Blue Coat ProxySG Operating System, v3.2.4.8 Security Target
September 1, 2005
BCS-0290-(1) Blue Coat ProxySG v3-2-4-8 Security Target

Blue Coat Systems, Inc.
650 Almanor Ave.
Sunnyvale, CA 94085

Phone: 408-220-2200
Fax: 408-220-2250

DOCUMENT INTRODUCTION

Prepared By:	Prepared For:
Blue Coat Systems	Blue Coat Systems
650 Almanor Avenue	650 Almanor Avenue
Sunnyvale, CA 94085	Sunnyvale, CA 94085

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Blue Coat ProxySG Operating System, v3.2.4.8. This Security Target (ST) defines a set of assumptions about the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which satisfy the set of requirements.

REVISION HISTORY

Rev	Description
	May 16, 2003 Initial release.
1	May 30, 2003, Added models 400-0 and 400-1 to section 2.2
2	June 2, 2003, Corrected formatting issues
3	July 9, 2003, Addressed comments from COACT
4	July 28, 2003, Addressed comments from COACT, Inc.
5	July 31, 2003, Corrected items regarding explicitly stated SFR and SOF
6	March 27, 2004, Updated TOE to reflect certification of the ProxySG (SG3) and the features added to this release.
7	July 9, 2004, Updated to reflect use of CLI for creating users
8	July 13, 2004, Updated to use v3.2.4, other consistency changes
9	September 14, 2004, Updated front matter for 3.2.4, SOF

10 November 5, 2004, Clarify controlled protocols

11 December 2, 2004, Updated to v3.2.4.8

12 June 24, 2005, Updated FPT_SEP and FPT_RVM

13 July 7, 2005, Addressed comments from evaluators

14 September 1, 2005 Updated document references in Table 10 and removed line numbering.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

1 Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Blue Coat ProxySG Operating System, v3.2.4.8. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.1*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9* and all National Information Assurance Partnership (NIAP) interpretations through June 30, 2003. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

This section provides identifying information for the Blue Coat ProxySG Operating System, v3.2.4.8 Security Target by defining the Target of Evaluation (TOE).

1.1.1 Security Target Name

Blue Coat ProxySG Operating System, v3.2.4.8 Security Target

1.1.2 TOE Reference

Blue Coat ProxySG Operating System, v3.2.4.8

1.1.3 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) from the *Common Criteria for Information Technology Security Evaluation, Version 2.1*.

1.1.4 Keywords

Proxy, Gateway, Traffic Filtering, Content Filtering, Transparent Authentication, Proxy SFP, Web Security, Safe Browsing.

1.2 TOE Overview

Blue Coat ProxySG Operating System, v3.2.4.8 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. This layer of security can be used to control, protect, and monitor the Internal Network's use of controlled protocols on the External Network. The *controlled protocols* are HTTP, FTP, SOCKS and AIM, MSN and Yahoo Instant Messenger. This is achieved by enforcing a configurable policy on external controlled protocol

traffic to and from the Internal Network users. The policy may include authentication, authorization, content filtering, and auditing. Also, internal IP addresses are obfuscated through the proxy, thereby helping to protect internal machines from direct Internet attack.

1.2.1 Security Target Organization

Chapter 1 of this ST provides introductory and identifying information for the TOE.

Chapter 2 describes the TOE and provides some guidance on its use.

Chapter 3 provides a security environment description in terms of assumptions, threats and organisational security policies.

Chapter 4 identifies the security objectives of the TOE and of the Information Technology (IT) environment.

Chapter 5 provides the TOE security and functional requirements, as well as requirements on the IT environment.

Chapter 6 is the TOE Summary Specification, a description of the functions provided by the TOE to satisfy the security functional and assurance requirements.

Chapter 7 identifies claims of conformance to a registered Protection Profile (PP).

Chapter 8 provides a rationale for the security objectives, requirements, TOE summary specification and PP claims.

1.3 Common Criteria Conformance

The Blue Coat ProxySG Operating System, v3.2.4.8 is compliant with the Common Criteria (CC) Version 2.1 functional requirements (Part 2), assurance requirements (Part 3), and all National Information Assurance Partnership (NIAP) interpretations through June 30, 2003.

1.4 Protection Profile Conformance

The Blue Coat ProxySG Operating System, v3.2.4.8 does not claim conformance to any registered Protection Profile.

1.5 Document Conventions

The CC defines four operations on security functional requirements. The font conventions below identify the conventions for the operations defined by the CC.

Assignment: indicated with bold text

Selection: indicated with underlined text

Refinement: ***indicated with bold text and italics***

Iteration: indicated with typical CC requirement naming followed by a number in parenthesis for each iteration (e.g., FMT_MOF.1 (1))

CHAPTER 2

2 TOE Description

This section describes the target of evaluation (TOE) configuration of the Blue Coat ProxySG Operating System, v3.2.4.8 (SGOS). It distinguishes the physical and logical boundaries of the TOE. It also describes the user types, highlights the assets and capabilities of the TOE, and defines the protection mechanisms and access rights to these assets.

2.1 Overview

Blue Coat ProxySG Operating System, v3.2.4.8 (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. This layer of security can be used to control, protect, and monitor the Internal Network's use of controlled protocols on the External Network. The *controlled protocols* are HTTP, FTP, SOCKS and AIM, MSN and Yahoo Instant Messenger. This is achieved by enforcing a configurable policy (Proxy SFP) on controlled protocol traffic to and from the Internal Network users. The policy may include authentication, authorization, content filtering, and auditing. Also, internal IP addresses are obfuscated through the proxy, thereby helping to protect internal machines from direct Internet attack.

2.2 Architecture Description

The TOE is an operating system that is delivered on a proprietary hardware device. A discussion of secure usage will be given to put the components of the SGOS in context.

Administrative access to the TOE is provided by using a terminal emulator over a direct serial connection to the appliance: the Serial Console. The Serial Console is part of the TOE and controls access to the Setup Console (outside the TOE, used for initial configuration) 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.

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, DNS server, the Console Administrator username and password, and the Setup Console password. Once the TOE is operational, the Setup Console is no longer used. Access to the Setup Console is mediated by the Serial Console (which is inside the TOE) and in the evaluated

configuration is protected by a password. Additional configuration and policy definition is done through the Command Line Interface (CLI) by selecting the CLI from the Serial Console menu. Although the Administrator can use SSH through the Internal Network interface to access the CLI of SGOS or use a Web interface over an encrypted SSL connection to configure the SGOS using a graphical interface, the TOE does not include the SSH or SSL interfaces. The TOE will employ the CLI via the Serial Console to administer the machine as described above.

In order to act as a proxy and control controlled protocol traffic from the Internal Network to the External Network, that controlled protocol 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. 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. This traffic is presented to the Internal Network port on the proxy. The users' software is not changed and the user may be unaware that controlled protocol traffic is traversing the proxy.

After initial configuration via the Setup Console, the TOE is operational and behaves as a proxy that denies all traffic (as the default). To enable controlled protocol traffic flow, an administrator defines information flow policy rules, which comprise the Proxy SFP. These rules can require authentication of End Users; an administrator creates End Users by using the CLI 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 ProxySG Content Policy Language Guide.

The assets of the TOE are the local user list, the Proxy SFP Rules, the Administrative Access SFP Rules, the audit logs, and the system configuration. The two primary security capabilities of the TOE are restricting controlled protocol traffic between the networks and managing the SGOS. The tangible assets and management functions are protected by restricting access to administrators. Only administrators can log into the TOE CLI, access its configuration and configure policies. There are also assets of the IT Environment that need to be enumerated,

for they are protected by the TOE as well. The TOE protects the IP addresses of Internal Network machines and protects these machines from malicious content delivered via controlled protocols. An End User's Internal Network IP address is obfuscated by SGOS when their controlled protocol traffic is sent to the External Network. Also, malicious content carried by controlled protocols from the External Network can be blocked by the Proxy SFP.

Model	WAN bandwidth	Disk	RAM	Interfaces	Number of users	Size
400-0	1.5 MBit/s	40 GB	256 MB	2 10/100 Base T	100	1U
400-1	1.5 MBit/s	80 GB	512 MB	2 10/100 Base T	100	1U
800-0	1.5 MBit/s	18 GB	512 MB	2 10/100 Base T	100	1U
800-0B	3 MBit/s	36 GB	768 MB	2 10/100 Base T	200	1U
800-1	4 MBit/s	72 GB	1 GB	2 10/100 Base T	400	1U
800-2	8 MBit/s	144 GB	1.5 GB	2 10/100 Base T	700	1U
800-3	10 MBit/s	288 GB	2 GB	2 10/100 Base T	1500	1U
8000-1	35 MBit/s	146 GB	1 GB	4 integrated 10/100/1000 on board ports, optional fiber available	1500	4U
8000-2	45 MBit/s	288 GB	2 GB	4 integrated 10/100/1000 on board ports, optional fiber available	3000	4U
8000-3	80 MBit/s	434 GB	3 GB	4 integrated 10/100/1000 on board ports, optional fiber available	5000	4U
8000-4	90 MBit/s	576 GB	4 GB	4 integrated 10/100/1000 on board ports, optional fiber available	8000	4U

Table 1 - Supported Hardware Platforms

SGOS is delivered on one of several appliances manufactured by Blue Coat Systems. These included the SG400 line, SG800 line and the SG8000 line of products. Every appliance runs the same software, the TOE. Differences in each model are to allow for different performance and scalability requirements in each customer site. All models use motherboards with Intel processors. Differences in throughput are driven by processor speed, number of processors, amount of memory, and number and size of disks within each product. In addition, the SG8000 product line offers redundant power supplies and multiple Gigabit Ethernet network interface cards with optional fiber cards.

