Blue Coat Systems, Inc.
ProxySG v5.3.1.9 running on SG510, SG810, and SG8100

Security Target

Evaluation Assurance Level: EAL 2+
Document Version: 0.6

Prepared for:

Blue Coat Systems, Inc.
650 Almanor Avenue
Sunnyvale, CA 94085
Phone: (408) 220-2200

http://www.bluecoat.com

Prepared by:

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

http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2007-11-19	Amy Nicewick	Initial draft.
0.2	2008-02-28	Greg Milliken Amy Nicewick	Added “Modes of Operation” section (1.4.3). Addressed OR #1.
0.3	2008-07-03	Amy Nicewick	Updated to final product version.
0.4	2008-09-09	Greg Milliken	Updated version numbers in Table 16, changed TOE name in title to include “running on…”.
0.5	2008-10-07	Amy Nicewick	Addressed CB OR #1.
0.6	2008-10-21	Amy Nicewick	Updated version and build numbers, added hardware configurations and iteration of FCS_COP.1 for remote management.

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is the Blue Coat ProxySG v5.3.1.9 Appliance, and will hereafter be referred to as the TOE, or ProxySG, throughout this document. The TOE is a proprietary operating system developed specifically for use on a hardware appliance that serves as an Internet proxy and WAN optimizer. 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), and to provide acceleration and compression of transmitted data.

1.1 Purpose

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

- Security Target Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), ST Protection Profile, and Evaluation Assurance Level (EAL) package claims.
- Security Problem Definition (Section 3) – Describes the threats, policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components Definition (Section 5) – Identifies new components (extended SFRs[1] and extended SARs[2]) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE and by the TOE's environment.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and the SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms used within this ST.

[1] SFR – Security Functional Requirement

[2] SAR – Security Assurance Requirement

1.2 Security Target and TOE References

Table 1 - ST and TOE References

ST Title	Blue Coat Systems, Inc. ProxySG v5.3.1.9 running on SG510, SG810, and SG8100 Security Target
ST Version	Version 0.6
ST Author	Corsec Security, Inc. Amy Nicewick and Matt Keller
ST Publication Date	2008/10/21
TOE Reference	Blue Coat ProxySG® v5.3.1.9 Appliance Build number 36410 running on the SG510, SG810, and SG8100
Keywords	Proxy, Blue Coat, Gateway, Traffic Filtering, Content Filtering, Transparent Authentication, Proxy SFP, Administrative Access SFP, WAN Optimization SFP, Web Security, Safe Browsing, WAN Optimization, ADN, Application Delivery Network, VPM, Visual Policy Manager

1.3 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The Blue Coat ProxySG v5.3.1.9 Appliance (ProxySG) is a proprietary operating system and hardware appliance that together serve 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), and to provide WAN optimization for traffic passing between networks.

The ProxySG is one of several appliances manufactured by Blue Coat Systems. The TOE appliances include the SG510, SG810, and SG8100 lines of products. All appliances run TOE software that differs only in platform-specific configuration data, which describes the intended hardware platform to the operating system. Differences between product models allow for different performance and scalability options.

Figure 1 shows a typical deployment configuration of the TOE:

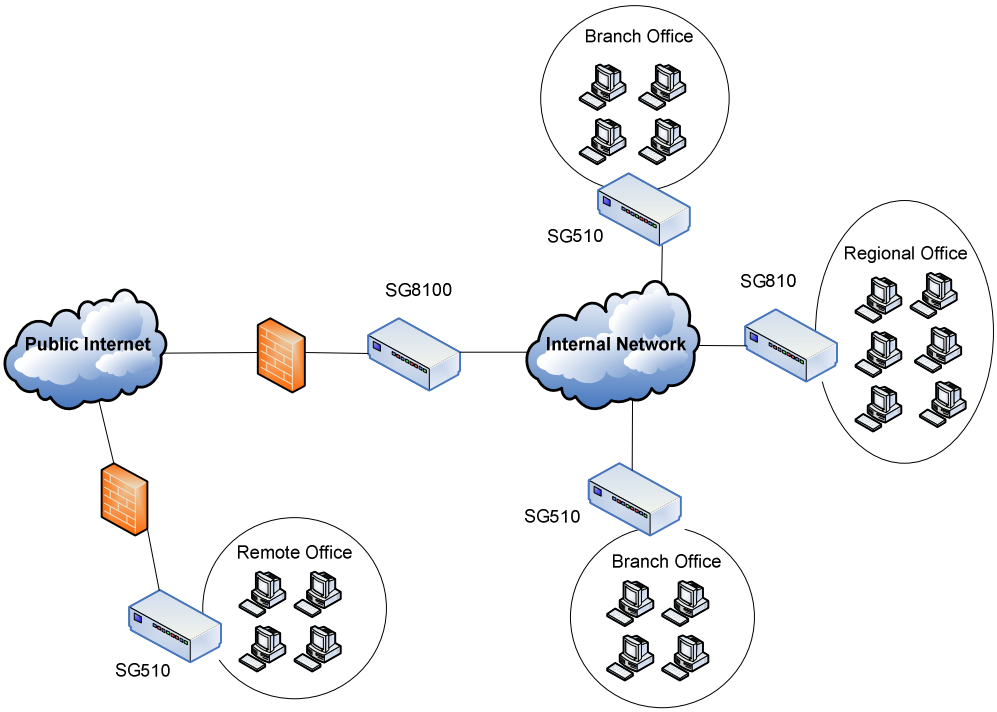

Figure 1 – Typical Deployment Configuration of the TOE

The security provided by the ProxySG can be used to control, protect, and monitor the Internal Network's use of controlled protocols on the External Network. The ProxySG appliances offer a choice of two "editions" via licensing: Mach 5 and Proxy. The Mach 5 edition appliances have some proxy features disabled (as indicated below). The controlled protocols implemented in the evaluated configuration are:

- Hypertext Transfer Protocol (HTTP)
- Secure Hypertext Transfer Protocol (HTTPS)
- File Transfer Protocol (FTP)
- SOCKS (not included with Mach 5 edition)
- Instant Messaging (AOL, MSN/Windows LIVE Messenger, and Yahoo!) (not included with Mach 5 edition)
- Common Internet File System (CIFS)
- Real-Time Streaming Protocol (RTSP)
- Microsoft Media Streaming (MMS)
- Messaging Application Programming Interface (MAPI)
- Transmission Control Protocol (TCP) tunneling protocols (e.g., Secure Shell (SSH), IMAP[3], POP3[4], SMTP[5])

[3] IMAP - Internet Message Access Protocol

[4] POP3 – Post Office Protocol version 3

- Telnet

Control is achieved by enforcing a configurable policy (Proxy SFP[6]) on controlled protocol traffic to and from the Internal Network users. The policy may include authentication, authorization, content filtering, and auditing. In addition, the ProxySG provides optimization of data transfer between ProxySG nodes on a WAN. Optimization is achieved by enforcing a configurable policy (WAN Optimization SFP) on traffic traversing the WAN.

1.3.1 ProxySG Concepts

1.3.1.1 Administrative Access

Administrative access to the TOE is provided by the ProxySG Serial Console and Management Console. Users access the Serial Console using a terminal emulator over a direct serial connection to the appliance. The Serial Console controls access to the Setup Console (used for initial configuration only) and the Command Line Interface (CLI), which is used for normal administrative operations. Users can also access the CLI over an SSH connection. Users access the Management Console over an HTTPS connection, and it is used for normal administrative operations.

1.3.1.2 Initial Configuration

The TOE must be configured using the Setup Console before it is installed into the client's network. The Setup Console is used to specify the Internet Protocol (IP) address, subnet mask, default gateway, Domain Name System (DNS) server, the Console username and password, the Enable (privileged-mode) password (if applicable), the edition of the software (Mach 5 or Proxy), and the default policy for proxied services. Note that in this evaluated configuration, once the TOE is operational, the Setup Console is no longer used.

