Blue Coat® Systems
SG™ Appliance

SGOS 5.x Upgrade Guide

Version SGOS 5.1.4

Contact Information

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

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

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

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

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

Document Number: 231-02867

Document Revision: SGOS 5.1.4—03/2007

Contents

Chapter 1: Upgrading—Overview

Chapter 2: Upgrade Behavior, General

Chapter 3: Feature-Specific Upgrade Behavior

Chapter 1: Upgrading—Overview

Blue Coat® strongly recommends that you read this document before attempting to upgrade to SGOS 5.x from previous SGOS operating systems.

Existing features and policies might not perform as with previous versions, and upgrading to this version might require some additional configuration tuning.

Note: SGOS 5.x contains many new features for branch office acceleration, but maximizing the new features requires deployment at branch/data center endpoints. Do not upgrade to this release if you will not utilize this type of deployment.

SGOS 5.x Upgrades

Upgrades are permitted only from SGOS 4.2.1.6. For information on the correct upgrade path, see Table 2-1, "Upgrade Paths" on page 7.

If you attempt to download the next major release and you receive an error message saying that the download failed due to policy deprecations, your policy uses constructs that are no longer supported in SGOS 5.x. You must correct any policy syntax problems before upgrading.

If the upgrade path is followed, most of the current settings on the SG appliance are maintained after the upgrade. New or transformed settings in SGOS 5.x are taken from the original settings wherever possible.

About the Document Organization

This document is organized for easy reference, and is divided into the following sections and chapters:

Table 1-1. Document Organization

Chapter Title	Description
Chapter 1 – *Introducing the Upgrade/Downgrade Guide*	SGOS 5.x upgrades are discussed. Blue Coat documentation and documentation conventions are also discussed.
Chapter 2 – *Upgrade Behavior, General*	This chapter discusses general upgrade issues, including the required upgrade path and licensing.
Chapter 3 – *Upgrade Behavior, Specifics*	This chapter identifies new features in SGOS 5.x and discusses any upgrade/downgrade issues.

Related Blue Coat Documentation

❒ *Blue Coat SG200 Installation Guide*

❒ *Blue Coat SG400 Series Installation Guide*

- *Blue Coat SG510 Installation Guide*
- *Blue Coat SG800 Installation Guide*
- *Blue Coat SG810 Installation Guide*
- *Blue Coat SG8000 Installation Guide*
- *Blue Coat SG8100 Installation Guide*
- The 12-volume *Blue Coat SG Appliance Configuration and Management Guide Suite* includes the following documents:
    - *Volume 1: Introduction to the Blue Coat SG Appliance*
    - *Volume 2: Getting Started*
    - *Volume 3: Proxies and Proxy Services*
    - *Volume 4: Web Communication Proxies*
    - *Volume 5: Securing the Blue Coat SG Appliance*
    - *Volume 6: Advanced Networking*
    - *Volume 7: VPM and Advanced Policy*
    - *Volume 8: Managing Content*
    - *Volume 9: Access Logging*
    - *Volume 10: Managing the Blue Coat SG Appliance*
    - *Volume 11: Content Policy Language Guide*
    - *Volume 12: Command Line Interface Reference*

Document Conventions

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

Table 1-2.   Typographic Conventions

Conventions	Definition
Italics	The first use of a new or Blue Coat-proprietary term.
`Courier font`	Command line interface text that appears on your administrator workstation.
`Courier Italics`	A command line variable that is to be substituted with a literal name or value pertaining to the appropriate facet of your network system.
`Courier Boldface`	Text that must be entered as shown.
{ }	One of the parameters enclosed within the braces must be supplied
[ ]	Encompasses one or more optional parameters.

Table 1-2. Typographic Conventions (Continued)

<table>
<tr><th>Conventions</th><th>Definition</th></tr>
<tr><td>|</td><td>This pipe character delineates options in a mandatory or optional list.
For example:
configure {terminal | network url}</td></tr>
</table>

Chapter 2: Upgrade Behavior, General

Upgrading

Following the upgrade path provided maintains most of the current settings, the exceptions being those features that were substantially enhanced in SGOS 5.x.

Note: Downgrading to an earlier version of SGOS is not supported for new systems that ship with SGOS 5.1.1 installed.

The following table provides the upgrade paths for these earlier versions.

