Blue Coat Systems, Inc.
ProxySG Operating System v4.2.5.1

Security Target

Evaluation Assurance Level: EAL2+
Document Version: 0.94

Prepared for:

Blue Coat Systems, Inc.
420 N. Mary Avenue
Sunnyvale, CA 94085
Phone: (408) 220-2200

http://www.bluecoat.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050

http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2007-01-05	Darryl H. Johnson	Initial draft.
0.2	2007-01-29	Darryl H. Johnson	Made additions/revisions to reflect Management Console web interface and other new capabilities.
0.3	2007-02-07	Darryl H. Johnson	Incorporated customer feedback regarding consistent description of the various administrators and administrative access methods, account lockout parameters, and secure network paths.
0.4	2007-03-12	Darryl H. Johnson	Addressed issues from lab in “DOMUS OR 01” (2007-02-12)
0.5	2007-03-19	Darryl H. Johnson	Incorporated lab/customer feedback regarding SOF and network path vulnerabilities.
0.6	2007-03-26	Darryl H. Johnson	Addressed minor editorial issues.
0.7	2007-03-29	Darryl H. Johnson	Addressed comments from evaluator.
0.8	2007-06-25	Justin Dubbs Nathan Lee	Added SSH and SSL exclusion. Changed the product version number.
0.9	2007-07-24	Elizabeth Pugrud	Address issues from lab in “DOMUS OR 06,” 2007-06-28.
0.91	2007-09-13	Elizabeth Pugrud	Updated TOE version number throughout.
0.92	2007-10-03	Elizabeth Pugrud	Updates to assumptions and objectives based on DOMUS OR 08, July 13, 2007.
0.93	2007-10-19	Nathan Lee	DOMUS OR 9: Updated A.PASSWORD and OE.PASSWORD to harmonize them with the AVA’s SOF.
0.94	2007-10-19	Nathan Lee	DOMUS OR 9: Deleted Sections 8.8.1 and 8.8.2 as no SOF calculations or proof are required in the ST.

Table of Contents

Table of Figures

List of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), ST conventions, ST conformance claims, and the ST organization. The Target of Evaluation is the Blue Coat ProxySG Operating System v4.2.5.1, and will hereafter be referred to as SGOS or the TOE throughout this document. The TOE is a proprietary operating system developed specifically for use on a hardware appliance that serves as an Internet proxy. The purpose of the appliance is to provide a layer of security between an Internal and External Network (typically an office network and the Internet).

1.1 Purpose

This ST contains the following sections to provide mapping of the Security Environment to the Security Requirements that the TOE meets in order to remove, diminish, or mitigate the defined threats:

- Security Target Introduction (Section 1) – Provides a brief summary of the content of the ST and describes the organization of other sections of this document.
- TOE Description (Section 2) – Provides an overview of the TOE security functions and describes the physical and logical boundaries of the TOE.
- Security Environment (Section 3) – Describes the threats and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Security Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE and by the TOE's environment.
- TOE Summary Specification (Section 6) – Describes the security functions provided by the TOE to satisfy the security requirements and objectives.
- Protection Profile Claims (Section 7) – Provides the identification of any ST Protection Profile (PP) claims as well as a justification to support such claims.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target, TOE and CC Identification and Conformance

Table 1 – ST, TOE, and CC Identification and Conformance

ST Title	Blue Coat Systems, Inc. ProxySG Operating System v4.2.5.1 Security Target
ST Version	Version 0.94
Author	Corsec Security, Inc. Darryl H. Johnson and Nathan Lee
TOE Identification	Blue Coat ProxySG Operating System v4.2.5.1
Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 (aligned with ISO/IEC 15408:2005); CC Part 2 extended; CC Part 3 augmented; PP claim (none); Parts 2 and 3 Interpretations from the Interpreted CEM as of 2007-01-05 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+
Keywords	Proxy, Blue Coat, Gateway, Traffic Filtering, Content Filtering, Transparent Authentication, Proxy SFP, Web Security, Safe Browsing

1.3 Conventions, Acronyms, and Terminology

1.3.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The Common Criteria for Information Technology Security Evaluation (CC) allows for several operations to be performed on security requirements: assignment, refinement, selection, and iteration. All of these operations are used within this ST. These operations are presented in the same manner in which they appear in Parts 2 and 3 of the CC with the following exceptions:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [*underlined italicized text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Iterations are identified by appending a letter in parenthesis following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

1.3.2 Acronyms and Terminology

The acronyms and terms used within this ST are described in Section 9 – "Acronyms."

2 TOE Description

This section provides a general overview of the TOE as an aid to understanding the general capabilities and security requirements provided by the TOE. The TOE description provides a context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product Type

The Blue Coat ProxySG Operating System v4.2.5.1 (SGOS) is a proprietary operating system developed specifically for use on a hardware appliance that serves as an Internet proxy. The purpose of the appliance is to provide a layer of security between an Internal and External Network (typically an office network and the Internet).

2.2 Product Description

SGOS is delivered on one of several appliances manufactured by Blue Coat Systems. These appliances include the SG200, SG510, SG810, and SG8100 lines of products. Every appliance runs the same TOE software binary image. Differences in each model are to allow for different performance and scalability requirements in each customer site.

Figure 1 below shows the details of a typical enterprise deployment scenario.

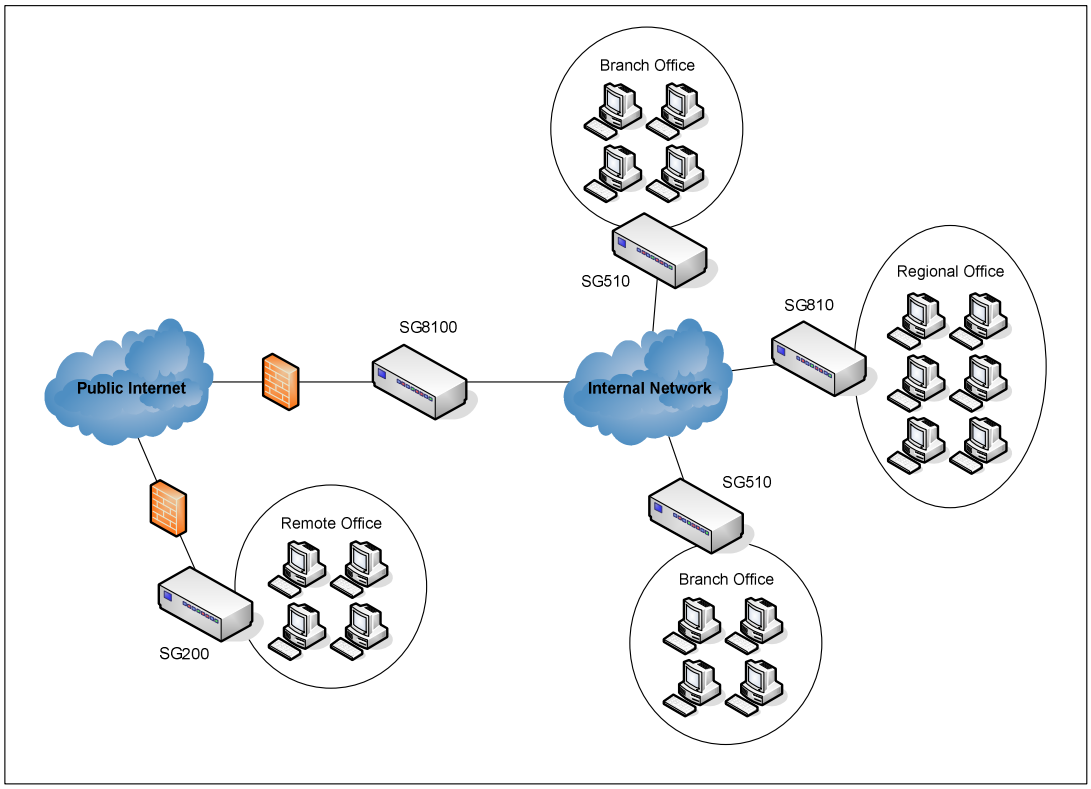

Figure 1 – Typical Enterprise Deployment of the TOE

The security provided by the SGOS can be used to control, protect, and monitor the Internal Network's use of controlled protocols on the External Network. The controlled protocols implemented in the evaluated configuration are:

- Hypertext Transfer Protocol (HTTP)
- File Transfer Protocol (FTP)
- SOCKS
- Instant Messaging (AOL, Microsoft Network, and Yahoo!)

Control is achieved by enforcing a configurable policy (Proxy SFP[1]) on controlled protocol traffic to and from the Internal Network users. The policy may include authentication, authorization, content filtering, and auditing.

2.2.1 SGOS Concepts

2.2.1.1 Administrative Access

Administrative access to the TOE is provided by the ProxySG Serial Console. Users access the Serial Console using a terminal emulator over a direct serial connection to the appliance. The Serial Console controls access to the Setup Console (used for initial configuration only) and the Command Line Interface (CLI), which is used for normal administrative operations. The Serial Console offers a menu with choices for the Setup Console and the CLI.

2.2.1.2 Initial Configuration

The TOE must be configured using the Setup Console before it is installed into the client's network. The Setup Console is used to specify the IP address, subnet mask, default gateway, Domain Name System (DNS) server, the Console username and password, and the Setup Console password. Note that in this evaluated configuration, once the TOE is operational, the Setup Console is no longer used. Access to the Setup Console is mediated by the Serial Console and (in the evaluated configuration) is protected by a password. Additional configuration and policy definition is done through the CLI by selecting the CLI from the Serial Console menu.

2.2.1.3 Security Functional Policies

After initial configuration, the TOE is considered operational and behaves as a proxy that, by default, denies all traffic. To enable controlled protocol traffic flow, an authorized administrator defines information flow policy rules, which comprise the Proxy SFP.

These rules can require authentication of End Users. An authorized administrator creates End Users by using the management interfaces to create unique user accounts in a local user list. End Users can be granted administrative privileges by defining access control policy rules, which comprise the Administrative Access SFP.

The policy rules that define the Proxy SFP and Administrative Access SFP are expressed using the syntax and rules described in the Blue Coat Systems, Inc. ProxySG Content Policy Language Guide, 4.2.5 (Document Number 231-02780).

2.2.1.4 Explicit and Transparent Network Environments

In order to act as a proxy and manage controlled protocol traffic between the Internal and External Network, all of the targeted traffic must flow through the appliance. Arranging for controlled protocol traffic to flow through the appliance requires configuration of the organization's network environment. There are two kinds of network deployments: explicit and transparent. In an explicit deployment, the users' client software (e.g. a web browser) is configured to access the External Network via the proxy. The client software presents the traffic to the Internal Network port of the proxy for service. In a transparent deployment, the network and proxy are configured so that the proxy can intercept controlled protocol traffic intended for the External Network. The users' software is not changed and the user may be unaware that controlled protocol traffic is passing through the proxy.

[1] SFP – Security Functional Policy

2.2.1.5 Deployment Configurations

ProxySG appliances are deployed in two different configurations: Forward Proxy Deployment (or Gateway Proxy) and Reverse Proxy Deployment (or Server Proxy). The Forward Proxy deployment is more common for customers, and allows a ProxySG device to apply policy rules for clients in a single area such as an office or local area network (LAN).

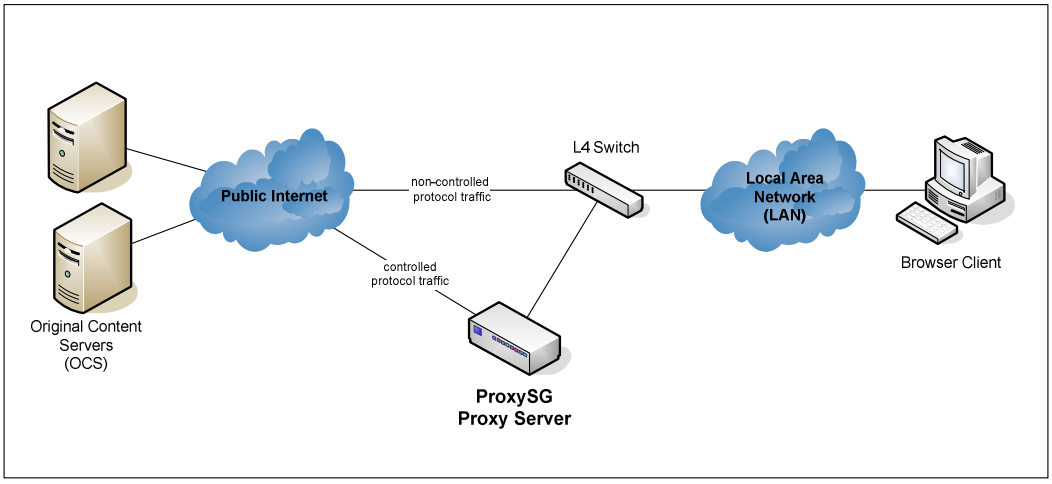

Figure 2 – Forward (Gateway) Proxy Deployment

In the Forward Proxy deployment (depicted in Figure 2 above), all controlled protocol traffic flows through the ProxySG, forcing browsers to access all Original Content Servers (OCS) through the ProxySG. This allows ProxySG to act as a policy enforcement node before serving up web pages. A layer-four switch can redirect all other traffic around the ProxySG. In this configuration, non-controlled protocol traffic flows normally and clients are unaware of the existence of the proxy. Thus, no client configuration is required after ProxySG installation.