2.3 Physical Boundaries

The physical boundary of the TOE is the ProxySG Operating System software as shown in Figure 1 below.

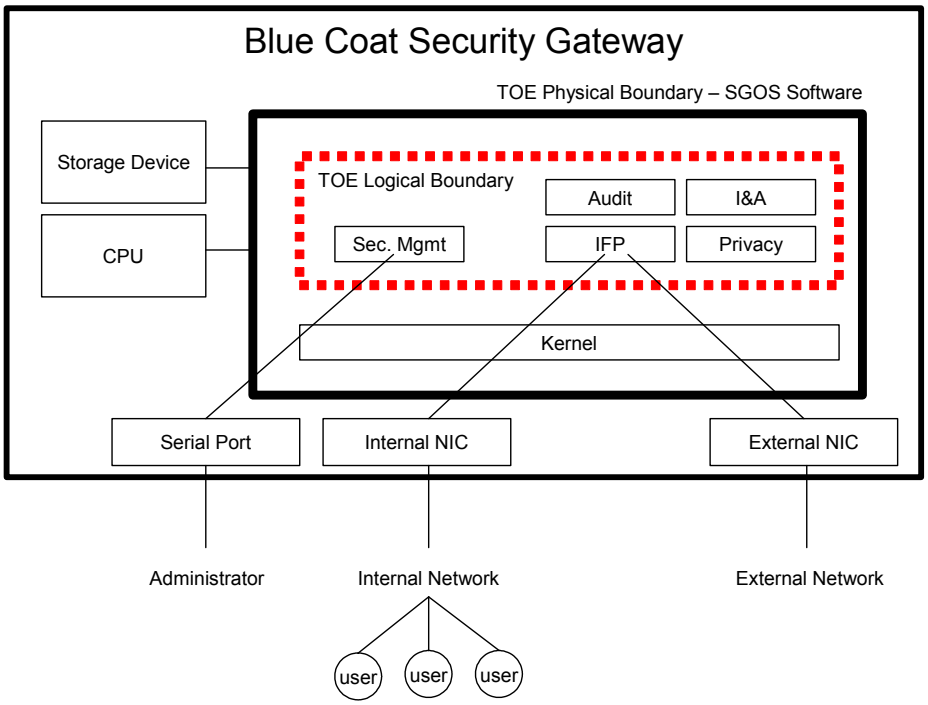

Figure 1 - Architecture Diagram

The physical boundary includes the kernel and all of the security and management engines of SGOS. SGOS has specific requirements of the hardware on which it runs. These requirements are described in the IT Environment Assumptions section below.

2.4 Logical Boundaries

The logical boundaries of the TOE are defined by the protection mechanisms provided by the TOE as shown in Figure 1 above and detailed below.

2.4.1 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 includes 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 using the administrative CLI.

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, W3C, and NCSA are provided for convenience. 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. The NCSA format is described for the purposes of this ST. If the 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.

2.4.2 Configurable Policies (SFPs)

The TOE provides the administrator with the ability to define security policy using the ProxySG Content Policy Language (CPL). There is also a graphical user interface known as the Visual Policy Manager (VPM) that provides an easier interface to configuration and generates the CPL policy in the background for the administrator. The VPM is not part of the TOE. The CPL language allows rules to be created that perform certain actions based on a set of conditions. The conditions and actions depend on the kind of policy being written. Policy written in CPL is evaluated according to the rules described in the ProxySG Content Policy Language Guide.

2.4.2.1 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, allowing or denying access.

2.4.2.2 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 characteristics of the controlled protocol traffic such as user identity, URL, time, method (requested action) and content-type. 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.

2.4.3 Identification & Authentication

Users (both administrative users and end users) are identified by user name and authenticated by passwords. Authentication is tied to the user's session. Users are defined by adding user accounts to the local user list. Once accounts are defined, they can be referred to by the Proxy SFP Rules or Administrative Access SFP Rules. The Console Administrator is a distinguished user name that is configured rather than defined in a local user list. It defines an administrative user that is exempt from the Administrative Access SFP rules.

End user sessions are established when the user's user agent (e.g. browser) establishes a TCP/IP connection to the proxy appliance. Initially the session is unauthenticated. If the user's controlled protocol traffic matches a Proxy SFP rule that requires authentication, the user will be required to provide appropriate credentials. Once the credentials have been verified, the session is considered authenticated and controlled protocol traffic will be permitted (subject of course to the rest of the Proxy SFP). All further requests on that session will be treated as already authenticated.

If a user (other than the console administrator) fails authentication, they are again challenged for credentials. Once the number of authentication failures reaches a configurable threshold, the account is disabled. A disabled account cannot be used; an attempt to use it results in immediate denial without checking the offered password. The account can be enabled manually, or it may automatically re-enable after a configurable time.

Authentication details differ depending on whether transparent or explicit authentication is being used. Explicit authentication is done according to the HTTP proxy authentication specification (RFC 2616). Explicit authentication requires an explicit proxy deployment.

Transparent authentication is somewhat more complex. The first time authentication is required for the End User, an HTTP redirect response is sent to the user's client (if the client understands redirects). The target of this redirect is the proxy appliance itself (a so-called authentication virtual URL); this URL contains the complete original URL. The client submits the original request to the virtual URL. The proxy intercepts this request and authenticates the user using server authentication as specified in RFC 2616. If authentication is successful, the proxy generates a *surrogate credential.* The proxy then redirects the client to the client to the original URL with the surrogate credential as a query. When the proxy

processes this request it verifies that the surrogate credential is valid. If so, the proxy generates another redirect response. This response is to the original URL (without the surrogate credential query) and sets a cookie in the client containing the surrogate credential. The browser now requests the originally requested URL, and supplies the cookie. The proxy again validates the surrogate credential, and if it is valid, processes the request normally. Future requests to the same domain will carry the surrogate credential cookie, and the session will be authenticated without doing the redirect (for the lifetime of the surrogate credential, which is configured by administrators). If the user's client does not understand HTTP redirect messages, authentication is done using server authentication as specified in RFC 2616; no surrogate credential is used. Transparent authentication can be used in explicit or transparent deployments.

An administrative session is requested when a user of the Serial Console requests the CLI (via a menu choice). An administrator must correctly authenticate before being granted access to the SGOS CLI. If an administrator fails authentication, they continue to be prompted for correct credentials.

2.4.4 Security Management

SGOS provides for two different kinds of administrators: console administrators and (ordinary) administrators. Console administrators are those individuals that know the configured console administrator username and password; they are not subject to the rules in the Administrative Access SFP. Ordinary administrators are users (from the local user list) who have been granted administrator privilege by the Administrative Access SFP and so are subject to those rules. The term "administrator" refers to both in contexts where the distinction is unimportant.

There are as well two administrative roles: normal and privileged. Privileged administrators can modify the TOE configuration and define policies. Administrators become privileged by successfully executing the "enable" command, which requires a password. Console administrators must know the configured "enable" password to become privileged. Ordinary administrators are granted privileged access by a rule in the Administrative Access SFP (they are re-authenticated when executing the "enable" command).

An SGOS Administrator has a variety of configuration and policy capabilities. An administrator can configure SGOS security attributes including the network interfaces, Proxy

SFP, Administrative Access SFP, auditing, and End User accounts. The default configuration of the TOE is to deny all traffic. A Proxy SFP can then be created that explicitly defines the controlled protocol traffic that is allowed to pass. Administrators are responsible for crafting policies that reflect their organization needs.

2.4.5 Privacy

The only IP address sent out from the TOE to the External Network is the IP address of the TOE itself. Internal IP addresses are never broadcast beyond the TOE. This protects Internal Network machines from a direct external attack via controlled protocols.

2.4.6 Evaluated Configuration

The evaluated configuration consists of the following security services functionality to be included in the evaluation:

Policy architecture triggers: define control through multiple triggers, such as user/group, time, protocol, application, file/MIME type, request method

Policy architecture actions: Multiple actions including allow, deny, rewrite, redirect, email management, log request, authenticate and set authentication mode.

Proxy or transparent installation: Intercepts non-proxied requests and applies policy.