To perform first-time configuration of the TOE involves a three-step approach:

- Step 1: Entering the IP address, IP subnet mask, IP gateway address, DNS address, Console password, "enable" password, setup password, and the choice of edition (Mach 5 or Proxy)
- Step 2: Enabling Federal Information Processing Standard (FIPS) mode through the CLI on the Serial port, causing a reboot into FIPS mode
- Step 3: Entering the Application Delivery Network Settings (optional), traffic types to be intercepted, and initial policy

There are four ways to perform Step 1 of the first-time configuration:

- Front Panel configuration method (excluded from CC mode)
- Web setup wizard (excluded from CC mode)
- Automatic registration with the Director management application (excluded from CC mode)
- Serial Console configuration method

There are several ways to complete Step 3 of the first-time configuration:

- log on to the CLI through the serial connection, via SSH, or via Telnet[7] using the configured administrative credentials
- log on to the Management Console through HTTP[8] or HTTPS

[5] SMTP – Simple Mail Transfer Protocol

[6] SFP – Security Functional Policy

[7] Telnet access to the Management Console is not included in the evaluated configuration

After first-time configuration is completed, the administrator must log in to the TOE via the ProxySG Command Line Interface (CLI) or the Management Console Web interface to fully configure the appliance, and to perform normal administrative activities. Administrators may also perform normal administrative activities by logging on to the CLI through SSH. Note that first-time configuration can be re-run at any time to change the values of the configuration settings that are considered part of the first-time configuration.

1.3.1.3 Security Functional Policies

After initial configuration, the TOE is considered operational and behaves as a proxy that either denies or allows all proxied transactions through the TOE. During initial configuration, the administrator must choose which policy (allow or deny) is the default. To further manage controlled protocol traffic flow, an authorized administrator defines information flow policy rules, which comprise the Proxy SFP.

These rules can require authentication of End Users. An authorized administrator creates End Users by using the management interfaces to create unique user accounts in a local user list, if a local authentication realm is being used. If off-box authentication is in use, the administrator does not have to create users on the appliance. 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, WAN Optimization SFP, and Administrative Access SFP are expressed using the syntax and rules described in the Blue Coat Systems, Inc. ProxySG Content Policy Language Guide, 5.3.1.

1.3.1.4 Explicit and Transparent Network Environments

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

1.3.1.5 Deployment Configurations

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

[8] HTTP access to the Management Console is not included in the evaluated configuration

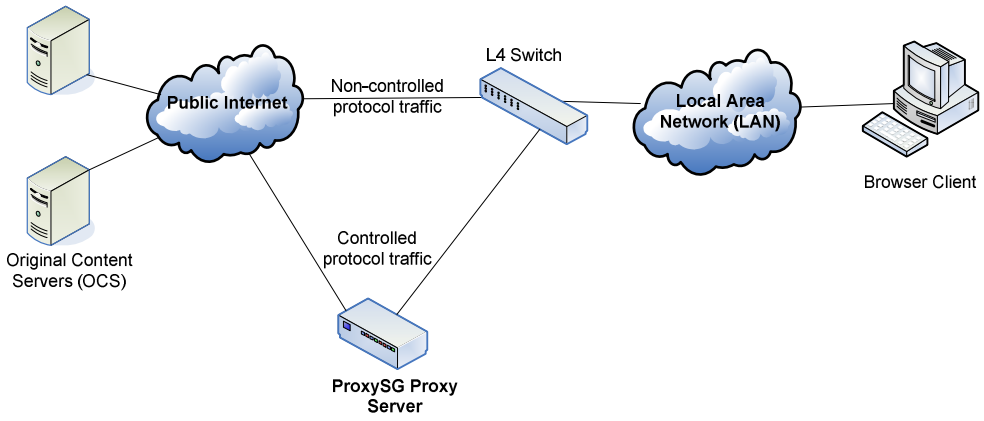

Figure 2 – Transparent Forward (Gateway) Proxy Deployment

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

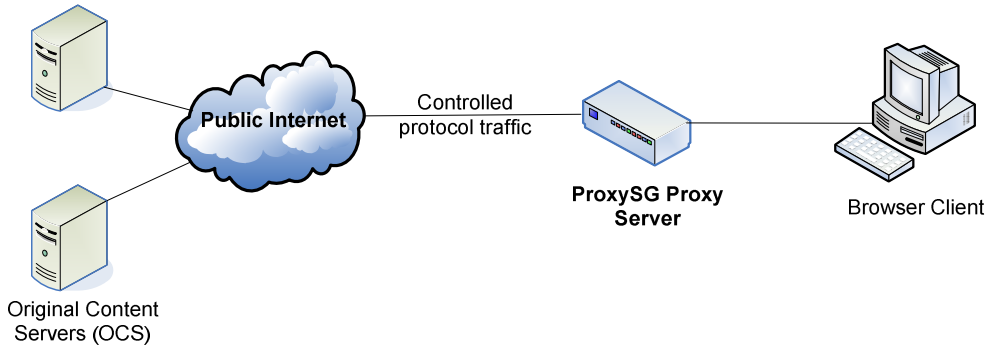

Figure 3 – Explicit Forward (Gateway) Proxy Deployment

In the Explicit Forward Proxy deployment (depicted in Figure 3 above), all controlled protocol traffic flows through the ProxySG, forcing browsers to access all Original Content Servers (OCS) through the ProxySG. This allows ProxySG to act as a policy enforcement node before serving up web pages. Client configuration is required after ProxySG installation to point to the ProxySG.

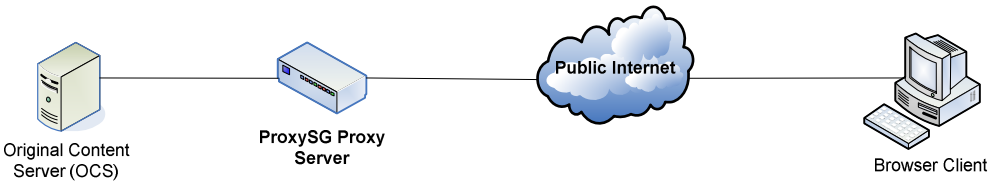

Figure 4 – Reverse (Server) Proxy Deployment

In the Reverse Proxy deployment, a ProxySG is associated with an OCS web server (as depicted in Figure 4 above). The ProxySG can cache and deliver pictures and other non-variable content rapidly, offloading those efforts from the OCS. This frees the OCS to perform application-based services (such as dynamic web page generation).

1.3.1.6 WAN Optimization

The ProxySG's Application Delivery Network (ADN) implements byte caching[9] and acceleration techniques to provide WAN optimization for a network. ADNs require two-sided deployments, with a ProxySG appliance at each end of the WAN link. ADN also uses bandwidth management, data compression, and object caching[10] to provide acceleration for the WAN. Figure 5 (below) shows a typical WAN Optimization deployment for email exchange across a WAN.

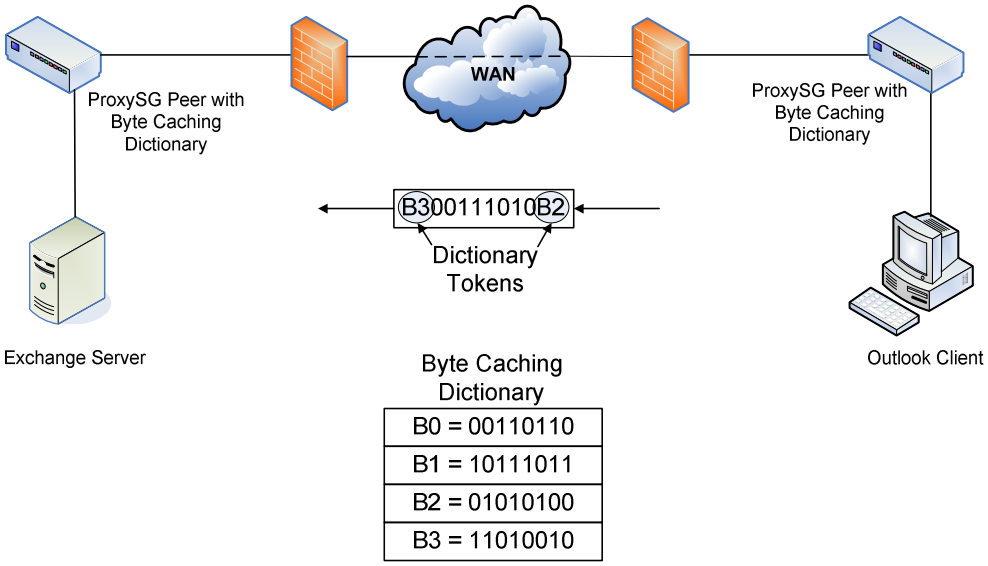

Figure 5 - WAN Optimization Deployment

[9] Byte caching – technique in which the TOE replaces large blocks of repeated data with small tokens representing that data prior to transmission.

[10] Object caching - enables clients to retrieve previously received data from a cache, rather than across the WAN.

The components required for an ADN implementation include an ADN manager to provide routing information and control access to the ADN network, and ADN nodes in branch offices and data centers that can be authenticated and authorized. An ADN node is any non-manager TOE appliance that is configured for ADN optimization in the network. However, ADN managers may also act as ADN nodes.