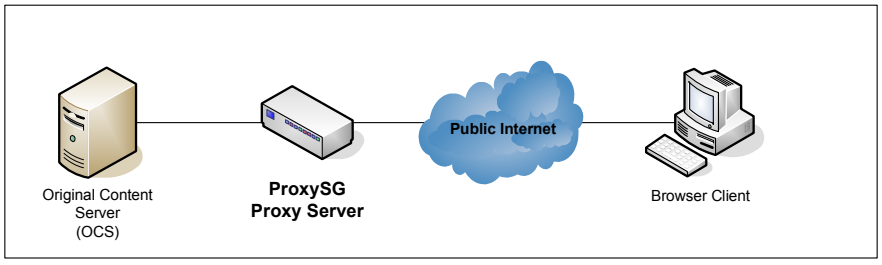

Figure 3 – Reverse (Server) Proxy Deployment

In the Reverse Proxy deployment, a ProxySG is associated with an OCS web server (as depicted in Figure 3 above). The ProxySG can cache and deliver pictures and other non-variable content rapidly, offloading those efforts from the OCS. This frees the OCS to perform application-based services (such as dynamic web page generation).

2.2.1.6 Protection of TOE Assets and Functions

The assets of the TOE are the:

- Local user list
- Proxy SFP rules
- Administrative Access SFP rules
- Audit logs
- System configuration

The two primary security capabilities of the TOE are (1) restricting controlled protocol traffic between the Internal and External Networks and (2) managing the SGOS. The tangible assets and management functions are protected by restricting access to administrators. Only administrators can log into the TOE management interfaces, access the SGOS configuration, and configure policies.

2.3 TOE Boundaries and Scope

This section addresses what physical and logical components of the TOE are included in evaluation. Figure 4 illustrates the physical and logical boundaries of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

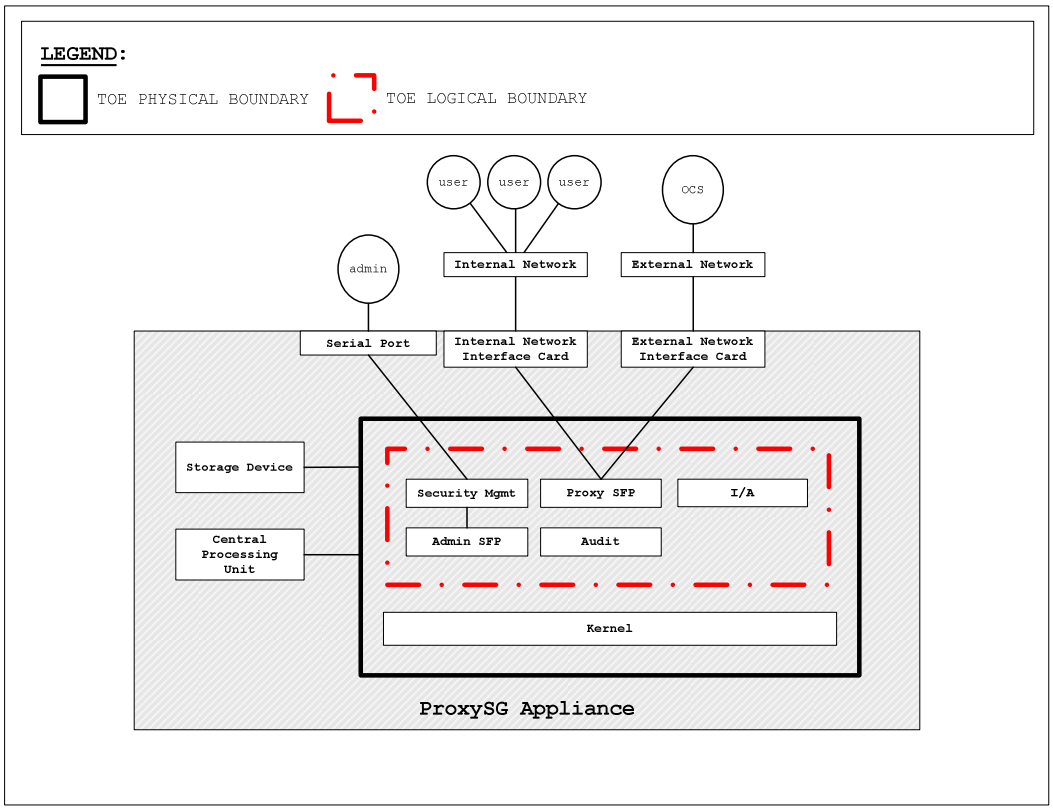

Figure 4 – TOE Physical and Logical Boundaries

2.3.1 Physical Boundary

The TOE is a proprietary operating system which runs on custom, purpose-built hardware. The physical boundary includes the kernel and all of the security and management engines of the SGOS. The kernel provides the basic

operating system functions, including system resource management and communications between the hardware and software.

2.3.1.1 TOE Environment

The TOE is intended to be deployed in a physically secured data center with the appropriate level of physical access control and physical protection (e.g. fire control, locks, alarms, etc.). Access to the physical console port on the appliance itself should be restricted via a locked data cabinet within the data center as well. The TOE is intended to be managed by administrators operating under a consistent security policy.

The TOE provides a layer of security between an Internal and External Network, and is meant to control, protect, and monitor the Internal Network's use of controlled protocols on the External Network. For this to operate correctly, all plaintext controlled protocol traffic must traverse the appliance on which the TOE runs. The TOE environment is required to provide for this configuration.

2.3.2 Logical Boundary

The logical boundary includes the security and management engines of SGOS (see Figure 4**)** which address the security functional requirements imposed on the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- User Data Protection
- Identification and Authentication
- Protection of the TOE Security Function (TSF)
- Security Management

2.3.2.1 Security Audit

The SGOS has two separate auditing capabilities to provide an audit trail of security relevant events. These are System Event Logging and Access Logging. The System Event Log records system boot events, authentication events, changes to the SGOS configuration, and errors like failed communication to external devices. The System Event log can be viewed by Privileged Administrators.

Access Logging makes a record of all controlled protocol traffic that enters the TOE. An administrator can specify exactly what information goes into these records. Standard logging formats like SQUID and NCSA[2] are provided for convenience, and custom log formats can be defined using W3C[3]. Depending on the policy, the SGOS can create multiple log files for different policy actions. For example, single user actions or group actions can be logged where necessary. If an audit log ever fills to its configured capacity, the oldest records will be overwritten with new records. Access logs can be transferred to another machine (as configured by an administrator) for analysis.

2.3.2.2 User Data Protection

User data protection defines how users of the TOE are allowed to perform operations on objects.

The TOE provides authorized administrators with the ability to define security policies using the ProxySG Content Policy Language (CPL). The CPL provides for the creation of rules that perform certain actions based on a set of conditions. The conditions and actions depend on the kind of policy being written. Policies written in CPL are evaluated according to the rules described in the Blue Coat Systems, Inc. ProxySG Content Policy Language Guide, 4.2.3 (Document Number 231-02780).

[2] NCSA – National Center for Supercomputing Applications

[3] W3C – World Wide Web Consortium

2.3.2.2.1 Administrative Access Control Policy

An Administrative Access SFP is defined by the system administrator to control access to the administrative functions of the TOE. The conditions for these policies can be constructed from attributes of the request, such as user identity and kind of access needed (read-only or read/write). Other attributes include time of day and date. The actions include requiring an authenticated session and allowing or denying access.

2.3.2.2.2 Information Flow Protection (IFP) Policy

A Proxy SFP is defined by the system administrator to control controlled protocol traffic through the proxy appliance. The conditions can be constructed from a set of attributes including whether the traffic originated from the Internal Network or the External Network and any combination of characteristics of the controlled protocol traffic such as:

- User identity
- Universal Resource Locator (URL)
- Time
- Method (requested action)
- Content type
- HTTP compression
- Required bandwidth

SGOS also offers a policy-based feature called Apparent Data Type filtering. This feature identifies data content associated with Microsoft DOS[4] and Windows executable files. When used in a deny policy, drive-by installation of spyware is blocked. File types that are blocked include:

- Executable files (.exe)
- Data link libraries (.dll)
- OLE[5] custom controls (.ocx)
- Cabinet (compressed archive) files(.cab)

The actions that policies can take are allow, deny, require an authenticated session, select the authentication mode, rewrite a portion of the traffic (e.g. URL redirect), strip active content, present corporate instructions to End Users, and email a warning. For example, policies can be written to restrict access to certain URLs for some or all End Users, restrict traffic for specified URLs to authorized End Users or to specific times of day, or strip specific content types from controlled protocol traffic in either direction. These policies can be applied based on characteristics such as the user, group, time of day, and network address.

2.3.2.3 Identification and Authentication

The TOE provides the ability for administrators to manage the security functions of the TOE. The Identification and Authentication security function ensures that access to this management capability is restricted to authorized TOE administrators and protected by the entry of credentials. Administrators are assigned a role to determine what aspects of the TOE they are allowed to manage.

2.3.2.4 Protection of the TSF

The Protection of the TSF function provides the integrity and management of the mechanisms that protect the TSF. The SFRs in this evaluation are impossible to bypass because the TOE is designed in such a way that no access is possible without passing through key security features, such as identification and authentication and access control

[4] DOS – Disk Operating System

[5] OLE – Object Linking and Embedding

mediation. The TOE maintains its own domain for execution and does not share any hardware with other applications.

2.3.2.5 Security Management

The Security Management function provides administrators with the ability to properly manage and configure the TOE to store and access its IT[6] assets. Using a proprietary policy-drafting language, SGOS allows administrators to create Administrative Access SFP rules that grant and govern administrative access, and to create Proxy SFP rules that control the flow of controlled protocol traffic.

2.3.3 Excluded Features and Functionality

The following physical/logical features and functionality are not included in the evaluated configuration of the TOE:

- The following proxies:
  - Streaming proxies (Microsoft Media Server, Real Time Streaming Protocol)
  - Shell proxies (Secure Shell (SSH), telnet)
  - Peer-to-Peer (P2P) network proxies (BitTorrent, eDonkey, Gnutella, Kazaa)
  - Secure Sockets Layer (SSL) proxy
  - Transmission Control Protocol (TCP) Tunneling proxy
  - DNS proxy
  - Remote Procedure Call (RPC) Endpoint Mapper proxy
- Off-box content filtering and virus scanning
- Remote management via telnet
- Remote management via SSH
- Remote management via Management Console web interface
- Bridging (hardware and software)
- Dynamic and Static Bypass
- Refresh and Pipelining
- Internet Control Protocol (ICP) and Web Cache Control Protocol (WCCP)
- Visual Policy Manager
- Attack-detection
- Authentication realms other than “local”
- Clusters, fail-over, and chained proxies
- RADIUS[7] and TACACS+[8] splash pages
- Content-management commands
- syslog, health monitoring, health checks, heartbeats, and diagnostics
- Simple Network Management Protocol (SNMP) and Simple Mail Transfer Protocol (SMTP) alerts
- <forward> policy
- authenticate.mode() settings other than as described in this document
- Encrypted access logs
- Session Monitor
- Certificate Revocation Lists
- Dynamic Real-Time Rating (DRTR™)

[6] IT – Information Technology

[7] RADIUS – Remote Authentication Dial-In User Service

[8] TACACS+ – Terminal Access Controller Access Control System

3 Security Environment

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains:

- All assumptions about the secure usage of the TOE, including physical, personnel, and connectivity aspects
- All known and presumed threats countered by either the TOE or by the security environment
- All organizational security policies with which the TOE must comply

3.1 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The specific conditions listed in Table 2 below are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 2 – Assumptions

Assumption	Description
A.ENVIRON	The TOE is located in an environment that provides physical security, uninterruptible power, air conditioning, and all other conditions required for reliable operation of the hardware. Physical access to the appliance is restricted to authorized persons.
A.INSTALL	The SGOS device has been installed and configured according to the appropriate installation guides.
A.NETWORK	All plaintext controlled protocol traffic between the Internal and External Networks traverses the SGOS device; there is no other connection between the Internal and External Networks for plaintext controlled protocol traffic.
A.NO_EVIL_ADMIN	Administrators are non-hostile and follow all administrator guidance when using the TOE. Administration is competent and on-going.
A.PASSWORD	Passwords for administrative access to the TOE and for End User accounts are at least eight characters in length and comprise at least one letter (from a set of 26 upper-case letters and 26 lower-case letters), one special character or symbol (from a set of 32), and one number (from a set of 10).
A.PLATFORM	The hardware platform used to host the TOE supports all required SGOS functions, and is dedicated to supporting SGOS only.
A.SECURE_PATH	Security-related TOE data transmitted to and from the TOE over a network connection is protected from compromise by appropriate measures.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.

3.2 Threats to Security

Table 3 below identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings/parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings/parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution, and mitigation of the threats are through the objectives identified in Section 4 of this document.

Table 3 – Threats

Name	Description
T.EXTERNAL_NETWORK	A user or process on the Internal Network may access or post content on the External Network that has been deemed inappropriate or potentially harmful to the Internal Network.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T. TAMPERING	A user or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.
T.UNAUTHORIZED_ACCESS	A user may gain access to security data on the TOE for which they are not authorized according to the TOE security policy through the improper use of valid credentials.

3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. The specific security objectives are listed in Table 4 below.

Table 4 – Organizational Security Policies

Name	Description
P.ACTIVE_CONTENT	The TOE shall provide a means to remove active content (e.g. Java, JavaScript, ActiveX) in HTML[9] pages delivered via controlled protocols.
P.ADMIN	Only authorized individuals shall have the ability to perform administrative actions on the TOE.
P.AUDIT	The TOE shall record events of security relevance at the "basic level" of auditing. The TOE shall record the resulting actions of the Proxy SFP.
P.CONTENT_TYPE	End Users shall not access unauthorized content types via controlled protocols on the External Network.