Table 2-1. Upgrade Paths

Current OS (Range)	Direct Upgrade to Latest Version?	Next OS version required
SGOS 2.1.x, where x >= 07	No	SGOS 3.2.6
SGOS 3.1.x	No	SGOS 3.2.6
SGOS 3.2.x, where x<=3	No	SGOS 3.2.6
SGOS 3.2.x, where x>=4	No	SGOS 4.2.1.6
SGOS 4.1.x	No	SGOS 4.2.1.6
SGOS 4.2.1.x, where x<=6	No	SGOS 4.2.1.6
SGOS 4.2.1.x, where x>6	Yes	SGOS 5.1.1

CPL Notes

Deprecation warnings are issued for CPL syntax that is abandoned in the current release. Use of abandoned syntax causes CPL compiler errors, the policy fails to install and the SG appliance will use the default policy of ALLOW or DENY for all traffic. Following the recommended upgrade process ensures that policy integrity and therefore, network security, are maintained.

Restoring to Previous Versions

When upgrading from the SGOS 4.2.1.6 or higher release, a copy of the settings is saved prior to any transformations by SGOS 5.x so that the original settings are available if the SG appliance is downgraded to SGOS 4.2.1.6.

Keep in mind that changes made after upgrade are not preserved on a downgrade. After an upgrade and a downgrade, the state is exactly what it was before the upgrade.

Changing Between SGOS 5.x Versions

When moving from one SGOS 5.x release to another SGOS 5.x release, the system maintains all settings. Changes made after an upgrade continue to be available after a subsequent downgrade as long as the setting is relevant to the downgraded release.

Note: When upgrading or downgrading between versions of SGOS 5.x, copies of version-specific configurations are not retained. Instead, all configurations created in an upgrade are retained if the configuration is relevant to the downgrade version.

Care should be taken when using policy features introduced in a minor release. These cause compilation errors if you fall back to a previous version of the same major release in which those features were unsupported.

To prevent accidental fallbacks, you should remove unused system images (using the `installed_systems delete` *`number`*, from the `(config installed-systems)` prompt).

Licensing

You can upgrade to SGOS 5.1.x from SGOS 4.2.1.6.

Upgrading from SGOS 4.2.1.6

If you upgraded from SGOS 4.2.1.6 with valid Support entitlement, you should already have an SGOS 5 license; no further action is required. If you do not have an SGOS 5 license, contact Support Services.

There are three types of licensable components:

- Required—The SGOS base.
- Included—Additional features provided by Blue Coat.
- Optional— If applicable, any additional purchased features.

When the license key file is created, it consists of all three components. The SGOS base is a required component of the license key file. The following table lists the SG appliance licensable components, categorized by type.

Table 2-2. Licensable Components

Type	Component	Description
Required	SGOS 5 Base	The SG appliance operating system, plus base features: HTTP, FTP, TCP-Tunnel, SOCKS, and DNS proxy.
Included	3rd Party Onbox Content Filtering	Allows use with third-party vendor databases: Intersafe, Optenet, Proventia, SmartFilter, SurfControl, Websense, and Webwasher.
Included	Websense Offbox Content Filtering	For Websense off-box support only.
Included	ICAP Services	External virus and content scanning with ICAP servers.

Table 2-2. Licensable Components (Continued)

Type	Component	Description
Included	Bandwidth Management	Allows you to classify, control, and, if required, limit the amount of bandwidth used by different classes of network traffic flowing into or out of the SG appliance.
Included	Windows Media Standard	MMS proxy; no caching or splitting; content pass-through. Full policy control over MMS.
Included	Real Media Standard	RTSP proxy for Real Media content; no caching or splitting; content pass-through. Full policy control over RTSP.
Included	Apple QuickTime	RTSP proxy for QuickTime content; no caching or splitting; content pass-through. Full policy control over RTSP.
Included	Netegrity SiteMinder	Allows realm initialization and user authentication to SiteMinder servers.
Included	Oracle COREid	Allows realm initialization and user authentication to COREid servers.
Included	Peer-to-Peer	Allows you to recognize and manage peer-to-peer P2P activity relating to P2P file sharing applications.
Included	Compression	Allows reduction to file sizes without losing any data.
Optional	SSL Proxy	Native SSL proxy and Reverse HTTPS Proxy (SSL termination) on the SG appliance. Includes an SSL accelerator card to be installed on the appliance. Upon upgrading to SGOS 4.2, the license description for an existing SSL license changes to "SSL Proxy" instead of "SSL Termination." This is simply a description change. SSL termination and SSL Proxy functionality are available (when licensed).
Optional	IM	AOL Instant Messaging: AIM proxy with policy support for AOL Instant Messenger. MSN Instant Messaging: MSN proxy with policy support for MSN Instant Messenger. Yahoo Instant Messaging: Yahoo proxy with policy support for Yahoo Instant Messenger.
Optional	Windows Media Premium	MMS proxy; content caching and splitting. Full policy control over MMS. When the maximum concurrent streams is reached, all further streams are denied and the client receives a message.
Optional	Real Media Premium	RTSP proxy for Real Media content; content caching and splitting. Full policy control over RTSP. When the maximum concurrent streams is reached, all further streams are denied and the client receives a message.