Traffic accelerated between nodes is automatically compressed before transmission. This decreases bandwidth usage and optimizes response time. ADN compression is used in conjunction with byte caching and object caching to increase optimization of data transmission.

1.3.1.7 Protection of TOE Assets and Functions

The assets of the TOE are the:

- Local user list (if present)
- Proxy SFP rules
- Administrative Access SFP rules
- WAN Optimization SFP rules
- Audit logs
- System configuration

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

1.3.2 TOE Environment

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

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

1.4 TOE Description

This section will primarily address the physical and logical components of the TOE included in the evaluation. Figure 6 illustrates the boundaries of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

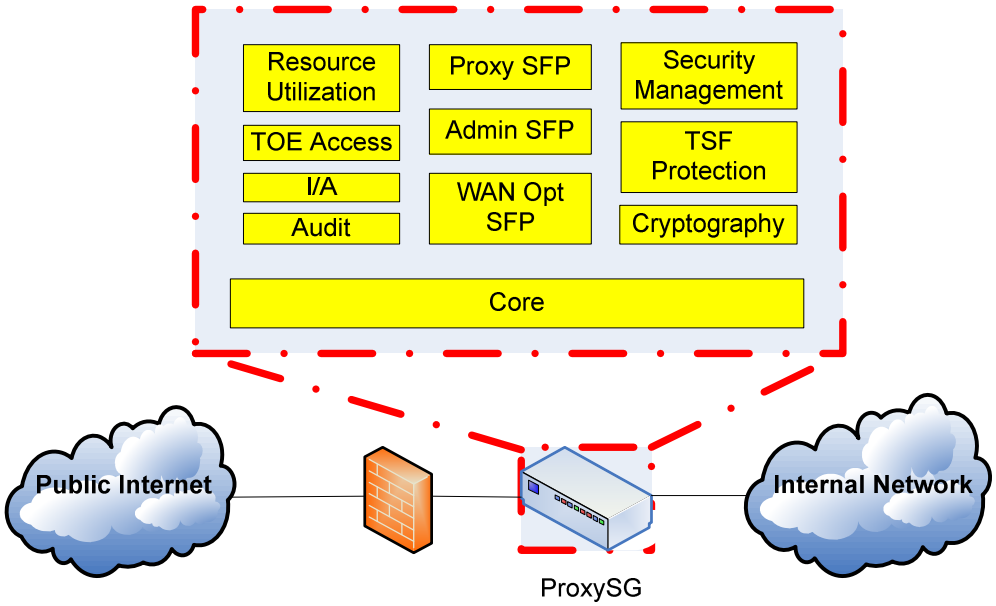

Figure 6 – TOE Boundary

1.4.1 Physical Scope

The TOE is a proprietary operating system and the custom, purpose-built hardware on which it runs. The physical boundary includes the hardware, the Core and all of the security and management engines of the software. The Core provides the basic operating system functions, such as system resource management and communications between the hardware and software, plus other core functionality, such as object store, network stack, etc.

1.4.1.1 TOE Software

The TOE is a software and hardware TOE. For the evaluated configuration, the TOE software must be installed and run on one of the following Blue Coat appliance configurations:

- SG510 with no SSL card
- SG510 with a Cavium CN1010 SSL card

- SG510 with a Broadcom 5825 SSL card
- SG810 with no SSL card
- SG810 with a Cavium CN1010 SSL card
- SG810 with a Broadcom 5825 SSL card
- SG8100 with no SSL card
- SG8100 with a Cavium CN1010 SSL card
- SG8100 with a Broadcom 5825 SSL card

1.4.2 Logical Scope

The logical boundary includes the security and management engines of ProxySG (see Figure 6**)** that address the security functional requirements imposed on the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- Cryptographic Support
- Administrative Access SFP
- Proxy SFP
- WAN Optimization SFP
- Identification and Authentication
- Security Management
- Protection of the TOE Security Function (TSF)
- Resource Utilization
- TOE Access

1.4.2.1 Security Audit

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

Access Logging makes a record of all Proxy SFP-controlled protocol traffic that enters the TOE. An administrator can specify exactly what information goes into these records. Standard logging formats like SQUID and NCSA[11] are provided for convenience, and custom log formats can be defined using W3C[12]. Depending on the policy, the ProxySG can create multiple log files for different policy actions. For example, single user actions or group actions can be logged where necessary. If an audit log ever fills to its configured capacity, the oldest records will be overwritten with new records. Access logs can be transferred to another machine (as configured by an administrator) for analysis. Access logs can also be encrypted and digitally signed prior to storage.

1.4.2.2 Cryptographic Support

The Cryptographic Support function provides encryption and decryption of all data transmitted between the TOE and the client running the CLI or Management Console. TLS may also be used for communication between the TOE and Lightweight Directory Access Protocol (LDAP) and Integrated Windows Authentication (IWA) authentication servers. In addition, access logs are encrypted using an external certificate associated with a private key. The TOE uses x.509 certificates for various applications, including authenticating the identity of a server,

[11] NCSA – National Center for Supercomputing Applications

[12] W3C – World Wide Web Consortium

authenticating another SG appliance, and securing an intranet. Cryptographic operations are performed by a FIPS 140-2-validated cryptographic module, certificate #XXX.

Comment [MSOffice1]: To the Evaluator: The FIPS certificate number will be added when the FIPS evaluation has completed.

1.4.2.3 User Data Protection

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

The TOE provides authorized administrators with the ability to define security policies using the ProxySG Content Policy Language (CPL). The CPL provides for the creation of rules that perform certain actions based on a set of conditions. The conditions and actions depend on the kind of policy being written. Policies written in CPL are evaluated according to the rules described in the Blue Coat Systems, Inc. ProxySG Content Policy Language Guide, 5.3.1.

1.4.2.3.1 Administrative Access SFP

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

1.4.2.4 Proxy SFP

The Proxy security function defines how the TOE controls proxy services. A Proxy SFP is defined by the system administrator to manage controlled protocol traffic through the proxy appliance. The conditions can be constructed from a set of attributes including whether the traffic originated from the Internal Network or the External Network and any combination of characteristics of the controlled protocol traffic.

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

Administrators can create policies either by composing them in the Blue Coat Content Policy Language (CPL), or by using the Visual Policy Manager (VPM), a user interface that creates underlying Blue Coat CPL.

1.4.2.5 WAN Optimization SFP

The WAN Optimization security function defines how the TOE performs byte caching and acceleration techniques such as compression and object caching on data being transmitted through the TOE. The TOE enforces the WAN Optimization SFP on specified TOE subjects, objects, and operations. The architecture of the TOE ensures that all operations between the specified objects and subjects are regulated by the TOE based upon the criteria defined in the WAN Optimization SFP.

1.4.2.6 Identification and Authentication

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

1.4.2.7 Security Management

The Security Management function provides administrators with the ability to properly manage and configure the TOE to store and access its IT[13] assets. Using a proprietary policy-drafting language (CPL), the ProxySG allows administrators to create Administrative Access SFP rules that grant and govern administrative access, to create Proxy SFP rules that control the flow of controlled protocol traffic, and to create WAN Optimization SFP rules that control byte-caching, compression, and acceleration of transmitted data.

1.4.2.8 Protection of the TSF

The TOE provides reliable timestamp information for its own use. The TOE software retrieves the timestamp from the hardware clock, which is set during installation of the appliance. The order of the audit records can be determined by the value of the timestamps.

The time can be synchronized to Coordinated Universal Time manually through the configuration settings. Administrators are assumed to be trusted and competent, and may change the system time whenever necessary.

1.4.2.9 Resource Utilization

The TOE enforces administrator-defined quotas on the number and duration of network connections and bandwidth utilization. The TOE can also be configured to send alerts to notify the administrator of changes in the health status of the TOE.

1.4.2.10 TOE Access

The TOE restricts the number of concurrent sessions that belong to the same End User by policy. If an End User exceeds the number of concurrent session permitted, the TOE will log the user off of one or more sessions, depending on the number permitted.

The TOE will also terminate an End User session after an administrator-defined interval of inactivity. Each time a login is completed, the inactivity-timeout value is updated. If the time since the last activity time exceeds the inactivity-timeout value, the End User is logged out.