[9] HTML – Hypertext Markup Language

Name	Description
P.FILTERED_URLS	End Users shall not access unauthorized URLs via controlled protocols on the External Network.
P.MANAGE	The TOE shall provide secure management of the system configuration, the Proxy SFP, and the Administrative SFP.
P.NON_ANONYMOUS	Access to some resources via controlled protocols on the External Network may be restricted to particular End Users.
P.POST_TYPE	End Users shall not post unauthorized content types to the External Network using controlled protocols.

4 Security Objectives

This section identifies the security objectives for the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the TOE's security needs.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 5 below.

Table 5 – Security Objectives for the TOE

Name	Description
O.AUDIT	The TOE must record events of security relevance at the "basic level" of auditing. The TOE must record the resulting actions of the Proxy SFP.
O.AUTHENTICATE	The TOE must require the Administrator to authenticate before gaining access to the administrative interfaces of the TOE, and End Users to authenticate if their controlled protocol traffic matches a Proxy SFP rule which requires authentication[10].
O.MANAGE	The TOE must provide secure management of the system configuration, the Administrative Access SFP and the Proxy SFP.
O.NO_TOE_TAMPER	The TOE must protect itself against external interference or tampering by untrusted subjects, or attempts by untrusted subjects within the scope of its control to bypass the TOE security functions.
O.REMOVE_ACTIVE	The TOE must be able to remove active content from HTML pages delivered via a controlled protocol as defined by the Proxy SFP.
O.SCREEN_TYPE	The TOE must disallow controlled protocol traffic of given content types as defined by the Proxy SFP.
O.SCREEN_URL	The TOE must disallow controlled protocol traffic for given URLs as defined by the Proxy SFP.

4.2 Security Objectives for the Environment

4.2.1 IT Environment Security Objectives

The following table lists the specific IT security objectives to be satisfied by the environment.

Table 6 – IT Security Objectives for the TOE Environment

Name	Description
OE.NETWORK	All plaintext controlled protocol traffic between the Internal and External Networks must traverse the SGOS device.

[10] Not all Proxy SFP rules require authentication. See FDP_IFF.1 for details of the Proxy SFP.

Name	Description
OE.NO_HW_TAMPER	The hardware platform hosting the TOE must protect the TOE against external interference or tampering by untrusted subjects, or attempts by untrusted subjects within the scope of control of the hardware to bypass the TOE security functions.
OE.PLATFORM	The TOE hardware must support all required SGOS functions; this platform must be dedicated to supporting SGOS processes only, and must function according to the documentation for the SGOS.
OE.SECURE_PATH	The IT environment must provide a means to protect against the compromise of security-related TOE data transmitted to and from the TOE.
OE.TIMESTAMP	The hardware platform hosting the TOE must provide a reliable timestamp for use by the TOE.

4.2.2 Non-IT Environment Security Objectives

The following non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 7 – Non-IT Security Objectives for the TOE Environment

Name	Description
OE.ADMIN	The administrator must be non-malicious and competent, and must follow all guidance.
OE.ENVIRON	The physical environment must be suitable for supporting a computing device in a secure setting.
OE.PASSWORD	Passwords for the Administrator and End User accounts and the “enable” password will be at least eight characters in length and comprise at least one letter (from a set of 26 upper-case letters and 26 lower-case letters), one special character or symbol (from a set of 32), and one number (from a set of 10).

5 Security Requirements

This section defines the SFRs and SARs met by the TOE, as well as SFRs met by the TOE IT environment. These requirements are presented following the conventions identified in Section 1.3.1.

5.1 TOE Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 8 identifies all SFRs implemented by the TOE and indicates the ST operations (if applicable) performed on each requirement. Any explicit-stated requirements are also indicated in the table.

Table 8 – TOE Security Functional Requirements

Name	Description	S	A	R	I	E
FAU_GEN.1	Audit data generation	✓	✓	✓		
FAU_SAR.1(a)	Audit review		✓		✓	
FAU_SAR.1(b)	Audit review		✓		✓	
FAU_STG.1	Protected audit trail storage	✓				
FAU_STG.4	Prevention of audit data loss	✓				
FDP_ACC.1	Subset access control		✓			
FDP_ACF.1	Security attribute based access control		✓	✓		
FDP_IFC.1	Subset information flow control		✓			
FDP_IFF.1	Simple security attributes		✓	✓		
FIA_ADM_PCR.1(a)	Password controlled role				✓	✓
FIA_ADM_PCR.1(b)	Password controlled role				✓	✓
FIA_AFL.1	Authentication failure handling	✓	✓	✓		
FIA_UAU.1(a)	Timing of authentication		✓	✓	✓	
FIA_UAU.1(b)	Timing of authentication		✓	✓	✓	
FIA_UAU.5	Multiple authentication mechanisms		✓	✓		
FIA_UAU.6(a)	Re-authenticating		✓	✓	✓	
FIA_UAU.6(b)	Re-authenticating		✓	✓	✓	
FIA_UAU.7	Protected authentication feedback		✓	✓		
FIA_UID.1(a)	Timing of identification		✓	✓	✓	

Name	Description	S	A	R	I	E
FIA_UID.1(b)	Timing of identification		✓	✓	✓	
FMT_MOF.1	Management of security functions behaviour	✓	✓			
FMT_MSA.1(a)	Management of security attributes	✓	✓		✓	
FMT_MSA.1(b)	Management of security attributes	✓	✓		✓	
FMT_MSA.3	Static attribute initialisation	✓	✓			
FMT_MTD.1(a)	Management of TSF data	✓	✓		✓	
FMT_MTD.1(b)	Management of TSF data	✓	✓		✓	
FMT_MTD.2	Management of limits on TSF data		✓			
FMT_SMF.1	Specification of management functions		✓			
FMT_SMR.1	Security roles		✓			
FMT_SMR.3	Assuming roles		✓			
FPT_RVM.1	Non-bypassability of the TSP					
FPT_SEP.1	TSF domain separation					

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration; E=Explicitly Stated

Section 5.1 contains the functional components from the CC Part 2 with the operations completed. For the conventions used in performing CC operations, please refer to Section 1.3.1.

5.1.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [*basic*] level of audit; and

c) [C*ommunication errors with external IT devices; and*

d) All actions resulting from the Proxy SFP].

The following table lists the events specified by (b).

Table 9 – Basic-Level Auditable Events

Component	Level	Auditable Event
FAU_SAR.1	Basic	Reading of the audit records
FAU_STG.4	Basic	Actions taken due to audit storage failure
FDP_ACF.1	Basic	All requests to perform an operation on an object covered by the Administrative Access SFP
FDP_IFF.1	Basic	All decisions on requests for information flow
FIA_AFL.1	Basic	Reaching the threshold for account lockout; the action taken, and the re-enabling of the account
FIA_UAU.1	Basic	All use of the authentication mechanisms
FIA_UAU.5	Basic	The result of each activated mechanism together with the final decision
FIA_UAU.6	Basic	All re-authentication attempts
FIA_UID.1	Basic	All use of the user identification mechanisms, including the user identity provided
FMT_MOF.1	Basic	All modifications to the behavior of the functions in the TSF
FMT_MSA.1	Basic	All modifications to the security attributes
FMT_MSA.3	Basic	All modifications of the initial values of security attributes
FMT_MTD.1	Basic	All modifications to the values of TSF data
FMT_MTD.2	Basic	All modifications to the limits on TSF data All modifications in the actions to be taken in case of violation of the limits
FMT_SMF.1	Basic	Use of the management functions
FMT_SMR.1	Minimal	Modifications to the group of users that are part of a role

Component	Level	Auditable Event
FMT_SMR.3	Minimal	Explicit request to assume a role
FPT_STM.1	Minimal	Changes to the time

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*for the Access Log, nothing; for the Event log, the source IP address, first line of traffic, and number of bytes returned to the End User*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1(a) Audit review

Hierarchical to: No other components.

FAU_SAR.1.1(a)

The TSF shall provide [*Privileged Administrators*] with the capability to read [*all information in the System Event Log*] from the audit records.

FAU_SAR.1.2(a)

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1(b) Audit review

Hierarchical to: No other components.

FAU_SAR.1.1(b)

The TSF shall provide [*external IT entities configured as Access Log upload targets by Privileged Administrators*] with the capability to read [*all information in Access Logs*] from the audit records.

FAU_SAR.1.2(b)

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1

The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2

The TSF shall be able to [*prevent*] unauthorised modifications to the stored audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3

FAU_STG.4.1

The TSF shall [*overwrite the oldest stored audit records*] and [*no other actions*] if the audit trail is full.

Dependencies: FAU_STG.1 Protected audit trail storage

5.1.2 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1

The TSF shall enforce the [A*dministrative Access SFP*] on [*TOE administrators performing the operations "establish an administrative session" and "request the Privileged Administrator role" over the selected TOE interface*].

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1

The TSF shall enforce the [*Administrative Access SFP*] to objects based on the following:

[

TOE administrator (subject) attributes:

1. *Authenticated Identity*
2. *Group Membership*
3. *Time of Day/Date*

and attributes of the operation:

1. *admin.access*

].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

1. *Establish an administrative session via the Serial Console: evaluate (with admin.access=READ) the <admin> layers of the configured policy rules according to the CPL specification and permit establishment if the resulting action is "allow", otherwise deny establishment.*
2. *Request the Privileged Administrator role via the Serial Console: evaluate (with admin.access=WRITE) the <admin> layers of the configured policy rules according to the*

CPL specification and permit execution if the resulting action is "allow", otherwise prevent execution.[11]

].

FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

[

1. *Establish an administrative session: establishment is permitted if the TOE administrator has credentials for "Administrator" role access.*
2. *Request the Privileged Administrator role: execution is permitted if the TOE administrator has the proper credentials for "Privileged Administrator" role access.*

].

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on **no additional rules** ~~the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]~~.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1

The TSF shall enforce the [*Proxy SFP*] on

[

1. *(Subjects) external IT entities attempting to send controlled protocol traffic through the TOE,*
2. *(Information) controlled protocol traffic sent through the TOE to other subjects,*
3. *(Operations) passing controlled protocol traffic through the TOE to the other network.*

].

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1 Simple security attributes

[11] Note that execution of the "enable" command does not automatically result in the Privileged Administrator role when using the Serial Console; an additional authentication step is required as specified by FIA_UAU.6.1(b) and FIA_ADM_PCR.1.1(a).

Hierarchical to: No other components.

FDP_IFF.1.1

The TSF shall enforce the [*Proxy SFP*] based on the following types of subject and information security attributes:

[

Subject attributes:

1. *Username*
2. *User group membership*

Information attributes:

1. *Source IP address*
2. *Destination IP address*
3. *Destination port*
4. *Protocol*
5. *URL*
6. *Time of day*
7. *Date*
8. *Originating application*
9. *MIME[12] type*
10. *Request method (the requested operation)*
11. *Any part of an HTTP request other than the body (e.g. header fields.[13])*
12. *HTTP response header fields*
13. *HTTP response body*

].

FDP_IFF.1.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*Evaluate the <proxy> and <cache> layers of the*

[12] MIME – Multipurpose Internet Mail Extensions

[13] Field matching is achieved by defining a string of text in the traffic which identifies information of interest, such as a keyword for an HTTP header (for example, defining the text of an HTTP header name and reading the value that immediately follows it).

configured policy rules and allow controlled protocol traffic to flow if the result of the evaluation is "allow", otherwise controlled protocol traffic flow is not permitted].

FDP_IFF.1.3

The TSF shall enforce **no additional information flow control SFP rules** ~~the [assignment: additional information flow control SFP rules]~~.

FDP_IFF.1.4

The TSF shall provide the following **actions that can be implemented as part of a Proxy SFP Rule:**

[

1. *Require authentication of the originating End User for an information flow originating from the Internal Network.*
2. *Rewrite a field of the information flow, e.g. URL.*
3. *Email a message to a specified address.*
4. *Strip active content from the information flow.*
5. *Provide a splash screen with a corporate message to the End User.*

]

FDP_IFF.1.5

The TSF shall explicitly authorise an information flow based on **no additional rules** ~~the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows]~~.

FDP_IFF.1.6

The TSF shall explicitly deny an information flow based on the following rules: [*If the information flow is from the External Network and the traffic is not in response to a previous request forwarded by the SGOS to the External Network*].

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

5.1.3 Class FIA: Identification and Authentication

FIA_ADM_PCR.1(a) Password controlled role

Hierarchical to: No other components.

FIA_ADM_PCR.1.1(a)

The TSF shall authenticate an Administrator under the conditions that the Administrator has requested the Privileged Administrator role by entering the proper password at the "enable" command prompt on the Serial Console.

Dependencies: No dependencies

FIA_ADM_PCR.1(b) Password controlled role

Hierarchical to: No other components.

FIA_ADM_PCR.1.1(b)

The TSF shall authenticate a Serial Console user against the configured "setup" password under the conditions that the Serial Console user has requested the Setup Console Administrator role by selecting the Setup Console in the Serial Console menu.

Dependencies: No dependencies

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1

The TSF shall detect when [*five*] unsuccessful authentication attempts occur related to [*authentication attempts using accounts subject to automatic lockout since the unsuccessful authentication attempt counter for this account has been reset by re-enabling the account, changing the password, or a preset length of time has passed since the last unsuccessful authentication attempt*].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **take one of the following actions according to the configuration:**

[

1. *Disable the account until it is manually re-enabled.*
2. *Disable the account for 3600 seconds.*

].

Dependencies: FIA_UID.1(a) Timing of identification

FIA_UAU.1(a) Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1(a)

The TSF shall allow [*only actions that match a Proxy SFP Rule that do not require authentication*] on behalf of the **End User** ~~user~~ to be performed before the user is authenticated.

