClient 3.1.x and 3.2.x*

### SGOS 5.5.5.1 Contents

See the following sections for information on this release.

- ❑ "Fixed Security Advisory Issues in SGOS 5.5.5.1" on page 45
- ❑ "Fixes in SGOS 5.5.5.1" on page 45
- ❑ "Known Issues in SGOS 5.5.5.1" on page 49
- ❑ "SGOS 5.5.4 Documentation Errata" on page 61
- ❑ "Limitations in SGOS 5.5.x" on page 89
- ❑ "SGOS 5.5.x — Support Files and Support for Other Products" on page 92

### Fixed Security Advisory Issues in SGOS 5.5.5.1

This section lists fixes provided in SGOS 5.5.5.1. that addresses specific security threats.

- ❑ BCAA Stack overflow vulnerability fixed (B# 157410). See Security Advisory SA55 (<https://kb.bluecoat.com/index?page=content&id=SA55>)

### Fixes in SGOS 5.5.5.1

This section lists issues reported in previous versions that have been resolved in SGOS 5.5.5.1.

#### Access Logging

- ❑ Fixed issue where active FTP uploads of access logs caused the ProxySG appliance to stop responding. This fix enables subsequent access log uploads to go through successfully. (B# 151034, SR 2-331734772)

#### ADN

- ❑ Fixed issue seen in the Concentrator, where software restart in Process "bdc.contrl.cw.028D2E04.2F90E000" in "bdc.dll" at .text+0x18da04, when a branch joined in the first time and started to run traffic. (B# 155764, SR 2-354753160)

#### Authentication

- ❑ Fixed software restart in "transactions.dll" at .text+0x79a5f whilst running an authentication function "Construct\_LDAP\_attribute\_cache". (B# 153153, SR 2-348277782)

- ❑ LDAP search failed to compare and match the group policy locally (on the ProxySG appliance) when an AD user group contained more than 1500 users. (B# 155272, SR 2-349293832)
- ❑ Fixed an issue with the list of 'Display by User' in ProxySG's Management Console, where users could not be logged out based only on the IP address provided, without having their user name included as well. (B# 155631, SR 2-355213592)
- ❑ Changed the BCAA installer to disable the sync port by default (changed value "EnableSyncServer=0" in sso.ini). This does not change pre-existing settings. (B#157410)

## Cache Engine

- ❑ Fixed an issue where the ProxySG appliance's software restarted in `Process "Cache Administrator" in "Kernel.dll"`, due to an out of memory condition caused by an incorrect calculation of reclaimable memory statistic. (B# 155835, SR 2-354467352, 2-360302662)

## Management Console

- ❑ Fixed issue where ProxySG appliance restarted frequently due to a memory leak caused by the Client Manager component. (under **Configuration > ProxyClient**). (B# 146057, SR 2-318895821)

## FTP Proxy

- ❑ Fixed issue where the ProxySG appliance returned FTP message "421 Service not available, closing control connection" when using active FTP uploads (STOR) in conjunction with ICAP service with REQMOD (Request Modification) configuration. (B#157090, SR 2-359357872)

## HTTP Proxy

- ❑ Fixed issue where the access log showed denied client access requests change from: `TCP_DENIED` to `TCP_ERR_MISS`, when the policy checks the response headers. (B# 149642, SR 2-329642017)
- ❑ Fixed issue where YouTube videos could not be downloaded to an iPhone going through the ProxySG appliance. (B# 149143, SR 2-329987064, 2-332219754)
- ❑ Fixed HTTP POST request header issue, where the HTTP proxy couldn't recognize `"\r\n\r\n" (0d0a0d0a)` as continuous data belonging to the last chunking packet. (B# 152608, SR 2-334000342)
- ❑ Fixed issue where in some cases, a HTTP POST/PUT request may have caused the ProxySG appliance to restart when the feature **"Tunnel on error"** is enabled, in the Management Console. (B# 155172, SR 2-349855122)

- ❑ Fixed the issue where ProxySG appliance would restart in Process "ALOGAdmin:http" in "transactions.dll" at .text+0x29fb4. (B# 153407, SR 2-293666912, 2-335214182)

## IM Proxy

- ❑ Fixed software restart in Process "AOL IM Worker 17CFF7D4" in "Kernel.dll" at .text+0xe786. The fix prevents an infinite loop caused by large IM data which got stored in a non-refreshable temporary object. (B# 151723, SR 2-342544331)
- ❑ Fixed issue where login to Windows Live Messenger failed occasionally when attempting to do so through the ProxySG appliance. (B#151063, SR 2-337467972)

## IPv6

- ❑ Fixed issue where ProxySG appliance failed to forward connections to a Load Balancing service, where the IPv6 targets belonging to an IPv6 forwarding group used the "Least-Connection" method. (B# 153738)

## MAPI Proxy

- ❑ Fixed the Endpoint Mapper issue where it did not restrict an interception to the configured source IP address. Endpoint Mapper connections are now intercepted/bypassed according to the defined EPMapper policy. (B# 142066, SR 2-299794688, 2-346080511)

## Real Media Proxy

- ❑ Fixed issue where the proxySG appliance restarts in Process "HTTP CW C47F5EC0" in "tcpip.dll" at .text+0x169309, where HTTP Handoff is enabled for Windows Streaming, in a transparent proxy deployment. (B# 153903, SR 2-352443012, 2-352571262, 2-353028901, 2-353165432, 2-353994865, 2-354471842, 2-356011042, 2-356051662, 2-356113951, 2-356294901, 2-357561132)

## Services

- ❑ Fixed upgrade issue where after upgrading to SGOS 5.5.3.7, the Management Console and SSH become inaccessible. (B# 152339, SR 2-342582066)

## Sky UI

- ❑ Fixed issue with Time Service where changing the time scale for **Last 10 minutes** under the Monitor tab resulted in incorrect times.(B# 142576, SR 2-340300092)

## SNMP

- ❑ Added missing MIB definitions for ProxySG 300, ProxySG 9000, ProxyAV 1200 and ProxyAV 1400 models. (B# 157087, SR 2-362145655)

## TCP/IP and General Networking

- ❑ The ProxySG appliance restarted in Process "pcap\_admin" in "packet\_capture.dll" at .text+0xe68. (B# 151475, SR 2-340750672)
- ❑ Fixed an issue where ProxySG appliance restarted in Process "tcpip" in "tcpip.dll" at .text+0x15554e, caused by a TCP RST (reset) being sent using a buffer with a destination interface not yet set. (B# 152508, SR 2-318803769)
- ❑ The ProxySG appliance detected a loop status and muted the interface during a GLBP fail-over (occurred when the router moved the Virtual MAC to the fail-over interface). (B# 152773, SR 2-342497122)
- ❑ The ProxySG appliance restarted in Process "tcpip" in "tcpip.dll" at .text+0x13a448, (caused when a bridged adapter configured in an ifnet structure of a VLAN interface was used). (B# 154573, SR 2-352867831)
- ❑ WCCP traffic is no longer dropped when a router is set to a loopback IP. (B# 151649, SR 334297292)
- ❑ ADN forwarding implementation—Enabling inbound RTS (Return to Sender) option caused unexpected behavior in ADN forwarding implementation. Packets were returned back to the forwarding ProxySG appliance. (B# 155943, SR 2-357422511)
- ❑ When a cable between the primary router and the Pass-Through card (2:2 interface) is disconnected, it creates a fail-over that is propagated to the Pass-Through card 2:1 interface. In this scenario the ProxySG appliance will not be reachable when attempting to use either the IP addresses configured on the bridge Pass-Through nor the IP defined on the Pass-Through interface 2:2. (B#155701, SR 2-355857723)
- ❑ The ProxySG appliance restarted in Process "tcpip" in "Kernel.dll" at .text+0xe786. (B# 156138, SR 2-357837851)
- ❑ Configuring a delay in the ProxySG appliance's Health Check procedure fixed an issue where ProxySG appliance restarted in Process "tcpip" in "tcpip.dll" at .text+0x134ca6, after upgrade to SGOS 5.5.4.4. (B# 157148, SR 2-362231112)
- ❑ The ProxySG appliance generated high CPU utilization following improper memory handling. (B#157516, SR 2-360458012, 2-362316796)

## VPM

- ❑ Using the VPM Browser failed to view users (through LDAP) where the OU's object names are double-byte names. (B# 155130, SR 2-354718532, 2-362278432)



## Windows Media Proxy

- ❑ The ProxySG appliance restarted in Process "RTSP\_WM\_Dispatcher" in "kernel\_shim.dll" at .text+0xcfc, caused by a client POST request received on the same connection as GET, or a GET request received on the same connection as POST. (B# 146888, SR 2-326914242)
- ❑ The ProxySG appliance restarted at HWE:0x0 SWE:0x30000 PFLA:0x0 Process "RTSP\_WM\_Client" in "Kernel.dll" at .text+0xe786. Caused when **log\_message** policy was used; the RTSP Proxy crashed if the stream fails to play. (B# 147185, SR 2-327607262)

## Known Issues in SGOS 5.5.5.1

This section describes known issues in SGOS 5.5.5.1 that might impact your environment. See also the known issues in earlier 5.5.x versions.

### Active Sessions

- ❑ When the ProxySG is handling a large number of sessions, the list of proxied active sessions sometimes does not display in the Management Console and the MC becomes unresponsive.  
A workaround for this situation is to set a limit in the **Display the most recent connections** field. (B# 136362)

### ADN

- ❑ FTP uploads using FileZilla FTP client, via the ADN tunnel fails when on a Gigabit Ethernet LAN. (B# 141384, SR 2-303033170)

### Authentication

- ❑ Defining eight or more nested group levels causes a ProxySG restart. (B#158515)

### CIFS Proxy

- ❑ Picture files intermittently get deleted when being rotated using Windows Picture and Fax Viewer on the MACH5 Edition of SGOS 5.5.3.3. (B#151078, SR 2-335186972)

### HTTP Proxy

- ❑ In certain circumstances where the OCS response contains a combination of cache-control and expires headers, the ProxySG will not cache the response; therefore no "Age" header will be included in the response. Subsequent requests for the same content are served from the OCS, not from the cache. (B#150152)
- ❑ Incorrect VLAN tags set by the ProxySG appliance cause packet drops at the firewall. (B# 153542, SR 2-348239943)

- ❑ CLI Console and Management Console do not accept a max-cache-size value larger than 2047MB. This max-cache-size issue is applicable only if you downgrade to an SGOS version earlier than SGOS 5.4.3.7.  
For example, if you downgrade from SGOS 5.5.3.1 to SGOS 5.4.2.1, the max-cache size value in your configuration will be reset to 2047MB. This reset occurs because versions earlier than SGOS 5.4.3.7, store this value in 32 bits and the maximum supported value is 2047MB (2GB approx.) In SGOS 5.4.3.7 and later, the max-cache-size value is stored in 64-bits and supports a value of up to 8448MB (8.25GB). (B#137864)

## Services

- ❑ CIFS intercepts are set incorrectly while upgrading from SGOS 5.4.x to 5.5.x. (B#131303)

## TCP/IP and General Networking

- ❑ When the ProxySG appliance receives fragmented packets (from a router) and the Reflect Client IP is enabled, the appliance is not rebuilding the fragmented packets prior to forwarding them to the client. This results in the client failing to access a Website.  
The current workaround is to use a forward rule on the edge proxies and disable Reflect Client IP for this domain only. (B# 150796, SR 2-336431112)

## Section M: SGOS 5.5.4.1, build 53805

*Release Date: 01/18/2011, build 53805*

*BCAAA Protocol Version: "Important Notes about SGOS 5.5.x" on page 5*

*Compatible with: SGME 5.5.x, Reporter 8.x and 9.x, ProxyAV 3.x, and ProxyClient 3.1.x and 3.2.x*

### SGOS 5.5.4.1 Contents

See the following sections for information on this release.

- ❑ ["Vulnerability Fixes in SGOS 5.5.4.1" on page 52](#)
- ❑ ["Fixes in SGOS 5.5.4.1" on page 52](#)
- ❑ ["Known Issues in SGOS 5.5.4.1" on page 59](#)
- ❑ ["SGOS 5.5.4 Documentation Errata" on page 61](#)
- ❑ ["Limitations in SGOS 5.5.x" on page 89](#)
- ❑ ["SGOS 5.5.x — Support Files and Support for Other Products" on page 92](#)

### Descriptions of Features Introduced In SGOS 5.5.4.1

This section describes new functionality introduced in the SGOS 5.5.4.1 release.