1.4.3 Modes of Operation

The TOE has two modes of operation: FIPS Mode and Non-FIPS Mode. The TOE must be running in FIPS Mode as part of the evaluated configuration. FIPS Mode provides additional security measures beyond the defaults set when the TOE ships. A more detailed list of what FIPS Mode includes can be found in the Blue Coat Systems, Inc. ProxySG v5.3.1.9 Appliance Development: Functional Specification, TOE Design, and Security Architecture.

1.4.4 Physical/Logical Features and Functionality Not Included in the Evaluated Configuration of the TOE

Features/Functionality that are not part of the evaluated configuration of the TOE are:

- SGClient
- Remote management over Telnet
- Front panel configuration
- Remote management over HTTP
- XML authentication realm
- Session Monitor
- Unauthenticated access to the VPM

[13] IT – Information Technology

- Unauthenticated administrative access granted via policy
- All functionality excluded from FIPS mode
- Network Time Protocol (NTP)
- Link State Propagation feature

2 Conformance Claims

This section provides the identification for any CC, Protection Profile, and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 2 - CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, September 2007; CC Part 2 extended; CC Part 3 conformant; Parts 2 and 3 Interpretations from the Interpreted CEM as of 2007/11/15 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL 2+ augmented with ALC_FLR.1

3 Security Problem Definition

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

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

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

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

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

The following threats are applicable:

Table 3 - Threats

Name	Description
T.EXTERNAL_NETWORK	A user or process on the Internal Network may access or post content on the External Network that has been deemed inappropriate or potentially harmful to the Internal Network.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.UNAUTHORIZED_ACCESS	A user may gain access to security data on the TOE for which they are not authorized according to the TOE security policy through the improper use of valid credentials.
T.NACCESS	An unauthorized person or external IT entity may be able to view or modify data that is transmitted between the TOE and a remote authorized external entity.
T.RESOURCE	TOE users or attackers may cause network connection resources to become overused and therefore unavailable.
T.HEALTH	TOE users may perform actions that compromise the health of the TOE.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. The following OSPs are presumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration:

Table 4 - Organizational Security Policies

Name	Description
P.ACTIVE_CONTENT	The TOE shall provide a means to remove active content (e.g. Java, JavaScript, ActiveX) in HTML[14] pages delivered via controlled protocols.
P.ADMIN	Only authorized individuals shall have the ability to perform administrative actions on the TOE.
P.AUDIT	The TOE shall record events of security relevance at the "basic level" of auditing. The TOE shall record the resulting actions of the Proxy SFP.
P.CONTENT_TYPE	End Users shall not access unauthorized content types via controlled protocols on the External Network.
P.FILTERED_URLS	End Users shall not access unauthorized URLs via controlled protocols on the External Network.
P.MANAGE	The TOE shall provide secure management of the system configuration, the Proxy SFP, the WAN Optimization SFP, and the Administrative SFP.
P.NON_ANONYMOUS	Access to some resources via controlled protocols on the External Network may be restricted to particular End Users.
P.POST_TYPE	End Users shall not post unauthorized content types to the External Network using controlled protocols.
P.PASS_TRAFFIC	The TOE shall enforce the WAN Optimization SFP on traffic passing from the internal network to the external network.

3.3 Assumptions

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

[14] HTML – Hypertext Markup Language

Table 5 - Assumptions

Name	Description
A.ENVIRON	The TOE is located in an environment that provides physical security, uninterruptible power, air conditioning, and all other conditions required for reliable operation of the hardware. Physical access to the appliance is restricted to authorized persons.
A.INSTALL	The ProxySG device has been installed and configured according to the appropriate installation guides.
A.NETWORK	All Proxy SFP-controlled protocol traffic between the Internal and External Networks traverses the ProxySG device; there is no other connection between the Internal and External Networks for Proxy SFP-controlled protocol traffic.
A.NO_EVIL_ADMIN	Administrators are non-hostile and follow all administrator guidance when using the TOE. Administration is competent and on-going.
A.PASSWORD	Passwords for administrative access to the TOE and for End User accounts are at least five characters in length, and are not dictionary words.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment. A mapping of the objectives to the threats, OSPs, and assumptions included in the security problem definition can be found in section 8.2. This mapping also provides rationale for how the threats, OSPs, and assumptions are effectively and fully addressed by the security objectives.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 6 - Security Objectives for the TOE

Name	Description
O.AUDIT	The TOE must record events of security relevance at the "basic level" of auditing. The TOE must record the resulting actions of the Proxy SFP.
O.AUTHENTICATE	The TOE must require the Administrator to authenticate before gaining access to the administrative interfaces of the TOE, and End Users to authenticate if their controlled protocol traffic matches a Proxy SFP rule which requires authentication[15].
O.MANAGE	The TOE must provide secure management of the system configuration, the Administrative Access SFP, the WAN Optimization SFP, and 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.SCREEN_TYPE	The TOE must disallow controlled protocol traffic of given content types as defined by the Proxy SFP.
O.SCREEN_URL	The TOE must disallow controlled protocol traffic for given URLs[16] as defined by the Proxy SFP.
O.TIMESTAMP	The TOE must provide a timestamp for use by the TOE.
O.VALIDATED_CRYPTO	The TOE shall provide cryptographic functions for its own use. These functions will be provided by a FIPS 140-2 validated cryptographic module.
O.PROTECT	The TOE must have the capability to protect management traffic from unauthorized reading or modification.

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

[16] URL – Uniform Resource Locator

Name	Description
O.QUOTA	The TOE must be able to place quotas on network connection resources.
O.ALERT	The TOE must alert the administrator of changes in TOE health.
O.PASS_TRAFFIC	The TOE must pass traffic from the internal network to the external network as defined by the WAN Optimization SFP.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 7 - IT Security Objectives

Name	Description
OE.NETWORK	All Proxy-SFP controlled protocol traffic between the Internal and External Networks must traverse the ProxySG device.

4.2.2 Non-IT Security Objectives

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

Table 8 - Non-IT Security Objectives

Name	Description
OE.ADMIN	The administrator must be non-malicious and competent, and must follow all guidance.
OE.ENVIRON	The physical environment must be suitable for supporting a computing device in a secure setting.
OE.PASSWORD	Passwords for the Administrator and End User accounts and the “enable” password will be at least five characters in length and not be a dictionary word.

5 Extended Components Definition

This section defines the extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs) met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 9 identifies all extended SFRs implemented by the TOE

Table 9 - Extended TOE Security Functional Requirements

Name	Description
FIA_ADM_PCR.1(a)	Password controlled role
FIA_ADM_PCR.1(b)	Password controlled role
EXT_FRU_ARP.1	Health check alarms

5.1.1 Class FIA: Identification and Authentication

Identification and Authentication functions establish and verify a claimed user identity. The extended family FIA_ADM_PCR: Password controlled role was modeled after the CC family FIA_UAU: User authentication. The extended component FIA_ADM_PCR.1: Password controlled role was modeled after the CC component FIA_UAU.6: Re-authenticating.

5.1.1.1 Password controlled role (FIA_ADM_PCR)

Family Behaviour

This family defines the requirements for authenticating an authorized user to another role.

Component Leveling

Figure 7 – FIA_ADM_PCR Password Controlled Role family decomposition

FIA_ADM_PCR.1 Password controlled role, provides the capability to authenticate an authorized user to another role.

Management: FIA_ADM_PCR.1

The following actions could be considered for the management functions in FMT:

- If an authorized user could request authentication as a new role, the management includes an authentication request.

Audit: FIA_ADM_PCR.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Failure of authentication to the new role;
- Basic: All authentication requests to the new role.

FIA_ADM_PCR.1 Password controlled role

Hierarchical to: No other components

Dependencies: No dependencies

This component will provide authorized administrators the capability to authenticate as a new role.

FIA_ADM_PCR.1.1 The TSF shall authenticate a [assignment: *role*] under the conditions that the [assignment: *role*] has requested the [assignment: *new role*] role by [assignment: *list of conditions under which authentication is required*].

5.1.2 Class FRU: Resource Utilization

Resource utilization functions support the availability of required resources such as processing capability or storage capacity. The extended family EXT_FRU_ARP: Health check alarms was modeled after the CC family FAU_ARP: Security audit automatic response. The extended component EXT_FRU_ARP.1: Health check alarms was modeled after the CC component FAU_ARP.1: Security alarms.

5.1.2.1 Health check alarms (EXT_FRU_ARP)

Family Behaviour

This family defines the response to be taken in case of a change in the health status of the TOE.

Component Leveling

Figure 8 – EXT_FRU_ARP Health check alarms family decomposition

At EXT_FRU_ARP.1 Health check alarms, the TSF shall take actions in case a change in the status of the health of the TOE is detected.