FIA_UAU.1.2(a)

The TSF shall require each **End User** ~~user~~ to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1(a) Timing of identification

FIA_UAU.1(b) Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1(b)

The TSF shall allow [*only the selection of the Setup Console or CLI on the Serial Console*] on behalf of the **Serial Console** user to be performed before the user is authenticated.

FIA_UAU.1.2(b)

The TSF shall require each **Serial Console** user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1(b) Timing of identification

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1

The TSF shall provide

[

1. *Username and password (configured or from the local user list) for Serial Console access*
2. *Configured "enable" password*
3. *Configured "setup" password*
4. *Authenticate.mode(proxy) with username and password from local list*
5. *Authenticate.mode(origin-cookie-redirect) with username and password from local list*
6. *Authenticate.mode(origin-cookie-redirect) with surrogate credential*

]

to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the **following rules:**

[

1. *On the Serial Console, verification of the configured console username and password authenticates the user as an Administrator;*

2. *On the Serial Console, verification of the configured "enable" password entered by an Administrator authenticates use of the Privileged Administrator role;*

3. *On the Serial Console, verification of the user's password from the local user list (if allowed by policy) entered by an Administrator authenticates use of the Privileged Administrator role;*

4. *On the Setup Console, verification of the configured "setup" password authenticates use of the Setup Console Administrator role;*

5. *For End User requests, if the Proxy SFP specifies authenticate.mode(proxy):*

    a. *If the client supports proxy authentication, authentication shall follow the protocol for proxy authentication from RFC[14] 2616, validating the offered username and password against the local list.*

    b. *Otherwise authentication shall follow the protocol for server authentication from RFC 2616, validating the offered username and password against the local list.*

6. *For End User requests, if the Proxy SFP specifies authenticate.mode(origin-cookie-redirect) and the request contains a valid, unexpired surrogate credential, authentication will succeed using the username as specified by the surrogate credential.*

7. *For End User requests, if the Proxy SFP specifies authenticate.mode(origin-cookie-redirect) and the request does not contain a valid, unexpired surrogate credential:*

    a. *If the client supports HTTP redirects, the client will be redirected to the configured virtual URL.*

    b. *Otherwise authentication shall follow the protocol for server authentication from RFC 2616.*

8. *For End User requests, if the Proxy SFP specifies authenticate.mode(origin-cookie-redirect) and the request is to the configured virtual URL and does not contain a valid, unexpired surrogate credential, authentication shall follow the protocol for server authentication from RFC 2616, validating the offered username and password against the local list. If authentication is successful, a surrogate credential shall be generated and the client redirected to the original URL with the surrogate credential.*

].

Dependencies: No dependencies

[14] RFC – Request for Comments

FIA_UAU.6(a) Re-authenticating

Hierarchical to: No other components.

FIA_UAU.6.1(a)

The TSF shall re-authenticate the **End User** ~~user~~ under the conditions [*that (1) the user's controlled protocol traffic matches a Proxy SFP rule that requires transparent authentication, as defined by FDP_IFF.1.4 and (2) the surrogate credential is expired or invalid*].

Dependencies: No dependencies

FIA_UAU.6(b) Re-authenticating

Hierarchical to: No other components.

FIA_UAU.6.1(b)

The TSF shall re-authenticate **an Administrator** ~~the user~~ under the conditions [*that the Administrator has requested the role "Privileged Administrator" by invoking the "enable" command on the Serial Console*].

Dependencies: No dependencies

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

FIA_UAU.7.1

The TSF shall provide ~~only~~ [*no visual feedback*] to the **Serial Console** user while the authentication is in progress.

Dependencies: FIA_UAU.1(b) Timing of authentication

FIA_UID.1(a) Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1(a)

The TSF shall allow [*only actions that match a Proxy SFP Rule that do not require authentication*] on behalf of the **End User**~~ user~~ to be performed before the user is identified.

FIA_UID.1.2(a)

The TSF shall require each **End User**~~ user~~ to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

FIA_UID.1(b) Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1(b)

The TSF shall allow [*only the selection of the Setup Console or CLI on the Serial Console*] on behalf of the **Serial Console** user to be performed before the user is identified.

FIA_UID.1.2(b)

The TSF shall require each **Serial Console** user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

5.1.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to [*modify the behaviour of*] the functions [*Proxy SFP and Administrative Access SFP*] to [*Privileged Administrators*].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1(a) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1(a)

The TSF shall enforce the [*Administrative Access SFP*] to restrict the ability to [*query*] the security attributes [*user group membership*] to [*TOE administrators*].

Dependencies: FDP_ACC.1 Subset access control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1(b) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1(b)

The TSF shall enforce the [*Administrative Access SFP*] to restrict the ability to [*modify, delete*] the security attributes [*user group membership, user password*] to [*Privileged Administrators*].

Dependencies: FDP_ACC.1 Subset access control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1

The TSF shall enforce the [*Administrative Access SFP*] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*Privileged Administrators*] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1(b) Management of security attributes
FMT_SMR.1 Security roles

FMT_MTD.1(a) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1(a)

The TSF shall restrict the ability to [*query*] the [*system configuration, Administrative Access SFP, and Proxy SFP*] to [*TOE administrators*].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1(b) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1(b)

The TSF shall restrict the ability to [*modify*] the [*system configuration, Administrative Access SFP, and Proxy SFP*] to [*Privileged Administrators*].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.2 Management of limits on TSF data

Hierarchical to: No other components.

FMT_MTD.2.1

The TSF shall restrict the specification of the limits for [*audit logs*] to [*Privileged Administrators*].

FMT_MTD.2.2

The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [*overwrite the oldest audit records*].

Dependencies: FMT_MTD.1(b) Management of TSF data
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions:

[

1. *Proxy SFP management*
2. *Administrative Access SFP management*
3. *local user list management*
4. *system configuration (including settings for audit records and logs)*

].

Dependencies: No dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*"Administrator", "Privileged Administrator", and "Setup Console Administrator", as identified in Table 10*].

Table 10 – Authorized Roles

Role	Method of Authentication
Administrator	• The user is a Serial Console user and authenticates to the CLI using the configured Serial Console credentials. • The user is a Serial Console user and authenticates to the CLI using a username and password that is allowed access to the Administrator role by the Administrative Access SFP rules.
Privileged Administrator	• The user is a Serial Console user and authenticates to the "enable" CLI command using the configured enable password. • The user is an ordinary administrator, is allowed access to the Privileged Administrator role by the Administrative Access SFP rules, and re-authenticates to the "enable" CLI command using the appropriate password.
Setup Console Administrator	• The user is a Serial Console user and authenticates to the Setup Console using the Setup Console password.

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1(b) Timing of identification

FMT_SMR.3 Assuming roles

Hierarchical to: No other components.

FMT_SMR.3.1

The TSF shall require an explicit request to assume the following roles: [*Privileged Administrator (via the Serial Console) and Setup Console Administrator*].

Dependencies: FMT_SMR.1 Security roles

5.1.5 Class FPT: Protection of the TSF

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC[15] is allowed to proceed.

Dependencies: No dependencies

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2

The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

[15] TSC – TSF Scope of Control

5.2 IT Environment Security Functional Requirements

Table 11 below lists the SFRs for the TOE IT environment, and indicates the ST operations (if applicable) performed on each requirement. The stated Security Functional Requirements on the IT Environment of the TOE presented in this section have been drawn from Part 2 of CC Version 2.3 or have been explicitly stated. Any explicitly-stated requirements are noted in the table as well.

Table 11 – IT Environment Security Functional Requirements

Name	Description	S	A	R	I	E
FPT_ITC_ENV.1	TSF data confidentiality during transmission					✓
FPT_RVM_HW.1	Non-bypassability of the TSP for hardware					✓
FPT_SEP_HW.1	TSF domain separation for hardware					✓
FPT_STM.1	Reliable time stamps			✓		

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration; E=Explicitly Stated

5.2.1 Class FPT: Protection of the TSF

FPT_ITC_ENV.1 TSF data confidentiality during transmission

Hierarchical to: No other components.

FPT_ITC_ENV.1.1

The IT Environment shall protect all TSF data from unauthorized disclosure during transmission between the TSF and a remote trusted IT product.

Dependencies: No dependencies

FPT_RVM_HW.1 Non-bypassability of the TSP for hardware

Hierarchical to: No other components.

FPT_RVM_HW.1.1

The hardware of the IT Environment shall ensure that TSP enforcement functions are invoked before each function within the scope of control of the hardware is allowed to proceed.

Dependencies: No dependencies

FPT_SEP_HW.1 TSF domain separation for hardware

Hierarchical to: No other components.

FPT_SEP_HW.1.1

The hardware of the IT Environment shall maintain separate security domains that protect the TOE from interference and tampering by untrusted subjects.

FPT_SEP_HW.1.2

The hardware of the IT Environment shall enforce separation between the security domains of subjects in the scope of control of the hardware.

Dependencies: No dependencies

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1

The **IT environment** ~~TSF~~ shall be able to provide reliable time stamps for **the TOE's** ~~its own~~ use.

Dependencies: No dependencies

5.3 Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and comprise the requirements for an Evaluation Assurance Level 2 (EAL2) augmented with ALC_FLR.1. Table 12 below summarizes the requirements.

Table 12 – Assurance Requirements

Class	Assurance Requirements
Class ACM: Configuration Management	ACM_CAP.2 Configuration items
Class ADO: Delivery and Operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Class AGD: Guidance Documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ALC : Life Cycle Support	ALC_FLR.1 Basic flaw remediation
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability Assessment	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

6 TOE Summary Specification

This section presents information to detail how the TOE meets the functional and assurance requirements described in previous sections of this ST.

6.1 TOE Security Functions

The table below provides a mapping of each TOE security function to the security functional requirements that it satisfies. This mapping serves to both illustrate the association between the TSF and the SFRs and demonstrate that every security function contributes to the satisfaction of at least one TOE SFR.

Table 13 – Mapping of TOE Security Functions to SFRs

Security Functional Requirements \ TOE Security Function	Identification and Authentication	Protection of the TSF	Security Audit	Security Management	User Data Protection
FAU_GEN.1			✓		
FAU_SAR.1(a)			✓		
FAU_SAR.1(b)			✓		
FAU_STG.1			✓		
FAU_STG.4			✓		
FDP_ACC.1					✓
FDP_ACF.1					✓
FDP_IFC.1					✓
FDP_IFF.1					✓
FIA_ADM_PCR.1(a)	✓				
FIA_ADM_PCR.1(b)	✓				
FIA_AFL.1	✓				
FIA_UAU.1(a)	✓				
FIA_UAU.1(b)	✓				
FIA_UAU.5	✓				
FIA_UAU.6(a)	✓				
FIA_UAU.6(b)	✓				

TOE Security Function / Security Functional Requirements	Identification and Authentication	Protection of the TSF	Security Audit	Security Management	User Data Protection
FIA_UAU.7	✓				
FIA_UID.1(a)	✓				
FIA_UID.1(b)	✓				
FMT_MOF.1				✓	
FMT_MSA.1(a)				✓	
FMT_MSA.1(b)				✓	
FMT_MSA.3				✓	
FMT_MTD.1(a)				✓	
FMT_MTD.1(b)				✓	
FMT_MTD.2				✓	
FMT_SMF.1				✓	
FMT_SMR.1				✓	
FMT_SMR.3				✓	
FPT_RVM.1		✓			
FPT_SEP.1		✓			

The sections that follow describe each security function and how it specifically satisfies each of its related functional requirements. This serves to both describe the security functions and to provide rationale that the security functions are suitable to satisfy the necessary requirements.

6.1.1 Security Audit

The SGOS Audit function generates audit records for all system events related to audit, authentication, administration activities, and communication with external IT devices. These records are stored in the System Log. These event records contain, at minimum, the following information:

- Date and time of the event
- Type of event
- Identity of subject
- Outcome of the event

The events stored in the System Log can be displayed using the administrative interfaces; this function is restricted to Privileged Administrators.

All actions related to information flow protection are stored in the Access Log. These events record the outcome of every application of the Proxy SFP. These event records include, at minimum, the following information:

- Date and time of the event
- Type of event
- Identity of the subject
- Outcome of the event
- Source IP address
- First line of traffic
- The number of bytes returned to the End User

Each controlled protocol can create an Access Log record at the end of each transaction for that protocol. The ProxySG can create Access Logs in selectable log formats, and additional log types can be created using custom or W3C Extended Log File Format (ELFF) strings. The log file formats supported are:

- NCSA Common
- SQUID (and SQUID-compatible)
- Custom (using selectable strings)
- SmartReporter (using ELFF)
- SurfControl (using ELFF)
- Websense (using ELFF)

Access Logs can be uploaded to another system for later analysis. Configuring the target systems and decisions regarding when and what to upload are restricted to Privileged Administrators. Additionally, the System Log and the Access Log are protected against unauthorized deletion and modification. If the space for logging becomes full, the oldest stored records (on a per log basis) will be overwritten.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1(a), FAU_SAR.1(b), FAU_STG.1, FAU_STG.4

6.1.2 User Data Protection

The SGOS allows authorized administrators to enforce a very flexible policy using the ProxySG CPL. Figure 5 below shows a sample of CPL.

```
                <proxy>
                client_address=10.25.0.0/16 authenticate(bankabc)
                client_address=10.26.0.0/16 authenticate(bankxyz)
        <proxy>
                [Rule] group=”bankabc-execs”
                allow
                [Rule] group=”bankabc-tellers”
                        allow url=intranet.bankabc.com/hr/benefits
                        deny url=intranet.bankabc.com/hr
                        deny url=intranet.bankabc.com/execs
                        allow url_domain=intranet.bankabc.com
                        allow url=www.123loans.com/rates
                        allow category=Investing
                        deny
                [Rule] group=”bankabc-hr”
                        block_category=(Sex,Criminal_Skills,Politics/Religion)
                        deny url=intranet.bankabc.com/execs
                        allow url_domain=intranet.bankabc.com
                        deny
                [Rule] group=”bankabc-contractors”
                        allow url=intranet.bankabc.com/contractors
                        deny
        <admin>
                authenticate(administrators)
        <admin>
                group=privileged admin.access=write allow

                deny
```

Figure 5 – Sample Configurable Policy

6.1.2.1 Administrative Access Control

Using CPL, an authorized administrator can craft policies controlling administrative access by users (excluding Administrators authenticating with console credentials, which are not subject to the Administrative Access Control policy). This allows administrative access to be granted or denied based on the username, the groups to which the user belongs, and the time of day.