Table 2-2. Licensable Components (Continued)

Type	Component	Description
Optional	SG Client	Entitles you to support a certain number of SG Clients in your enterprise; however, the license does not limit the number of ADN tunnels to which clients can have access. SG Client licenses are upgradeable so you can support a larger number of users. **Note**: Only the appliance designated as the SG Client Manager requires a license. To use SG Clients in your enterprise, apply the license only to the Client Manager and not to any other appliances in the ADN network.

Hardware Supported

Blue Coat supports the following hardware:

- SG 200
- SG 400
- SG 510
- SG 800
- SG 810
- SG 8000
- SG 8100

Note: If you are upgrading an existing SG appliance that has already been registered with Blue Coat, you do not need to re-register the hardware. You can just mark the system as manually registered in the License Warning pane, which displays when you leave the Management Console home page. (You can also use the CLI to mark the hardware as registered by using the commands under `(config) licensing`.)

If you have a new SG appliance, you must register the hardware directly online and then license the software.

Documentation References

- *Volume 2: Getting Started*
- *Volume 10: Managing the Blue Coat SG Appliance*
- *Volume 12: Blue Coat SG Appliance Command Line Reference*

Chapter 3: Feature-Specific Upgrade Behavior

This chapter provides critical information concerning how specific features are affected by upgrading to SGOS 5.x (and, if relevant, downgrading from) and provides actions administrators must or are recommended to take as a result of upgrading.

This chapter contains the following sections:

- "App. Delivery Network" : You can upgrade your network to take advantage of WAN optimization appropriate acceleration techniques (bandwidth management, compression, protocol optimization, byte caching, and object caching) and security protections (host authentication and authorization, message integrity, and privacy) to all of an enterprise's key application.
- "Authentication" on page 16: COREid has several important considerations, and BCAAA installation has been clarified.
- "Bridging" on page 18: Bridging has been redone for SGOS 5.x.
- "Bypass Lists" on page 19: New behavior in SGOS 5.1.1.
- "Content Filtering" on page 21: A new content filtering provider has been added for SGOS 5.x.
- "Policy" on page 21: Objects to support Application Delivery Networks have been added to both CPL and VPM.
- "Services" on page 22: New framework has been created for proxies and proxy services.
- "SSL" on page 23: The `ssl-verify-server` commands under HTTP, and the corresponding CLI and Management Console commands, have been removed.
- "Statistics" on page 24: Statistics behavior has changed since SGOS 4.x.

App. Delivery Network

The Application Delivery Network (ADN) is aimed at enhancing the experience of users in WAN environments. Blue Coat offers two approaches to upgrading and securing your network; both approaches allow you to keep the network in operation during the upgrade.

Note: If you are configuring a new ADN installation, you do not need to worry about keeping a network in operation and secure; no live traffic is going through the ADN nodes. You can choose either approach discussed below or you can create your own custom approach.

- Breadth-first: This is the operation-centric approach, where each operation is done on each ADN node before the next operation is started. For more information, see "Upgrading using the Breadth-First Approach" on page 13.

- Rolling: This is the device-centric configuration, where a set of operations is done to a specific device before you move to the next device. The rolling approach works best when there's a clear separation of roles; for example, you have dedicated managers, concentrators, and branches. You don't have ADN nodes that function as both managers and concentrators. The recommended upgrade order for the rolling approach is to upgrade the ADN managers first, then the concentrators, and the branches last. This method allows deployment in staged manner. For more information, see "Upgrading using the Rolling Approach" on page 14.

Note that you must be at SGOS 5.1.3.3 or higher if you want to keep the network in operation during the upgrade.

New System Defaults

On a new system or a newly upgraded system, default settings are for insecure mode operation. Security must be explicitly enabled. The backwards-compatible ADN manager runs on the existing plain ADN manager port. This manager can handle ADN nodes running both SGOS 5.1.4 and SGOS 5.1.3.

- Advertised, explicit, routes are used (Connect transparent is enabled, but the prefer transparent setting is disabled.) Servers where explicit routes exist are routed through explicit tunnels.
- Security settings:
  - Authentication and authorization are disabled until a valid profile is selected.
  - ADN routing and tunnel connection requests are unauthenticated.
  - All ADN protocol messaging and compressed application data are transferred in plaintext.
  - Device-auth-profile: **None**.

    The ADN device-auth-profile must be configured on the ADN managers before any outbound connections can be set to a secure mode on any ADN node.

    The profile also must be configured on all concentrators for a specific branch before securing any outbound tunnel connections on the branch.
  - Authorization: **Disabled**.