Management: EXT_FRU_ARP.1

The following actions could be considered for the management functions in FMT:

- The management (addition, removal, or modification) of actions.

Audit: EXT_FRU_ARP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Actions taken due to change in health status.

EXT_FRU_ARP.1 Health check alarms

Hierarchical to: No other components

Dependencies: No dependencies

FIA_ADM_PCR.1.1 The TSF shall take [assignment: *list of actions*] upon detection of a change in health check status.

5.2 Extended TOE Security Assurance Components

There are no extended SARs for this TOE.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

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

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Parts 2 and 3 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [*underlined italicized text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.

Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 10 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 10 - TOE Security Functional Requirements

SFR Short Name	SFR Long Name	CC Operations			
		S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓	✓	
FAU_SAR.1(a)	Audit review		✓		✓
FAU_SAR.1(b)	Audit review		✓		✓
FAU_STG.1	Protected audit trail storage	✓			
FAU_STG.4	Prevention of audit data loss	✓	✓		
FCS_CKM.1	Cryptographic key generation		✓	✓	
FCS_CKM.4	Cryptographic key destruction		✓		

SFR Short Name	SFR Long Name	CC Operations			
		S	A	R	I
FCS_COP.1(a)	Cryptographic operation		✓	✓	✓
FCS_COP.1(b)	Cryptographic operation		✓	✓	✓
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓	✓	
FDP_IFC.1(a)	Subset information flow control		✓		✓
FDP_IFF.1(a)	Simple security attributes		✓	✓	✓
FDP_IFC.1(b)	Subset information flow control		✓		✓
FDP_IFF.1(b)	Simple security attributes		✓		✓
FIA_ADM_PCR.1(a)	Password controlled role		✓	✓	✓
FIA_ADM_PCR.1(b)	Password controlled role		✓		✓
FIA_AFL.1	Authentication failure handling	✓	✓	✓	
FIA_UAU.1	Timing of authentication		✓	✓	
FIA_UAU.2	User authentication before any action			✓	
FIA_UAU.5	Multiple authentication mechanisms		✓	✓	
FIA_UAU.6(a)	Re-authenticating		✓	✓	✓
FIA_UAU.6(b)	Re-authenticating		✓	✓	✓
FIA_UAU.7(a)	Protected authentication feedback		✓	✓	✓
FIA_UAU.7(b)	Protected authentication feedback		✓	✓	✓
FIA_UID.1(a)	Timing of identification		✓	✓	✓
FIA_UID.1(b)	Timing of identification		✓	✓	✓

SFR Short Name	SFR Long Name	CC Operations			
		S	A	R	I
FIA_UID.2	User identification before any action			✓	
FMT_MOF.1	Management of security functions behaviour	✓	✓		
FMT_MSA.1(a)	Management of security attributes	✓	✓		✓
FMT_MSA.1(b)	Management of security attributes	✓	✓		✓
FMT_MSA.2	Secure security attributes				
FMT_MSA.3(a)	Static attribute initialisation	✓	✓		
FMT_MSA.3(b)	Static attribute initialisation	✓	✓		
FMT_MSA.3(c)	Static attribute initialisation	✓	✓		
FMT_MTD.1(a)	Management of TSF data	✓	✓		✓
FMT_MTD.1(b)	Management of TSF data	✓	✓		✓
FMT_MTD.2	Management of limits on TSF data		✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FMT_SMR.3	Assuming roles		✓		
FPT_STM.1	Reliable timestamps				
EXT_FRU_ARP.1	Health check alarms		✓		
FRU_RSA.1	Maximum quotas	✓	✓		
FRU_RSA.2	Minimum and maximum quotas	✓	✓		
FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions		✓		
FTA_SSL.3	TSF-initiated termination		✓	✓	

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

FAU_GEN.1.1

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

- Start-up and shutdown of the audit functions;
- All auditable events, for the [*basic*] level of audit; and
- [*Communication errors with external IT devices; and*
- *All actions resulting from the Proxy SFP*].

The following table lists the auditable events for the basic or minimal levels of audit..

Table 11 - Basic-Level Auditable Events

Component	Level	Auditable Event
FAU_SAR.1	Basic	Reading of information from the audit records
FAU_STG.4	Basic	Actions taken due to the audit storage failure
FCS_CKM.1	Basic	The object attribute(s), and object value(s) excluding any sensitive information (e.g., secret or private keys)
FCS_CKM.4	Basic	The object attribute(s), and object value(s) excluding any sensitive information (e.g., secret or private keys)
FCS_COP.1(a)	Basic	Any applicable cryptographic mode(s) of operation, subject attributes and object attributes
FCS_COP.1(b)	Basic	Any applicable cryptographic mode(s) of operation, subject attributes and object attributes
FDP_ACF.1	Basic	All requests to perform an operation on an object covered by the Administrative Access SFP
FDP_IFF.1(a)	Basic	All decisions on requests for information flow
FDP_IFF.1(b)	Basic	All decisions on requests for information flow
FIA_ADM_PCR.1	Basic	All authentication requests to the new role

Component	Level	Auditable Event
FIA_AFL.1	Minimal	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.2	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 re-authentication attempts
FIA_UID.1	Basic	All use of the user identification mechanisms, including the user identity provided
FIA_UID.2	Basic	All use of the user identification mechanisms, including the user identity provided
FMT_MOF.1	Basic	All modifications in the behavior of the functions in the TSF
FMT_MSA.1	Basic	All modifications to the security attributes
FMT_MSA.2	Minimal	All offered and rejected values for a security attribute
FMT_MSA.3	Basic	Modifications of the default setting of permissive or restrictive rules 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
FPT_STM.1	Minimal	Changes to the time
EXT_FRU_ARP.1	Minimal	Actions taken due to change in health status
FRU_RSA.1	Basic	All attempted uses of the resource allocation functions for resources that are under control of the TSF

Component	Level	Auditable Event
FRU_RSA.2	Basic	All attempted uses of the resource allocation functions for resources that are under control of the TSF
FTA_MCS.2	Minimal	Rejection of a new session based on the limitation of multiple concurrent sessions
FTA_SSL.3	Minimal	Termination of an interactive session by the session locking mechanism

FAU_GEN.1.2

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*for the Access Log, the source IP address; for the Event log, nothing*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1(a) Audit review

Hierarchical to: No other components.

FAU_SAR.1.1(a)

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

FAU_SAR.1.2(a)

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1(b) Audit review

Hierarchical to: No other components.

FAU_SAR.1.1(b)

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

FAU_SAR.1.2(b)

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1

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

FAU_STG.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

FAU_STG.4.1

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

Dependencies: FAU_STG.1 Protected audit trail storage

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*cryptographic key generation algorithm* **– see table below**] and specified cryptographic key sizes [*cryptographic key sizes* **– see table below**] that meet the following: [*list of standards* **– see table below**].

Table 12 - Cryptographic Key Generation Standards

Key Generation Type	Algorithm and Key Size	Standards (Certificate #)
Random Number Generator (RNG)	N/A	ANSI X9.31 (FIPS 186-2 certificate # 491)
Digital Signature Algorithm (DSA)	1024	FIPS 186-2 (certificate # 310)
Rivest, Shamir, and Adelman (RSA)	1024, 1536, 2048, 3072, 4096	ANSI X9.31 31 (FIPS 186-2 certificate # 413)

Dependencies: FCS_COP.1(a) Cryptographic operation
FCS_COP.1(b) Cryptographic operation
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2 zeroization requirements*].

Dependencies: FCS_CKM.1 Cryptographic key generation

FCS_COP.1(a) Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1(a)

The TSF shall perform [*list of cryptographic operations* **– see table below**] in accordance with a specified cryptographic algorithm [*cryptographic algorithm* **– see table below**] and cryptographic key sizes [*cryptographic key sizes* **– see table below**] that meet the following: [*list of standards* **– see table below**].