CPL also allows normal or privileged access to be granted or denied based on the same information. An Administrator authenticating with console credentials becomes a Privileged Administrator by executing the “enable” command and successfully authenticating via its password challenge. A user from the local user list with administrative access also gains privileges via the “enable” command; however, the allowed privileges are subject to policy control. The “enable” command will fail immediately if these Administrators are not allowed access for the condition “admin.access=WRITE”.

6.1.2.2 Information Flow Protection

Using CPL, an administrator can craft policies to control the controlled protocol traffic exactly according to the deployment site’s security needs. The language is flexible enough to allow rules based on subject attributes like username and group. The rules may also use information attributes such as all IP related information, URL, time, date, source application, MIME type, required bandwidth, content type, parts of the HTTP request, and any part of the HTTP response. The actions that policies can take are allow, deny, require an authenticated session, rewrite a portion of the traffic (e.g. URL redirect), strip active content, prompt a user with a message, and email a warning. In

addition, external controlled protocol traffic is only allowed through the TOE if it is in response to a previous request forwarded by the SGOS to the External Network.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1

6.1.3 Identification and Authentication

SGOS users are identified by their username and in the evaluated configuration authentication is via a password. Authentication is tied to the session, either the Administrative session or the End User session.

6.1.3.1 Administrator Authentication

When a terminal is connected to the Serial Console, a menu is offered presenting the options of the Setup Console (used for installation) and the CLI (used for administration). In the evaluated configuration, the Setup Console function is never used after the TOE is operational, and its use is protected from End User access by a "setup" password. Serial Console users are directed to always choose the CLI.

There are several authentication mechanisms for administrators. SGOS makes use of a Serial Console user (i.e. Administrator) account that is set up during installation with a username and password. Administrators authenticating with these credentials are Administrators, and are exempt from policy control. With the appropriate administrative policy rules in place, user accounts in the local user list can also be used for administration by using a username from the local user list and supplying the associated password; these users are "ordinary" administrators.

The Privileged Administrator role (the only way to make configuration or policy changes) is also subject to authentication. To assume the Privileged Administrator role on the Serial Console, an authenticated Administrator must execute the "enable" command, which challenges for a password. Administrator-role users authenticate as Privileged Administrators by supplying the "enable" password that is part of system configuration. Ordinary administrators authenticate to the "enable" command with their associated password from the local user list (access to the "enable" command by ordinary administrators is controlled by policy).

6.1.3.2 End User Authentication

End Users establish a session with SGOS when the user agent in use establishes a TCP/IP connection with the SGOS in preparation for accessing a resource on the External Network. This session is initially unauthenticated. Requests for resources on the External Network will be permitted on the unauthenticated connection provided the request matches a Proxy SFP Rule that allows access without authentication. The first time a request requiring authentication is made on the connection, the user will be challenged for credentials. The information displayed to the End User during authentication depends on the user agent the End User is using. Additional requests made using the same session (TCP/IP connection) will be considered authenticated.

In the evaluated configuration, the SGOS supports two authentication modes: proxy and origin-cookie-redirect. Proxy authentication uses the protocol described in the HTTP 1.1 RFC (RFC 2616) for clients capable of it, otherwise it uses server authentication from the same RFC. Origin-cookie-redirect authentication redirects clients to a virtual URL followed by server authentication (RFC 2616) followed by redirect back to the original URL with a proxy-generated surrogate credential (carried in the query or a cookie). For clients incapable of HTTP redirects, server authentication from RFC 2616 is used.

6.1.3.3 Automatic Account Lockout

In the evaluated configuration, automatic account lockout is enabled. The SGOS counts the number of authentication failures for a given user account, and if number of failed attempts reaches five, the account will be disabled. A disabled account cannot be used, even if the correct password is provided. No information about whether a submitted password is valid is obtained from attempting to authenticate to a disabled account. The account can be left disabled until manually re-enabled, or it can automatically re-enable after a preset time of 3600 seconds. The failed authentication counter is reset to zero when the account is enabled or the password is changed.

TOE Security Functional Requirements Satisfied: FIA_ADM_PCR.1(a), FIA_ADM_PCR.1(b), FIA_AFL.1, FIA_UAU.1(a), FIA_UAU.1(b), FIA_UAU.5, FIA_UAU.6(a), FIA_UAU.6(b), FIA_UAU.7, FIA_UID.1(a), FIA_UID.1(b)

6.1.4 Security Management

SGOS security is managed by administrators, who have varying degrees of authority to review and modify the configuration of the security attributes of TOE. Levels of administrative authority are based on the credentials used to authenticate and (for "ordinary" administrators) any associated policies defined in the Administrative Access SFP (refer to paragraph 6.1.3.1 for details regarding authentication methods for the various administrators). All administrators are allowed to review such attributes as credentials, audit settings, network settings, and policies. Privileged Administrators can also modify the TOE configuration and define Administrative Access SFP and the Proxy SFP rules. Serial Console users that authenticate using the configured "enable" password at the "enable" command challenge are granted full read/write privileges, while those administrators defined by the local user list that are allowed Privileged access are granted privileges based on policy.

There is also a Setup Console Administrator role that, in the evaluated configuration of SGOS, is used only for the initial configuration of the TOE before installation into the target network; once setup is complete, this role (and this function) is no longer used. The Setup Console Administrator role allows for the specification of the IP address, subnet mask, default gateway, DNS server, Serial Console user credentials, and the Privileged Administrator password.

The attributes integral to the Proxy SFP and Administrative Access SFPs are restrictive by default. After installation and until a policy is loaded, the SGOS will not pass any controlled protocol traffic and only the Administrator account is configured for use.

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1(a), FMT_MSA.1(b), FMT_MSA.3, FMT_MTD.1(a), FMT_MTD.1(b), FMT_MTD.2, FMT_SMF.1, FMT_SMR.1, FMT_SMR.3

6.1.5 Protection of the TSF

The TOE is installed between an Internal and External Network such that all controlled protocol traffic is presented to the Internal Network interface on the TOE. Therefore, controlled protocol traffic must be handled by the TOE to move from one network to the other. The TOE is designed so that all controlled protocol traffic must be reviewed by the policy enforcement engine before it is allowed to be retransmitted on a network interface.

The TOE protects itself from tampering by specifying that only administrators can log in to the management interfaces using a username/password combination, and that the Setup Console can be accessed only after presenting the configured password for such access. Each SGOS appliance is completely self-contained. There are no external interfaces into the TOE other than the physical ports provided, each of which is carefully controlled. No general purpose operating system, disk storage, or programming interface is provided. The TOE protects its management functions by isolating them through authentication. SGOS is a proprietary operating system that executes in a single, dedicated security domain.

TOE Security Functional Requirements Satisfied: FPT_RVM.1, FPT_SEP.1

6.2 TOE Security Assurance Measures

EAL2+ was chosen to provide a basic level of independently assured security. The following table provides a mapping of the TOE assurance classes and components of the TOE for a CC EAL2+ level of assurance to the assurance measures used for the development and maintenance of the TOE.

Table 14 – Mapping of TOE Assurance Components to Documentation

Assurance Class	Assurance Component	Document
Configuration Management	ACM_CAP.2	Blue Coat Systems, Inc. ProxySG Operating System - Configuration Management: Capabilities
Delivery and Operation	ADO_DEL.1 ADO_IGS.1	Blue Coat Systems, Inc. ProxySG Operating System - Delivery and Operation
Development	ADV_FSP.1 ADV_HLD.1 ADV_RCR.1	Blue Coat Systems, Inc. ProxySG Operating System - Development: Functional Specification, High Level Design, and Representation Correspondence
Guidance Documents	AGD_ADM.1 AGD_USR.1	Blue Coat ProxySG Operating System v4.2.5.1 Installation, Generation, Startup, and Administrative Guidance Readme Blue Coat ProxySG SGOS 4.2.5 CLI Reference Blue Coat ProxySG SGOS 4.2.5 Configuration Management Guide Blue Coat ProxySG SGOS 4.2.3 Content Policy Language Guide Blue Coat ProxySG SGOS 4.2.3 Deployment Guide Blue Coat ProxySG SGOS 4.2.3 Upgrade Guide
Life Cycle Support	ALC_FLR.1	Blue Coat Systems, Inc. ProxySG Operating System - Life Cycle Support: Flaw Remediation
Tests	ATE_COV.1	Blue Coat Systems, Inc. ProxySG Operating System - Tests: Coverage
	ATE_FUN.1	Blue Coat Systems, Inc. ProxySG Operating System - Tests: Functional Tests
Vulnerability Assessment	AVA_SOF.1 AVA_VLA.1	Blue Coat Systems, Inc. ProxySG Operating System - Vulnerability Assessment

The sections that follow describe the assurance measures (i.e. assurance documentation) that meet the TOE security assurance requirements.

6.2.1 Configuration Management

The Configuration Management document contains assurance component ACM_CAP.2, and provides a description of the various tools used to control the configuration items and how they are used internally at Blue Coat. This document provides a complete configuration item list and a unique referencing scheme for each configuration item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

6.2.2 Delivery and Operation

The Delivery and Operation document contains assurance components ADO_DEL.1 and ADO_IGS.1. ADO_DEL.1 provides a description of the secure delivery procedures implemented by Blue Coat to protect against TOE modification during product delivery.

The ADO_IGS.1 Installation, Guidance, and Start-Up documentation details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the TOE Users(s) on configuring the TOE and how they affect the TSF.

6.2.3 Development

The Blue Coat Development Document consists of several related assurance components that address the TOE at different levels of abstraction.

The ADV_FSP.1 Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and error messages for each external TSF interface.

The ADV_HLD.1 High Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.

The ADV_RCR.1 Representation Correspondence demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the High-Level Design.

6.2.4 Guidance Documents

The Guidance documentation contains assurance components AGD_ADM.1 and AGD_USR.1. Administrator Guidance is given in AGD_ADM.1, and provides detailed procedures for the administration of the TOE and description of the security functions provided by the TOE.

The User Guidance documentation with component AGD_USR.1 generally directs end users on how to operate the TOE in a secure manner, and explains the user-visible security functions and how they need to be exercised. However, end users direct interaction with the TOE is limited to the entry of a password for policy-controlled access to controlled-protocol traffic. Since the configuration of the policies is discussed in the Administrator Guidance, that document is considered to contain the User Guidance component as well.

6.2.5 Life Cycle Support

The Life Cycle Support documentation contains assurance component ALC_FLR.1, and outlines the steps taken at Blue Coat to capture, track and remove bugs as part of their basic flaw remediation process. This document shows that all flaws are recorded and that the system tracks them to completion.

6.2.6 Tests

There are a number of components that make up the Tests documentation. The ATE_COV.1 Test Coverage Analysis document demonstrates that testing is performed against the functional specification. It also demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided in order to meet the assurance requirement ATE_FUN.1 Functional Testing.

6.2.7 Vulnerability Assessment

The Vulnerability Assessment document contains assurance components AVA_VLA.1 and AVA_SOF.1. AVA_VLA.1, the Vulnerability Analysis component, demonstrates ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, this document provides evidence of how the TOE is resistant to obvious attacks.

The AVA_SOF.1 Strength of TOE Security Function component of the document demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum Strength of Function (SOF) requirements.

7 Protection Profile Claims

This section provides the identification and justification for any Protection Profile conformance claims.

7.1 Protection Profile Reference

There are no protection profile claims for this security target.

8 Rationale

This section provides the rationale for the selection of the security requirements and objectives as they relate to the assumptions, organizational policies, and threats. In particular, it shows that the security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

8.1 TOE Security Objectives Rationale

This section traces each TOE security objective back to the applicable threats and/or policies identified in this Security Target. Table 15 demonstrates that the mapping of the TOE security objectives to the threats and policies is complete.

Table 15 – Mapping of TOE Security Objectives to Threats and Policies

Threats and Policies \ Security Objectives for the TOE	O.AUDIT	O.AUTHENTICATE	O.MANAGE	O.NO_TOE_TAMPER	O.REMOVE_ACTIVE	O.SCREEN_TYPE	O.SCREEN_URL
Threats							
T.EXTERNAL_NETWORK					✓	✓	✓
T.MASQUERADE		✓					
T.TAMPERING				✓			
T.UNAUTHORIZED_ACCESS		✓	✓				
Policies							
P.ACTIVE_CONTENT					✓		
P.ADMIN		✓	✓				
P.AUDIT	✓						
P.CONTENT_TYPE						✓	
P.FILTERED_URLS							✓
P.MANAGE			✓	✓			
P.NON_ANONYMOUS		✓					
P.POST_TYPE						✓	

8.1.1 Rationale for TOE Security Objectives Relating to Threats

Table 16 provides a detailed discussion regarding the rationale behind the objectives as they relate back to the threats.