    Authorization can be enabled only if verify-peer option is enabled in the selected ADN device-auth-profile.
  - Manager-listening-mode: **Plain-Only**.

    The Manager-listening-mode on the ADN managers can be set to **Secure-only** if all ADN nodes secure their routing connections.
  - Tunnel-listening-mode: **Plain-Only**.

    Tunnel-listening-mode on a concentrator can be set to **Secure-only** if all branches connect to the concentrator through secure connections.
  - Secure-outbound: **None**.
- Manager settings:
  - Pending-peers: **Enabled**

Upgrading using the Breadth-First Approach

The breadth-first approach requires that you do certain operations on each node before moving to the next node.

> **Note:** When upgrading to SGOS 5.1.4, backward compatibility is guaranteed only for devices running SGOS 5.1.3.3 or higher. Blue Coat appliances running SGOS 5.1.3.2 or lower must be upgraded to SGOS 5.1.3.3. Rolling back to SGOS 5.1.4 might not be possible after new features are enabled.

The overview for configuration is as follows:

1. Upgrade all ADN nodes to SGOS 5.1.4.
2. On each ADN node, configure the device authentication profile.

   Security parameters switch to authentication defaults after the device is configured with the device authentication profile:

   - Device-auth-profile: Set to the desired profile.
   - Authorization: **Enabled**, unless you disabled the authorization checkbox.

     If authorization is enabled, make sure the ADN managers' device IDs are entered.
   - Manager-listening-mode: **Both**.
   - Tunnel-listening-mode: **Both**.
   - Secure-outbound: **Secure-Proxies**.

   > **Note:** If you are upgrading a network with live ADN traffic, reset secure-outbound to **None** to avoid potential ADN service outages. Otherwise, you can continue with the procedures below.

   For more information, refer to "Device Authentication" and "Configuring an Application Delivery Network" in *Volume 6: Advanced Networking*.
3. Pre-configure the approved-peers list on each ADN manager.

   If a backup manager exists, the backup manager should be added to the approved-peers list on the ADN manager; in that case, the ADN manager should be added to the approved-peers list on the backup manager.
4. Enable outbound security on each ADN node:

   a. Secure-outbound: This setting can be configured to **Routing-only**, **Secure-proxies**, or **All**.

      When routing connection security is enabled, each node re-connects to the ADN managers using the secure protocol.

      - If the secure-outbound option is set to **Secure-proxies**, all future outbound secure-proxy connections are secured.

- If Secure-outbound is set to **All**, all future outbound connections are secured. Existing non-secure-proxy connections are upgraded to secure mode automatically. This is the most secure mode, allowing all ADN plain listeners to be disabled.

  Configure secure-outbound to at least **Routing-only**. If the routing managers are also branch nodes, configure secure-outbound to **Secure-proxies** or **All**.

5. Tighten up security by shutting down any unneeded plain (unsecured) listeners on each node:

   a. Manager-listening-mode: Configure this setting to **Secure-only** on each ADN manager.

      This setting can be selected only if the secure-outbound option is anything other than **None** on the ADN nodes. Note that you cannot select this option if you have SG Clients on the network.

   b. Tunnel-listening-mode: configure tunnel listening mode to **Secure-only** on each node.

      Tunnel listening mode can be set to **Secure-only** on each node if no other ADN branches or SG Clients attempt to connect to this concentrator through plain (unsecured) tunnel connections.

   For more information, refer to “Configuring an Application Delivery Network” in *Volume 6: Advanced Networking*.

Upgrading using the Rolling Approach

The rolling approach requires that you complete all pertinent operations on each node before configuring the next node.

Note: You must be at SGOS 5.1.3.3 or higher to upgrade if you want to keep the network in operation during this time. The systems that are used as the ADN manager and the backup ADN manager must be upgraded to SGOS 5.1.4 before any other upgrades are done.

ADN Manager Upgrade

Complete each step below for the ADN manager and backup ADN manager:

1. Upgrade the appliances to SGOS 5.1.4.
2. Configure the device authentication profile.

   Security parameters switch to authentication defaults after the device is configured with the device authentication profile:

   - Device-auth-profile: Set to the desired profile.
   - Authorization: **Enabled**, unless you disabled the authorization checkbox.

     If authorization is enabled, make sure the ADN managers’ device IDs are entered on the **Configuration > App. Delivery Network > General > Security** tab.
   - Manager-listening-mode: **Both**.
   - Tunnel-listening-mode: **Both**.
   - Secure-outbound: **Secure-Proxies**.

> **Note:** If you are upgrading a network with live ADN traffic, reset secure-outbound to **None** to avoid potential ADN service outages.

For more information, refer to "Device Authentication" and "Configuring an Application Delivery Network" in *Volume 6: Advanced Networking*.