#### *SNMP Support for Multiple CPU Cores*

The SNMP MIB has been extended to support multiple CPU cores. (B#149833)

#### *Support for SmartFilter Category Map 4*

SGOS 5.5.4 supports the SmartFilter category map, version 4. To use this category map, you can select **Version 4** in the Management Console (**Configuration > Content Filtering > SmartFilter**) or use the following CLI command:

```
(smartfilter)category-map-version 4
```

---

**Note:** If you have configured policy for the categories included in Version 2 or 3, and then switch to Version 4, you must re-evaluate the existing policy. This is because modifications in category names and the categorization of URLs in the database impact the effectiveness of policy.

---

#### *Dictionary Stream Enhancements*

Added enhanced ADN diagnostics and the ability to delete individual dictionary streams. Also, additional statistics are available to help isolate dictionary stream integrity and events. (B#136392)

## Vulnerability Fixes in SGOS 5.5.4.1

This section lists security vulnerabilities that have been addressed in 5.5.4.1.

- ❑ Fixed TLS renegotiation vulnerability (CVE-2009-3555). Refer to security advisory SA44 (<https://kb.bluecoat.com/index?page=content&id=SA44>). (B#140721, SR 2-317157350, 2-317472182, 2-317963726, 2-318132912, 2-318343742, 2-319239832, 2-319767527, 2-321407722, 2-323458972, 2-323570172, 2-324256432, 2-324394837, 2-327520932)

To address this issue, the following CLI command was introduced:

```
#(config ssl)force-secure-renegotiation
```

- ❑ Fixed the privilege escalation vulnerability. See Security Advisory SA45 (<https://kb.bluecoat.com/index?page=content&id=SA45>). (B#148090)
- ❑ Fixed cross-site scripting vulnerability. For details, see Security Advisory SA47 (<https://kb.bluecoat.com/index?page=content&id=SA47>). (B#140797)
- ❑ Script detection improvements in active content transformation. See Security Advisory SA48 (<https://kb.bluecoat.com/index?page=content&id=SA48>). (B#143411)
- ❑ Fixed OpenSSL cipher suite downgrade vulnerability. See Security Advisory SA53 (<https://kb.bluecoat.com/index?page=content&id=SA53>). (B#151152)
- ❑ For security purposes, the SMB signing password no longer appears in the event log. (B#147281, SR 2-328319582)

## Fixes in SGOS 5.5.4.1

This section lists issues reported in previous versions that have been resolved in SGOS 5.5.4.1.

### Access Logging

- ❑ Fixed the inaccurate message that appeared when attempting to set the FTP/HTTP log filename to a value that expanded to greater than 63 characters; previously the error said that it cannot be greater than 256 characters, but the actual limit is 63. (B#145551, SR 2-319031082)

### ADN

- ❑ Fixed software restart at 0x810002 in Process "bdc.tunnel.sw.008005CA" due to a connection not getting unregistered from the control manager during cleanup of tunnel state machine. (B#144716, SR 2-317893922)
- ❑ Fixed issue where large file transfers between two ProxySG appliances stalled or reset while being optimized. (B#146190, SR 2-287851671, 2-318702762, 2-326790156, 2-334863042)
- ❑ To fix an issue with establishing connections through ADN, the ProxySG now always replies to the client's MAC address and not the router's, on all intercepted (inbound) connections. (B#149245, SR 2-314101291)

- ❑ Fixed hardware restart in Process "bdc.rtg.nw-ps.004001D0.44F83A1B0" in "libcfssl.exe.so" while running HTTPS traffic. (B#150486, SR 2-337457382)

## Authentication

- ❑ Fixed the issue in which Novell SSO intermittently logged out users after a period of inactivity. (B#140227, SR 2-294026382)
- ❑ After upgrading to 5.4.3.7, when users authenticated against a domain that had a two-way trust with a user name longer than 15 characters, the following error appeared: "Username could not be converted to Kerberos name." This error displayed even though the IAW realm was set for NTLM and Basic, not Kerberos. This issue has been fixed. (B#141219, SR 2-309774082, 2-312175960, 2-325088773, 2-329942592, 2-333852152)
- ❑ Fixed issue with "origin-cookie" not working as expected for '.co.jp' domain URLs when the cookies were set at the wrong level. (B#145177, SR 2-318457572)
- ❑ Fixed RADIUS server connection issue that occurred because the proxy routing table changed after the initial connection attempt. The RADIUS realm now periodically reinitializes its UDP socket when it doesn't get a response from the server, allowing it to be aware of any route changes. (B#146253, SR 2-324812722)
- ❑ Fixed the cause of benign error messages "Cannot find IP address for host(...)" logged by the BCAA service into the Windows event log. (B#147245, SR 2-325268132)
- ❑ Fixed the authentication issue where LDAP users failed to authenticate when there was more than 64 requests outstanding at one time. (B#147688, SR 2-326330206, 2-331777294)
- ❑ When a BCAA realm was configured using the DNS name of the BCAA server instead of its IP address, and the DNS query failed, the ProxySG did not re-attempt the query until the realm was re-initialized. This fix retries the query after failed attempts to connect to BCAA. (B#148575, SR 2-328712765)

## BCAAA

- ❑ Fixed an issue in which BCAA stopped working with Exception: c0000005 (access violation) and a manual restart was needed. (B#140730, SR 2-298842102)

## Management Console

- ❑ The expiration date of the Management Console's application certificate has been extended, eliminating the Java Applet certificate expiration error message. (B#142531, SR 2-312880212)
- ❑ Fixed the sorting problem with the columns in the Active Sessions and Errored Sessions reports in the MACH 5 edition. (B#143363, SR 2-313914342)

- ❑ Fixed an issue where binary files (such as packet captures) could not be downloaded via Director. (B#146678, SR 2-324918882)
- ❑ Windows that use advanced URLs (such as **Statistics > Authentication > display by user**) now display correct data when the ProxySG Management Console is accessed from Director. (B#147181, SR 2-322766012)

### *CIFS Proxy*

- ❑ Fixed the issue with intermittent, prolonged CPU spikes caused by CIFS connections reading large amounts of server side data. (B#141199)
- ❑ Fixed the connectivity issue that occurred when the CIFS proxy attempted "to read a not present page." (B#142429)
- ❑ Fixed the erroneous sharing violation message that Excel displayed while saving a file on a share, even though no other user had opened the same file. (B#142437)
- ❑ Fixed software restart in Process "CIFS::Worker: Connection 41 (running)" in "ce\_admin.dll" at .text+0x2da6. (B#142895, SR 2-314630501)
- ❑ Reflect client IP via forward policy now works for CIFS. (B#145794)
- ❑ Fixed issue with running data backups through CIFS. Before this fix, when a server performed a data backup through CIFS, the data passed once and then subsequently failed. (B#148994, SR 2-331708801)

### *CLI*

- ❑ The `load forwarding` CLI command is now available on all SGOS editions, not just the Proxy edition. (B#141342, SR 2-302057422)
- ❑ To fix the issue in which advanced URLs were not opening from Director, the `show advanced-url` CLI command now includes support for HTML output. (B#147806, SR 2-322766012)

### *DNS Proxy*

- ❑ Fixed the DNS issue in which large responses were being truncated. Fix is to allow up to 100 records returned for a DNS query on TCP transport and up to 34 records returned for a DNS query on UDP transport. (B#147156, SR 2-326942312)

### *FTP Proxy*

- ❑ Fixed the restart issue that was caused by the access log function being called after the control channel socket was closed. (B#143753, SR 2-316821444, 2-337871482)

## HTTP Proxy

- ❑ Fixed the restart that occurred during trickling (error in process "ALOGAdmin:main" in "http.dll" at .text+0x63853). (B#135157, SR 2-243256052, SR 2-335214182)
- ❑ Fixed an issue in which the patience page failed to display to the user when the browser was Internet Explorer 7 or 8. (B#141623, SR 2-306596972)
- ❑ Fixed the discrepancy between connections shown on the active sessions list and those displayed in the TCP connection table; sometimes active sessions showed a few old client and server connections as active while the TCP connection table did not show these connections. (B#142116, SR 2-323966412)
- ❑ Fixed the issue in which the ProxySG failed to close the persistent connection with the client if the OCS closed the TCP session by RST. (B#142698, SR 2-312875609)
- ❑ Fixed issue with connection to SSL sites that required affinity; this happened after upgrading to 5.5.x from 5.4.x or earlier. The connection to some SSL sites were broken when a DNS server returned two IP addresses, as the ProxySG tried to connect to both IP addresses. (B#143274, SR 2-311071381, 2-313197102, 2-316003452, 2-317564209)
- ❑ Fixed caching issue when non-standard accept-encoding x-gzip is present in an HTTP request. This fix uses gzip to look up the cache if the request has accept-encoding x-gzip. (B#144123, SR 2-318001457)
- ❑ Fixed issue with downloading local content-filter database over FTP when ICAP trickle at start was enabled; this issue occurred after upgrading to 5.5.3.1 from 5.5.1.1. (B#144380, SR 2-313929692, 2-314858480, 2-317859692, 2-318855992, 2-318860762, 2-319764069, 2-325150012)
- ❑ The HTTP proxy now uses the proper flush mode at the end of the compression of the response object so it will generate the CRC and ISize trailers in the gzipped object. (B#145787)
- ❑ Fixed issue with HTTP proxy failing to serve new client request and the client receiving a 500 Internal Server Error. (B#146747, SR 2-326450231)
- ❑ When Websense is used as an offbox content filtering solution, the ProxySG was responding with 400 Bad Request after a request was blocked by Websense. With the implemented fix, the ProxySG will not sent the 400 Bad Request response, but will instead log the message in the debug log. (B#148027)
- ❑ Addressed the issue where an OCS does not send an RFC-compliant "Last-Modified" header in the original response. If the last 304 (Not Modified) response from the OCS does not contain a Last-Modified header, the ProxySG code now compares the If-Modified-Since date against the Last-Modified header value from the original 200 OCS response. (B#146945, SR 2-326971282)

## ICAP

- ❑ A clearer error message now appears when the ICAP service is not available; the previous error text for the ICAP REQmod object may have confused customers into thinking that a transaction currently in process could continue without further ICAP processing. (B#140684)

The new choices in the error message are:

- Deny the client request (recommended)
- Continue without further ICAP processing

## IPv6

- ❑ Fixed an issue in which users were not able to access websites via IPv6 if the local database contained IPv4 addresses. (B#141411, SR 2-307821662)

## MAPI Proxy

- ❑ The Endpoint Mapper now restricts interception to the configured source IP address. (B#142066, SR 2-299794688)
- ❑ Fixed the Outlook hanging issue when user manually downloaded an address book while the Endpoint Mapper was set to bypass. (B#143801, SR 2-317230011)
- ❑ Users at remote site are now able to load Outlook forms when batching is enabled on the MAPI service on the edge ProxySG. (B#146341, SR 2-312687822)
- ❑ Fixed issue in which the MAPI Proxy terminated the connection with Exchange OCS for certain image attachments. (B#151214, SR 2-336192573)

## Policy

- ❑ Clarified the error message that appears when upgrading the malware threat protection archive, and the current installed archive is more recent than the one on the BTO website. The message now informs you that the currently installed archive is up to date, so there is no need to upgrade the archive. (B#147947, SR 2-326311472, 2-328030614)

## ProxyClient

- ❑ The MACH5 Edition now allows ProxyClient locations to be promoted and demoted in the **Configuration > ProxyClient > General > Locations** screen. (B#147955, SR 2-321404582)

## Miscellaneous

- ❑ Fixed an issue with the `restore-default keep-console` command; it will now keep console services that have been modified and restore the other proxy services to their defaults. (B#143587, SR 2-316421812)



- ❑ Fixed the issue with some Advanced URL statistics not displaying in read-only mode after upgrading to SGOS 5.5.3.1. (B#143607, SR 2-316890152, 2-329269996)
- ❑ Fixed the issue in which active sessions could not be terminated because HTTP truncated the object; this happened when the HTTP response did not contain the content length, and the size of the object was greater than 500K. (B#145294, SR 2-317195422)
- ❑ Fixed an upgrade/downgrade issue which made the Management Console and CLI inaccessible. This occurred after upgrading to SGOS 5.5.3.1 from SGOS 5.4.x. (B#147667, SR 2-327104550, 2-341469482)

## SNMP

- ❑ Fixed the SNMP error in the event log: "SNMP error [priority 3]: error on subcontainer 'ipRouteTable container' (...)" that was due to duplicate entries in the IP route table. The fix includes a mechanism for detecting duplicate entries. (B#145849)
- ❑ The Blue Coat MIB has been modified to include a new SNMP trap for disk read/write errors (`io_error`). You must download the modified Blue Coat private MIB file (`BLUECOAT-SG-DISK-MIB`) to take advantage of this new trap. (B#146793)

You can download the MIB from the [ProxSG Download page for SGOS 5.5](#); then click the MIBS link.