Table 16 – TOE Security Objectives Rationale Relating to Threats

Threat	Objective	Rationale
T.EXTERNAL_NETWORK A user or process on the Internal Network may access or post content on the External Network that has been deemed inappropriate or potentially harmful to the Internal Network.	O.REMOVE_ACTIVE The TOE must be able to remove active content from HTML pages delivered via a controlled protocol as defined by the Proxy SFP.	O.REMOVE_ACTIVE ensures that active content on HTML pages is removed prior to being delivered to the Internal Network, thereby minimizing the risk of attack to the Internal Network.
	O.SCREEN_TYPE The TOE must disallow controlled protocol traffic of given content types as defined by the Proxy SFP.	O.SCREEN_TYPE ensures that controlled protocol traffic of the specified content type(s) is disallowed, thereby minimizing the risk of Internal Network users accessing the External Network for non-approved activities.
	O.SCREEN_URL The TOE must disallow controlled protocol traffic for given URLs as defined by the Proxy SFP.	O.SCREEN_URL ensures that controlled protocol traffic from the specified URL(s) is disallowed, thereby minimizing the risk of Internal Network users accessing the External Network for non-approved activities.
T.MASQUERADE A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.AUTHENTICATE The TOE must require the Administrator to authenticate before gaining access to the administrative interfaces of the TOE, and End Users to authenticate if their controlled protocol traffic matches a Proxy SFP rule which requires authentication.	O.AUTHENTICATE ensures that Administrators and End Users supply login credentials (including strong passwords) before being granted access to services or information, thereby reducing the risk of access by masquerading.
T. TAMPERING A user or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.	O.NO_TOE_TAMPER The TOE must protect itself against external interference or tampering by untrusted subjects, or attempts by untrusted subjects within the scope of its control to bypass the TOE security functions.	O.NO_TOE_TAMPER ensures that the protection mechanisms of the TOE designed to prevent tampering with TOE IT assets are in place and functioning properly, and that these mechanisms cannot be bypassed.
T.UNAUTHORIZED_ACCESS A user may gain access to security data on the TOE for which they are not authorized according to the TOE security policy.	O.AUTHENTICATE The TOE must require the Administrator to authenticate before gaining access to the administrative interfaces of the TOE, and End Users to authenticate if their controlled protocol traffic matches a Proxy SFP rule which requires authentication.	O.AUTHENTICATE ensures that users supply login credentials (including strong passwords) before being granted access to any security-related information, thereby reducing the risk of unauthorized access.
	O.MANAGE The TOE must provide secure management of the system configuration, the Administrative Access SFP and the Proxy SFP.	O.MANAGE provides the capability for an administrator to properly configure the management mechanisms of the TOE designed to mitigate this threat.

8.1.2 Rationale for TOE Security Objectives Relating to Policies

Table 17 provides a detailed discussion regarding the rationale behind the objectives as they relate back to the organizational security policies.

Table 17 – TOE Security Objectives Rationale Relating to Policies

Policy	Objective	Rationale
P.ACTIVE_CONTENT The TOE shall provide a means to remove active content (e.g. Java, JavaScript, ActiveX) in HTML pages delivered via controlled protocols.	O.REMOVE_ACTIVE The TOE must be able to remove active content from HTML pages delivered via a controlled protocol as defined by the Proxy SFP.	O.REMOVE_ACTIVE ensures that active content delivered from the External Network is removed as defined by the Proxy's policies, minimizing the risk of this type of exploit
P.ADMIN Only authorized individuals shall have the ability to perform administrative actions on the TOE.	O.AUTHENTICATE The TOE must require the Administrator to authenticate before gaining access to the administrative interfaces of the TOE, and End Users to authenticate if their controlled protocol traffic matches a Proxy SFP rule which requires authentication	O.AUTHENTICATE ensures that administrators enter credentials before access to the administrative interfaces of the TOE is granted.
	O.MANAGE The TOE must provide secure management of the system configuration, the Administrative Access SFP and the Proxy SFP.	O.MANAGE ensures that only administrators are given credentials allowing access to the administrative functions of the TOE.
P.AUDIT The TOE shall record events of security relevance at the "basic level" of auditing. The TOE shall record the resulting actions of the Proxy SFP.	O.AUDIT The TOE must record events of security relevance at the "basic level" of auditing. The TOE must record the resulting actions of the Proxy SFP.	O.AUDIT ensures that events of the appropriate security relevance are recorded at the appropriate level.
P.CONTENT_TYPE End Users shall not access unauthorized content types via controlled protocols on the External Network.	O.SCREEN_TYPE The TOE must disallow controlled protocol traffic of given content types as defined by the Proxy SFP.	O.SCREEN_TYPE ensures that End Users are prevented from accessing forbidden content types via controlled protocols by disallowing such traffic.
P.FILTERED_URLS End Users shall not access unauthorized URLs via controlled protocols on the External Network.	O.SCREEN_URL The TOE must disallow controlled protocol traffic for given URLs as defined by the Proxy SFP.	O.SCREEN_URL ensures that End Users are prevented from accessing forbidden URLs via controlled protocols by disallowing such traffic.

Policy	Objective	Rationale
P.MANAGE The TOE shall provide secure management of the system configuration, the Proxy SFP, and the Administrative SFP.	O.MANAGE The TOE must provide secure management of the system configuration, the Administrative Access SFP and the Proxy SFP.	O.MANAGE ensures that the TOE provides a mechanism by which it can be securely managed.
	O.NO_TOE_TAMPER The TOE must protect itself against external interference or tampering by untrusted subjects, or attempts by untrusted subjects within the scope of its control to bypass the TOE security functions.	O.NO_TOE_TAMPER ensures that the management mechanism remains secured by preventing untrusted subjects from tampering with the security features of the TOE.
P.NON_ANONYMOUS Access to some resources via controlled protocols on the External Network may be restricted to particular End Users.	O.AUTHENTICATE The TOE must require the Administrator to authenticate before gaining access to the administrative interfaces of the TOE, and End Users to authenticate if their controlled protocol traffic matches a Proxy SFP rule which requires authentication	O.AUTHENTICATE ensures that End Users authenticate to the system before being allowed access to controlled protocol traffic (if required by the Proxy SFP rules).
P.POST_TYPE End Users shall not post unauthorized content types to the External Network using controlled protocols.	O.SCREEN_TYPE The TOE must disallow controlled protocol traffic of given content types as defined by the Proxy SFP.	O.SCREEN_TYPE ensures that End Users cannot post unauthorized content types (as defined by the Proxy SFP rules) to the External Network via controlled protocols.

8.2 IT Environment Security Objectives Rationale

This section traces each IT environment security objective back to the applicable threats, policies, and/or assumptions identified in this Security Target. Table 18 demonstrates that the mapping of the IT environment security objectives to the threats, polices, and assumptions is complete.

Table 18 – Mapping of IT Environment Security Objectives to Threats, Assumptions, and Policies

Security Objectives for the IT Environment / Threats, Assumptions, and Policies	OE.ADMIN	OE.ENVIRON	OE.NETWORK	OE.NO_HW_TAMPER	OE.PASSWORD	OE.PLATFORM	OE.SECURE_PATH	OE.TIMESTAMP
Threats								
T.TAMPERING		✓		✓				

Threats, Assumptions, and Policies / Security Objectives for the IT Environment	OE.ADMIN	OE.ENVIRON	OE.NETWORK	OE.NO_HW_TAMPER	OE.PASSWORD	OE.PLATFORM	OE.SECURE_PATH	OE.TIMESTAMP
Assumptions								
A.ENVIRON		✓		✓				
A.INSTALL	✓							
A.NETWORK			✓					
A.NO_EVIL_ADMIN	✓							
A.PASSWORD					✓			
A.PLATFORM						✓		
A.SECURE_PATH							✓	
A.TIMESTAMP								✓
Policies								
P.AUDIT								✓

8.2.1 Rationale for IT Environment Security Objectives Relating to Threats

Table 19 provides a detailed discussion regarding the rationale behind the IT environment security objectives as they relate back to the threats.

Table 19 – IT Environment Security Objectives Rationale Relating to Threats

Threat	Objective	Rationale
T. TAMPERING A user or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.	OE.ENVIRON The physical environment must be suitable for supporting a computing device in a secure setting.	OE.ENVIRON ensures that the physical environment in which the TOE is running is secure, protecting the TOE from tampering attempts.
	OE.NO_HW_TAMPER The hardware platform hosting the TOE must protect the TOE against external interference or tampering by untrusted subjects, or attempts by untrusted subjects within the scope of control of the hardware to bypass the TOE security functions.	OE.NO_HW_TAMPER ensures that the hardware platform on which the TOE runs is sufficiently secure to protect the TOE from tampering attempts.

8.2.2 Rationale for IT Environment Security Objectives Relating to Assumptions

Table 20 provides a detailed discussion regarding the rationale behind the IT environment security objectives as they relate back to the assumptions.

Table 20 – IT Environment Security Objectives Rationale Relating to Assumptions

Assumption	Objective	Rationale
A.ENVIRON The TOE is located in an environment that provides physical security, uninterruptible power, air conditioning, and all other conditions required for reliable operation of the hardware. Physical access to the appliance is restricted to authorized persons.	OE.ENVIRON The physical environment must be suitable for supporting a computing device in a secure setting.	OE.ENVIRON ensures that the TOE IT environment is suitable to ensure the proper, secure, and on-going functioning of the TOE.
	OE.NO_HW_TAMPER The hardware platform hosting the TOE must protect the TOE against external interference or tampering by untrusted subjects, or attempts by untrusted subjects within the scope of control of the hardware to bypass the TOE security functions.	OE.NO_HW_TAMPER ensures that the hardware upon which the TOE executes provides a measure of physical security, protecting the TOE from compromise resulting from interference, tampering and TSF circumvention.
A.INSTALL The SGOS device has been installed and configured according to the appropriate installation guides.	OE.ADMIN The Administrator must be non-malicious and competent, and must follow all guidance.	OE.ADMIN reduces the risk of security vulnerabilities by ensuring that the administrator responsible for the SGOS device installed and configured the device according to the documented guidance.
A.NETWORK All plaintext controlled protocol traffic between the Internal and External Networks traverses the SGOS device; there is no other connection between the Internal and External Networks for plaintext controlled protocol traffic.	OE.NETWORK All plaintext controlled protocol traffic between the Internal and External Networks must traverse the SGOS device.	OE.NETWORK ensures that the IT environment is configured such that no plaintext controlled protocol traffic can travel between the Internal and External Networks without traversing the SGOS device.
A.NO_EVIL_ADMIN Administrators are non-hostile and follow all administrator guidance when using the TOE. Administration is competent and on-going.	OE.ADMIN The Administrator must be non-malicious and competent, and must follow all guidance.	OE.ADMIN ensures that the administrator is trusted, educated, competent, and has no malicious intent, thereby addressing this assumption.

Assumption	Objective	Rationale
A.PASSWORD Passwords for the Serial Console Administrator and End User accounts, and the "enable" passwords, are at least eight characters in length and comprise at least one letter (from a set of 26 upper-case letters and 26 lower-case letters), one special character or symbol (from a set of 32), and one number (from a set of 10).	OE.PASSWORD Passwords for the Administrator and End User accounts and the "enable" password will be at least eight characters in length and comprise at least one letter (from a set of 26 upper-case letters and 26 lower-case letters), one special character or symbol (from a set of 32), and one number (from a set of 10).	OE.PASSWORD ensures that the passwords selected by users are of sufficient strength to provide the desired level of security for TOE access.
A.PLATFORM The hardware platform used to host the TOE supports all required SGOS functions, and is dedicated to supporting SGOS only.	OE.PLATFORM The TOE hardware must support all required SGOS functions; this platform must be dedicated to supporting SGOS processes only, and must function according to the documentation for the SGOS.	OE.PLATFORM ensures that the TOE is hosted on a hardware platform dedicated to (and appropriate for) its proper functioning, maximizing its ability to perform as documented.
A.SECURE_PATH Security-related TOE data transmitted to and from the TOE over a network connection is protected from compromise by appropriate measures.	OE.SECURE_PATH The IT environment must provide a means to protect against the compromise of security-related TOE data transmitted to and from the TOE.	OE.SECURE_PATH ensures that appropriate mechanisms and/or protocols are in place in the TOE IT environment to protect sensitive TOE network traffic when transmitted between the TOE and another IT product.
A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIMESTAMP The hardware platform hosting the TOE must provide a reliable timestamp for use by the TOE.	OE.TIMESTAMP ensures that the hardware platform hosting the TOE can provide a reliable timestamp for use by the TOE, thereby addressing this assumption.

8.2.3 Rationale for IT Environment Security Objectives Relating to Policies

Table 19 provides a detailed discussion regarding the rationale behind the IT environment security objectives as they relate back to the policies.

Table 21 – IT Environment Security Objectives Rationale Relating to Policies

Policy	Objective	Rationale
P.AUDIT The TOE shall record events of security relevance at the "basic level" of auditing. The TOE shall record the resulting actions of the Proxy SFP.	OE.TIMESTAMP The hardware platform hosting the TOE must provide a reliable timestamp for use by the TOE.	OE.TIMESTAMP ensures that the hardware platform hosting the TOE can provide a reliable timestamp for use by the TOE's audit function, thereby addressing this policy.

8.3 Security Functional Requirements Rationale

This section traces each SFR back to the applicable security objective(s) identified in this Security Target. Table 22 demonstrates that the mapping of SFRs to the TOE security objectives is complete. Table 23 demonstrates that the mapping of SFRs to the IT environment security objectives is complete. Taken together, these tables represent a complete mapping, and demonstrate that all SFRs map to at least one objective.