HTTP port listen: Define non-8080 port for HTTP traffic

On box content filtering: Restrict access to sites, supporting subscription-based filtering from Websense, SmartFilter, SurfControl and locally defined lists

Active content control: Disallow active HTML content (Java, ActiveX controls, etc.)

Filter List (deny): Restrict access to certain sites

Header transformation: Referrer headers and other headers can be removed or replaced

Accept/Deny inbound connections separately for each interface: TOE can be configured in parallel with a firewall

Source IP access restriction: Restrict access based on client IP address

Custom error messages: End user error messages can be defined by administrator

FTP Proxy: full FTP proxy functionality

SOCKS v4/v5 proxy: Additional proxy service for IM and other SOCKS proxy applications

Instant Messenger traffic control: Allow/disallow IM text, allow/disallow file transfer/voice/video (by file type, size or global), allow/disallow chat room, log and action (kill message, email management) on keywords in IM stream.

Automatic Account Lockout: user accounts are automatically disabled after the number of wrong password attempts reaches a threshold.

2.4.7 Items Not Included in Evaluation

The ProxySG includes the following security functionality that will not be included in this evaluation:

Streaming
QuickTime Proxy
DNS Proxy
Telnet Proxy
Off box content filtering

Off box virus scanning

SSL termination

Remote management (browser, ssh, telnet)

Bridging (hardware or software)

Dynamic or Static Bypass

Refresh and Pipelining

ICP and WCCP

Visual Policy Manager

Attack-detection

Authentication realms other than "local"

Clusters, fail-over, chained proxies

RADIUS or TACACS+ splash pages

Content-management commands

Syslog, Health checks, SNMP, Heartbeats and Diagnostics

<forward> policy

authenticate.mode() settings other than as described in this document

Encrypted access logs

CHAPTER 3

3 TOE Security Environment

This chapter identifies assumptions (A), threats (T), and organisational security policies (P) related to the TOE. Assumptions are given to detail the expected environment and operating conditions of the TOE. Threats are those that are addressed by the TOE. In addition, organisational security policies are specific rules, procedures, or practices that are part of the TOE.

3.1 Threats

The threats identified in the following subsections are addressed by the TOE and IT environment, respectively. For the threats below, attackers are assumed to be of low attack potential.

T.TAMPER	The TOE is tampered with, bypassed, or cannot be verified as working properly.

3.2 Assumptions

Assumptions are divided into three groups: personnel assumptions, physical environment assumptions, and IT environment assumptions. Personnel assumptions describe characteristics of personnel who are relevant to the TOE. Physical environment assumptions describe characteristics of the non-IT environment that the TOE is deployed in. IT environment assumptions describe the technology environment that the TOE is operating within.

3.2.1 Personnel Assumptions

A.NOEVILADMIN	Administrators are non-hostile and follow all administrator guidance when using the TOE. Administration is competent and on-going.

3.2.2 Physical Environment Assumptions

A.ENVIRON	The TOE will be 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.

3.2.3 IT Environment Assumptions

A.PLATFORM	The platform used to host the TOE is one of the platforms listed in Table 1 and functions as documented for SGOS.
A.INSTALL	The SGOS device has been installed and configured according to the appropriate installation guides.
A.CONTROLLED	The protocols to be controlled by the SGOS device are HTTP, FTP, SOCKS and AIM, MSN and Yahoo Instant Messenger. These are the controlled protocols.
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.NOSSL	SSL (encrypted) traffic cannot by analysed by the SGOS device (as it cannot decrypt it), and so the device cannot enforce policy that requires content analysis on that traffic. Therefore, A.NOSSL states that SSL (encrypted) traffic is not subject to control by the SGOS device.
A.PASSWORD	Passwords for the Console Administrator and End User accounts, and the “enable” password are at least five characters in length, and may not be a dictionary word
A.DEDICATED	All controlled protocol network traffic is received directly by the TOE. The platform is dedicated to supporting the TOE and supports no other systems or processes.

3.3 Organisational Security Policies

P.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.
P.MANAGE	The TOE must provide secure management of the system configuration, the Proxy SFP and the Administrative Access SFP
P.FILTERED-URLS	End Users must not access unauthorized URLs, (e.g., URLs referring to pornographic content) via controlled protocols on the External Network.
P.CONTENT-TYPE	End Users must not access unauthorized content types via controlled protocols on the External Network. This may be because the content-type is deemed unsuitable (e.g., streaming media), or because it has a high risk of carrying hostile content (e.g., executables).
P.ACTIVE-CONTENT	The TOE must provide a means to remove active content (e.g. Java, JavaScript, ActiveX) in HTML pages delivered via controlled protocols.
P.POST-TYPE	End Users must not POST unauthorized content-types to the External Network using controlled protocols.
P.HIDE-IP	Internal client IP addresses must not be visible on the External Network when using controlled protocols.
P.NON-ANONYMOUS	Access to some resources via controlled protocols on the External Network may be restricted to particular End Users.
P.ADMIN	Only authorized individuals may perform administrative actions on the TOE.

CHAPTER 4

4 Security Objectives

The objectives identified in the following subsections are addressed by the TOE and the operating environment, respectively.

4.1 Security Objectives for the TOE

O.SCREEN_URL	The TOE must disallow controlled protocol traffic for given URLs 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.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.MASK_IP	The TOE must never transmit an internal client IP address to the External Network when using a controlled protocol.
O.AUTHENTICATE	The TOE must require the Administrator to authenticate before gaining access to the CLI (administrative interface) of the TOE, and End Users to authenticate if their controlled protocol traffic matches a Proxy SFP rule which requires authentication.[1]
O.NOTAMPER	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.

[1] Not all Proxy SFP rules require authentication. See FDP_IFF.1 for details 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.MANAGE	The TOE must provide secure management of the system configuration, the Administrative Access SFP and the Proxy SFP.

4.2 Security Objectives for the Environment

OE.ADMIN	The Administrator must be non-malicious and follow all guidance.
OE.NETWORK	All plaintext controlled protocol traffic between the Internal and External Networks traverses the SGOS device; SSL (encrypted) traffic does not.
OE.ENVIRON	The physical environment must be suitable for supporting a computing device in a secure setting.
OE.PLATFORM	The TOE hardware is one of the platforms listed in Table 1. This platform will function according to the documentation for SGOS.
OE.TIME	The platform hosting the TOE must provide a reliable timestamp for use by the TOE.
OE.PASSWORD	Passwords for the Administrator and End User accounts and the "enable" password will be at least five characters in length and not be a dictionary word.
OE.NOTAMPER	The hardware of the IT Environment 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.

4.3 Rationale for Security Objectives for the TOE

This section provides the rationale that all security objectives are traced back to aspects of the addressed threats, organizational security policies, or assumptions.

O.SCREEN_URL	Disallowing controlled protocol traffic to certain URLs will prevent End Users from accessing (either intentionally or accidentally) pornographic or other unauthorized URLs via a controlled protocol. This addresses P.FILTERED_URLS.
O.SCREEN_TYPE	Disallowing controlled protocol traffic of certain content types will prevent End Users from accessing (either intentionally or accidentally) via a controlled protocol resources having forbidden content types. This addresses P.CONTENT-TYPE and P.POST_TYPE.
O.REMOVE_ACTIVE	Removing active content from HTML pages delivered via a controlled protocol prevents this content from being executed on client machines, preventing the content from taking hostile actions. This addresses P.ACTIVE-CONTENT.
O. MASK_IP	Not transmitting the IP addresses of internal machines when using a controlled protocol will prevent external entities from tracking and targeting an internal machine. This addresses P.HIDE-IP.
O.AUTHENTICATE	Requiring End Users to authenticate to receive specific external resources via a controlled protocol prevents users from accessing those specific restricted resources without proving their identity. This addresses P.NON-ANONYMOUS. Requiring administrators to authenticate before taking administrative actions prevents unauthorized access to the administrative CLI. This addresses P.ADMIN.
O.NOTAMPER	A tamperproof, non-bypassable, verifiable TOE will enable administrators to ensure proper functioning of the TOE. This

partially addresses T.TAMPER (see OE.NOTAMPER as well).

O.AUDIT — Having an audit trail supports the diagnosis of attacks and the verification of proper system functionality to satisfy P.AUDIT.

O.MANAGE — Facilitating TOE configuration by the Administrator will enable the TOE to properly enforce its site-specific security policy. This addresses P.MANAGE.

	P.FILTEREDURLS	P.CONTENT-TYPE	P.ACTIVE-CONTENT	P.POST_TYPE	P.HIDE-IP	P.NON-ANONYMOUS	P.ADMIN	T.TAMPER	P.AUDIT	P.MANAGE
O.SCREEN_URL	X									
O.SCREEN_TYPE		X		X						
O.REMOVE_ACTIVE			X							
O.MASK_IP					X					
O.AUTHENTICATE						X	X			
O.NOTAMPER								X		
O.AUDIT									X	
O.MANAGE										X

Table 2 - Mappings Between Threats and Policies to Security Objectives for the TOE

4.4 Rationale for Security Objectives for the Environment

This section provides the rationale that all security objectives for the operating environment are traced back to aspects of the addressed threats, organizational security policies, or assumptions.