## SOCKS

- ❑ SOCKS proxy: When SOCKS packets are allowed by policy only from certain clients and only to certain remote servers, if the destination IP did not match any of the allowed ones, the DENY rule hit and the SOCKS transaction failed. (B#149623, SR 2-333713234)

## SSL/TLS

- ❑ Fixed the issue in which the ProxySG returned an "SSL Certificate Hostname Mismatch (`ssl_domain_invalid`)" exception when SSL intercept and **Server certificate validation** are enabled on the ProxySG. (B#139922, SR 2-298970093, 2-318235032, 2-320398192, 2-324695692)
- ❑ Fixed the software restart at 0x74 in Process "SSLW 942D2990" in "kernel\_shim.dll" due to a specific case of session expiration. (B#142885, SR 2-314045502, 2-317893922)
- ❑ Fixed the issue in which the ProxySG reset the OCS connection, and as a result, users were seeing page cannot display error messages. This was an issue with TLS 1.2; the ProxySG was sending TCP RST to clients instead of a proper FIN close. (B#147809, SR 2-32969069)
- ❑ Fixed software restart in Process "HTTP RW C0287D10" in "cfssl.dll" at .text+0x0. (B#148377)

## TCP/IP and General Networking

- ❑ A new CLI command is available to decrease the amount of time a connection stays in the FIN\_WAIT\_2 state when a misbehaving server does not send a FIN after the connection has been closed. This fix implements a faster timer (60 seconds) to clean up connections in the FIN\_WAIT\_2 state. To enable the fast timer, use the following CLI command:  

```
#(config)tcp-ip tcp-fast-finwait2-recycle enable
```
- ❑ Fixed the connectivity issue on the ProxySG 9000's interfaces 0:0 - 0:3 that occurred because their MAC addresses were reversed. (B#141938, SR 2-298683921, 2-299894406, 2-313952068, 2-335857026)
- ❑ Fixed an issue when using multiple default gateways and static/RIP routing. When an interface goes back up after being down, the ProxySG now correctly switches from the RIP/static route back to the interface route. (B#142638, SR 2-310920842)
- ❑ Improved the handling of deleted RIP routes so that the wrong interface route isn't deleted; for example, the system is now able to correctly delete a route when there are multiple routes with the same gateway but with different netmasks. (B#146013)
- ❑ Shortened the time to build the RIP routing table during bootup. (B#145745, SR 2-322528433)
- ❑ Fixed an issue in which FIN\_WAIT\_2 entries were stuck for ProxyAV ICAP communication. (B#141549)
- ❑ The %i variable in SGOS 5.5.4 now identifies the interfaces in the same order as previous versions (for example, the first interface is 0:0) and as a result, uses the expected IP addresses in SGOS 5.5 log filenames. (B#146019, SR 2-321759052)
- ❑ When an interface goes down, ARP packets are now dropped, instead of queued, preventing a continuous stream of ARP packets to the default gateway when the interface goes back up. (B#146083)
- ❑ To eliminate the "too many home routers" error when a configuration has multiple WCCP groups with multiple home routers, the WCCP global router affinity has been increased from 32 to 256. The number of routers supported per WCCP service group remains at 32. (B#147251, SR 2-32659832)
- ❑ Fixed the connectivity issue with VLAN interfaces after a reboot. This occurred when a non-bridge interface had auto link local disabled and did not have an IP address assigned. (B#147883, SR 2-324236302)
- ❑ Fixed the 503 Service Unavailable message that users received when browsing the Internet. This occurred when the default route failed, due to the default route internal active entry becoming null. (B#148170, SR 2-33121508)
- ❑ Fixed software restart in Process "tcpip" in "tcpip.dll" at .text+0x1380fa. (B#148900, SR 2-333429662)
- ❑ Fixed occasional bridge loop issue that occurred when using multiple bridge groups. (B#149420, SR 2-318192482)

- ❑ Fixed unexpected restart issue in Page fault in Process "tcpip" in "tcpip.dll" in `vlan_start()`. (B#150286, SR 2-337707572)
- ❑ Bandwidth management on the server side now works in a WCCP deployment. (B#150351, 2-322479552)
- ❑ Fixed issue with trust-dest-mac not working when the static-route was down. (B#142911)

## VPM

- ❑ Fixed the issue in which the rewrite url.host action didn't work when applied to MMS, RTSP, and RTMP streaming protocols. The Notify User object created a late condition if the action was a rewrite URL in the web access layer. (B#140536, SR 2-296775212)
- ❑ Modified the writing of Time object settings to consistently specify the time of day in the condition. Since any time constraint that is written and modified in the VPM introduces a time-of-day condition, the UI was updated to show this. The UI was re-organized to visually separate the time of day setting from the date selection options. (B#145660, SR 2-320894792)

## Windows Media Proxy

- ❑ Fixed the issue with Windows Media video-on-demand files failing to play via HTTP when they had SDP length greater than 262,144. (B#144598, SR 2-318325322)

## Known Issues in SGOS 5.5.4.1

This section describes known issues in SGOS 5.5.4.1 that might impact your environment. See also the known issues in earlier 5.5.x versions.

### Access Logging

- ❑ When a backslash is specified in the **Username** field of the Access Log FTP Upload Client, the backslash is stripped after the archived configuration is restored. A workaround to preserve the backslash when restoring the configuration is to escape the backslash with a second backslash (`\\`). (B#151282)

### Active Sessions

- ❑ When the ProxySG is handling a large number of sessions, the list of proxied active sessions sometimes does not display in the Management Console and the MC becomes unresponsive. To avoid this situation, set a limit in the **Display the most recent connections** field. (B# 136362)

## CIFS Proxy

- ❑ Picture files intermittently get deleted when being rotated using Windows Picture and Fax Viewer on the MACH5 Edition of SGOS 5.5.3.3. (B#151078, SR 2-335186972)

## HTTP Proxy

- ❑ In certain circumstances where the OCS response contains a combination of cache-control and expires headers, the ProxySG will not cache the response; therefore no "Age" header will be included in the response. Subsequent requests for the same content are served from the OCS, not from the cache. (B#150152)
- ❑ Denied requests appear in the access log as TCP\_ERR\_MISS instead of TCP\_DENIED, if policy checks response headers. (B#149642, SR 2-329642017)
- ❑ YouTube videos cannot be downloaded on an iPhone going through the ProxySG appliance. (B#149143, SR 2-329987064, 2-332219754)
- ❑ Safe-search policy is no longer effective for Ask.com, due to changes on their website. (B#141180)

## SSL Proxy

- ❑ In certain situations, there may be an issue with users accessing websites that don't support TLS extensions. When using the SSL proxy in explicit mode with detect protocol or in transparent mode, if a website does not support TLS extensions, Internet Explorer presents the message "The page cannot be displayed." The proxy event log contains an error message similar to the following: 2010-07-06 09:50:32-00:00UTC "SSL server internal failure" 0 310000:1 ../ssl\_proxy/sslproxy\_worker.cpp:3003

**Note:** IE6 behavior on Windows 2003 is different since it has different SSL protocol settings.

A workaround to this problem is to disable TLS support in IE8: **Tools > Internet Options > Advanced** and uncheck **Use TLS 1.0**. A workaround on the ProxySG is to disable protocol detection for this site.

- ❑ Resolved issue where memory is leaked if there is no responder certificate in the OCSP Response. (B#158329)

## TCP/IP and General Networking

- ❑ When the ProxySG appliance receives fragmented packets (from a router) and the Reflect Client IP is enabled, the appliance is not rebuilding the fragmented packets prior to forwarding them to the client. This results in the client failing to access a website.  
The current workaround is to use a forward rule on the edge proxies and disable Reflect Client IP for this domain only. (B# 150796, SR 2-336431112)

## SGOS 5.5.4 Documentation Errata

- ❑ The online help refers to an option (**Force HTTPS server certificate validation**) that no longer exists in the Management Console. (The option was removed from the GUI because it is now settable in policy.) However, the PDF version of this documentation is correct. See the Intercepting and Optimizing HTTP Traffic chapter in the *SGOS 5.5.x Administration Guide* PDF at <https://bto.bluecoat.com/doc/12586>. (B#150600)
- ❑ The Hardware Models and Licensed Users table in the online help does not list the ProxySG 300, 600, and 9000 models. For the updated list, see the *SGOS 5.5.x Administration Guide* PDF at <https://bto.bluecoat.com/doc/12586>. (B#137645)

## Section N: SGOS 5.5.3.31, build 51877

*Release Date: 12/13/2010, build 51877*

*BCAAA Protocol Version: "Important Notes about SGOS 5.5.x" on page 5*

*Compatible with: SGME 5.5.x, Reporter 8.x and 9.x, ProxyAV 3.x, and ProxyClient 3.1.x and 3.2.x*

### Descriptions of Features Introduced In SGOS 5.5.3.31

This section describes new functionality introduced in the SGOS 5.5.3.31 release.

#### *Support for the SG300 and SG600 Appliances*

SGOS 5.5.3.31 has added support for the SG300 and SG600 Series appliances.

---

**Note:** SGOS 5.5.3.31 is the minimum supported version for the SG 300 and SG600 appliances. Do not downgrade to a previous version of SGOS.

---

## Section O: SGOS 5.5.3.1, build 46382

*Release Date: 07/02/2010, build 46382*

*BCAAA Protocol Version: "Important Notes about SGOS 5.5.x" on page 5*

*Compatible with: SGME 5.5.x, Reporter 8.x and 9.x, ProxyAV 3.x, and ProxyClient 3.1.x and 3.2.x*

### SGOS 5.5.3.1 Contents

See the following sections for information on this release.

- ❑ ["Fixes in SGOS 5.5.3.1" on page 63](#)
- ❑ ["Known Issues in SGOS 5.5.3.1" on page 66](#)
- ❑ ["Limitations in SGOS 5.5.x" on page 89](#)
- ❑ ["SGOS 5.5.x — Support Files and Support for Other Products" on page 92](#)

### Fixes in SGOS 5.5.3.1

This sections lists issues reported in previous versions that have been resolved in SGOS 5.5.3.1.

#### *Access Logging*

- ❑ Fixed the software restart that occurred while attempting to write to disk when the file was not open (error in process "SSLW C40308D0" in "kernel\_shim.dll" at .text+0xcdc). (B#138738)
- ❑ Fixed the issue that changed the default value of the IM log format (**Configuration > Access logging >Logs**) after reinitializing the appliance. (B# 140799)

#### *Active Sessions*

- ❑ Enhanced some active sessions error messages. For example, the **TCP timeout (server)** error now reads **Server connection timeout occurred while waiting for data.** (B#137610, SR 2-296314999)

#### *ADN*

- ❑ Added enhanced ADN Diagnostics and the ability to delete individual dictionary streams. Also, additional statistics are available to help isolate dictionary stream integrity and events. (B#140246)

#### *Authentication*

- ❑ Fixed an LDAP authentication issue that caused a software restart in process "LDAP Authenticator" in "authenticator.dll" at .text+0x7d7e6 when using LDAP protocol version 3 on Windows Server 2008. (B#140046, SR 2-299086110)

- ❑ Fixed the issue with Novell SSO where users were being intermittently logged out after a period of inactivity. (B#140227, SR 2-294026382)

## Management Console

- ❑ Fixed the link to download PAC files. The links are located at **Statistics > Advanced > Miscellaneous Console URLs**. (B#138265, SR 2-292915560)

## Content Filtering

- ❑ Fixed the high CPU utilization during BCWF auto updates. (B#138361, SR 2-284136563)

## CLI

- ❑ Fixed a privilege escalation vulnerability. For details, see [SA45](#)(B#139110).