3. Configure the Manager-listening-mode to **Secure-only**.

> **Note:** Do not do this step until all nodes have been upgraded and the secure-outbound option has been set to secure routing connections. If you attempt to do this step before configuring all other nodes, the nodes fail to connect to the secure manager port.

This setting can be selected only if the secure-outbound option is anything other than None on the ADN nodes. Note that you cannot select this option if you have SG Clients on the network.

4. Configure the approved-peers list, if authorization is enabled, to avoid potential temporary ADN service outage on a node.

For more information, refer to "Configuring an Application Delivery Network" in *Volume 6: Advanced Networking*.

ADN Node Upgrade

Avoid making changes to ADN configuration on any ADN nodes until both managers have been upgraded to 5.1.4 and configured.

> **Note:** The recommended approach to upgrading the ADN nodes is to configure all concentrators first, followed by the branch appliances.

The overview for upgrading one ADN node is as follows:

1. Upgrade the appliance to SGOS 5.1.4.
2. Bring up the ADN node and complete basic ADN configuration. For more information, refer to "Configuring an Application Delivery Network" in *Volume 6: Advanced Networking*.
3. Configure the device authentication profile.

   Security parameters switch to authentication defaults after the device is configured with the device authentication profile:

   - Device-auth-profile: Set to the desired profile.
   - Authorization: **Enabled**, unless you disabled the authorization checkbox.

     If authorization is enabled, make sure the ADN managers' device IDs are configured.
   - Manager-listening-mode: **Both**.
   - Tunnel-listening-mode: **Both**.
   - Secure-outbound: **Secure-Proxies**.

Note: If you are upgrading a network with live ADN traffic, reset secure-outbound to **None** to avoid potential ADN service outages.

For more information, refer to *Volume 6: Advanced Networking*.

Enabling the Secure-outbound Security Option

This setting can be configured to **Routing-only**, **Secure-proxies**, or **All**.

- When routing connection security is enabled, each node re-connects to the ADN managers using the secure protocol.
- If the secure-outbound option is set to Secure-proxies, all future outbound secure-proxy connections are secured.
- If Secure-outbound is set to all, all future outbound connections are secured. Existing non-secure-proxy connections are upgraded to secure mode automatically. This is the most secure mode, allowing all ADN plain listeners to be disabled.

Setting Tunnel Listening Mode to Secure-Only

The tunnel listening mode can be set to **secure-only** if no other ADN branches or SG Clients attempt to connect to this concentrator through plain (unsecured) tunnel connections.

For more information, refer to “Configuring an Application Delivery Network” in *Volume 6: Advanced Networking*.

Downgrading an ADN Network

To downgrade your network, reverse the steps you did to upgrade. Note that any attempt to enable tunnel security on a down-versioned branch fails and the connection is closed.

Authentication

If you use COREid authentication, there are several important issues to be aware of. If you use IWA, COREid, or Netegrity, and want to use multiple versions of the BCAAA authentication service, read the “Upgrading the BCAAA Authentication Service” section to install the multiple versions correctly.

COREid Authentication

COREid: When the Oracle COREid 6.5 WebGate server software is upgraded to Oracle COREid 7.0, the single sign-on feature might stop working even if the IPValidation value in the WebGate configuration file (WebGateStatic.lst) is set to `false` by the administrator afterwards. The workaround is to uninstall and reinstall the Oracle COREid 7.0 WebGate software, and set IPValidation to `false`. Then restart the COREid Access server and the IIS server.

Upgrading the BCAAA Authentication Service

If you use one of the following authentication realms, you should upgrade to the latest release of the Blue Coat Authentication and Authorization Agent (BCAAA) service.

❐ Integrated Windows Authentication

❐ Oracle COREid

❐ Netegrity Siteminder

BCAAA is distributed as a zip file or UNIX shell script, to be installed on a Microsoft® Windows® system or a Solaris™ system. The zip file to download the BCAAA service is posted on the SGOS 5 Software Download Page at http://download.bluecoat.com/release/SGOS5/index.html.

Using Multiple Versions of the BCAAA Service

You can run multiple versions of the BCAAA service. Depending on the versions of BCAAA that you want to run, you might have to install different versions of the service. Each version of the BCAAA service that you want to run must reside on your system.

> **Note:** You cannot use an older version or a newer version than your proxy expects. For example, you must install BCAAA version 100 for SGOS 4.2.1; BCAAA version 110 for SGOS 4.2.2, or BCAAA version 120 for SGOS 4.2.3.