OE.ADMIN — Having a trusted, educated, and competent administrator addresses the assumptions of A.NOEVILADMIN.

OE.NETWORK — This objective supports A.NETWORK and A.NOSSL. To meet the organizational security policies as stated, the TOE must be able to analyse the content of the controlled protocol traffic between the Internal and External Networks, and must

	see all controlled protocol traffic that is subject to policy. This objective ensures that all controlled protocol traffic that flows through the SGOS device is plaintext (thus supporting A.NOSSL) and that all plaintext controlled protocol traffic flows through the device (thus supporting A.NETWORK).
OE.ENVIRON	Having a physical environment that is secure and fit for a computing device addresses A.ENVIRON.
OE.PLATFORM	This objective supports A.PLATFORM and A.DEDICATED. This is because the objective requires a specialized, dedicated hardware device to support the TOE and a reliable timestamp.
OE.TIME	This objective supports P.AUDIT by providing a reliable timestamp for use by the TOE.
OE.PASSWORD	This objective supports A.PASSWORD by ensuring that all passwords are at least five characters in length and are not a dictionary word.
OE.NOTAMPER	A tamperproof, non-bypassable, verifiable TOE will enable administrators to ensure proper functioning of the TOE. The IT Environment supports the TOE in protecting itself by providing hardware mechanisms for domain separation. This partially addresses T.TAMPER (see O.NOTAMPER as well).

	T.TAMPER	A.NOEVILADMIN	A.ENVIRON	A.PLATFORM	A.INSTALL	A.DEDICATED	A.PASSWORD	A.NOSSL	A.NETWORK	P.AUDIT
OE.ADMIN		X			X					
OE.NETWORK								X	X	
OE.ENVIRON			X							
OE.PLATFORM				X		X				
OE.TIME										X
OE.PASSWORD							X			

	T.TAMPER	A.NOEVILADMIN	A.ENVIRON	A.PLATFORM	A.INSTALL	A.DEDICATED	A.PASSWORD	A.NOSSL	A.NETWORK	P.AUDIT
OE.NOTAMPER	X									

Table 3 - Mappings Between Assumptions, Policies and Security Objectives for the Environment

CHAPTER 5

5 IT Security Requirements

This section contains the security requirements that are satisfied by the TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC. Explicitly stated components may exist.

The following table summarizes the security functional requirements claimed for the TOE and the IT Environment.

IT Security Functional Requirements	
FAU_GEN.1	Audit Data Generation
FAU_SAR.1	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_AFL.1	Authentication Failure Handling
FIA_UAU.1	Timing of Authentication
FIA_UAU.5	Multiple Authentication Mechanisms
FIA_UAU.6	Re-Authenticating
FIA_UAU.7	Protected Authentication Feedback
FIA_UID.1	Timing of Identification
FMT_MOF.1	Management of Security Functions Behaviour
FMT_MSA.1	Management of Security Attributes
FMT_MSA.3	Static Attribute Initialisation
FMT_MTD.1	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
FPR_UNO.1	Unobservability
FPT_RVM_SFT.1	Non-Bypassability of the TSP for Software TOEs
FPT_RVM_HW.1	Non-Bypassability of the TSP for Hardware
FPT_SEP_SFT.1	TSF Domain Separation for Software TOEs
FPT_SEP_HW.1	TSF Domain Separation for Hardware
FPT_STM.1	Reliable Time Stamps
SFP_AUD.1	Proxy SFP Audit Data Generation
ADM_PCR.1	Password Controlled Role

Table 4 - TOE Security Functional Requirements

5.1 TOE Security Functional Requirements

The TOE security functional requirements for this Security Target consist of the following components from Part 2 of the CC.

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1 Audit Data Generation

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[2];

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

c) **communication errors with external IT devices.**

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

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 mechanism
FIA_UAU.5	Basic	The result of each activated mechanism together with the final decision
FIA_UAU.6	Basic	All reauthentication attempts
FIA_UID.1	Basic	All use of the user identification mechanism, including the user identity provided.
FMT_MOF.1	Basic	All modifications to the behaviour 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
FMT_SMR.3	Minimal	Explicit request to assume a role
FMT_UNO.1	Minimal	The invocation of the unobservability mechanism
FPT_STM.1	Minimal	Changes to the time

Table 5 - Auditable Events

[2] Audit functions are always active while the SGOS is operational.

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) nothing.

Dependencies: FPT_STM.1 Reliable Time Stamps

5.1.1.2 FAU_SAR.1 Audit review

FAU_SAR.1.1(1) 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(1) 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.1.1(2) 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(2) 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

5.1.1.3 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to prevent modifications to the audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit Data Generation

5.1.1.4 FAU_STG.4 Prevention of Audit Data Loss

FAU_STG.4.1 The TSF shall overwrite the oldest stored audit records and **no other action** if the audit trail is full.

Dependencies: FAU_STG.1 Protected Audit Trail Storage

5.1.2 User Data Protection (FDP)

5.1.2.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **Administrative Access SFP** on **users of the Serial Console performing the operations "establish an administrative session" and "request the privileged administrator role (i.e. execute the enable command)" with the administrative CLI**

Dependencies: FDP_ACF.1 Security attribute based access control

5.1.2.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the Administrative Access SFP to objects based on the following: **attributes of users of the serial console:**

- **Authenticated Identity**
- **Group membership**
- **Time of Day/Date**

and the following attributes of the operation:

- **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:

- **Establish an administrative session: 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.**
- **Request the privileged administrator role (i.e. execute the enable command): 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.[3]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

- **Establish an administrative session: establishment is permitted if the Serial Console user has the identity "console administrator"**
- **Request the privileged administrator role (i.e. execute the enable command): execution is permitted if the Serial Console user has the identity "console administrator"**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the: **None**

5.1.2.3 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the **Proxy SFP** on

the following subjects:

external IT entities attempting to send controlled protocol traffic through the TOE,

the following information:

controlled protocol traffic sent through the TOE to other subjects,

for the following operations:

passing controlled protocol traffic through the TOE to the other network.

[3] Note that execution of the "enable" command does not automatically result in the privileged administrator role; an additional authentication step is required as specified by FIA_UAU.6.1(2) and ADM_PCR.1.1(1).

Dependencies: FDP_IFF.1 Simple Security Attributes

5.1.2.4 FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the **Proxy SFP** based on the following types of subject and information security attributes:

the following subject attributes:

- **username**
- **user group membership**

the following information attributes:

- **source IP address**
- **destination IP address**
- **destination port**
- **protocol**
- **URL**
- **time of day**
- **date**
- **originating application**
- **MIME type**
- **Request method (the requested operation)**
- **any part of an HTTP request other than the body (e.g. header fields.[4])**
- **HTTP response header fields**
- **HTTP response body**

[4] 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.

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 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 the **additional rules:**

None.

FDP_IFF.1.4 The TSF shall provide the following **actions that can be implemented as part of a Proxy SFP Rule:**

- **require authentication of the originating End User for an information flow originating from the Internal Network**
- **rewrite a field of the information flow, e.g. URL**
- **email a message to a specified address**
- **strip active content from the information flow.**
- **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 the following rules: **none**.

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 Identification and Authentication (FIA)

5.1.3.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when ***an administrator configurable positive integer within*** **1 to 65535** unsuccessful authentication attempts occur related to **authentication attempts since the unsuccessful authentication attempt counter for this account has been reset by re-enabling the account, changing the password, or (if so configured) a configurable length of time has passed since the last unsuccessful authentication attempt.**

FIA_AFL.1.2 When the defined number of unsuccessful 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 a configured period of time.**

Dependencies: FIA_UAU.1 Timing of Authentication

5.1.3.2 FIA_UAU.1 Timing of Authentication

FIA_UAU.1.1(1) The TSF shall allow **only actions that match a Proxy SFP Rule that does not require authentication** on behalf of the ***End User*** to be performed before the user is authenticated.

FIA_UAU.1.2(1) The TSF shall require each ***End User*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1.1(2) The TSF shall allow **only choice of the Setup Console or CLI on the Serial Console** on behalf of the ***serial console user*** before the user is authenticated.