## HTTP Proxy

- ❑ Fixed the issue that caused the HTTP proxy to stop working due to truncation/non-cacheable entries in overflow blocks. (B#133169, SR 2-301683692)
- ❑ Fixed the Internal Server Error that prevented access to the Web. This error was caused by malformed HTTP Response Header missing Carriage Return and Line Feed as the End Of Header marker. (B#137211, SR 2-295445531)

## ICAP

- ❑ Fixed the issue where the **Web Access** layer was not blocking the specified file types when trickling was enabled and the ProxySG appliance had a fail-open policy. (B#138215, SR 2-287853252)

## IPv6

- ❑ Fixed the issue whereby the ProxySG appliance awaits the completion of IPv6 DNS lookups before HTTP requests are sent out, even when DNS lookups are configured to **Prefer IPv4 over IPv6** addresses. (B#139106, SR 2-293079052)
- ❑ Fixed the issue whereby the ProxySG waits for IPv6 DNS lookups to complete before HTTP requests are sent out, when DNS lookups are configured to use **Prefer IPv4 over IPv6 addresses**. (B#139106, SR 2-293079052)

## Kernel

- ❑ Fixed the page fault when a lost interrupt caused the system to get stuck on the serial port in process `osconfig` in `"Kernel.dll"` at `.text+0x1934`. (B#138564)



## MAPI Proxy

- ❑ Fixed the page fault (0xe3ea4b40 in Process "EPM Worker" in "util.dll" at .text+0x12c0) when several MAPI, MSRPC threads access the Active Session memory simultaneously. (B# 139523, SR 2-298140409)

## Policy

- ❑ Fixed the issue with numerical IP addresses in policy that caused IPv6 DNS query to occur and negate IPv4 policy in the **Forward Layer**. (B#137483, SR 2-263998772, 2-288582512, 2-293142562, 2-293338872, 2-295363502, 2-297967278, 2-300312561, 2-300765922)
- ❑ Fixed the issue that caused the threat-protection settings to remain after the ProxySG appliance was restored to defaults. This issue disallowed the use of VPM for setting policy. (B#138650, SR2-260292752)
- ❑ Fixed the display to expand all object identifiers in **Statistics > Advanced URLs > Policy**. Before the fix only the first appearance of an object that occurs in several instances was expanded. (B#138863, SR 2-293985932)
- ❑ Fixed the issue in the VPM combined object, where clicking on any whitespace around the **Negate** checkbox selected the option. (B#140111, SR 2-293444585)

## SNMP

- ❑ Fixed the issue that caused event log error messages such as `Error on subcontainer ' ' insert (-1)`. These errors were due to a defect in the third-party net-snmp package. (B#137597, SR 2-292741737)

## System Statistics

- ❑ Fixed the issue that triggered SNMP traps only for CPU 0 when the CPU utilization percentage value exceeded the warning or critical thresholds on multi-processor ProxySG appliances. Now, SNMP traps are sent for each CPU that exceeds the configured CPU utilization threshold. (B#140082, SR 2-295364488)

## TCP/IP and General Networking:

- ❑ Fixed an asymmetric traffic flow issue in the network that restricted Internet access. This issue was caused because a recently added ProxySG appliance was not included in the WCCP mask assignment table. (B#137286)
- ❑ Added the ability to change the value for the two-hour keep alive timeout, the default, maintained on the ProxySG appliance. This change now allows you to adjust the keep-alive timeout value for protocols that use this value for client-side activity. (B#140474, SR 2-299041317)

- ❑ Fix for CVE-2008-4609 Sockstress TCP Attacks reported in Blue Coat security advisory SA41 (B#137210). For more information, see <https://kb.bluecoat.com/index?page=content&id=SA41&actp=LIST>

## Known Issues in SGOS 5.5.3.1

This section describes known issues discovered in SGOS 5.5.3.1. See also the known issues for earlier versions.

### HTTP Proxy

- ❑ The ProxySG appliance closes server-side persistent connections only after a delay when the `http persistent-timeout server` option is enabled. (B#137214)
- ❑ CLI Console and Management Console do not accept a max-cache-size value larger than 2047MB. This max-cache-size issue is applicable only if you downgrade to an SGOS version earlier than SGOS 5.4.3.7. For example, if you downgrade from SGOS 5.5.3.1 to SGOS 5.4.2.1, the max-cache size value in your configuration will be reset to 2047MB.

This reset occurs because versions earlier than SGOS 5.4.3.7, store this value in 32 bits and the maximum supported value is 2047MB (2GB approx.) In SGOS 5.4.3.7 and later, the max-cache-size value is stored in 64-bits and supports a value of up to 8448MB (8.25GB). (B#137864)

### Policy

- ❑ Phrasing of text in the VPM ICAP REQmod object `Continue without further ICAP processing` is inexact. When a loss of connectivity to the ICAP service occurs when an ICAP transaction is currently in process, the transaction cannot continue without further ICAP processing. In such instances the ProxySG appliance does not fail-open. Instead an ICAP errored session is recorded and an exception page is delivered to the client. (B#140684)

### Services

- ❑ CIFS intercepts are set incorrectly while upgrading from SGOS 5.4.x to 5.5.x. (B#131303)
- ❑ HTTP console information is not retained even while using the `keep-console` option in the `restore defaults` command. (B#139403)

### SSL/TLS and PKI

- ❑ The ProxySG appliance reports a certificate error during SSL interception if multiple **Subject Alternative Names** exist and the URL is not included in the first line. (B#139922, SR 2-298970093)

## *TCP/IP and General Networking*

- ❑ WCCP home routers that are deleted from the WCCP configuration continue to be included in WCCP handshakes. (B#139634, SR 2- 295906051)
- ❑ IPv6 DNS queries are triggered even though only DNS look-ups for IPv4 addresses are defined in policy. (B#140670, SR 2-301436116, 2-301635793)

## Section P: SGOS 5.5.2.1, build 45055

*Release Date: 3/24/2010, build 45055*

*BCAAA Protocol Version: "Important Notes about SGOS 5.5.x" on page 5*

*Compatible with: SGME 5.5.x, Reporter 8.x and 9.x, ProxyAV 3.x, and ProxyClient 3.1.x and 3.2.x*

### SGOS 5.5.2.1 Contents

See the following sections for information on this release.

- ❑ ["Descriptions of Features Introduced In SGOS 5.5.2.x"](#)
- ❑ ["Fixes in SGOS 5.5.2.x" on page 70](#)
- ❑ ["Known Issues in SGOS 5.5.2.x" on page 72](#)
- ❑ ["Limitations in SGOS 5.5.x" on page 89](#)
- ❑ ["SGOS 5.5.x — Support Files and Support for Other Products" on page 92](#)

### Descriptions of Features Introduced In SGOS 5.5.2.x

This section describes new functionality introduced in the SGOS 5.5.2.1 release.

#### *Session-Monitor Support Enhancements*

The ProxySG RADIUS feature now supports additional attributes as well as user-defined attributes. To retain full backward compatibility, reconfigure or delete the default attributes as necessary. The attributes stored by the session monitor can be accessed as CPL substitutions, authentication configurations, and as access logging fields.

To access the new commands to create user-defined RADIUS attributes, enter the following submode:

```
sg#(config) security radius attributes
```

To access the new commands to reference the RADIUS attributes to the session-monitor, enter the following submode:

```
sg#(config session-monitor) attributes
```

For complete information on the available commands and attributes, refer to the *Blue Coat ProxySG Command Line Reference*.

The attributes stored by the session monitor are accessed using the following CPL substitution:

```
$(session-monitor.attribute.<attribute name>)
```

---

**Note:** The existing CPL substitution, `$(session.username)` has been deprecated and will be removed in a future release. This substitution will continue to refer to contents of the RADIUS `calling-station-id` attribute. Blue Coat recommends updating the policy to use the new format: `session-monitor.attribute.calling-station-id`.

---

Test the session monitor attributes using the following new CPL condition:

```
session-monitor.attribute.<attribute name>=
```

For access logging purposes, use the following ELFF format:

```
x-session-monitor-attribute(<attribute name>)
```

## Upgrade/Downgrade Notes

See the *SGOS 5.5.x Feature Change Reference*.

## Documentation Reference

For complete information on the new / updated substitution and CPL conditions, see the *Blue Coat SGOS Content Policy Language Guide*.

For information on how to set up the ProxySG as a session-monitor, see the Monitoring chapter in the *Blue Coat SGOS Administration Guide*.

## IPv6 Support in RTSP Proxy

The RTSP proxy supports IPv6 in the following ways:

- ❑ RTSP is capable of making IPv6 upstream connections to the origin content server (OCS).
- ❑ RTSP can accept IPv6 client connections.
- ❑ RTSP can act as a transitional device between IPv4 and IPv6 networks.
- ❑ RTSP can act as a multicast station, retrieving content from an IPv6 OCS and multicast to IPv4 clients.
- ❑ ASX rewrite is IPv6 capable, but only for HTTP connections.

---

**Note:** The MMS proxy does not support IPv6 at this time.

---

## Support for ProxySG VA

SGOS 5.5.2.1 includes support for the ProxySG Virtual Appliance (VA). See the *ProxySG VA Initial Configuration Guide* for more information.

## Enhancements to Blue Coat Sky

Blue Coat Sky version 5.5.2 0310 includes several enhancements. Refer to the *Blue Coat Sky 5.5.x Release Notes* for descriptions of the new features and a list of resolved issues.

## Fixes in SGOS 5.5.2.x

This section lists issues reported in previous versions that have been resolved in SGOS 5.5.2.

### *Management Console*

- ❑ Fixed the issue that caused the Management Console to hang or not fully display when browsers had Phishing filters enabled. (B#110412)
- ❑ You can now enter IPv6 addresses for Common Name when creating self-signed SSL certificates and certificate signing requests. (B#133948, SR 2-263251252)

### *HTTP Proxy*

- ❑ Fixed the issue in which the HTTP proxy was unable to establish Web connections when the ProxySG had high memory utilization. (B#131561, SR 2-261299872, SR 2-278918702, SR 2-221642501, SR 2-237497321, SR 2-239141102, SR 2-239844392, SR 2-253039622, SR 2-260974611)
- ❑ Fixed the issue with Yahoo 10 clients failing to log in over port 80. (B#133708, SR 2-255473611)
- ❑ Host affinity now works for subdomains. (B#127942, SR 2-207212062)
- ❑ Fixed the restart issue during data trickling in Process "ALOGAdmin:main" in "http.dll" at .text+0x63853. (B#130555, SR 2-243256052)

### *MAPI Proxy*

- ❑ Fixed the restart issue that sometimes occurred when a client terminated the downloading of an Outlook attachment. (B#132673, SR 2-251560922, SR 2-262885041)
- ❑ Active Directory 2008 R2 replication is now able to establish connections. (B#135156, SR 2-263863702, SR 2-279327245)
- ❑ Fixed the issue with Outlook 2007 clients having intermittent problems connecting to Exchange 2007 when Outlook is configured to encrypt data. (B#135693, SR 2-278989210)

### *SSL Proxy*

- ❑ Changes to a Certificate Revocation List (CRL) now take effect immediately — the ProxySG no longer requires a restart after a CRL is modified. (B#132208)

### *Health Monitoring*

- ❑ The voltage sensors on the first CPU on the SG8100 are not always accurate, therefore the health monitoring system no longer reports on the first CPU bus voltage for this model. This change prevents the system from sending out SNMP traps or logging events that report a voltage problem that doesn't actually exist. (B#131719)

## SNMP

- ❑ Fixed the issue in which the SNMP values for IP octets were displayed in reverse order (for example, 1.0.0.127 instead of 127.0.0.1) when querying IP addresses. (B#132544, SR 2-248831322)