Table 13 - Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Digital signature verification	Digital Signature Algorithm (DSA)	1024	FIPS 186-2 (certificate #310)
	RSA	1024, 1536, 2048, 3072, 4096	PKCS #1 v1.5, PKCS #1 PSS, ANSI X9.31 (FIPS 186-2 certificate # 413)
Symmetric encryption and decryption	Advanced Encryption Standard (AES) (CBC[17], ECB[18], OFB[19], CFB[20] modes)	128, 192, 256	FIPS 197 (certificate #859)
	Triple-Data Encryption Standard (3DES[21]) (ECB, OFB, CFB modes)	1-key and 2-key	FIPS 46-3 (certificate #706)
Hashing	Secure Hash Algorithm 1 (SHA-1)	Not Applicable	FIPS 180-2 (certificate #854)
	Secure Hash Algorithm 224 (SHA -224)	Not Applicable	FIPS 180-2 (certificate #854)

[17] CBC – Cipher Block Chaining

[18] ECB – Electronic Codebook

[19] OFB – Output Feedback

[20] CFB – Cipher Feedback

[21] 3DES – Triple Data Encryption Standard

	Secure Hash Algorithm 256 (SHA -256)	Not Applicable	FIPS 180-2 (certificate #854)
	Secure Hash Algorithm 385 (SHA -385)	Not Applicable	FIPS 180-2 (certificate #854)
	Secure Hash Algorithm 512 (SHA -512)	Not Applicable	FIPS 180-2 (certificate #854)
Message Authentication	Keyed-Hash Message Authentication Code (HMAC) with Secure Hash Algorithm1 (SHA -1) (MAC size 10)	Not Applicable	FIPS 198 (certificate #476)
	Keyed-Hash Message Authentication Code (HMAC) with Secure Hash Algorithm 224 (SHA -224) (MAC size 14)	Not Applicable	FIPS 198 (certificate #476)
	Keyed-Hash Message Authentication Code (HMAC) with Secure Hash Algorithm 256 (SHA -256) (MAC size 16)	Not Applicable	FIPS 198 (certificate #476)
	Keyed-Hash Message Authentication Code (HMAC) with Secure Hash Algorithm 385 (SHA -385) (MAC size 24)	Not Applicable	FIPS 198 (certificate #476)
	Keyed-Hash Message Authentication Code (HMAC) with Secure Hash Algorithm 512 (SHA -512) (MAC size 32)	Not Applicable	FIPS 198 (certificate #476)

Dependencies: **FCS_CKM.1 Cryptographic key generation**
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1(b) Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1(b)

The TSF shall perform [*list of cryptographic operations* **– see table below**] in accordance with a specified cryptographic algorithm [*cryptographic algorithm* **– see table below**] and cryptographic key sizes [*cryptographic key sizes* **– see table below**] that meet the following: [*list of standards* **– see table below**] **for data passing between the TOE and the Management Console**.

Table 14 - Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Digital signature verification	RSA	1024, 1536, 2048, 3072, 4096	PKCS #1 v1.5, PKCS #1 PSS, ANSI X9.31 (FIPS 186-2 certificate # 413)
Symmetric encryption and decryption	Advanced Encryption Standard (AES) (CBC mode)	128, 192, 256	FIPS 197 (certificate #859)
	Triple-Data Encryption Standard (3DES) (CBC mode)	1-key and 2-key	FIPS 46-3 (certificate #706)
Hashing	Secure Hash Algorithm 1 (SHA-1)	Not Applicable	FIPS 180-2 (certificate #854)

Dependencies: **FCS_CKM.1 Cryptographic key generation**
FCS_CKM.4 Cryptographic key destruction

6.2.3 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1

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

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1

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

[

TOE administrator (subject) attributes:

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

and attributes of the operation:

1. *admin.access*

].

FDP_ACF.1.2

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

[

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

2. Request the Privileged Administrator role via the CLI: 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.[22]

3. Establish an administrative session via the Management Console: evaluate (with admin.access=WRITE) the <admin> layers of the configured policy rules according to the CPL specification and permit execution of the resulting action is "allow", otherwise prevent execution.

].

FDP_ACF.1.3

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

[

1. *Establish an administrative session: establishment is permitted if the TOE administrator has credentials for "Administrator" role access, or has authenticated via the SSH RSA public key mechanism, and the TOE Administrator's IP address is an allowed administrative interface.*

2. *Request the Privileged Administrator role: execution is permitted if the TOE administrator has the proper credentials for "Privileged Administrator" role access (either configured username/password plus "enable" password, or SSH RSA public key authentication plus "enable" password)*

].

FDP_ACF.1.4

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

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3(a) Static attribute initialization

FDP_IFC.1(a) Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1(a)

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

[

1. *(Subjects) external IT entities attempting to send controlled protocol traffic through the TOE,*

2. *(Information) controlled protocol traffic sent through the TOE to other subjects,*

3. *(Operations) passing controlled protocol traffic through the TOE to the other network*

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

].

Dependencies: FDP_IFF.1(a) Simple security attributes

FDP_IFF.1(a) Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1(a)

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

[

Subject attributes:

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

Information attributes:

1. *Source IP address*
2. *Destination IP address*
3. *Destination port*
4. *Protocol*
5. *URL*
6. *Time of day*
7. *Date*
8. *Originating application*
9. *MIME[23] type*
10. *Request method (the requested operation)*
11. *Any part of an HTTP request other than the body (e.g. header fields[24])*
12. *HTTP response header fields*
13. *HTTP response body*

[23] MIME – Multipurpose Internet Mail Extensions

[24] 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(a)

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 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(a)

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

FDP_IFF.1.4(a)

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

FDP_IFF.1.5(a)

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 ProxySG to the External Network*].

Dependencies: FDP_IFC.1(a) Subset information flow control
FMT_MSA.3(b) Static attribute initialisation

FDP_IFC.1(b) Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1(b)

The TSF shall enforce the [*WAN Optimization SFP*] on [*hosts on either side of the TOE (subjects), the TOE (subject), all data flowing between the subjects (information), and the passing of controlled data traffic traversing the TOE in accelerated form (operations)*].

Dependencies: FDP_IFF.1(b) Simple security attributes

FDP_IFF.1(b) Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1(b)

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

Subject attributes:

1. *none*

Information attributes:

1. *Source IP address*
2. *Destination IP address*
3. *Source Port*
4. *Destination Port*
5. *Subnet address*
6. *Proxy service type*

].

FDP_IFF.1.2(b)

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*All network traffic traversing the TOE between a local network and a remote network is allowed to flow in an accelerated form unless:*

1. *acceleration has been disabled for information with the specified attribute(s).*

If the above-listed condition applies, the information is permitted to flow only in its original form

].

FDP_IFF.1.3(b)

The TSF shall enforce the [*no additional WAN Optimization SFP rules*].

FDP_IFF.1.4(b)

The TSF shall explicitly authorise an information flow based on the following rules: [*none*].

FDP_IFF.1.5(b)

The TSF shall explicitly deny an information flow based on the following rules: [*none*].

Dependencies: FDP_IFC.1(b) Subset information flow control
FMT_MSA.3(c) Static attribute initialisation

6.2.4 Class FIA: Identification and Authentication

FIA_ADM_PCR.1(a) Password controlled role

Hierarchical to: No other components.

FIA_ADM_PCR.1.1(a)

The TSF shall authenticate ~~a~~ **an** [*Administrator*] under the conditions that the [*Administrator*] has requested the [*Privileged Administrator*] role by [*entering the proper password at the "enable" command prompt in the CLI*].

Dependencies: No dependencies

FIA_ADM_PCR.1(b) Password controlled role

Hierarchical to: No other components.

FIA_ADM_PCR.1.1(b)

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

Dependencies: No dependencies

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1

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

FIA_AFL.1.2

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

[

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

].

Dependencies: FIA_UAU.1(a) Timing of authentication

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1

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

FIA_UAU.1.2

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

Dependencies: FIA_UID.1(b) Timing of identification

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1

The TSF shall require each **Management 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

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1

The TSF shall provide

[

1. *Username and password access to the CLI via the serial port or SSH*
2. *Configured "enable" password for CLI privileged role access*
3. *Configured "setup" password for Setup Console access*
4. *Username and password for Management Console access*
5. *RSA public key authentication for SSH access to the CLI*
6. *For End User authentication, the following authentication modes:*
    a. *Auto*
    b. *Proxy*
    c. *Proxy-IP*

d. *Origin*

e. *Origin-IP*

f. *Origin-cookie*

g. *Origin-cookie-redirect*

h. *Origin-IP-redirect*

i. *SG2*

j. *Form-IP*

k. *Form-cookie*

l. *Form-cookie-redirect*

m. *Form-IP-redirect*

]

to support user authentication.