FIA_UAU.1.2(2) 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 Timing of Identification

5.1.3.3 FIA_UAU.5 Multiple Authentication Mechanisms

FIA_UAU.5.1 The TSF shall provide:

- **Configured console username and password**
- **Configured "enable" password**
- **Configured "setup" password**
- **Authenticate.mode(proxy) with username and password from local list**
- **Authenticate.mode(origin-cookie-redirect) with username and password from local list**
- **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 **rules:**

- **On the Serial Console CLI, verification of the configured console username and password authenticates the user as a Console Administrator;**
- **On the Serial Console CLI, verification of the configured "enable" password entered by a console administrator authenticates use of the Privileged Administrator role;**
- **On the Serial Console Menu, verification of the configured "setup" password authenticates use of the Setup Console Administrator role;**
- **For End User requests, if the Proxy SFP specifies authenticate.mode(proxy):**

1. **If the client supports proxy authentication, authentication shall follow the protocol for proxy authentication from RFC 2616, validating the offered user name and password against the local list.**

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

- **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 user name as specified by the surrogate credential.**

- **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:**

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

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

- **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, authentiation shall follow the protocol for server authentication from RFC 2616, validating the offered user name 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.**

5.1.3.4 FIA_UAU.6 Re-Authenticating

FIA_UAU.6.1(1) The TSF shall re-authenticate the ***End 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.6.1(2) The TSF shall re-authenticate an ***Ordinary Administrator*** under the conditions **that the administrator has requested the role "privileged administrator" by invoking the "enable" command.**

Dependencies: No Dependencies

5.1.3.5 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only **no output** to the ***administrator user*** while the authentication is in progress[5].

Dependencies: FIA_UAU.1 Timing of Authentication

[5] Authentication feedback for End Users is done by the user agent (e.g. browser) and so is outside the TOE.

5.1.3.6 FIA_UID.1 Timing of Identification

FIA_UID.1.1(1) The TSF shall allow **only actions that match a Proxy SFP Rule that does not require authentication** on behalf of the user to be performed before the ***End User*** is identified.

FIA_UID.1.2(1) The TSF shall require each ***End User*** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No Dependencies

FIA_UID.1.1(2) The TSF shall allow **only selection of the Setup Console or CLI on the Serial Console** on behalf of the ***administrator user*** before the user is identified.

FIA_UID.1.2(2) The TSF shall require each ***administrator user*** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No Dependencies

5.1.4 Security Management (FMT)

5.1.4.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to determine the behaviour of, 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

5.1.4.2 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1(1) The TSF shall enforce the **Administrative Access SFP** to restrict the ability to query the security attributes **user group membership** to **an administrator.**

Dependencies: [FDP_ACC.1 Subset Access Control OR

FDP_IFC.1 Subset Information Flow Control]

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security Roles

FMT_MSA.1.1(2) The TSF shall enforce the **Administrative Access SFP** to restrict the ability to modify or delete the security attributes **user group membership, user password** to **a privileged administrator.**

Dependencies: [FDP_ACC.1 Subset Access Control OR

FDP_IFC.1 Subset Information Flow Control]

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security Roles

5.1.4.3 FMT_MSA.3 Static Attribute Initialisation

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 **a privileged administrator** to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of Security Attributes

FMT_SMR.1 Security Roles

5.1.4.4 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1(1) The TSF shall restrict the ability to query the **system configuration, Administrative Access SFP, and Proxy SFP** to **administrators.**

FMT_MTD.1.1(2) 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

5.1.4.5 FMT_MTD.2 Log File Size Limits

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 limts: **overwrite the oldest audit records.**

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security Roles

5.1.4.6 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

- **determine the behaviour of the Proxy SFP**
- **modify the behaviour of the Proxy SFP.**

Dependencies: No Dependencies

5.1.4.7 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles:

- **Administrator**
- **Privileged Administrator**
- **Setup Console Administrator**

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of Identification

5.1.4.8 FMT_SMR.3 Assuming Roles

FMT_SMR.3.1 The TSF shall require an explicit request to assume the following roles: **Privileged Administrator and Setup Console Administrator.**

Dependencies: **FMT_SMR.1 Security roles**

5.1.5 Privacy (FPR)

5.1.5.1 FPR_UNO.1 Unobservability

FPR_UNO.1.1 The TSF shall ensure that **external IT entities** are unable to observe the operation **any operation (including tests for existence)** on **the client's IP address on the Internal Network** by **the client on the Internal Network.**.

Dependencies: No Dependencies

5.2 Security Requirements for the IT Environment

The security functional requirements for the IT Environment consist of the following components from Part 2 of the CC.

5.2.1 Protection of the TSF (FPT)

5.2.1.1 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The ***IT environment*** shall be able to provide reliable time-stamps for ***the TOE's*** use.

Dependencies: No Dependencies

5.3 Explicitly Stated TOE Security Functional Requirements

The security functional requirements detailed in this section are explicitly stated requirements that identify security functional requirements of the TOE that are not currently defined in Part 2 of the CC.

5.3.1 Protection of the TSF (FPT)

5.3.1.1 FPT_RVM_SFT.1 Non-Bypassability of the TSP for Software TOEs

FPT_RVM_SFT.1.1 The TSF, when invoked shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No Dependencies

Rationale for explicitly-stated SFR: Non-bypassability can only be partially satisfied by the TOE since hardware must also play a role. Reference FPT_RVM_HW.1 levied on the It Environment.

5.3.1.2 FPT_SEP_SFT.1 TSF Domain Separation for Software TOEs

FPT_SEP_SFT.1.1 The TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects in the TSC.

FPT_SEP_SFT.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No Dependencies

Rationale for explicitly-stated SFR: Separation can only be partially satisfied by the TOE since hardware must also play a role. Reference FPT_SEP_HW.1 levied on the It Environment.

5.3.2 Security Audit

5.3.2.1 SFP_AUD.1 Proxy SFP Audit Data Generation

SFP_AUD.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) **all actions resulting from the Proxy SFP.**

SFP_AUD.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 **the source IP address, first line of traffic, and number of bytes returned to the End User.**

Dependencies: FPT_STM.1 Reliable Time Stamps

5.3.2.2 ADM_PCR.1 Password Controlled Role

ADM_PCR.1.1(1) The TSF shall authenticate **a Console Administrator** against the **configured "enable" password** under the conditions that the **Console Administrator** has requested the **privileged administrator** role by **entering the "enable" command**.

Dependencies: None

ADM_PCR.1.1(2) 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: None

5.4 Explicitly Stated IT Environment Security Functional Requirements

The security functional requirements detailed in this section are explicitly stated requirements that identify security functional requirements of the TOE that are not currently defined in Part 2 of the CC.

5.4.1 Protection of the TSF (FPT)

5.4.1.1 FPT_RVM_HW.1 Non-Bypassability of the TSP for Hardware

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

Rationale for explicitly-stated SFR: Non-bypassability can only be partially satisfied by the TOE since hardware must also play a role. Reference FPT_RVM_SFT.1 levied on the It Environment.

5.4.1.2 FPT_SEP_HW.1 TSF Domain Separation for Hardware

FPT_SEP_SFT.1.1 The hardware of the IT Environment shall maintain separate security domains that protects the TOE from interference and tampering by untrusted subjects in the scope of control of the hardware.

FPT_SEP_SFT.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

Rationale for explicitly-stated SFR: Separation can only be partially satisfied by the TOE since hardware must also play a role. Reference FPT_SEP_SFT.1 levied on the It Environment.

5.5 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2 as defined by Part 3 of the CC. These assurance requirements are summarized in the following table.

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.2	Configuration Items
Delivery and Operation	ADO_DEL.1	Delivery Procedures
Delivery and Operation	ADO_IGS.1	Installation, Generation, and Start-Up Procedures
Development	ADV_FSP.1	Informal Functional Specification
Development	ADV_HLD.1	Descriptive High-Level Design
Development	ADV_RCR.1	Informal Correspondence Demonstration
Guidance Documents	AGD_ADM.1	Administrator Guidance
Guidance Documents	AGD_USR.1	User Guidance
Tests	ATE_COV.1	Evidence of Coverage
Tests	ATE_FUN.1	Functional Testing
Tests	ATE_IND.2	Independent Testing - Sample
Vulnerability Assessment	AVA_SOF.1	Strength of TOE Security Function Evaluation
Vulnerability Assessment	AVA_VLA.1	Developer Vulnerability Analysis

Table 6 - Assurance Requirements

5.6 TOE Strength of Function Claim

The only probabilistic or permutational mechanisms in SGOS are the password mechanisms used to authenticate End Users and administrators. The SFR that specifies these mechanisms are FIA_UAU.1. The claimed minimum strength of function for these SFR's is SOF-basic.

5.7 Rationale for TOE Security Functional Requirements

This section provides the rationale for mapping functional requirements to the security objectives of the TOE.

FAU_GEN.1	This requirement supports O.AUDIT by requiring the TOE to produce audit records for system security events.
FAU_SAR.1	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.
FDP_ACC.1	This requirement supports O.MANAGE by defining the scope of Administrative Access SFP to include access to the administrative interface and the privileged administrator role. These are the only mechanisms by which the TOE can be managed.
FDP_ACF.1	This requirement supports O.MANAGE by defining the enforcement of the Administrative Access SFP.
FDP_IFC.1	This requirement supports O.SCREEN_URL, O.REMOVE_ACTIVE and O.SCREEN_TYPE by defining the domain of the information flow control policies to include controlled protocol traffic screening functions for the TOE.