## VPM

- ❑ A second object with the same name is no longer created when editing a Return Redirect object in the Visual Policy Manager. (B#132559, SR 2-247861522)
- ❑ Sub-categories no longer disappear after installing a VPM-XML policy file. (B#131564, SR 2-231438972)

## TCP/IP

- ❑ Fixed the restart issue in Process "tcpip" in "tcpip.dll" at .text+0x16cf78 (tcp\_timer\_rexmt). (B#131825)
- ❑ The WCCP assignment type no longer gets changed from mask to hash when the Edit button is clicked. (B#134287, SR 2-272828612)

## Access Logging

- ❑ Fixed the issue in which empty (0-byte) access logs were sometimes uploaded to Reporter. (B#133754, SR 2-260188602, 2-261385980, 2-261496642, 2-264176132, 2-264195569, 2-264422431, 2-278233970, 2-279668092, 2-279855732)

## CLI Console

- ❑ Fixed the page fault in Process "CLI\_Worker\_2" in "cli.dll" at .text+0x121471 when attempting to import an SSL keyring greater than 8192 bytes. (B#132329, SR 2-249811824)
- ❑ Fixed the page fault in Process "director@ssh" in "sshd.dll" at .text+0x1388d when multiple SSH clients attempted to connect to the ProxySG at the same time. (B#136036, SR 2-284319582)

## Policy

- ❑ Fixed the issue in which a server\_url.dns\_lookup(IPv4-Only) object in the proxy layer worked only in conjunction with a forward rule. (B#133411, SR 2-255804882, SR 2-263547212, SR 2-281097310)

## Miscellaneous

- ❑ Fixed the software restart in Process "Cache Administrator" in "Kernel.dll" at .text+0x1b67f. (B#133588, SR 2-259329101)
- ❑ The central policy file no longer downloads unless it has been changed. (B#133768, SR 2-255877132)

## Known Issues in SGOS 5.5.2.x

This section lists the recently-found known issues when running SGOS 5.5.2.x. You should also refer to issues found in SGOS 5.5.1.x; see "[Known Issues in SGOS 5.5.1.x](#)" on page 85.

### *Installation/Upgrading/Downgrading*

#### **Installation**

- ❑ When using the Setup Wizard to configure the ProxySG, the initial gateway ping will fail. This is benign and the ProxySG finds the gateway when the unit is operational. (B#129700)

#### **Upgrading**

- ❑ After upgrading to SGOS 5.5.x, the CIFS service sometimes has only one of its ports (445) set to **Intercept**; the other (139) is set to **Bypass**. If this occurs, edit the service to intercept port 139. (B#131303)

#### **Downgrading**

- ❑ To downgrade from SGOS 5.5.2 without losing bin entries, all the slaves must be downgraded first. The master must be downgraded last. (B#136378)

### *Authentication*

- ❑ When LDAP is used for authentication, the access log and exception page truncates the last character of the user name [`$(user.name)`]. (B#136228, SR 2-282419503, 2-283016262, 2-285187382)
- ❑ When a master ProxySG goes back online after a failover, the Backup Information section of the Session Monitor Statistics contains duplicate entries of backups. (B#136559)
- ❑ The `cluster retry-delay` CLI command for the Session Monitor feature accepts a wider range of values than it should; the range should be 0-1440 seconds. In addition, the configured retry delay value is not listed in the output of the Session Monitor's `view` command. (B#136707)
- ❑ When the Session Monitor is configured in a failover replication cluster, there is a small window of time during initialization that may cause the ProxySG to reboot. This situation only occurs when the ProxySG is re-initializing itself as a master or slave in the cluster. (B#136815)

### *Cache Engine*

- ❑ Web traffic through the HTTP proxy may slow down due to truncation and non-cacheable entries in overflow blocks. If this happens, set the value for `max-cache-size` to its default setting (1024 MB) and reinitialize the disks. (B#133587, SR 2-258631824)



## CLI Consoles

- ❑ Administrator login and read/write events are repeating every second in the event log. (B#132112)

## CIFS Proxy

- ❑ Page fault in process "CIFS::Worker: Connection 215 (running)" in "cifs.dll" at .text+0x2d87. The workaround is to configure the CIFS ports to use the TCP Tunnel proxy. (B#133002, SR 2-255782702)

## HTTP Proxy

- ❑ Users might receive intermittent TCP errors when accessing sites in a reverse proxy because the ProxySG is not sending a FIN after receiving a FIN from the origin content server. As a workaround to this issue, disable persistent connections to the server. (B#134205, SR 2-214607225)

## MAPI Proxy

- ❑ The following issues apply to the MAPI proxy when using Outlook with Exchange Server 2010: (B#133955)
  - Outlook 2010 — Active Sessions does not display the MAPI 2010 protocol, and the Keep-Alive feature does not work because Outlook 2010 does not disconnect opened policy handles.
  - Outlook 2007 — No issues to list.
  - Outlook 2003 — ReadStream fetching of attachments does not work properly; the server returns an RPC fault when the Core begins to fetch data with multiple ReadStream requests.
  - Outlook 2000 — Not supported.

## Virtual Appliance (ProxySG VA)

The following are known issues on the ProxySG VA running SGOS 5.5.2.

- ❑ When the ProxySG VA is under heavy load and has high RAM usage, the memory alarm might trigger in vCenter Server. Because the ProxySG VA has its own health monitoring system for memory state, Blue Coat recommends disabling the memory alarm in vCenter. (B#119353)
- ❑ When you attempt to shut down the ProxySG VA in vSphere, an error message displays about VM Tools not being installed. The workaround is to use the following vSphere command to power off the virtual machine:  
**Inventory > Virtual Machine > Power > Power off**
- ❑ Because the virtual appliance does not support CPU monitoring, the `cpu_monitor` snapshot is not applicable to the ProxySG VA. If you enable collection of this snapshot, an error message displays. (B#135642)

- ❑ *Stolen time* is an issue with any virtual machine. Stolen time is the difference between *real time* (as measured on the host server's clock) and *apparent time* (as measured on the ProxySG); small amounts of stolen time are an inevitable occurrence on virtual machines. Stolen time might become excessive when the ProxySG VA is running at 100% CPU utilization, the ESX server is overloaded, and the recommended resources for the ProxySG are not reserved. Refer to the *ProxySG VA Initial Configuration Guide* for more information about stolen time.

## SGOS 5.5.2 Documentation Errata

- ❑ Several updates were performed to the Licensing chapter in the *SGOS 5.5.x Administration Guide* after the Online Help was produced. These changes include updates for the MACH 5 Edition License. To read the updates, access the PDF at <https://bto.bluecoat.com/doc/12586>.
- ❑ In the Online Help module accessible from **Configuration > Access Logging > Formats**, the **Action Field Values** table (four right-arrow clicks) is missing two values:
  - TCP\_ACCELERATED: For CONNECT tunnels that are handed off to the following proxies: HTTP, SSL, Endpoint mapper, and P2P for BitTorrent/EDonkey/Gnutella.
  - TCP\_AUTH\_FORM: Forms-based authentication is being used, and a form challenging the user for credentials is served in place of the requested content.

The Access Logging Format chapter in the *SGOS 5.5.x Administration Guide* contains the updated version (<https://bto.bluecoat.com/doc/12586>).

## Section Q: SGOS 5.5.1.1, build 43412

*Release Date: 11/16/2009, build 43412*

*BCAAA Protocol Version: "Important Notes about SGOS 5.5.x" on page 5*

*Compatible with: SGME 5.4.2.5 and 5.5.x, Reporter 8.x and 9.x, ProxyAV 3.x, and ProxyClient 3.1.x and 3.2.x*

### SGOS 5.5.1.1 Contents

See the following sections for information on this release.

- ❑ ["Descriptions of Features Introduced In SGOS 5.5.1.x"](#)
- ❑ ["Known Issues in SGOS 5.5.1.x" on page 85](#)
- ❑ ["Limitations in SGOS 5.5.x" on page 89](#)
- ❑ ["SGOS 5.5.x — Support Files and Support for Other Products" on page 92](#)

### Descriptions of Features Introduced In SGOS 5.5.1.x

This section describes new functionality introduced in the SGOS 5.5.1.1 release.

#### *IPv6 Support*

SGOS 5.5 supports the use of IPv6 addresses with many of the Blue Coat Secure Web Gateway protocol proxies and features:

HTTP/HTTPS, SSL, DNS, TCP-Tunnel, Telnet, Advanced Forwarding, Active Sessions, and supports the FTP application layer over IPv6.

---

**Note:** This is high-level list of supported features and components, not a complete list.

---

For these protocols, the ProxySG Management Console, Blue Coat Sky UI, CLI, Visual Policy Manager (VPM), and Content Policy Language (CPL) allow the use of IPv6-style addresses for configuration.

#### *Related Documentation*

*Blue Coat SGOS 5.5.x Administration Guide, IPv6 chapter*

### *ADN Enhancements*

Many enhancements have been made to the ADN protocol to improve performance. In addition, the following new acceleration features have been added:

#### **Fast Transparent Tunnels**

The ADN protocol has been enhanced to speed up transparent tunnel establishment. To take advantage of this feature, make sure to upgrade all ADN nodes in the following order:

1. Upgrade the Primary ADN manager and Backup ADN manager.
2. Upgrade all appliances that serve as Concentrator peers only.
3. Upgrade all appliances that serve as Branch peers.

### **Adaptive Compression**

You can now enable the ProxySG to adjust its compression level based on CPU usage. When adaptive compression is enabled, the ProxySG will automatically increase its compression level when CPU usage is low and decrease its compression level when CPU usage is high. The ProxySG determines whether to increase or decrease the compression level based on its internal compression index. Because adaptive compression uses extra CPU when it is available, you will notice that your CPU usage levels are higher when this feature is enabled. If, however, you notice that the compression index remains low when adaptive compression is enabled (indicating that the compression level is decreased), this may indicate that your appliance is under-sized. In this case, you should consider a hardware upgrade. By default, adaptive compression is enabled on multi-processor appliances and disabled on single processor appliances.

### **Peer Deletion**

Peers that the ProxySG determines are no longer valid or useful are now automatically deleted. In addition, you can now manually delete peers that do not match the automatic deletion criteria.

### **Port Consolidation**

To reduce the number of ports that you use for ADN, you can now change the ADN manager ports to the same port numbers used for ADN tunnel connections: 3035 (plain) and 3037 (secure) by default. For backward compatibility, the ADN manager ports are still by default set to 3034 (for plain routing connections) and port 3036 (for secure routing connections).

### **MAPI**

- ❑ MAPI 2007:
  - Attachment upload and download optimization.
  - Keep-alive support.
  - Cross-protocol byte cache support.
- ❑ MAPI 2003: Attachment download optimization.

### ***Related Documentation***

*Blue Coat SGOS 5.5.x Administration Guide*, Configuring the Application Delivery Network chapter

## Proxy Services

### Redesign

The **Proxy Services** tab redesign presents more logically grouped services.

#### Location

**Configuration > Services > Proxy Services > Proxy Services** tab

#### Summary

There are now three default service groups: **Standard**, **Bypass Recommended**, and **Tunnel Recommended**. Expand each group to see which group contains which services. The **Standard** group contains the most commonly intercepted protocols.

---

**Note:** This description applies to new installations of SGOS 5.5.x or the behavior following restoring SGOS 5.5.x factory defaults. An upgrade to SGOS 5.5.x from a previous version preserves all services existing before the upgrade.

---

You can also:

- ❑ Create custom groups and move any service—default or custom—to that group.
- ❑ Add source IP addresses to listeners.

### Listen on Source IP Address

When creating or editing a service, a source IP address or subnet can be specified as a listener (in addition to destination IP which was already available). This feature gives administrators the ability to test services in a production environment, without service interruption to users. For example, you can create a service that specifies the source IP of the administrator's machine in order to intercept traffic from the administrator's PC only. After the service has been successfully tested on this single PC, the source can be expanded to include all IP addresses (or a specific subnet).

To add a source address for a service, go to the **Configuration > Services > Proxy Services** page, edit/create the service and then edit/add a listener.

#### Related Documentation

*Blue Coat SGOS 5.5.x Administration Guide*, Proxy Services chapter

## Content Filtering Redesign

The tabs in the **Content Filtering** menu are redesigned.