Table 22 – Mapping of SFRs to TOE Security Objectives

Security Functional Requirements \ Security Objectives for the TOE	O.AUDIT	O.AUTHENTICATE	O.MANAGE	O.NO_TOE_TAMPER	O.REMOVE_ACTIVE	O.SCREEN_TYPE	O.SCREEN_URL
FAU_GEN.1	✓						
FAU_SAR.1(a)	✓						
FAU_SAR.1(b)	✓						
FAU_STG.1	✓						
FAU_STG.4	✓						
FDP_ACC.1			✓				
FDP_ACF.1			✓				
FDP_IFC.1					✓	✓	✓
FDP_IFF.1					✓	✓	✓
FIA_ADM_PCR.1(a)		✓	✓				
FIA_ADM_PCR.1(b)		✓	✓				
FIA_AFL.1		✓					
FIA_UAU.1(a)		✓					
FIA_UAU.1(b)		✓					
FIA_UAU.5		✓					
FIA_UAU.6(a)		✓					
FIA_UAU.6(b)		✓					
FIA_UAU.7		✓					
FIA_UID.1(a)		✓					
FIA_UID.1(b)		✓					
FMT_MOF.1			✓				
FMT_MSA.1(a)			✓				
FMT_MSA.1(b)			✓				
FMT_MSA.3			✓				

Security Objectives for the TOE / Security Functional Requirements	O.AUDIT	O.AUTHENTICATE	O.MANAGE	O.NO_TOE_TAMPER	O.REMOVE_ACTIVE	O.SCREEN_TYPE	O.SCREEN_URL
FMT_MTD.1(a)			✓				
FMT_MTD.1(b)			✓				
FMT_MTD.2			✓				
FMT_SMF.1			✓				
FMT_SMR.1			✓				
FMT_SMR.3			✓				
FPT_RVM.1				✓			
FPT_SEP.1				✓			

Table 23 – Mapping of SFRs to IT Environment Security Objectives

Security Objectives for the IT Environment / Security Functional Requirements	OE.NETWORK	OE.NO_HW_TAMPER	OE.PLATFORM	OE.SECURE_PATH	OE.TIMESTAMP
FPT_ITC_ENV.1				✓	
FPT_RVM_HW.1	✓	✓			
FPT_SEP_HW.1			✓		
FPT_STM.1					✓

8.3.1 Rationale for SFRs Relating to TOE Security Objectives

The following table provides detailed evidence of coverage for each TOE security objective.

Table 24 – Rationale for SFRs of the TOE

Objective	Requirement Addressing the Objective	Rationale

Objective	Requirement Addressing the Objective	Rationale
O.AUDIT The TOE must record events of security relevance at the "basic level" of auditing. The TOE must record the resulting actions of the Proxy SFP.	FAU_GEN.1	This requirement supports O.AUDIT by requiring the TOE to produce audit records for system security events and for actions caused by enforcement of the Proxy SFP.
	FAU_SAR.1(a)	This requirement supports O.AUDIT by requiring the TOE to make the recorded audit records available for review.
	FAU_SAR.1(b)	This requirement supports O.AUDIT by requiring the TOE to make the recorded audit records available for review.
	FAU_STG.1	This requirement supports O.AUDIT by requiring the TOE to prevent unauthorized deletion of the audit records.
	FAU_STG.4	This requirement supports O.AUDIT by requiring the TOE to mitigate audit data loss due to hardware limitations such as disk full.
O.AUTHENTICATE The TOE must require the Administrator to authenticate before gaining access to the administrative interfaces of the TOE, and End Users to authenticate if their controlled protocol traffic matches a Proxy SFP rule which requires authentication.	FIA_ADM_PCR.1(a)	This requirement supports O. AUTHENTICATE by requiring a TOE administrator to enter the proper password before assuming the Privileged Administrator role.
	FIA_ADM_PCR.1(b)	This requirement supports O. AUTHENTICATE by requiring a Serial Console user to enter the "setup" password before assuming the Setup Console Administrator role (which allows bypassing the TSF).
	FIA_AFL.1	This requirement supports O. AUTHENTICATE by ensuring that users' passwords are protected from brute-force guessing.
	FIA_UAU.1(a)	This requirement supports O. AUTHENTICATE by preventing unauthenticated End Users from performing actions that require authentication.
	FIA_UAU.1(b)	This requirement supports O. AUTHENTICATE by ensuring that the only action permitted on behalf of an unauthenticated Serial Console user is the selection of the Setup Console or the CLI on the Serial Console.
	FIA_UAU.5	This requirement supports O. AUTHENTICATE by defining the authentication mechanisms for End Users and Serial Console users.
	FIA_UAU.6(a)	This requirement supports O. AUTHENTICATE by ensuring the End Users are authenticated before any other TSF-mediated actions taken on their behalf are performed. Only actions that match Proxy SFP rules not requiring identification are allowed before authentication is performed.
	FIA_UAU.6(b)	This requirement supports O. AUTHENTICATE by ensuring that the only action permitted on behalf of an unauthenticated Serial Console user is the selection of the Setup Console or the CLI on the Serial Console.

Objective	Requirement Addressing the Objective	Rationale
	FIA_UAU.7	This requirement supports O. AUTHENTICATE by requiring that characters are not echoed when administrators type their password on the Serial Console.
	FIA_UID.1(a)	This requirement supports O. AUTHENTICATE by ensuring the End Users are identified before any other TSF-mediated actions taken on their behalf are performed. Only actions that match Proxy SFP rules not requiring identification are allowed before identification is performed.
	FIA_UID.1(b)	This requirement supports O. AUTHENTICATE by ensuring that the only action permitted on behalf of an unidentified Serial Console user is the selection of the Setup Console or the CLI on the Serial Console.
O.MANAGE The TOE must provide secure management of the system configuration, the Administrative Access SFP and the Proxy SFP.	FDP_ACC.1	This requirement supports O.MANAGE by including a policy language that enables administrators to construct rules that control the access of administrators to the administrative interfaces of the TOE. The function then enforces those rules and takes the action specified.
	FDP_ACF.1	This requirement supports O.MANAGE by supporting several attributes that can be used in the Administrative Access SFP to control access to the administrative interfaces.
	FIA_ADM_PCR.1(a)	This requirement supports O. MANAGE by requiring a TOE administrator to enter the proper password before assuming the Privileged Administrator role for accessing administrative functions.
	FIA_ADM_PCR.1(b)	This requirement supports O. MANAGE by requiring a TOE administrator user to enter the “setup” password before assuming the Setup Console Administrator role (which allows bypassing the TSF) for accessing system configuration functions on the Serial Console.
	FMT_MOF.1	This requirement supports O. MANAGE by specifying which functions of the TOE can be managed, and defining who can manage those functions.
	FMT_MSA.1(a)	This requirement supports O.MANAGE by allowing all TOE administrators to query the security attribute user group membership.
	FMT_MSA.1(b)	This requirement supports O.MANAGE by allowing only Privileged Administrators to modify and delete the security attributes user group membership and user password.
	FMT_MSA.3	This requirement supports O.MANAGE. Both the Administrative Access and Proxy SFPs are restrictive by default.

Objective	Requirement Addressing the Objective	Rationale
	FMT_MTD.1(a)	This requirement supports O.MANAGE by permitting all TOE administrators to view the system configuration, Administrative Access SFP rules, and Proxy SFP rules.
	FMT_MTD.1(b)	This requirement supports O.MANAGE by permitting only Privileged Administrators to modify the system configuration, Administrative Access SFP rules, and Proxy SFP rules.
	FMT_MTD.2	This requirement supports O.MANAGE by permitting Privileged Administrators to modify the limit on the size of the audit logs.
	FMT_SMF.1	This requirement supports O.MANAGE by specifying that the TOE supports configuration of the Proxy SFP.
	FMT_SMR.1	This requirement supports O.MANAGE by supporting three roles: Administrator, Privileged Administrator, and Setup Console Administrator.
	FMT_SMR.3	This requirement supports O.MANAGE by ensuring that Serial Console users can assume the Privileged Administrator and Setup Console Administrator roles on the Serial Console only by executing the required command, and providing the appropriate password.
O.NO_TOE_TAMPER The TOE must protect itself against external interference or tampering by untrusted subjects, or attempts by untrusted subjects within the scope of its control to bypass the TOE security functions.	FPT_RVM.1	This requirement supports O.NO_TOE_TAMPER by ensuring that all controlled protocol traffic received by the TOE is subject to the Proxy SFP. This ensures non-bypassability of the TSF when it is invoked.
	FPT_SEP.1	This requirement supports O.NO_TOE_TAMPER by ensuring that there are no other processes in the TSC that have access to the TSF or TSF data. The TOE itself is a dedicated operating system that has no other purpose but to provide the TSF.
O.REMOVE_ACTIVE The TOE must be able to remove active content from HTML pages delivered via a controlled protocol as defined by the Proxy SFP.	FDP_IFC.1	This requirement supports O.REMOVE_ACTIVE by including a policy language that enables the administrator to construct rules representing their site's information flow policy. The function then enforces those rules and takes the action specified.
	FDP_IFF.1	This requirement supports O.REMOVE_ACTIVE by supporting a wide range of attributes that can be used in the Proxy SFP to control the flow of information between the Internal and External Networks.
O.SCREEN_TYPE The TOE must disallow controlled protocol traffic of given content types as defined by the Proxy SFP.	FDP_IFC.1	This requirement supports O.SCREEN_TYPE by including a policy language that enables the administrator to construct rules representing their site's information flow policy. The function then enforces those rules and takes the action specified.

Objective	Requirement Addressing the Objective	Rationale
	FDP_IFF.1	This requirement supports O.SCREEN_TYPE by supporting a wide range of attributes that can be used in the Proxy SFP to control the flow of information between the Internal and External Networks.
O.SCREEN_URL The TOE must disallow controlled protocol traffic for given URLs as defined by the Proxy SFP.	FDP_IFC.1	This requirement supports O.SCREEN_URL by providing a policy language that enables authorized administrators to construct rules representing their site's information flow policy. The function then enforces those rules and takes the action specified.
	FDP_IFF.1	This requirement supports O.SCREEN_URL by supporting a wide range of attributes that can be used in the Proxy SFP to control the flow of information between the Internal and External Networks.

8.3.2 Rationale for SFRs Relating to IT Environment Security Objectives

The following table provides detailed evidence of coverage for each IT environment security objective.

Table 25 – Rationale for SFRs of the IT Environment

Objective	Requirement Addressing the Objective	Rationale
OE.NETWORK	FPT_RVM_HW.1	This requirement supports OE.NETWORK by requiring that all controlled protocol traffic must be routed through the TOE, ensuring that the target traffic cannot bypass the security functionality of the TOE hardware.
OE.NO_HW_TAMPER	FPT_RVM_HW.1	This requirement supports OE.NO_HW_TAMPER by requiring that secure access to the TOE can only be accomplished using the defined interfaces, ensuring that TOE security functions cannot be bypassed by tampering or interfering with the TOE hardware.
OE.PLATFORM	FPT_SEP_HW.1	This requirement supports OE.PLATFORM by requiring that the hardware platform hosting the TOE be dedicated only to TOE functions and processes.
OE.SECURE_PATH	FPT_ITC_ENV.1	This requirement supports OE.SECURE_PATH by ensuring that the IT environment provides mechanisms for the protection of TSF data being transmitted between the TOE and another IT product.
OE.TIMESTAMP	FPT_STM.1	This requirement supports OE.TIMESTAMP by requiring the IT environment to provide a reliable timestamp for the TOE's use.

8.4 Explicitly-Stated Requirements Rationale

Table 26 below provides rationale regarding the use of the explicitly-stated requirements found in this document.

Table 26 – Rationale for Use of Explicitly-Stated Requirements

Name	Description	Rationale
FIA_ADM_PCR.1(a)	Password controlled role	This SFR was stated explicitly (rather than using FIA_UAU.6) to specify that the re-authentication process requires verification against Privileged Administrator credentials that are different that those that were originally entered by the TOE administrator.
FIA_ADM_PCR.1(b)	Password controlled role	This SFR was stated explicitly (rather than using FIA_UAU.6) to specify that the re-authentication process requires verification against the Setup Console Administrator password that is different that those that were originally entered by the TOE administrator.
FPT_ITC_ENV.1	TSF data confidentiality during transmission	This SFR was stated explicitly (rather than using FPT_ITC.1) to specify that the IT environment (and not the TSF) is responsible for maintaining the confidentiality of TSF data being transmitted between the TSF and another IT product
FPT_RVM_HW.1	Non-bypassability of the TSP for hardware	This SFR was stated explicitly (rather than using FPT_RMV.1) to specify the need for the SGOS appliance to be placed in the network environment such that controlled protocol network traffic cannot bypass the security functionality provided by the appliance.
FPT_SEP_HW.1	TSF domain separation for hardware	This SFR was explicitly stated (rather than using FPT_SEP.1) to specify the responsibility of IT environment for providing and maintaining separate network paths for controlled protocol traffic and non-controlled protocol traffic.

8.5 Security Assurance Requirements Rationale

EAL2+ was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. At EAL2+, the TOE will have undergone a search for obvious flaws to support its introduction into the non-hostile environment.

8.6 Dependency Rationale

This ST satisfies all the requirement dependencies of the Common Criteria. Table 27 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met. In instances where a dependency is met through a component that is hierarchical to another component, explanations are provided in the Rationale column.