FDP_IFF.1	This requirement supports O.SCREEN_URL, O.SCREEN_TYPE and O.REMOVE_ACTIVE by defining the enforcement of the Proxy SFP.
FIA_AFL.1	This requirement supports O.AUTHENTICATE by protecting the users' passwords from brute-force guessing.
FIA_UAU.1	This requirement supports O.AUTHENTICATE by preventing unauthenticated End Users from performing actions that require authentication and preventing unauthenticated users from gaining access to the CLI.
FIA_UAU.5	This requirement supports O.AUTHENTICATE by defining the authentication mechanisms for End Users and administrators.
FIA_UAU.6	This requirement supports O. AUTHENTICATE by defining exactly when End Users and administrators need to re-authenticate.
FIA_UAU.7	This requirement supports O. AUTHENTICATE by defining exactly what feedback an administrator user receives during authentication.
FIA_UID.1	This requirement supports O.AUTHENTICATE by preventing unidentified End Users from performing actions that require authentication, and administrative users from gaining access to the CLI before authenticating.
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	This requirement supports O. MANAGE by defining the security attributes of the TOE which can be administered by authorized users.
FMT_MSA.3	This requirement supports O. MANAGE by making security attributes restrictive by default.
FMT_MTD.1	This requirement supports O.MANAGE by defining who can access and change TSF data.
FMT_MTD.2	This requirement supports O.MANAGE and O.AUDIT by restricting changes to the audit log limits to authorized administrators.
FMT_SMF.1	This requirement supports O.MANAGE by defining the security management functions in the TSF.
FMT_SMR.1	This requirement supports O.MANAGE by requiring the TOE to provide roles to perform TOE management.
FMT_SMR.3	This requirement supports O.MANAGE by requiring an explicit request to become a privileged administrator.
FPR_UNO.1	This requirement supports O.MASK_IP by preventing an internal source-IP-address from being sent over the External Interface.
FPT_RVM_SFT.1	This requirement supports O. NOTAMPER by preventing attackers from subverting the TSF when it is invoked
FPT_SEP_SFT.1	This requirement supports O. NOTAMPER by preventing attackers from tampering with the TSF processes domain space in the TSC.
SFP_AUD.1	This requirement supports O.AUDIT by requiring the TOE to produce audit records for actions caused by enforcement of the Proxy SFP. Because Access Logging as described in the

	TSS is a distinct process generating distinct logs, it was desired to have the TSS feature map clearly to the functional requirement. This auditing requirement was stated explicitly, because FAU_GEN.1 of the Common Criteria, Part 2 was found to be too broad. FAU_GEN.1 includes general system-level events that are not recorded by Access Logging. An iteration of FAU_GEN.1 for Access Logging with a refinement stripping the generic auditing requirements was found not permissible as the refinement would change the scope of the SFR.
ADM_PCR.1.1(1)	This requirement supports O.MANAGE and O.AUTHENTICATE by requiring the TOE to verify that a console administrator knows the "enable" password in order to assume the privileged administrator role. This was stated explicitly because FIA_UAU.6 specifies re-authentication, and this requires checking against a password different than the password associated with the console administrator username.
ADM_PCR.1.1(2)	This requirement supports O.NOTAMPER by requiring the TOE to verify that a serial console user knows the "setup" password in order to assume the Setup Console Administrator role (which allows bypassing the TSF). This was stated explicitly because FIA_UAU.6 specifies re-authentication, and this requires checking against a password different than the password associated with the any user's account.

The following table contains a mapping of the functional requirements and the security objectives.

	O.SCREEN_URL	O.SCREEN_TYPE	O.REMOVE_ACTIVE	O. AUDIT	O.MASK_IP	O.AUTHENTICATE	O.MANAGE	O. NOTAMPER
FAU_GEN.1				X				
FAU_SAR.1				X				
FAU_STG.1				X				
FAU_STG.4				X				
FDP_ACC.1							X	
FDP_ACF.1							X	
FDP_IFC.1	X	X	X					
FDP_IFF.1	X	X	X					
FIA_AFL.1						X		
FIA_UAU.1						X		
FIA_UAU.5						X		
FIA_UAU.7						X		
FIA_UID.1						X		
FMT_MOF.1							X	
FMT_MSA.1							X	
FMT_MSA.3							X	
FMT_MTD.1							X	
FMT_MTD.2				X			X	
FMT_SMF.1							X	
FMT_SMR.1							X	
FMT_SMR.3							X	
FPR_UNO.1					X			
FPT_RVM_SFT.1								X
FPT_SEP_SFT.1								X
SFP_AUD.1				X				
ADM_PCR.1						X	X	X

Table 7 - Mappings Between Functional Requirements and Objectives for the TOE

5.8 Rationale for IT Environment Security Requirements

This section provides the rationale for mapping functional requirements to the security objectives of the IT environment.

FPT_RVM_HW.1	This requirement supports OE. NOTAMPER by preventing attackers from bypassing the TSF via hardware paths.
FPT_SEP_HW.1	This requirement supports OE. NOTAMPER by providing multiple domains for execution of the TOE.
FPT_STM.1	This requirement supports OE.TIME by requiring the IT environment to provide a reliable timestamp for the TOE's use.

The following table contains a mapping of the functional requirements and the security objectives for the IT Environment.

	OE.TIME	OE>NOTAMPER
FPT_RVM_HW.1		X
FPT_SEP_HW.1		X
FPT_STM.1	X	

Table 8 - Mappings Between Functional Requirements and Objectives for the TOE

5.9 Rationale for IT Security Requirement Dependencies

The following table lists the claimed TOE and IT Environment security requirements and their dependencies. This section also contains rationale for any dependencies that are not satisfied.

SFR	Dependencies	Hierarchical To
FAU_GEN.1	FPT_STM.1	None
FAU_SAR.1	FAU_GEN.1	None
FAU_STG.1	FAU_GEN.1	None
FAU_STG.4	FAU_STG.1	FAU_STG.3
FDP_ACC.1	FDP_ACF.1	None
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	None
FDP_IFC.1	FDP_IFF.1	None
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	None
FIA_AFL.1	FIA_UAU.1	None
FIA_UAU.1	FIA_UID.1	None
FIA_UAU.5	None	None
FIA_UAU.6	None	None
FIA_UAU.7	FIA_UAU.1	None
FIA_UID.1	None	None
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	None
FMT_MSA.1	[FDP_ACC.1 OR FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	None
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	None
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	None
FMT_MTD.2	FMT_MTD.1 FMT_SMR.1	None
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	None
FMT_SMR.3	FMT_SMR.1	None
FPR_UNO.1	None	None

SFR	Dependencies	Hierarchical To
FPT_RVM_HW.1	None	None
FPT_RVM_SFT.1	None	None
FPT_SEP_HW.1	None	None
FPT_SEP_SFT.1	None	None
FPT_STM.1	None	None
SFP_AUD.1	FPT_STM.1	None
ADM_PCR.1	None	None

Table 9 - Functional Requirements Dependencies

5.10 Rationale for TOE Security Assurance Requirements

EAL2 was chosen to provide a low to moderate level of independently assured security. The chosen assurance level is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks is considered of low potential and the product will have undergone a search for obvious flaws.

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.

5.11 Rationale for Strength of Function Claim

SOF-basic is defined in CC Part 1 section 2.3 as: "A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential." Because this ST identifies threat agents with low attack potential, SOF-basic was chosen.

CHAPTER 6

6 TOE Summary Specification

6.1 TOE Security Functions

This section describes the security functions implemented by the TOE to meet the TOE SFRs.

6.1.1 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 the date, time, type of event, identity of subject, and outcome of the event. The events stored in the system log can be displayed using a command in the administrative CLI; this command is restricted to privileged administrators.

Also, 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 the date, time, type of event, identity of subject, outcome of the event, source IP address, first line of traffic, and the number of bytes returned to the End User. Access logs can be uploaded to another system for later analysis. Configuring the target systems and the decision on 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 per log will be overwritten.