#### Location

**Configuration > Content Filtering > General > General** tab

**Configuration > Content Filtering > Third-Party Databases**

## Summary

A new menu item, **Third-Party Databases**, replaces all of the previous individually listed third-party content filter database vendors. This new page contains four new tabs: **Websense**, **SmartFilter**, **Proventia**, and **Optenet**. These are the only third-party vendors supported in the Management Console. You can maintain previously supported third-party vendors, but you must use the CLI to do so.

On the **General** tab, if you select a deprecated third-party database other than the Management Console-supported vendors, a CLI configuration requirement message displays.

The **WebPulse** tab moved to the new **Threat Protection** menu. See "[Threat Protection](#)" on page 79.

## Related Documentation

*Blue Coat SGOS 5.5.x Administration Guide*, Content Filtering chapter

## Visual Policy Manager Enhancements

SGOS 5.5.1 introduces the following VPM enhancements.

### CPL Layer

You can add a new layer from which you can compose CPL (rather than add objects to rules) just as you would in a text file. You can construct policy for one or more layers, define conditions, and define actions. You can also add layer guards as part of the layer definition—you cannot add a layer guard by right-clicking the layer name, as you can with the other layers.

You can manage the **CPL Layer** just as you can other layers (such as rename it and change its order among the layers).

### File Extension Object

The **File Extension** object in previous versions required you to scroll a long list of extensions. Furthermore, there was not a way to add extensions currently not in the list. The updated object enables you to enter extension strings, which narrows the available choices, and add new extensions.

### Return Redirect Object: Support for 301 and 307 Return Codes

Previously, this object supported **302** (found) return codes. The updated object allows you to select **301** (moved permanently) and **307** (temporary redirect) return codes.

### Usability Enhancements

Within the VPM, you can now select and move multiple rules up and down (or delete them) within a layer—the rules must be in consecutive order to move.

## Documentation Reference

*SGOS 5.5.x Visual Policy Manager and Advanced Policy Reference*

## Threat Protection

SGOS 5.5 introduces a new menu item in the **Configuration** menu named **Threat Protection**.

- ❑ **WebPulse**—Formerly under **Content Filtering**, this tab provides the same functionality as in previous versions, plus the addition of two links. The **Blue Coat WebFilter** status link displays the **Content Filtering > General** tab and the **Last Download** link displays the **Content Filtering > Blue Coat WebFilter** tab.
- ❑ **Malware Scanning**—This new tab provides a simple dialog that allows you to add a ProxyAV malware scanner service. You only need to enter the installed ProxyAV IP address and select plain ICAP or secure ICAP connection mode. The new service is placed in a service group called **proxyav** (viewable on the **External Services > Service Groups** page).

---

**Note:** You can still use the **External Services > ICAP** page to create non-ProxyAV malware services or edit existing services.

---

### Related Documentation

*Blue Coat SGOS 5.5.x Administration Guide*, Threat Protection chapter

## WCCP Enhancements

### WCCP Router Affinity

When this feature is enabled, the ProxySG always sends client and server bound back through the originating WCCP router through the negotiated return method (GRE or L2) and bypass route lookup. This is a per-service group configurable feature. This feature also allows client- and server-side connections to enable this feature independently.

This feature simplifies the deployment of the ProxySG by:

- ❑ Minimizing the amount of route configuration on the ProxySG. This reduces the potential of misrouted outbound ProxySG packets.
- ❑ Allowing policy-based routing to continue to be maintained at a single point on the existing routers. Therefore, these policies do not need to be replicated on the ProxySG.

Management Console location: **Configuration > Network > WCCP**

### WCCP Service Groups

SGOS 5.5.x increases the number of supported WCCP service groups from 100 to 256.

## CIFS Proxy

### Pre-Population CLI Commands

*Pre-population* refers to the process of copying files from the origin server to the ProxySG cache. The `content distribute` and `content revalidate` CLI commands now support the pre-population of CIFS files and directories. The syntaxes of these commands are:

```
content distribute cifs://domain;username:password@server/share/path-to-file
content revalidate [regex regex | url url]
```

The following new CLI commands are available for listing the contents of a CIFS directory on the ProxySG cache or for showing file information specific to CIFS files:

```
show cifs directory cifs://server/share/path-to-file
show cifs file cifs://server/share/path-to-file
```

The Blue Coat Sky management console offers a configuration screen for making CIFS pre-population requests.

### Related Policy Note

With the inclusion of the CIFS pre-population feature in SGOS 5.5.x, it is no longer necessary to use a CIFS rewrite policy to copy files into the cache. The rewrite policy in previous SGOS versions used a CIFS URL that included a server IP address; in SGOS 5.5.x, the IP address has been removed from the CIFS URL. If you created this policy in a previous release and upgrade to SGOS 5.5.x, the policy will not work. Any old policies using the CIFS URL can be removed; use the CIFS pre-population feature instead.

The following is an example of pre-5.5.x policy:

Here is an example of CIFS URL rewrite policy that was used before SG5.5:

```
inline policy local eof
<Proxy>
action.rewrite_url(yes)
define action rewrite_url
rewrite( url, "cifs://10.200.1.40/(.*)", "cifs://10.200.1.31/${1}",
cache) end
eof
```

### Related Documentation

*Blue Coat Sky Release Notes*

### SMB Signing

SGOS 5.5.x supports the SMB signing security mechanism, which is designed to eliminate man-in-the-middle attacks. The ProxySG uses the specified authentication credentials to act as a virtual user for signing purposes only. Traffic between the client and the ProxySG is downgraded to non-signing mode and is not subjected to signing, but traffic between the ProxySG and the origin content



server is signed only if signing is required (the server and the client are SMB-configured). Because the user is not used for any other authorization purposes, acceleration, and optimization benefits are achieved.

Configure this on the Concentrator ProxySG, *not* the branch ProxySG.

**Location:** Configuration > Proxy Settings > CIFS Proxy

---

**Note:** Enabling this option might incur a slight performance hit.

This feature alters the typical Windows behavior. Without this feature enabled, when a native Windows client with SMB signing disabled attempts to connect to native Windows server with SMB signing required, a disconnect occurs. When SMB signing is enabled on the ProxySG, such a client is able to connect.

---

### *Related Documentation*

*Blue Coat SGOS 5.5.x Administration Guide*, Acceleration File Sharing chapter

## *HTTP Proxy*

### **HTTP Network Error Transparency**

When an upstream server connection error occurs, the ProxySG (if configured to do so) returns exception pages to users. If the user is running an custom application, this exception page might interfere with its operation. Because of this, the user or anyone evaluating a ProxySG might believe that the ProxySG is at fault when the problem is with the Web server connection. SGOS 5.5.x provides a CLI command (no Management Console option) that allows to control whether or not the ProxySG sends an exception when a connection/network error occurs:

```
SG#(config) no http exception-on-network-error
```

---

**Note:** For a MACH5 license, this option is enabled by default upon upgrading to SGOS 5.5.x from a previous version.

---

### **Tunnel on Protocol Error**

Some HTTP parsing errors might cause the proxy to send users an exception, thus breaking the application. This occurs from non-HTTP requests from the client, HTTP requests that contain non-HTTP components, or line/header formatting errors. When enabled, this feature tunnels non-HTTP traffic on any HTTP service.

For the SSL proxy, the **Tunnel on Protocol Error** option applies when non-SSL traffic arrives at the SSL port (443 by default) or for SSL errors that might occur because of problems during the initial SSL handshake. Examples are:

- ❑ The server does not present a certificate.
- ❑ The ProxySG does not support the cipher, compression, or SSL version that the client or server negotiate.

Management Console location: **Configuration > Proxy Settings > General**

---

**Note:** For a MACH5 license (of the acceleration profile was selected during initial configuration), this option is enabled by default upon upgrading to SGOS 5.5.x from a previous version.

---

### Trust Destination IP for Client-less Connections

Improved cache look-up logic to address object lookup issues with CDN and Adaptive Asynchronous Refresh (AAR). Code improvements; not configurable.

### Limiting Client-less Connections

Enables you to prevent client-less connections, which are essential for caching and optimization, from overwhelming the OCS and the ProxySG. Strongly recommended when **Pipelining** or **Bandwidth Gain** options are enabled or if pre-populating caches with HTTP content.

Management Console location: **Configuration > Proxy Settings > HTTP Proxy > Policies**.

The default limits vary by model.

#### *Related Documentation*

*Blue Coat SGOS 5.5.x Administration Guide*, Proxy Services chapter

*Blue Coat SGOS 5.5.x Administration Guide*, HTTP Proxy chapter.

## SSL Proxy

### SSL Connection Bypassing for Client Certificates

Minimizes traffic disruption when the SSL proxy intercepts secure traffic. In cases where the OCS requires client certificate authentication to allow SSL traffic, the SSL proxy does not have enough information to continue intercepting traffic. This feature prevents the SSL proxy from abruptly terminating the connection request when the OCS requests client certificate authentication. You have the option to configure the ProxySG to:

- ❑ Tunnel the traffic thereafter if policy detects this scenario and is set to tunnel.
- ❑ Intercept the traffic and generate an exception page if policy detects this scenario.

New static VPM object: **Client Certificate Requested**—checks if client certificate is required. The **SSL Intercept Layer** now contains the **Service** column.

Access log field: When SSL proxy is in intercept mode and client certificate authentication fails, a new log value records the reason of SSL failure:

```
"x-bluecoat-ssl-failure-reason: SSL client certificate not supported"
```

**Statistics > Sessions > Active Sessions:** Error message: **SSL client certificate not supported**.

#### *Related Documentation*

*SGOS 5.5.x Visual Policy Manager and Advanced Policy Reference*, Visual Policy Manager chapter, Section C, search for object.

## *Nameable Interfaces*

Enables you to associate ProxySG interfaces with the connection purpose. For example, label an interface **wan-sfo** to indicate a WAN-OP connection to Concentrator in San Francisco.

### *Location*

**Configuration > Network > Adapters > Adapters** tab

### *Related Documentation*

*Blue Coat SGOS 5.5.x Administration Guide*, Adapters chapter

## *DNS Proxy*

### **Domain Name Suffixes**

The ProxySG now supports 30 DNS domain name suffixes (up from 6).

## *Access Log Enhancements*

### **Copy Existing Log Schema to a New Custom Schema**

Enables users to view and copy read-only access log formats, allowing them to create access log formats based on existing formats. The Management Console access logging page has several relabeled buttons to better indicate updated functions.

Management Console Location: **Configuration > Access Logging > Formats**

### **Logging the Proxy Source Port When Connecting to a Remote Site**

Logs the source port of the ProxySG when attempting to access a remote site. When the access log field is added to an access log format, the source port is available in HTTP, HTTPS, FTP, and WebFTP logs.

Access log field: `s-source-port`

Management Console Location: **Configuration > Access Logging > Formats**

### *Related Documentation*

*Blue Coat SGOS 5.5.x Administration Guide*, Access Logging chapter

## *Event Logging Enhancements*

### **Log when Syslog is Enabled or Disabled**

When system logging is enabled or disabled, a message indicating the change is sent to the syslog server. This feature is being added to provide an additional layer of security.

Management Console Location: **Maintenance > Event Logging > Syslog**

## Multiple Syslog Servers

This feature allows you to specify more than one syslog server to which event log messages are simultaneously sent. Sending event log information to multiple servers provides customers redundancy and data availability.

Management Console Location: **Maintenance > Event Logging > Syslog**

### *Related Documentation*

*Blue Coat SGOS 5.5.x Administration Guide*, Monitoring the ProxySG chapter, Event Logging section

## *Health Checks*

### Email Alerts Subject Line

Health check e-mail alerts now include the following information in the e-mail subject line:

- ❑ The assigned name of the appliance where the error occurred.
- ❑ The health state change.

## Known Issues in SGOS 5.5.1.x

This section lists the currently known issues when running SGOS 5.5.1.x.

### ADN

ADN connections may not be re-established after downgrading from SGOS 5.5 to SGOS 5.4. This issue occurs only in cases where both the ADN tunnel and the ADN Manager are listening on the same port. The workaround is to apply a different port number for either the ADN tunnel or the ADN Manager, before or after downgrading to 5.4.x. This modification will allow the listeners to restart and establish the ADN connection. (B#133007)

### CLI

When the user invokes CDN command, such as a content pull, using the serial console and the command cannot be exited by hitting Ctrl-C. The CDN command will not complete until it gets unblocked, thereby holding on to the serial console until then.