Table 27 – Functional Requirements Dependencies

SFR ID	Dependency	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1(a)	FAU_GEN.1	✓	
FAU_SAR.1(b)	FAU_GEN.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.4	FAU_STG.1	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	
	FMT_MSA.3	✓	
FIA_ADM_PCR.1(a)	No dependencies	✓	
FIA_ADM_PCR.1(b)	No dependencies	✓	
FIA_AFL.1	FIA_UAU.1(a)	✓	
FIA_UAU.1(a)	FIA_UID.1(a)	✓	
FIA_UAU.1(b)	FIA_UID.1(b)	✓	
FIA_UAU.5	No Dependencies	✓	
FIA_UAU.6(a)	No Dependencies	✓	
FIA_UAU.6(b)	No Dependencies	✓	
FIA_UAU.7	FIA_UAU.1(b)	✓	
FIA_UID.1(a)	No dependencies	✓	
FIA_UID.1(b)	No dependencies	✓	
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(a)	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(b)	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	

SFR ID	Dependency	Dependency Met	Rationale
FMT_MSA.3	FMT_MSA.1(b)	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(a)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(b)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.2	FMT_MTD.1(b)	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1(b)	✓	
FMT_SMR.3	FMT_SMR.1	✓	
FPT_ITC_ENV.1	No dependencies	✓	
FPT_RVM.1	No dependencies	✓	
FPT_RVM_HW.1	No dependencies	✓	
FPT_SEP.1	No dependencies	✓	
FPT_SEP_HW.1	No dependencies	✓	
FPT_STM.1	No dependencies	✓	

8.7 TOE Summary Specification Rationale

8.7.1 TOE Summary Specification Rationale for the Security Functions

Each subsection in the TOE Summary Specification (section 6) describes a security function of the TOE. Each subsection includes a set of requirements and describes how the requirements are satisfied by aspects of the corresponding security function. Table 28 below provides rationale as to how each SFR is met by the associated security function. The correspondence that the table provides also demonstrates that all security requirements are addressed and all security functions are necessary (i.e., they correspond to at least one security requirement). The set of security functions work together to satisfy all of the SFRs. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality. This section, in conjunction with the TOE Summary Specification section, provides evidence that the security functions are suitable to fulfill the TOE security requirements.

Table 28 – Rationale for TOE Security Functions Meeting SFRs

TOE Security Function	SFR Met	Rationale
Identification and Authentication	FIA_ADM_PCR.1(a) Password controlled role	The Identification and Authentication TSF meets this requirement by ensuring that Administrators use proper credentials to assume the Privileged Administrator role.

TOE Security Function	SFR Met	Rationale
	FIA_ADM_PCR.1(b) Password controlled role	The Identification and Authentication TSF meets this requirement by ensuring that Administrators use proper credentials to assume the Serial Console Administrator role.
	FIA_AFL.1 Authentication failure handling	The Identification and Authentication TSF meets this requirement by providing measures to handle failed authentication attempts.
	FIA_UAU.1(a) Timing of authentication	The Identification and Authentication TSF meets this requirement by ensuring that end users provide credentials (if required by the Proxy SFP) before being granted access to controlled actions.
	FIA_UAU.1(b) Timing of authentication	The Identification and Authentication TSF meets this requirement by ensuring that Serial Console users authenticate before being granted access to Serial Console functions.
	FIA_UAU.5 Multiple authentication mechanisms	The Identification and Authentication TSF meets this requirement by providing multiple (based on the login location and the desired role), well-defined methods of authenticating to the TOE.
	FIA_UAU.6(a) Re-authenticating	The Identification and Authentication TSF meets this requirement by ensuring that end users must provide credentials for each access to controlled protocol traffic requiring authentication.
	FIA_UAU.6(b) Re-authenticating	The Identification and Authentication TSF meets this requirement by ensuring that TOE Administrators re-authenticate (using a specific password) before assuming the Privileged Administrator role on the Serial Console.
	FIA_UAU.7 Protected authentication feedback	The Identification and Authentication TSF meets this requirement by displaying no feedback to the Serial Console during the authentication process.
	FIA_UID.1(a) Timing of identification	The Identification and Authentication TSF meets this requirement by ensuring that end users are properly identified before allowing any other TSF-mediated actions to be performed.
	FIA_UID.1(b) Timing of identification	The Identification and Authentication TSF meets this requirement by ensuring that Serial Console users are properly identified before allowing any other TSF-mediated actions to be performed.
Protection of the TSF	FPT_RVM.1 Non-bypassability of the TSP	The Protection of the TSF TSF meets this requirement by ensuring that the TSP enforcement mechanisms must be executed before allowing any TSF-mediated actions to be performed.
	FPT_SEP.1 TSF domain separation	The Protection of the TSF TSF meets this requirement by ensuring that the TOE has a separate, dedicated, and secure domain in which to operate.
Security Audit	FAU_GEN.1 Audit data generation	The Security Audit TSF meets this requirement by providing an audit generation capability that records the necessary information about the required events.

TOE Security Function	SFR Met	Rationale
	FAU_SAR.1(a) Audit review	The Security Audit TSF meets this requirement by providing Privileged Administrators with the ability to read and interpret all information in the System Events log.
	FAU_SAR.1(b) Audit review	The Security Audit TSF meets this requirement by providing a mechanism for Access Log upload targets to read and interpret all information in the Access Logs.
	FAU_STG.1 Protected audit trail storage	The Security Audit TSF meets this requirement by protecting stored audit records from unauthorized deletion.
	FAU_STG.4 Prevention of audit data loss	The Security Audit TSF meets this requirement by providing a mechanism for overwriting older audit records when the audit trail is full.
Security Management	FMT_MOF.1 Management of security functions behaviour	The Security Management TSF meets this requirement by restricting the ability to manage the Proxy SFP and Administrative SFP to only Privileged Administrators.
	FMT_MSA.1(a) Management of security attributes	The Security Management TSF meets this requirement by enforcing administrative access policies allowing TOE administrators to query on the security attribute *user group membership*.
	FMT_MSA.1(b) Management of security attributes	The Security Management TSF meets this requirement by enforcing administrative access policies allowing only Privileged Administrators to modify and delete information associated with the security attributes *user group membership* and *user password*.
	FMT_MSA.3 Static attribute initialisation	The Security Management TSF meets this requirement by providing restrictive default values (which can be overridden by Privileged Administrators) for attributes used to enforce the TOE's security mechanisms.
	FMT_MTD.1(a) Management of TSF data	The Security Management TSF meets this requirement by allowing TOE administrators to query information regarding the system's configuration, Administrative SFP, and Proxy SFP.
	FMT_MTD.1(b) Management of TSF data	The Security Management TSF meets this requirement by allowing only Privileged Administrators to change defaults and modify information regarding the system's configuration, Administrative SFP, and Proxy SFP.
	FMT_MTD.2 Management of limits on TSF data	The Security Management TSF meets this requirement by allowing only Privileged Administrators to set limits on audit log sizes, and by providing a mechanism to overwrite the oldest audit log records if that limit is reached or exceeded.
	FMT_SMF.1 Specification of management functions	The Security Management TSF meets this requirement by providing specific management functions for administering the TOE.

TOE Security Function	SFR Met	Rationale
	FMT_SMR.1 Security roles	The Security Management TSF meets this requirement by maintaining the roles *Administrator*, *Privileged Administrator*, and *Setup Console Administrator*.
	FMT_SMR.3 Assuming roles	The Security Management TSF meets this requirement by requiring that assuming the role of Privileged Administrator (using the Serial Console) or Setup Console Administrator can only be accomplished via an explicit request.
User Data Protection	FDP_ACC.1 Subset access control	The User Data Protection TSF meets this requirement by enforcing access control policies on TOE administrators requesting the Privileged Administrator role.
	FDP_ACF.1 Security attribute based access control	The User Data Protection TSF meets this requirement by enforcing policy-based controls for objects based on certain security attributes of both the requesting subject and the requested access operation.
	FDP_IFC.1 Subset information flow control	The User Data Protection TSF meets this requirement by enforcing proxy policies on the flow of controlled protocol traffic traversing the TOE.
	FDP_IFF.1 Simple security attributes	The User Data Protection TSF meets this requirement by implementing and enforcing Proxy policies to control the flow of information based on certain security attributes of both the requesting subject and the information itself.

The only security mechanism that is realized by a probabilistic or permutational implementation is the password mechanism. For an analysis of the Strength of Function, refer to section 8.8 of this document.

8.7.2 TOE Summary Specification Rationale for the SARs

EAL2+ was chosen to provide a basic level of independently assured security in the absence of ready availability of the complete development record from the vendor. The chosen assurance level is consistent with the postulated threat environment.

While the TOE may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in (or protected by) other products designed to address threats that correspond with the intended environment. The chosen assurance level was also selected for conformance with the client's needs.

8.7.2.1 Configuration Management

The Configuration Management documentation provides a description of tools used to control the configuration items and how they are used at Blue Coat. The documentation provides a complete configuration item list and a unique reference for each item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

Corresponding CC Assurance Components:

- ACM_CAP.2 – Configuration Items

8.7.2.2 Delivery and Operation

The Delivery and Operation documentation provides a description of the secure delivery procedures implemented by Blue Coat to protect against TOE modification during product delivery. The Installation Documentation provided by Blue Coat details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the administrator on the TOE configuration parameters and how they affect the TSF.

Corresponding CC Assurance Components:

- ADO_DEL.1 – Delivery Procedures
- ADO_IGS.1 – Installation, Generation and Start-Up Procedures

8.7.2.3 Development

The Blue Coat design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and errors message for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, and all externally-visible TSF interfaces.
- The Correspondence Analysis demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the High-Level Design.

Corresponding CC Assurance Components:

- ADV_FSP.1 – Informal Functional Specification
- ADV_HLD.1 – Descriptive High-Level Design
- ADV_RCR.1 – Informal Representation Correspondence

8.7.2.4 Guidance Documentation

The Blue Coat Guidance documentation provides administrator guidance on how to securely operate the TOE. The Administrator Guidance provides descriptions of the security functions provided by the TOE. Additionally, it provides detailed accurate information on how to administer the TOE in a secure manner and how to effectively use the TSF privileges and protective functions.

This assurance class also requires the inclusion of a User Guidance component to direct end users in the proper use of the TOE. However, end users direct interaction with the TOE is limited to the entry of a password for policy-controlled access to controlled-protocol traffic. Since the configuration of the policies is discussed in the Administrator Guidance, that single document is considered to contain both components. However, for completeness, both assurance components are noted in the bulleted list below.

Corresponding CC Assurance Components:

- AGD_ADM.1 – Administrator Guidance
- AGD_USR.1 – User Guidance

8.7.2.5 Life Cycle Support

The Life Cycle Support documentation outlines the steps taken at Blue Coat to capture, track and remove bugs as part of their basic flaw remediation process. This document shows that all flaws are recorded and that the system tracks them to completion.

Corresponding CC Assurance Components:

- ALC_FLR.1 – Basic Flaw Remediation

8.7.2.6 Tests

There are two components that make up the Test documentation. The Coverage Analysis demonstrates the testing performed against the functional specification. It also demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. Blue Coat Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided.

Corresponding CC Assurance Components:

- ATE_COV.1 – Evidence of Coverage
- ATE_FUN.1 – Functional Testing

8.7.2.7 Vulnerability Assessment

The Vulnerability Assessment consists of two components. The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum SOF requirements. A Vulnerability Assessment is provided to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, the document provides evidence of how the TOE is resistant to obvious attacks.

Corresponding CC Assurance Components:

- AVA_SOF.1 – Strength of TOE Security Function Evaluation
- AVA_VLA.1 – Developer Vulnerability Analysis

8.8 Strength of Function

A strength of function rating of SOF-basic was claimed for this TOE to meet the EAL2+ assurance requirements, this SOF is sufficient to resist the threats identified in Section 3. Section 4 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Section 8 demonstrates that the security objectives for the TOE and the IT environment are satisfied by the security requirements. The evaluated TOE is intended to operate in commercial and DoD low robustness environments processing unclassified information. The overall TOE SOF claim is SOF-basic because this SOF is sufficient to resist the threats identified in Section 3.2.

The relevant security functions and security functional requirements which have probabilistic or permutational functions are:

- FIA_ADM_PCR.1(a) – Password controlled role
- FIA_ADM_PCR.1(b) – Password controlled role
- FIA_UAU.1(a) – User authentication before any action
- FIA_UAU.1(b) – User authentication before any action

9 Acronyms

Table 29 lists the acronyms used throughout this document.

Table 29 – Acronyms

Acronym	Definition
CC	The Common Criteria for Information Technology Security Evaluation
CEM	The Common Methodology for Information Technology Security Evaluation
CLI	Command Line Interface
CPL	Content Policy Language
DNS	Domain Name System
DOS	Disk Operating System
DRTR	Dynamic Real-Time Rating™
EAL	Evaluation Assurance Level
ELFF	Extended Log File Format
FTP	File Transfer Protocol
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ICP	Internet Control Protocol
IFP	Information Flow Protection
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
MIME	Multipurpose Internet Mail Extensions
MMS	Microsoft Media Server
NCSA	National Center for Supercomputing Applications
OCS	Original Content Server
OLE	Object Linking and Embedding
OS	Operating System
P2P	Peer-To-Peer
PP	Protection Profile
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments
RPC	Remote Procedure Call
RTSP	Real Time Streaming Protocol
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement

Acronym	Definition
SGOS	ProxySG Operating System
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOF	Strength of Function
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TACACS+	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
URL	Universal Resource Locator
W3C	World Wide Web Consortium
WCCP	Web Cache Control Protocol