The SGOS Audit function meets the following SFRs:

FAU_GEN.1	Audit Data Generation
FAU_SAR.1	Audit review
FAU_STG.1	Protected Audit Trail Storage
FAU_STG.4	Prevention of Audit Data Loss
SFP_AUD.1	Proxy SFP Audit Data Generation

6.1.2 Configurable Policies

The SGOS allows system administrators to enforce a very flexible policy using the ProxySG Content Policy Language. The figure below shows a sample of the CPL language:

```
<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 2 - Sample Configurable Policy

6.1.2.1 Administrative Access Control

Using this language an administrator can craft policies controlling administrative access by users (other than the console administrator, which is not subject to the Administrative Access Control policy). This allows administrative access to be granted or denied based on the user name, 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 becomes a privileged administrator by executing the "enable" command and successfully authenticating to its password challenge. The "enable" command will fail immediately if the (ordinary) administrator is not allowed access for the condition "admin.access=WRITE".

The SGOS Administrative Access Control Function meets the following SFRs:

FDP_ACC.1

FDP_ACF.1

6.1.2.2 Information Flow Protection

Using this language an administrator can craft policies to control the controlled protocol traffic exactly according to the site's security needs. The language is flexible enough to allow rules based on subject attributes like user name and group. The rules may also use information attributes such as all IP related information, URL, time, date, source application, MIME type, some 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.

The SGOS Information Flow Protection function meets the following SFRs:

FDP_IFC.1	Subset Information Flow Control
FDP_IFF.1	Simple Security Attributes

6.1.3 Identification and Authentication

SGOS users are identified by their user name 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 giving a choice of the Setup Console (used for installation) and the CLI (used for administration). In the evaluated configuration, the Setup Console is never used after the TOE is operational and is protected from end user access by a password. Administrators are directed to always choose the CLI.

There are several authentication mechanisms for administrators. SGOS provides a console administrator account that is set up during installation with a username and password. Administrators authenticating with this password are console administrators and are exempt from policy control. With appropriate administrative policy rules installed user accounts in the local user list can 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, an already authenticated administrator executes the "enable" command, which challenges for a password. Console administrators authenticate as privileged administrators by supplying the "enable" password that is part of system configuration. Ordinary administrators authenticate with their associated password (access to the enable command by ordinary administrators is controlled by policy, described above).

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 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, 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. SGOS counts the number of authentication failures for a given user account, and if the configured threshold (60 in the evaluated configuration) is reached or exceeded, 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 configured time (3600 seconds in the evaluated configuration). The failed authentication counter is reset to zero when the account is enabled or the password is changed.

The SGOS Identification and Authentication function meets the following SFRs:

FIA_AFL.1	Authentication failure handling
FIA_UAU.1	Timing of Authentication
FIA_UAU.5	Multiple Authentication Mechanisms
FIA_UAU.6	Re-Authenticating
FIA_UAU.7	Protected Authentication Feedback
FIA_UID.1	Timing of Identification
ADM_PCR.1	Password Controlled Role

6.1.4 Security Management

SGOS security is managed by administrators, who have the capability to review or (if privileged) modify any part of the configuration of the SGOS, including credentials, audit settings, and network settings. Administrators can also review and (if privileged) modify the policy rules that define the Administrative Access SFP and the Proxy SFP. The attributes integral to the Proxy SFP and Administrative Access SFPs are restrictive by default. After

installation and until a policy is loaded, SGOS will not pass any controlled protocol traffic and the only administrator is the Console Administrator. The SGOS Security Management function meets the following SFRs:

FMT_MOF.1	Management of Security Functions Behaviour
FMT_MSA.1	Management of Security Attributes
FMT_MSA.3	Static Attribute Initialisation
FMT_MTD.1	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

6.1.5 Privacy

SGOS has an important feature to help protect the identities of those on the Internal Network. The SGOS ensures that the real source IP address that the user is coming from is not available to anyone receiving controlled protocol traffic. Unlike network address translation (NAT) approaches, all controlled protocol traffic coming from the SGOS will have the same source IP address, namely the IP address of the External Interface of the device.

The SGOS Privacy function meets the following SFRs:

FPR_UNO.1	Unobservability

6.1.6 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 exit on a network interface.

The TOE protects itself from tampering by specifying only administrators can log in to the management interface using a username/password combination, and that the setup console can be accessed only after presenting a password. 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 consists of a single process in a single security domain.

The SGOS Protection of the TSF function meets the following SFRs:

FPT_RVM_SFT.1 Non-Bypassability of the TSP for Software TOEs

FPT_SEP_SFT.1 TSF Domain Separation for Software TOEs

ADM_PCR.1 Password controlled role

6.2 Security Assurance Measures and Rationale

The assurance measures provided by the TOE satisfy all of the assurance requirements listed in the following table, which provides a reference between each TOE assurance requirement and the related vendor documentation that satisfies each requirement.

Assurance Component	Documentation Satisfying Component	Rationale
ACM_CAP.2	http://ice.bluecoat.com/scm/process/docs/SoftwareCMProcess.html SG3.2.4.8 Build	The following Configuration Management procedures are described in this documentation: Use of the CVS tool for revision control Use of documented procedures for product builds Use of documented procedures for product test Use of documented procedures for release to manufacturing Use of documented procedures for distribution to customers List of configuration items and evidence that they are maintained by the CVS tool.
ADO_DEL.1	Blue Coat Order Fulfillment Process, Document #601-02640, Revision 00C	This document includes descriptions of the process used to create distribution copies of the TOE and the procedures used to ensure consistent delivery of the TOE. This document includes instructions for installing and setting-up the SGOS.
ADO_IGS.1	SGOS Configuration and Management Guide, Document #231-02629, Revision 2.1.07 04/28/2003 BCS SG400 Series Port 80 Security Appliance Quick Start, Document #231-02651, Revision 00A 01/2003	This document describe the procedures necessary for secure installation, generation, and start-up of the TOE. This document includes instructions for installing and setting-up the SGOS.
ADV_FSP.1	Blue Coat Systems ProxySG Operating System 3.2.4.8 Functional Specification, Revision 4.1, July 5, 2005	This document provides the purpose and method of use of all external TSF interfaces and completely represents the TSF.

Assurance Component	Documentation Satisfying Component	Rationale
ADV_HLD.1	Blue Coat Systems ProxySG Operating System 3.2.4.8 High Level Design , Revision 1.5, July 5, 2005	This document describes the high level design. It contains a representation of the TSF in terms of subsystems, identifying the TSP-enforcing subsystems, and describes the security functions. All subsystem interfaces are identified and the externally visible ones are noted. The purpose and method of use of all interfaces to the TSF subsystems are described.
ADV_RCR.1	Blue Coat Systems ProxySG Operating System 3.2.x, Representation Correspondence, Revision 1.1, November 10, 2004	The correspondence between the TOE security functions and the high-level design subsystems is described in this document.
AGD_ADM.1	SGOS Configuration and Management Guide, Document #231-02629, Revision 2.1.07 04/28/2003	Guidance to administrators is effectively supported by the listed documentation for this requirement.
AGD_USR.1	Blue Coat Systems ProxySG Operating System 3.2.x, Revision 1.1, 10 November 2004	Guidance to non-administrative users is effectively supported by the listed documentation for this requirement.
ATE_COV.1	Blue Coat Systems Release Test Plan, Revision 0.7, ProxySG 3.2.4 Test Plan, 31 March 2005	This document describes the functional and penetration tests performed and their results.
ATE_FUN.1	Blue Coat Systems Release Test Plan, Revision 0.7, ProxySG 3.2.4 Test Plan, 31 March 2005	This document describes the functional and penetration tests performed and their results.
ATE_IND.2	Blue Coat Systems Release Test Plan, Revision 0.7, ProxySG 3.2.4 Test Plan, 31 March 2005	This document describes the functional and penetration tests performed and their results.
AVA_SOF.1	This document, section 5.10	This document includes a strength of function analysis to support the SOF-basic claim. The analysis includes identifying the TOE password space and the probability of a password being compromised.
AVA_VLA.1	Blue Coat Systems Release Test Plan, Revision 0.7, ProxySG 3.2.4 Test Plan, 31 March 2005	This document describes the vulnerability analysis performed and the results of the analysis.

Table 10 - Assurance Measures and Rationale

6.3 Rationale for TOE Security Functions

The following section provides a rationale showing how each Security Functional Requirement is supported by the security functions enforced by the TOE.

FAU_GEN.1	Audit Data Generation specifies the System Logging mechanism and is supported by the Audit function. The Audit function logs system events as specified by FAU_GEN.1.
FAU_SAR.1	Audit review specifies that the audit records can be reviewed by authorized users and is supported by the Audit function. The Audit function provides mechanisms to view the System Event log, and to upload the Access Logs to another system.
FAU_STG.1	Protected Audit Trail Storage is supported by the Audit function. The Administrator is the only account type that can logon to SGOS administrative interface (CLI). No other users have access to the stored audit trail.
FAU_STG.4	Prevention of Audit Data Loss is supported by the Audit function. The Audit function mitigates audit data loss by overwriting the oldest logs.
FDP_ACC.1	Subset Access Control (Administrative Access SFP) is supported by the Administrative Access Control function. This function includes a policy language that enables administrators to construct rules that control the access of administrators to the administrative interface of the TOE. The function then enforces those rules and takes the action specified.