### Health Checks

If you upgrade the ProxySG from a MACH5 license to a Proxy Edition license, a reboot is required to activate some health checks (DNS, Authentication, and Forwarding). (B#110098)

### Management Console

- ❑ Java versions 1.6.0\_14 and later might cause Management Console access problems. Also, the same Java version might work with one browser but not another. (B#128691)
- ❑ With Java version 1.6.0\_15, the Management Console fails to load and issues a debug trace in the console if you have configured Java to *not* store temporary files on the local hard disk. The workaround is to select **Control Panel > Java > General tab > Temporary Internet Files box > Settings button > enable "Keep temporary files on my computer"**. (B#122403)
- ❑ JRE 1.5 does not support the following cipher suites:
  - AES256-SHA
  - EXP-RC2-CBC-MD5
  - DES-CBC3-MD5
  - RC2-CBC-MD5
  - DES-CBC-MD5

Furthermore, some cipher suites are not supported by Firefox and some are not supported by IE. For example: Firefox supports cipher suite AES128-SHA but Internet Explorer does not. If the browser supports a particular cipher suite, but JRE does not support it, an attempt to access the Management Console displays the following error:

```
"Error connecting to the ProxySG"
```

(B#108226)

- ❑ Browsers with Phishing filters enabled might cause the Management Console to hang or not fully display. Try clicking visible tabs. (B#110412 -- fixed in SGOS 5.5.2)
- ❑ When an IP address is configured to a default hardware bridge passthru-2 on a ProxySG 8100, the Management Console displays that the interface link state goes from **Auto 100Mbps FDX** to **Down**. It remains displayed as **Down** even though executing the `show interface 2:0` CLI command displays the interface as auto-sensed to full duplex, 100 megabits/sec network. Also, the **Statistics > Summary > Network Utilization** page displays 2:0 as up. A browser refresh returns the link state to **Auto 100Mbps FDX**. (B#129486)

## Networking

### CIFS

- ❑ SGOS 5.5.x does not support CIFS pre-population URLs that resolve to a DFS-redirected share. (B#126686)
- ❑ The `content distribute url cifs-url` command has several error-checking limitations. The following conditions do not produce error messages:
  - The password is invalid for the user in the domain.
  - The user does not have permission to access the specified path.
  - The path-to-file does not exist.
  - The authentication method is not supported. (Kerberos authentication is not currently supported.)

These errors are not reported; the command outputs `OK` even when the operation did not successfully pre-populate the cache. To verify a pre-population request, use the `show cifs` CLI command. (B#129597)

- ❑ Apple Mac OS clients: To avoid known issues with Mac OS (whether proxied or not), Blue Coat recommends always ejecting a network share before disconnecting it. (B#109011)

## Policy

### HTTP Proxy

The default value for `http.server.accept_encoding()` is not correctly accepted. The policy does work when you use it as follows:

```
<Proxy>
http.server.accept_encoding(client)
http.server.accept_encoding.allow_unknown(no)
```

(B#127379)

## Skype

This known issue occurs if you enable the **Tunnel on Protocol Error** option (see ["Tunnel on Protocol Error"](#) on page 81) and the following conditions are present. Skype has a TCP read timeout (typically 20 seconds) that is usually lower than the ProxySG timeout value (the default is 300 seconds). When Tunnel on Protocol Error is enabled and all ports except 80 and 443 are blocked on the Skype client, Skype logins fail. This occurs because when the Skype node connects to port 443 through the ProxySG (that is intercepting SSL traffic), the ProxySG waits for the server certificate for 300 seconds; however, the Skype node is not sending one. The Skype node breaks the connection after its second read timeout, which causes a login failure. The workaround is to set the ProxySG value to less than the Skype timeout value, which switches the connection to a tunnel because of the server certificate absence. The CLI command to change this value is:

```
# (config ssl) ssl-nego-timeout seconds
```

## SSL Proxy

- ❑ When intercepting SSL forward proxy, the DNS lookup occurs when SSL is attempting to connect to the upstream server. Therefore, the DNS policy must be in the <Forward> layer for this upstream connection to take effect. For example:

```
<Forward>  
server_url.dns_lookup(prefer-ipv6)
```

The SSL upstream DNS lookup does not honor the <Proxy> layer policy, so you must place the DNS policy in the <Forward> layer. (B#124658)

- ❑ With an SSL explicit proxy, Firefox does not properly form the IPv6 literal and port. This improper form causes ambiguity in the initial CONNECT header and prevents the ProxySG from parsing the header properly. (B#124658)

## Threat Protection

If you delete a ProxyAV service from the service group, the **Cannot delete the service specified, it is in use** error displays if health checking is also occurring with the service. Attempting to delete the service again should work. (B#128922)

## Documentation Errata

The following documentation issues could not be fixed before production cut-off.

### Content Filtering

The Online Help section for Blue Coat Web Filter lists the following command:

```
SGOS#(config bluecoat) download {all-day | auto | between-hours |  
encrypted-password | full-get-now | get-now | password | url |  
username}
```

The **full-get-now** option was not added to this release.

## **Proxy Services**

The Online Help section for Restricted Intercept states that it applies to explicit connections. This is incorrect. Restricted Intercept only applies to transparent connections.



## Section R: Limitations in SGOS 5.5.x

This section lists limitations of the SGOS 5.5.x release.

- ❑ The FTP Proxy changes a 226 Response Line from the Origin Content Server (OCS). (B#179670, SR-2-494512202)
- ❑ Speed and duplex information is not reported in the Event log when a link comes up on the SG9000 platform's Broadcom NICs. (B#183745)  
For more information, refer to the following:

<https://kb.bluecoat.com/index?page=content&id=KB5394>

- ❑ The SSL renegotiating feature causes a situation where when an IIS Server or a HTTP Server asks for the certificate, the following policy rule on the SSL Proxy will not work: `client.certificate.requested=yes`.  
The reason for this limitation is that the SSL Proxy does not run any policy rules during SSL renegotiations.

**Workaround:** Create a policy for these websites where SSL tunneling is setup instead of an intercept option. For example:

```
<ssl-intercept>  
url=http://www.example.com ssl.forward_proxy(no)  
(B#159541)
```

- ❑ The ProxySG appliance closes server-side persistent connections only after a delay when the `http persistent-timeout` server option is enabled. (B#137214)
- ❑ MD2 is no longer supported by ProxySG appliance, due to security reasons. The workaround is to disable protocol detection from the specific website, use this policy modification: `if url=<web addr> detect_protocol(no)`. (B#159335, SR 2-368297422)
- ❑ On occasion, the redirection of the PAC/WPAD file using policy fails with 400-invalid\_request. When using PAC/WPAD redirects, it is recommended to use the policy gesture "request\_redirect" instead of "redirect". The "request\_redirect" gesture was first introduced in SGOS (B#145454, SR 2-307668872)
- ❑ The `client.protocol=cifs reflect_ip(client)` property must be defined under the Proxy Layer. (B#132106)
- ❑ Because the `url.path` condition tests only the path component of a URL, use the `url` condition to specify a URL that contains a query component. (B#133951, SR 2-261130432)

For example:

```
DENY url=http://maps.google.co.jp/maps?hl=ja
```

Alternatively, you can separate out each component of the URL, as follows:

```
DENY url.scheme=http url.host=maps.google.co.jp url.path=/maps  
url.query=?hl=ja
```

- ❑ When a master ProxySG fails over to one of the backup appliances in the group, the session start value in the session monitor statistics is twice what it should be. If the original master comes online again, its session start values are doubled as well. (B#136557)
- ❑ The `show session-monitor` and `view session-monitor` CLI commands are not currently working in the `session-monitor attributes` sub-mode. (B#136707)
- ❑ Although the following ciphers still appear in the CLI, they have been deprecated and should not be used (B# 138255):
  - RC4-64-MD5
  - EXP1024-RC4-MD5
  - EXP1024-RC4-SHA
  - EXP1024-RC2-CBC-MD5
  - EXP1024-DES-CBC-SHA
- ❑ At the beginning of some connections, the Active Sessions screen in the Management Console indicates they are going through the ADN tunnel when they actually are not. This is a Firefox browser display issue and does not occur in Internet Explorer. (B#139000, SR 2-295043078)
- ❑ SMB traffic is not passed through when the SMB Signing account is configured with a wrong password. The workaround is to configure the right login credentials on the ProxySG. (B#142789, SR 2-310816546)
- ❑ If you want to test the read-write attribute of communities and users, use OID .1.3.6.1.6.3.1.1.6.1.0 in the BLUECOAT-SG-DISK-MIB; this is the only object that is writable. Note that it is a generally accepted industry practice not to allow the setting or writing of objects via SNMP. (B#151919)
- ❑ Taking a disk offline may result in the event log being shortened. (B#143132)
- ❑ In SGOS 5.2 or earlier, users could retrieve MMS streaming content by entering the following URL in the Windows Media address bar:  
`http://<Proxy_SG_IP>/redirect?mms://<URL>`  
SGOS 5.3 and higher changed the way the ProxySG handles WM content, so users must enter the following URL:  
`http://<Proxy_SG_IP>/redirect?http://<URL>`
- ❑ When an SMTP gateway server is configured on the ProxySG appliance, make sure that it can properly relay SMTP traffic on behalf of the ProxySG. SMTP messages that are denied and/or are unsuccessfully transmitted can queue up on the ProxySG and progressively cause increased memory pressure. After you disable and/or correct the SMTP gateway, the memory consumed on the ProxySG will slowly recover. (B#174625)

- ❑ When the ProxySG appliance receives fragmented packets (from a router) and reflect-client IP is set, the SG does not rebuild the fragment prior to forwarding them to the client. This may result in failing to access a site. (B#150796, SR 2-336431112)  
**Workaround:** Use a forward rule on the edge proxies and disable reflect-client-IP for this domain only.)
- ❑ On occasion, the PAC/WPAD redirection failed with `400-invalid_request` when policy was used. Blue Coat recommends using policy gesture `request_redirect` instead of `redirect`. This was first introduced in SGOS 5.5.7.1. (B#166557)
- ❑ Content filtering supports at most 16 categories per URL. (B#169824)

## Section S: SGOS 5.5.x — Support Files and Support for Other Products

This section lists third-party products that interact with the ProxySG.

### Support Files

This section provides links to files and documents referenced in the ProxySG documentation set.

#### *.htpasswd File (Perl Script)*

This file is used during Local Realm (Authentication) configuration.

- ❑ <https://bto.bluecoat.com/doc/13282>

#### *XML Schemas for SOAP*

These schemas are used in authentication and authorization responses and requests.

- ❑ <http://www.bluecoat.com/xmlns/xml-realm/1.0/xml-realm-1-0.xsd>
- ❑ <http://www.bluecoat.com/xmlns/xml-realm/1.0/xml-realm-1-1.xsd>

### Support for Other Products

This section provides the required versions of other products that interact with the ProxySG.

#### *Supported Clients and Browsers*

The following are the combinations of OS, browser, and Sun Java Runtime Environment (JRE) versions supported for the Web-based Management Console (MC) and the Visual Policy Manager (VPM).

#### **Supported Operating Systems**

The supported operating systems for the Management Console and VPM are as follows:

- ❑ Microsoft Windows™ 2000 Pro (SP4 or later)
- ❑ Windows XP (SP2 or later)
- ❑ Windows Vista

## Supported Browser Versions

The supported browser versions for the MC and VPM are as follows:

- Internet Explorer 6.0 (SP1 or later)
- Internet Explorer 7.0--9.0
- Firefox 3.6--7.0
- Firefox 9.x

The following table lists the operating system and browser compatibility.