Table 3-1. Supported Versions of the BCAAA Service

SGOS Version	BCAAA Version Supported
SGOS 3.2.6	Upgrade to BCAAA version 99 http://download.bluecoat.com/PR/SG4/4.1.3/24757_SG4.1.3.20_bcaaa.zip or higher http://download.bluecoat.com/release/SGOS4/index.html
SGOS 4.1.x	Upgrade to BCAAA version 99: http://download.bluecoat.com/PR/SG4/4.1.3/24757_SG4.1.3.20_bcaaa.zip or higher http://download.bluecoat.com/release/SGOS4/index.html
SGOS 4.2	100 (Download from: http://download.bluecoat.com/release/SGOS4/index.html
SGOS 4.2.2	110 (Download from http://download.bluecoat.com/release/SGOS4/index.html
SGOS 5.1.1.x	100 (Download from http://download.bluecoat.com/release/SGOS5/index.html)
SGOS 5.1.2	100 (Download from: http://download.bluecoat.com/release/SGOS5/index.html)
SGOS 5.1.3	110 (Download from http://download.bluecoat.com/release/SGOS5/index.html)

Install the lowest version of the BCAAA service first and the highest version of BCAAA last, allowing each version to uninstall the previous version. This leaves behind the `bcaaa.ini` and `bcaaa-nn.exe` files for that version.

Notes

- Only one listening port is used, no matter how many versions you are running. The BCAAA service hands off the connection to the appropriate BCAAA version.
- Installation instructions for BCAAA are located in *Volume 5: Securing the Blue Coat SG Appliance* in the *Blue Coat SG Appliance Configuration and Management Guide Suite* documentation suite that is accessible through WebPower account access.
- The BCAAA service cannot be installed on Windows NT.
- The firewall on Windows systems must be disabled for the BCAAA service to work. If the firewall is enabled, the SG appliance won't be able to connect to BCAAA.

Documentation References

- *Volume 5: Securing the Blue Coat SG Appliance*

Bridging

Changes to bridging include:

- You can no longer configure a bridge during initial configuration of the system.
- A bridge is now considered to be a set of assigned interfaces and does not have an IP address.
- Interfaces are no longer identified by ports.
- Interface configuration is no longer done in the bridge editing submode.

Bridge IP Addressing

Bridges do not have IP addresses. In previous releases, the bridge took over the IP address of the first interface. Now, the bridge is simply considered to be the set of all assigned interfaces. Each interface can have its own optional IP address. The routing decision is based on the interface's IP address; the bridging code ensures that outgoing packets go through the right interface.

Interface Changes

Interfaces are no longer attached to the bridge ports.

Interfaces Are Not Configured Using the Bridging Feature

Because a bridge is considered to be a set of assigned interfaces, you cannot configure interfaces using the bridge editing submode. All interface configuration is done using the `#(config) interface` command.

Upgrade Behavior

The bridge-related settings have been migrated from previous SGOS releases to SGOS 5.1.3. The behavior changes include:

- IP address, subnet: These have been moved to the lowest- numbered interface attached to the bridge.

- mtu-size: On upgrade, mtu-size from a SGOS 4.2.x bridge is reflected to all the interfaces that belong to the bridge on SGOS5.1.3.
- accept-inbound. On upgrade, accept inbound settings from a SGOS 4.2.x bridge are reflected to all the interfaces that belong to the bridge on SGOS 5.1.3. In SGOS 5.x, it has been renamed `reject-inbound`.
- speed: Speed is upgraded for both software and hardware bridges. In the case of hardware bridges, the speed from the first port of a hardware bridge on SGOS 4.2.x is copied onto both interfaces belonging to the hardware bridge on SGOS 5.1.3. In the case of a software bridge, speed is copied over from each port of a software bridge on SGOS 4.2.x to the corresponding interface of the software bridge on SGOS 5.1.3.
- half-duplex/full-duplex: Duplex (half-duplex/full-duplex) is upgraded incase of both software and hardware bridges. In the case of hardware bridges, the duplex from the first port of a hardware bridge on SGOS 4.2.x is copied onto both interfaces belonging to the hardware bridge on SGOS 5.1.3. In the case of a software bridge, duplex is copied over from each port of a software bridge on SGOS 4.2.x to the corresponding interface of the software bridge on SGOS 5.1.3.
- link-autosense: Link-autosense is upgraded incase of both software and hardware bridges. In the case of hardware bridges, the link-autosense, if set on the first port of a hardware bridge on SGOS 4.2.x, it is reflected onto both interfaces belonging to the hardware bridge on SGOS 5.1.3. In the case of a software bridge, link-autosense, if set for a particular port of a software bridge on SGOS 4.2.x, it is reflected to the corresponding interface of the software bridge on SGOS 5.1.3.
- static-fwtable-entry: Static forwarding entries are migrated from each of the individual ports on SGOS 4.2.x to the corresponding interfaces on SGOS 5.1.3.
- instructions (PAC Files): Incase of hardware bridges, instructions from an SGOS 4.2.x bridge are automatically upgraded onto the first interface of the hardware bridge in SGOS 5.1.3. In the case of software bridges, instructions from a SGOS 4.2.x bridge are upgraded onto an interface with an IP address and that belongs to that bridge in SGOS 5.1.3.