FIA_UAU.5.2

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

[

1. *On the SSH Port,*

   a. *verification of the SSH RSA public key credentials authenticates the user as an Administrator, and*

   b. *if the "enable" command is entered, verification of the "enable" password authenticates the use of the Privileged Administrator role;*

2. *On the SSH Port,*

   a. *verification of the configured console username and password authenticates the user as an Administrator, and*

   b. *If the "enable" command is entered, verification of the "enable" password authenticates the use of the Privileged Administrator role;*

3. *On the SSH Port,*

   a. *verification of the user's id and password against the Administrative Access SFP authenticates the user as an Administrator, and*

   b. *if the "enable" command is entered, verification of the user's password authenticates the use of the Privileged Administrator role;*

4. *On the Serial Port, if the user selects the CLI menu item on the Serial Console,*

   a. *verification of the configured console username and password authenticates the user as an Administrator, and*

b. *if the "enable" command is entered, verification of the user's password authenticates the use of the Privileged Administrator role;*

5. *On the Serial Port, If the user selects the CLI menu item on the Serial Console,*

   a. *verification of the user's id and password against the Administrative Access SFP authenticates the user as an Administrator, and*

   b. *If the "enable" command is entered, verification of the user's id and password authenticates the use of the Privileged Administrator role;*

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

7. *On the Management Console,*

   a. *verification of the configured console username and password, or*

   b. *verification of Administrative Access SFP policy rules*

   authenticates the user as an Administrator or Privileged Administrator;

8. *For End User requests, authentication will proceed according to the configured authentication mode challenge type and credential type, and the configured Proxy SFP rules.*

].

Dependencies: No dependencies

FIA_UAU.6(a) Re-authenticating

Hierarchical to: No other components.

FIA_UAU.6.1(a)

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

Dependencies: No dependencies

FIA_UAU.6(b) Re-authenticating

Hierarchical to: No other components.

FIA_UAU.6.1(b)

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

Dependencies: No dependencies

FIA_UAU.7(a) Protected authentication feedback

Hierarchical to: No other components.

FIA_UAU.7.1(a)

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

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7(b) Protected authentication feedback

Hierarchical to: No other components.

FIA_UAU.7.1(b)

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

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UID.1(a) Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1(a)

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

FIA_UID.1.2(a)

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

Dependencies: No dependencies

FIA_UID.1(b) Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1(b)

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

FIA_UID.1.2(b)

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

Dependencies: No dependencies

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1

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

Dependencies: No dependencies

6.2.5 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1

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

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

FMT_MSA.1(a) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1(a)

The TSF shall enforce the [*Administrative Access SFP*] to restrict the ability to [*query*] the security attributes [*user group membership, user name, time of day/date, admin.access*] to [*TOE administrators*].

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

FMT_MSA.1(b) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1(b)

The TSF shall enforce the [*Administrative Access SFP*] to restrict the ability to [*modify, delete*] the security attributes [*user group membership, user password, user name, time of day/date, admin.access*] to [*Privileged Administrators*].

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

FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

FMT_MSA.2.1

The TSF shall ensure that only secure values are accepted for [*Username, User group membership*].

Dependencies: **[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]**
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3(a) Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1(a)

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(a)

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

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

FMT_MSA.3(b) Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1(b)

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

FMT_MSA.3.2(b)

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

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

FMT_MSA.3(c) Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1(c)

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

FMT_MSA.3.2(c)

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

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

FMT_MTD.1(a) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

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

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

FMT_MTD.1(b) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

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

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

FMT_MTD.2 Management of limits on TSF data

Hierarchical to: No other components.

FMT_MTD.2.1

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

FMT_MTD.2.2

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

Dependencies: **FMT_MTD.1 Management of TSF data**
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

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

[

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

].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [[*"Administrator", "Privileged Administrator", and "Setup Console Administrator", as identified in Table 15*].

Table 15 - Authorized Roles

Role	Method of Authentication
Administrator	• The user authenticates over the SSH Port using SSH RSA public key credentials. • The user authenticates over the SSH Port using the configured console username and password. • The user authenticates over the SSH Port and against the Administrative Access SFP using the user's username and password. • The user authenticates to the CLI over the Serial Port using the configured console credentials. • The user authenticates to the CLI over the Serial Port and against the Administrative Access SFP using the user's username and password. • The user authenticates to the Management Console and against the Administrative Access SFP using the user's username and password.

Role	Method of Authentication
Privileged Administrator	• The user is an Administrator authenticated over the SSH Port using SSH RSA public key credentials, and then authenticates to the "enable" CLI command using the configured enable password. • The user is an Administrator authenticated over the SSH Port using the configured console username and password, and then authenticates to the "enable" CLI command using the configured enable password. • The user is an Administrator authenticated over the SSH Port using the user's username and password against the Administrative Access SFP, and then authenticates to the "enable" command using the user's password. • The user is an Administrator authenticated to the Serial Console using the configured console username and password, and then authenticates to the "enable" command using the configured "enable" password. • The user is an Administrator authenticated to the Serial Console using the user's username and password against the Administrative Access SFP, and then authenticates to the "enable" command using the user's username and password. • The user authenticates to the Management Console using the configured console username and password. • The user authenticates to the Management Console using a username and password that is allowed access to the Privileged Administrator role by the Administrative Access SFP rules.
Setup Console Administrator	• The user is a Serial Console user and authenticates to the Setup Console using the Setup Console password.

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.3 Assuming roles

Hierarchical to: No other components.

FMT_SMR.3.1

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

Dependencies: FMT_SMR.1 Security roles

6.2.6 Class FPT: Protection of the TSF

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

Dependencies: No dependencies

6.2.7 Class FRU: Resource Allocation

EXT_FRU_ARP.1 Health check alarms

Hierarchical to: No other components.

FAU_ARP.1.1

The TSF shall take [*one of the following notification actions: email, event logging, SNMP trap*] upon detection of a change in health check state.

Dependencies: No dependencies

FRU_RSA.1 Maximum quotas

Hierarchical to: No other components.

FRU_RSA.1.1

The TSF shall enforce maximum quotas of the following resources: [*number of connections, number of failed requests, number of warnings*] that [*subjects*] can use [*over a specified period of time*].

Dependencies: No dependencies

FRU_RSA.2 Minimum and maximum quotas

Hierarchical to: FRU_RSA.1 Maximum quotas

FRU_RSA.2.1

The TSF shall enforce maximum quotas of the following resources: [*bandwidth*] that [**a** *defined ~~group~~* **class** *of ~~users~~* **traffic]** can use [*simultaneously*].

FRU_RSA.2.2

The TSF shall ensure the provision of minimum quantity of ~~each~~ [*bandwidth*] that is available for [**a** *defined ~~group~~* **class** *of ~~users~~* **traffic**] to use [*simultaneously*].

Dependencies: No dependencies

6.2.8 Class FTA: TOE Access

FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

Hierarchical to: FTA_MCS.1

FTA_MCS.2.1

The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules

[*If an End User exceeds the number of concurrent logins defined by policy, the End User will be logged out of one or more sessions.*].

FTA_MCS.2.2

The TSF shall enforce, by default, a limit of [*an administrator-defined number of*] sessions per user.

Dependencies: FIA_UID.1 Timing of identification

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

FTA_SSL.3.1

The TSF shall terminate an interactive session after ~~a~~ **an** [*administrator-defined time interval of user inactivity*].

Dependencies: No dependencies

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.1. Table 16 - Assurance Requirements summarizes the requirements.

Table 16 - Assurance Requirements

Assurance Requirements	
Class ALC : Life Cycle Support	ALC_CMC.2 Use of a CM[25] system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.1 Basic Flaw Remediation
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6.4 TOE Security Assurance Measures

EAL 2+ was chosen to provide a basic level of independently assured security. This section of the Security Target maps the assurance requirements of the TOE for a CC EAL 2+ level of assurance to the assurance measures used for the development and maintenance of the TOE. The following table provides a mapping of the appropriate documentation to the TOE assurance requirements.