Table 1-1. Supported Operating Systems

| Operating System                               | IE v6.0<br>(SP1 or<br>later) | IE v7.0 | Firefox v9.x |
|------------------------------------------------|------------------------------|---------|--------------|
| Windows 2000<br>Professional (SP4<br>or later) | Yes                          | Yes     | Yes          |
| Windows XP                                     | Yes                          | Yes     | Yes          |
| Windows Vista                                  | No                           | Yes     | No           |

## Supported JRE Versions

Supported Java JRE versions:

- 1.5.0\_15 and later
- 1.6 (except 1.6\_05, which causes VPM Help problems)

## Notes

- ❑ On the Sun download page, Sun naming conventions refer to JRE 5.0 and JRE 1.5 interchangeably. JRE 5.0 is Sun's new name for JRE 1.5.
- ❑ You might experience a problem downloading the latest supported JRE through the Management Console if:
  - The browser does not support automatic download.
  - The automatic download hangs.
  - The Java Installer displays an error: HTTP Status Code=302 followed by a popup that java 1.5.x cannot be downloaded.

If you experience any of these issues, enter the following URL to get to the Sun download page (if the automatic download hangs, first terminate the download):

<http://java.sun.com/products/plugin/index.jsp>

- ❑ Network delays and/or slow processor speeds might affect JRE performance, slowing the display of Management Console menu selections and options.

- ❑ Enable the auto-detect encoding feature on your browser so that it uses the encoding specified in the console URLs. The browser does not use the auto-detect encoding feature by default. If auto-detect encoding is not enabled, the browser ignores the `charset` header and uses the native OS language encoding for its display.
- ❑ If your system is running JRE 1.6\_05, the VPM Help system does not display or function correctly.

## *Blue Coat Director, Reporter, and ProxyClient*

### **Director**

SGOS 5.5.x is compatible with SGME 5.5.x. If you are using Blue Coat Director to manage your ProxySG appliances, use overlays to fine-tune configuration specifics after upgrade. Do not push a device profile created in an earlier SGOS version to a ProxySG that has been upgraded. For more information on profiles and overlays, refer to the Director documentation.

Consult the following table before attempting to manage ProxySG appliances:

| <b>SGME version</b> | <b>Manages SGOS versions....</b>                                                     |
|---------------------|--------------------------------------------------------------------------------------|
| SGME6.1x            | SGOS 6.1.x, 6.2.x, and 6.3.x<br>SGOS 5.3.x, SGOS 5.4.x, and SGOS 5.5.x<br>SGOS 4.3.x |
| SGME 5.5.x          | SGOS 6.1.x, 6.2.x, and 6.3.x<br>SGOS 5.3.x, SGOS 5.4.x, and SGOS 5.5.x<br>SGOS 4.3.x |
| SGME 5.4.2.5        | SGOS 5.3.x, SGOS 5.4.x, and SGOS 5.5.1.1<br>SGOS 4.3.x                               |
| SGME 5.4.2.x        | SGOS 5.3.x and SGOS 5.4.x<br>SGOS 4.3.x                                              |
| SGME 5.4.1.x        | SGOS 5.4.x and all SGOS versions supported by SGME 5.3.x                             |

### **Reporter**

This release is compatible with the following Blue Coat Reporter releases:

- ❑ Reporter 8.x
- ❑ Reporter 9.x

### **ProxyClient**

ProxyClient versions 3.1.x and 3.2.x are compatible with SGOS 5.5.x. To download the latest version, refer to the *Blue Coat ProxyClient Release Notes*.

## Anti-Malware

The Blue Coat ProxySG with ProxyAV™ integration is a high-performance Web anti-malware solution. For more information, refer to the Blue Coat Web site.

This release is compatible with Blue Coat AVOS 2.x and AVOS 3.x.

In this release, SGOS is certified with the following third-party implementations of ICAP:

- ❑ Symantec AntiVirus Scan Engine (SAVSE) 4.3, version 4.3.0.15; ICAP 1.0
- ❑ WebWasher 5.3, build 1953; ICAP 1.0

## Instant Messaging

This section details the Instant Messaging proxy support for English language versions. While some versions of AIM and Windows Live Messenger (WLM) are not officially supported, they work in most situations.

Video and audio are not supported with any of the Instant Message protocols: MSN, Yahoo, AIM, and WLM.

### English Language Versions Supported

Table 1-1. IM Client Compatibility Matrix

| Client Version        | SGOS 5.5.x Support | Comments                                                                                                                                                                         |
|-----------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AIM 5.9               | Yes                |                                                                                                                                                                                  |
| AIM 6.1               | N/A                | No longer available. See <a href="#">"Partially Supported IM Protocol Versions"</a> below.                                                                                       |
| AIM 6.5               | Limited            | This version was not officially tested, but full proxy support should work. See <a href="#">"Partially Supported IM Protocol Versions"</a> below.                                |
| AIM 6.8               | Yes                | AIM 6.8 is supported in explicit SOCKSv5 and HTTP/HTTPS proxy configurations only. For AIM 6.8 support, you must purchase and import a CA signed SSL certificate on the ProxySG. |
| AIM 6.9               | Limited            | This version was not officially tested, but full proxy support should work.                                                                                                      |
| Windows Messenger 4.x | Yes                | (4.0-XP, 4.7-XP+SP2)                                                                                                                                                             |
| Windows Messenger 5.x | Yes                |                                                                                                                                                                                  |
| MSN Messenger 7.0     | Yes                | This is the last version that supports Windows 98 and Windows ME.                                                                                                                |
| MSN Messenger 7.5     | Yes                |                                                                                                                                                                                  |

Table 1-1. IM Client Compatibility Matrix

| Client Version      | SGOS 5.5.x Support | Comments                                                                                                                                                                                                                                                                                                           |
|---------------------|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WLM 8.0             | Yes                | Name changed from MSN to Windows Live Messenger (WLM); Microsoft deprecated this version in favor of WLM 8.1.                                                                                                                                                                                                      |
| WLM 8.1             | Yes                | In 2007, Microsoft rendered as obsolete all versions previous to 8.1 because of a security issue.                                                                                                                                                                                                                  |
| WLM 8.5             | Yes                | Beginning November 9th, 2009, clients are required to upgrade.                                                                                                                                                                                                                                                     |
| WLM 2009            | Yes                | In 5.5.x, WLM 2009 is tunneled. This version is also known as version 14.0. Beginning November 9th, 2009, Messenger 2009 (version 14) users must upgrade their clients. Users who have already installed the latest version, which was released Aug 18th 2009 (Build: 14.0.8089.726), are not required to upgrade. |
| Yahoo 5.5, 5.6      | N/A                | In April 2008, Yahoo! retired these client releases.                                                                                                                                                                                                                                                               |
| Yahoo 6.0, 7.0, 7.5 | No                 | In August 2009, Yahoo! retired the IM network that supported these versions.                                                                                                                                                                                                                                       |
| Yahoo 8.0, 8.1      | Yes                |                                                                                                                                                                                                                                                                                                                    |
| Yahoo 9.0           | Yes                | In 5.5.x, Yahoo 9.0 is tunneled.                                                                                                                                                                                                                                                                                   |

## Partially Supported IM Protocol Versions

### AIM

The ProxySG does not recognize transparent AIM 6.x as AIM (IM) traffic. In some ProxySG configurations, however, client login and chat do succeed.

#### □ AIM 6.x

- If a SOCKS proxy is configured in the client's Internet Explorer (IE) settings:
  - SOCKS proxy with detect protocol disabled on the ProxySG: The client can log in and chat normally.
  - SOCKS proxy with detect protocol enabled on the ProxySG: The client can log in and chat with a thirty-second delay.
- If an HTTP/Secure proxy is configured in the client PC's IE settings:
  - HTTP proxy with detect protocol disabled on the ProxySG: The client can log in and chat normally
  - HTTP proxy with detect protocol enabled on the ProxySG: The client login fails after about 30 seconds with the message `Connection lost`.



- Transparent deployment: AIM 6.1 cannot log in if an SSL service is configured on port 443. AIM can log in, with a 30-second delay, if a TCP tunnel service is configured on port 443 with protocol detection enabled. AIM can log in if the SSL forward proxy is also enabled and the ProxySG appliance's certificate is installed as the root certificate on the client's IE browser.

❑ AIM 6.5

- The client can log in and chat unless the SSL connection is intercepted by the SSL forward proxy. Supported deployments, if the SSL connection is not intercepted by the SSL forward proxy include transparent/TCP tunnel on port 443, transparent/SSL proxy on port 443, and HTTP proxy or SOCKS proxy.

To deny login for AIM 6.0, 6.1 clients, and for transparent proxy deployments of AIM 6.5 and 6.8 clients, the following policy can be used:

```
<Proxy>  
DENY url.host=kdc.uas.aol.com
```

## Open SSH

SGOS 5.5.x supports OpenSSH version 5.1.

## Open SSL

SGOS 5.5.x supports OpenSSL version 0.9.7m.

## Peer-to Peer (P2P)

SGOS 5.5.x supports the following P2P protocols:

- ❑ BitTorrent, with the exception of encrypted BitTorrent
- ❑ GNUTella
- ❑ eDonkey

## RSA SecurID

SGOS 5.5.x supports RSA 6.0 with SecurID.

## SOCKS

SGOS 5.5.x supports SOCKS v5, authentication protocol v1.

## Streaming

Streaming media support is limited to the following media players and servers:

- ❑ The ProxySG supports the following versions and formats:
  - Windows Media Player 7-11
  - Windows Media Server 9

---

**Important:** SGOS 5.5.x does not support older Windows Media Servers that do not support WM-HTTP when NTLM authentication is enabled.

Newer Windows Media Clients, such as 11.x, only use WM-HTTP and do not support MMS.

---

- ❑ The ProxySG supports the following Real Media Players and Servers:
  - RealOne Player, version 2
  - RealPlayer 8 and 10
  - RealServer 8 through 10
  - Helix Universal Server
  - Helix Player 11
- ❑ The ProxySG supports the following versions and servers, but in pass-through mode only:
  - QuickTime Players v7.x, 6.x, and 5.x
  - Darwin Streaming Server 4.1.x and 3.x

## WCCP

SGOS 5.5.x was tested with several releases of Cisco IOS: 12.0.7, 12.1.6E, 12.2.18. For a list of Cisco platforms that support L2 packet return, go to [www.cisco.com](http://www.cisco.com).

© 2013 Blue Coat Systems, Inc. All rights reserved. BLUE COAT, PROXYSG, PACKETSHAPER, CACHEFLOW, INTELLIGENCECENTER, CACHEOS, CACHEPULSE, CROSSBEAM, K9, DRTR, MACH5, PACKETWISE, POLICYCENTER, PROXYAV, PROXYCLIENT, SGOS, WEBPULSE, SOLERA NETWORKS, DEEPSEE, DS APPLIANCE, SEE EVERYTHING. KNOW EVERYTHING., SECURITY EMPOWERS BUSINESS, BLUETOUGH, the Blue Coat shield, K9, and Solera Networks logos and other Blue Coat logos are registered trademarks or trademarks of Blue Coat Systems, Inc. or its affiliates in the U.S. and certain other countries. This list may not be complete, and the absence of a trademark from this list does not mean it is not a trademark of Blue Coat or that Blue Coat has stopped using the trademark. All other trademarks mentioned in this document owned by third parties are the property of their respective owners. This document is for informational purposes only.

BLUE COAT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. BLUE COAT PRODUCTS, TECHNICAL SERVICES, AND ANY OTHER TECHNICAL DATA REFERENCED IN THIS DOCUMENT ARE SUBJECT TO U.S. EXPORT CONTROL AND SANCTIONS LAWS, REGULATIONS AND REQUIREMENTS, AND MAY BE SUBJECT TO EXPORT OR IMPORT REGULATIONS IN OTHER COUNTRIES. YOU AGREE TO COMPLY STRICTLY WITH THESE LAWS, REGULATIONS AND REQUIREMENTS, AND ACKNOWLEDGE THAT YOU HAVE THE RESPONSIBILITY TO OBTAIN ANY LICENSES, PERMITS OR OTHER APPROVALS THAT MAY BE REQUIRED IN ORDER TO EXPORT, RE-EXPORT, TRANSFER IN COUNTRY OR IMPORT AFTER DELIVERY TO YOU.

Americas:

**Blue Coat Systems, Inc.**

420 N. Mary Ave.

Sunnyvale, CA 94085

Rest of the World:

**Blue Coat Systems International SARL**

3a Route des Arsenaux

1700 Fribourg, Switzerland