Downgrade Behavior

Downgrade is not supported.

Documentation References

- *Volume 2: Getting Started*

Bypass Lists

If you upgrade to SGOS 5.x from SGOS 4.x, entries from the central and local bypass lists are migrated to the static bypass list. Because the static bypass list does not support listing gateways, any central or local bypass entries that included a gateway are converted to static route entries in the static route table. The converted static route entries are appended after the existing static route entries. Duplicate static route entries are silently ignored. (See "Services" on page 22 for more information on new bypass list behavior.

All traffic leaving the SG appliance is affected by the static route entries created from the SGOS 4.x bypass lists, not just traffic that matches that particular bypass list entry.

Several parameters of bypass lists are renamed in SGOS 5.1:

- `server_bypass_threshold` is now `server-threshold`. This contains the maximum number of client entries for a particular server before all client entries are collapsed into a wildcard entry that bypasses all clients going to that particular server. Default value remains at 16; the range is 1..256
- `max_dynamic_bypass_entry` is now `max-entries`. This defaults to 10000; the valid range is 100 to 50000.
- `dynamic_timeout` is now `timeout`. This defaults to 60 minutes and has a range between 1 and 86400 minutes.

Downgrade Behavior

Bypass list downgrade is not supported in 5.1.1.

CLI commands that are no longer used in SGOS 5.x include:

```
#show bypass-list <cr>
#(config) bypass-list central-path <url> <cr>
#(config) bypass-list local-path <url> <cr>
#(config) bypass-list no central-path <cr>
#(config) bypass-list no local-path <cr>
#(config) bypass-list no notify <cr>
#(config) bypass-list no subscribe <cr>
#(config) bypass-list notify <cr>
#(config) bypass-list poll-now <cr>
#(config) bypass-list subscribe <cr>
#(config) inline bypass-list central <eof marker> <cr>
#(config) inline bypass-list local <eof marker> <cr>
#(config) load bypass-list central <cr>
#(config) load bypass-list local <cr>
```

Documentation References

- *Volume 3: Proxies and Proxy Services*, Chapter 3

CIFS

The CIFS proxy on the SG appliance combines the benefits of the CIFS protocol with the abilities of the appliance to improve performance, reduce bandwidth, and apply basic policy checks. This solution is designed for branch office deployments because network administrators can consolidate their Windows file servers (at the core office) instead of spreading them across the network.

Upgrade Behavior

Systems that are upgraded from versions of SGOS that do not have a CIFS proxy behave the same as new systems in that they receive a default set of SMB services and settings; existing services listening on the default SMB TCP ports are not overwritten.

Downgrade Behavior

Downgrading to an SGOS 4.x has no effect on the box, except that the CIFS proxy is not available. The next time the upgrade is done, the settings from the previous upgrade will still exist.

Documentation References

- "Services" on page 22
- *Volume 3: Proxies and Proxy Services*

Content Filtering

One new content filtering vendor has been added for SGOS 5.x: The Internet Watch Foundation (IWF). This new vendor causes no upgrade issues. On a downgrade, the vendor `none` is selected instead of any unsupported choice.

Documentation References

- *Volume 8: Managing Content*, Chapter 2

Policy

CPL

The following properties have been added to the CPL to support Application Delivery Networks (ADN):

```
adn.server.optimize(yes|no|byte_cache|compress)
adn.server.optimize.inbound(yes|no|byte_cache|compress)
adn.server.optimize.outbound(yes|no|byte_cache|compress)
```

The following CPL syntax is being deprecated in favor of the ADN tunnel features.

```
socks.allow_compression(yes|no)
socks_gateway.request_compression(yes|no|default)
```

You can still use the deprecated syntax, but you will receive a warning.

The following conditions and properties have been added to the CPL to support QoS:

Conditions

```
server.connection.dscp( )
client.connection.dscp( )
```

Properties

```
server.connection.dscp( )
client.connection.dscp( )
```

Documentation References

- *Volume 11: ProxySG Content Policy Language Guide*

VPM

The following object has been added to VPM to support Application Delivery Networks (ADN):

- ADN Server Optimization

The following objects have been added to VPM to support QoS:

- **Client Connection DSCP Trigger** (Source)

- **Server Connection DSCP Trigger** (Destination)
- **Set Client Connection DSCP Value** (Action)
- **Set Server Connection DSCP Value** (Action)

Object Naming

Objects that can be named by the user no longer start with "_" (underscore character). The underscore character prefix is now used for internally-generated names to prevent name collisions between objects that can be named by the user and internally generated names.