FDP_ACF.1	Security attribute based access control (Administrative Access SFP) is supported by the by the Administrative Access Control function. The function supports several attributes that can be used in the Administrative Access SFP to control access to the administrative interface.
FDP_IFC.1	Subset Information Flow Control (Proxy SFP) is supported by the Information Flow Protection function. This function includes 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	Simple Security Attributes (Proxy SFP) is supported by the Information Flow Protection function. The Information Flow Protection function supports a wide range of attributes that can be used in the Proxy SFP to control information flow.
FIA_AFL.1	Authentication failure handling is supported by the Identification and Authentication function. This function monitors the number of failed authentication attempts and disables the account if the configured threshold is reached.
FIA_UAU.1	Timing of Authentication is supported by the Identification and Authentication function. This function requires administrators to authenticate by providing a valid user name and password when seeking access to the administrative CLI. It requires the End User to authenticate by providing a valid login name and password when the Proxy SFP requires authentication.
FIA_UAU.5	Multiple authentication mechanisms is supported by the Identification and Authentication function which provides authentication via a configured Console Administrator user name and password, privileged administrator authentication via a password, and End User authentication using either proxy or transparent modes, using a user name and password or a proxy-generated surrogate credential.
FIA_UAU.6	Re-Authenticating is supported by the Identification and Authentication function which re-authenticates (ordinary) administrators when seeking to assume the privileged administrator role. The I&A function challenges End Users

	for re-authentication if the traffic requires authentication and the offered surrogate credential is expired or invalid.
FIA_UAU.7	Protected Authentication Feedback is supported by the Identification and Authentication function; no characters are echoed when administrators type their password at the CLI. (End user authentication feedback is not part of the TOE).
FIA_UID.1	Timing of Identification is supported by the Identification and Authentication function. This function requires administrators to authenticate before obtaining access to the CLI, and requires End Users to identify and authenticate themselves when the Proxy SFP requires authentication and allows End Users to not be identified when the Proxy SFP does not require authentication.
FMT_MOF.1	Management of Security Functions Behaviour is supported by the Security Management function. The Security Management function describes the functions that the Administrator uses to configure the functions of the TOE.
FMT_MSA.1	Management of Security Attributes is supported by the Security Management function. The Security Management function describes the security attributes that the Administrator uses to configure the TOE.
FMT_MSA.3	Static Attribute Initialization is supported by the Security Management function. Both the Administrative Access and Proxy SFPs are by default restrictive.
FMT_MTD.1	Management of TSF data is supported by the Security Management function. This function permits administrators to view the system configuration and the Administrative Access and Proxy SFP rules; privileged administrators can modify these items.

FMT_MTD.2	Management of limits of TSF data is supported by the Security Management function. This function permits privileged administrators to modify the limit on the size of the audit logs.
FMT_SMF.1	Specification of Management Functions is supported by the Security Management function. This function specifies that the TOE supports configuration of the Proxy SFP.
FMT_SMR.1	Security Roles is supported by the Security Management function. This function supports two roles: administrator and privileged administrator. The function allows only privileged administrators to make changes to the system configuration or the SFPs.
FMT_SMR.3	Assuming Roles is supported by the Security Management function: administrators can be become privileged only by executing the "enable" command, and providing the appropriate password (the "enable" password for console administrators and the administrator's own password for ordinary administrators).
FPR_UNO.1	Unobservability is supported by the Privacy function. This function replaces the Internal Network IP address with the IP address of device on the External Network, thus preventing entities on the External Network from observing the client's internal IP address.
FPT_RVM_SFT.1	Non-Bypassability of the TOE for Software TOEs is supported by the Protection of the TSF function. This function ensures 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_SFT.1 TSF Domain Separation for Software TOEs is supported by the Protection of the TSF function. This function ensures 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.

SFP_AUD.1 Proxy SFP Audit Data Generation specifies the Access Logging mechanism and is supported by the Audit function. The Audit function logs Configurable Policy actions as specified by SFP_AUD.1.

ADM_PCR.1 Password Controlled Role is supported by the Security function. This function requires a console administrator to enter the "enable" password before assuming the privileged administrator role and requires a serial console user to enter the "setup" password before assuming the Setup Console Administrator role (which allows bypassing the TSF).

The following table shows the mapping between the Security Functional Requirements and the security functions enforced by the TOE, which are listed above.

	Audit	Administrative Access Control	Information Flow Protection	Identification & Authentication	Security Management	Privacy	Protection of the TSF
FAU_GEN.1	X						
FAU_SAR.	X						
FAU_STG.1	X						
FAU_STG.4	X						
FDP_ACC.1		X					
FDP_ACF.1		X					
FDP_IFC.1			X				
FDP_IFF.1			X				
FIA_AFL.1				X			
FIA_UAU.1				X			
FIA_UAU.5				X			
FIA_UAU.6				X			
FIA_UAU.7				X			

	Audit	Administrative Access Control	Information Flow Protection	Identification & Authentication	Security Management	Privacy	Protection of the TSF
FIA_UID.1				X			
FMT_MOF.1					X		
FMT_MSA.1					X		
FMT_MSA.3					X		
FMT_MTD.1					X		
FMT_MTD.2					X		
FMT_SMF.1					X		
FMT_SMR.1					X		
FMT_SMR.3					X		
FPR_UNO.1						X	
FPT_RVM_SFT.1							X
FPT_SEP_SFT.1							X
SFP_AUD.1	X						
ADM_PCR.1				X			X

Table 11 - Mappings Between Functional Requirements and SFRs

6.4 Rationale for Satisfaction of Strength of Function Claim

The claimed minimum strength of function is SOF-basic. Various password-based authentication mechanisms in use, namely FIA_UAU.1(1), FIA_UAU.1(2), ADM_PCR.1.1(1) and ADM_PCR.1.1(2) contain a permutational function requiring an SOF analysis. Therefore, an analysis for these mechanisms is presented:

Password space for the Console Administrator and Setup Passwords

The Console Administrator, enable and setup passwords are chosen when the TOE is initially configured and are not subject to automatic account lockout (to prevent denial of service attacks locking out the administrator). In the evaluated configuration the console administrator password, the enable password and the setup password can be used only from the serial port. These passwords can contain upper and lower case letters and digits, must be 5 characters long and are constrained not to be a dictionary word. This provides 62 distinct characters, and we can assume the entire space must be searched since a dictionary attack won't find the password. There is only one serial port, so only one guess can be made at a time. If an incorrect password is offered on the serial console, the system delays (ignoring input) for 1000 ms before allowing another attempt. Thus, at most 1 guess/second can be made. Therefore, the password space is calculated as follows:

Password length: p = 5

Unique characters: c = 62

Seconds per attempt: s = 1.00

Average length of successful attack in days =

= (s * c^p seconds) / (60 * 60 * 24 seconds per day) / 2

= (1.00 * 62^5) / (60 * 60 * 24) / 2

= 5301 days

Using the approach detailed in the CEM Part 2 Annex B, the values for "Identifying Value" and "Exploiting Value" in Table B.3 for each factor were summed. Given the simplicity of a brute force attack, all the values are 0 except for the Exploiting Value for Elapsed Time (8) and Access to TOE (9) for a total of 17. As shown in Table B.4, values between 10 and 17 indicate the mechanism is sufficient for a SOF Rating of 'Basic', resistant to an attack potential of 'low'.

Password space User Accounts:

The Administrator creates user passwords when crafting the user password file. The password can contain upper and lower case letters and digits, must be 5 characters long and is constrained not to be a dictionary word. This provides 62 distinct characters, and we can assume the entire space must be searched since a dictionary attack won't find the password. In the evaluated configuration, automatic account lockout is enabled. After 60 incorrect passwords, the attacked account will be disabled for 3600 seconds and no information about password correctness can be obtained during that time. Thus, the attacker can make at most 60 guesses per 3600 seconds, or 60 seconds per attempt. Therefore, the password space is calculated as follows (divided by two for average):

Password length: p = 5

Unique characters: c = 62

Seconds per attempt: s = 60.0

Average length of successful attack in days =

= (s * c^p seconds) / (60 * 60 * 24 seconds per day) / 2

= (60 * 62^5) / (60 * 60 * 24) / 2

= 318,000 days.

Using the approach detailed in the CEM Part 2 Annex B, the values for “Identifying Value” and "Exploiting Value" in Table B.3 for each factor were summed. Given the simplicity of a brute force attack, all the values are 0 except for the Exploiting Value for Elapsed Time (8) and Access to TOE (9) for a total of 17. As shown in Table B.4, values between 10 and 17 indicate the mechanism is sufficient for a SOF Rating of ‘Basic’, resistant to an attack potential of ‘low’.

CHAPTER 7

7 Protection Profile Claims

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Chapter 1, Section 1.4 Protection Profile Conformance.

7.1 Protection Profile Reference

This Security Target does not claim conformance to any registered Protection Profile.

7.2 Protection Profile Refinements

This Security Target does not claim conformance to any registered Protection Profile.

7.3 Protection Profile Additions

This Security Target does not claim conformance to any registered Protection Profile.

7.4 Protection Profile Rationale

This Security Target does not claim conformance to any registered Protection Profile.

CHAPTER 8

8 Rationale

This chapter provides rationale or references to rationale required for this Security Target.

8.1 Security Objectives Rationale

Sections 4.3 - 4.4 provide the security objectives rationale.

8.2 Security Requirements Rationale

Sections 5.7 - 5.11 provide the security objectives rationale.

8.3 TOE Summary Specification Rationale

Sections 6.2 – 6.4 provide the TSS rationale.

8.4 Protection Profile Claims Rationale

This Security Target does not claim conformance to any Protection Profile.