Cipher and Cipher Strength

Prior to the SGOS 4.2 release, the objects Cipher and Cipher Strength objects didn't have a Name entry field and had only fixed internal names. The internal names were something like __Cipher1 for the Cipher object and __CipherStrength1 for the Cipher Strength object.

Effective with SGOS 4.2, you can modify or change the names of these objects.

When preexisting Cipher and Cipher Strength objects are upgraded, these objects display the internal names with prefix ì__î. The underscore in the prefix is not a problem as long as you do not edit the object, and the object compiles properly when installing. If you modify an object with a name that includes the prefix "__", VPM will prompt you to remove this prefix.

Documentation References

- *Volume 7: VPM and Advanced Policy*, Chapter 2

Services

The services framework (the infrastructure used to manage proxy services) has been revamped to, among other things, support multiple listeners and ports for each service.

New features in services include:

- Multiple Listeners Per Service: A proxy service is comprised of one or more listeners. Each listener can be configured to intercept a particular destination IP subnet and port range. This provides considerable power in intercepting specific application data streams and protocols on the network.
- Port Ranges: A listener can now contain a port range. Since a service can have multiple listeners, many port ranges can be used for a particular service.
- Subnet Ranges: A listener can match
  - all traffic
  - only traffic that is not destined to the SG appliance (Transparent)
  - traffic specifically destined to the SG appliance (Explicit)
  - traffic that is destined to a particular IP address or subnet.
- Default Service: The default service matches all TCP traffic not otherwise matched by other service listeners. This provides the option to intercept all TCP traffic on the network so it can be accelerated and controlled by enforcing company policy on the traffic.

- Service Names in Policy: Each proxy service now requires a name. This name can contain spaces and can be used as a token in policy. This provides an easy mechanism to identify particular traffic flows in policy.
- Static Bypass: The static bypass is no longer an installable list. It is now configured under the Proxy Services and bypasses both TCP and UDP traffic.
- Separation of Console and Proxy Services: The console and proxy services are now configured using different commands. To configure a console service from the CLI, use the `console-services` command. To configure a proxy service from the CLI, use the `proxy-services` command. The services have separate GUI pages as well (**Configuration > Services > Proxy Services**, **Configuration > Services > Console Services**).

Upgrade Behavior

On upgrade, the old services configuration is upgraded to the new service framework. The new services name contain the old services type and generate a name with one of the following formats

- If there are more than one service with identical properties, one service is created with multiple listeners when upgraded. For example Yahoo IM has two service ports in SGOS 4.2, one on 5050 and one on 5101. Instead of creating two services, one service is created with two listeners.
- If there is only one proxy handler then the upgraded name should be the name indicated in the table located in section 2.4.1.3 Proxy Attribute List.
- If there are multiple proxies of the same type in the table, then the upgrade uses the format <proxy_name>-<number>. For example, if you had two HTTP services, the new names are HTTP-1 and HTTP-2.
- On upgrade, only the new SGOS 5.x services are added. Services that were purposefully deleted in SGOS 4.2 are not re-added in the upgrade.

Most attributes directly translate to the new services framework. The exceptions are:

- Application Delivery Networks (ADN) attributes are disabled
- The tunnel proxy attribute **detect protocol is** disabled.
- The transparent and explicit attributes are removed.
- the **send-client-ip** attribute in SGOS 4.2 maps directly to **reflect-client-ip** in SGOS 5.x.

Documentation References

- *Volume 3: Proxies and Proxy Services*

SSL

The ssl-verify-server under HTTP and the corresponding CLI and Management Console commands have been removed. If you are running SGOS 4.2.1.6 and you set this flag to no, then, after upgrade to SGOS 5.1.1 you must manually write the following policy to restore pre-upgrade server certificate verification behavior.

```
<ssl>
  server.certificate.validate(no)
```

The same policy can be created using the **SSL Access** layer in VPM and selecting the **Server certificate validation** object from the Action column.

Documentation References

- *Volume 3: Proxies and Proxy Services*

Statistics

- Persistent bandwidth statistics are not preserved on upgrade from SGOS 4.x. These statistics are now computed differently.
- Persistent statistics are kept differently in SGOS 5.x and SGOS 4.x. Statistics are imported (subject to the above limitation) on first upgrade. After that, SGOS 5.x statistics shows gaps when SGOS 4.x is running and vice-versa.

Documentation References

- *Volume 10: Managing the Blue Coat SG Appliance*