[25] CM – Configuration Management

Table 17 - Assurance Measures Mapping to TOE Security Assurance Requirements (SARs)

Assurance Component	Assurance Measure
ALC_CMC.2	Blue Coat ProxySG v5.3.1.9 running on SG510, SG810, and SG8100 - Life Cycle Support: CM Capabilities and Scope
ALC_CMS.2	Blue Coat ProxySG v5.3.1.9 running on SG510, SG810, and SG8100 - Life Cycle Support: CM Capabilities and Scope
ALC_DEL.1	Blue Coat ProxySG v5.3.1.9 running on SG510, SG810, and SG8100 - Life Cycle Support: Delivery
ALC_FLR.1	Blue Coat ProxySG v5.3.1.9 running on SG510, SG810, and SG8100 – Life Cycle Support: Flaw Remediation
ADV_ARC.1	Blue Coat ProxySG v5.3.1.9 running on SG510, SG810, and SG8100 - Development: Security Architecture, Functional Specification, and TOE Design
ADV_FSP.2	Blue Coat ProxySG v5.3.1.9 running on SG510, SG810, and SG8100 - Development: Security Architecture, Functional Specification, and TOE Design
ADV_TDS.1	Blue Coat ProxySG v5.3.1.9 running on SG510, SG810, and SG8100 - Development: Security Architecture, Functional Specification, and TOE Design
AGD_OPE.1	Blue Coat Systems SG Appliance Document Suite (SGOS version 5.3) Blue Coat SGOS 5.3.x Release Notes, Version: SGOX 5.3.x Blue Coat ProxySG v5.3.1.9 running on SG510, SG810, and SG8100 – Guidance Supplement
AGD_PRE.1	Blue Coat Systems SG510 Series Installation Guide (Version: SGOS 5.3.x) Blue Coat Systems SG810 Series Installation Guide (Version: SGOS 5.3.x) Blue Coat Systems 8100 Series Installation Guide (Version: SGOS 5.3.x) Blue Coat ProxySG v5.3.1.9 running on SG510, SG810, and SG8100 – Guidance Supplement
ATE_COV.1	Blue Coat ProxySG v5.3.1.9 running on SG510, SG810, and SG8100 – Coverage and Functional Tests
ATE_FUN.1	Blue Coat ProxySG v5.3.1.9 running on SG510, SG810, and SG8100 – Coverage and Functional Tests

6.4.1 ALC_CMC.2: Use of a CM system, ALC_CMS.2: Parts of the TOE CM coverage

The Configuration Management document provides a description of the various tools used to control the configuration items and how they are used internally at Blue Coat. This document provides a complete configuration item list and a unique referencing scheme for each configuration item. The documentation further details the TOE configuration items that are controlled by the configuration management system.

6.4.2 ALC_DEL.1: Delivery Procedures

The Delivery document provides a description of the secure delivery procedures implemented by Blue Coat to protect against TOE modification during product delivery to the customer.

6.4.3 ALC_FLR.1: Basic Flaw Remediation

The Flaw Remediation document outlines the steps taken at Blue Coat to capture, track and remove bugs. The documentation shows that all flaws are recorded and that the system tracks them to completion.

6.4.4 ADV_ARC.1: Security Architecture Description, ADV_FSP.2: Security-enforcing Functional Specification, ADV_TDS.1: Basic design

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

- The Security Architecture Description provides a description of the architecture-oriented features of domain separation, TSF self-protection, and non-bypassability of the security functionality.
- The Security-enforcing Functional Specification (FSP) provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose, method of use, parameters and parameter descriptions for each external TSF interface. In addition, the FSP describes the direct error messages that may result from security enforcing effects. The FSP also provides a mapping from the FSP to the SFRs.
- The Basic Design provides a design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF for a relatively simple TOE. The basic design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and a mapping from the TSF interfaces of the FSP to the lowest level of decomposition available in the TOE design.

6.4.5 AGD_OPE.1: Operational User Guidance, AGD_PRE.1: Preparative Procedures

The Operational User Guidance provides information about the proper usage of the TOE in its evaluated configuration. This guidance is intended to be used by all types of users: end-users, persons responsible for maintaining and administering the TOE in a correct manner for maximum security, and by others (e.g., programmers) using the TOE's external interfaces. Operational User Guidance describes the security functionality provided by the TSF, provides instructions and guidelines (including warnings), helps users to understand the TSF, and includes the security-critical information, and the security-critical actions required, for its secure use.

The Preparative Procedures are used to ensure that the TOE has been received and installed in a secure manner as intended by the developer. The requirements for preparation call for a secure transition from the delivered TOE to its initial operational environment.

6.4.6 ATE_COV.1: Evidence of coverage, ATE_FUN.1: Functional testing

There are a number of components that make up the Test documentation. The Coverage Analysis demonstrates that testing is performed against the functional specification. The Coverage Analysis demonstrates that all TSFIs in the FSP have been tested.

Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided in order to meet the assurance requirement Functional Testing.

7 TOE Summary Specification

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

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 18 - Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1(a)	Audit review
	FAU_SAR.1(b)	Audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(a)	Cryptographic operation
	FCS_COP.1(b)	Cryptographic operation
Administrative Access SFP	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
Proxy SFP	FDP_IFC.1(a)	Subset information flow control
	FDP_IFF.1(a)	Simple security attributes
WAN Optimization SFP	FDP_IFC.1(b)	Subset information flow control
	FDP_IFF.1(b)	Simple security attributes
Identification and Authentication	FIA_ADM_PCR.1(a)	Password controlled role

TOE Security Function	SFR ID	Description
	FIA_ADM_PCR.1(b)	Password controlled role
	FIA_AFL.1	Authentication failure handling
	FIA_UAU.1	Timing of authentication
	FIA_UAU.2	User authentication before any action
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.6(a)	Re-authenticating
	FIA_UAU.6(b)	Re-authenticating
	FIA_UAU.7(a)	Protected authentication feedback
	FIA_UAU.7(b)	Protected authentication feedback
	FIA_UID.1(a)	Timing of identification
	FIA_UID.1(b)	Timing of identification
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1(a)	Management of security attributes
	FMT_MSA.1(b)	Management of security attributes
	FMT_MSA.2	Secure security attributes
	FMT_MSA.3(a)	Static attribute initialisation
	FMT_MSA.3(b)	Static attribute initialisation
	FMT_MSA.3(c)	Static attribute initialisation
	FMT_MTD.1(a)	Management of TSF data
	FMT_MTD.1(b)	Management of TSF data

TOE Security Function	SFR ID	Description
	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
Protection of the TSF	FPT_STM.1	Reliable time stamps
Resource utilisation	EXT_FRU_ARP.1	Health check alarms
	FRU_RSA.1	Maximum quotas
	FRU_RSA.2	Minimum and maximum quotas
TOE Access	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.3	TSF-initiated termination

7.1.1 Security Audit

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

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

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

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

- Date and time of the event
- Type of event
- Identity of the subject
- Outcome of the event
- Source IP address

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

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

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

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

7.1.2 Cryptographic Support

The Cryptographic Support function provides encryption and decryption of all data transmitted between the TOE and the client running the CLI and Management Console. This data is transmitted using the SSH v2 or HTTPS protocols. The TOE username and password, and the privileged mode passwords, which the administrator defines during initial configuration, are encrypted prior to storage and display. In addition, TLS may be used for communication between the TOE and LDAP and IWA authentication servers.

Passwords that the TOE uses to authenticate itself to outside services are encrypted using 3DES on the TOE appliance and using RSA public key encryption for output with the show config CLI command. These passwords include the access log FTP client passwords, the archive configuration FTP password, the RADIUS[26] primary and alternate secret, the LDAP search password, and the content filter download passwords.

The TOE uses x.509 certificates for various applications, including authenticating the identity of a server, authenticating another SG appliance, and securing an intranet. X.509 is a cryptographic standard for public key infrastructure (PKI) that specifies standard formats for public key certificates. The TOE uses SSL certificates, Certificate Authority (CA) certificates, and external certificates (certificates for which the TOE does not have the private key).

Access logs are encrypted using an external certificate. Administrators can digitally sign access logs to certify that a particular SG appliance wrote and uploaded a specific log file to the TOE. Each log file has a signature file associated with it that contains the certificate and the digital signature used for verifying the log file.

A number of cipher suites are included as part of the TOE. Cipher suites specify the algorithms used to secure an encrypted connection. All cipher suites supported by the TOE use the RSA key exchange algorithm, which uses the public key encoded in the server's certificate to encrypt a piece of secret data for transfer from the client to the server. This secret is then used at both endpoints to compute encryption keys.

In addition, a default keyring (containing a public/private keypair with a customized keylength and a certificate or certificate signing request) is generated when the TOE boots from the uninitialized state, and is used for accessing the Management Console. The user can choose to use a different keyring, however. The default keyring can also be used for other purposes.

For two-way encrypted communication, symmetric keys are generated using an ANSI X9.31 RNG algorithm. Each endpoint of the communication generates a symmetric encryption key, encrypts it with the other endpoint's public key, and then sends it.

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

The TOE destroys cryptographic keys in accordance with FIPS 140-2 zeroization requirements.

Certificate Revocation Lists (CRLs) enable checking server and client certificates against lists provided and maintained by CAs that show certificates that are no longer valid. The TOE administrator can import CRLs from trusted CAs and then use them to determine if the TOE's certificates are still valid.

The TOE's claimed cryptographic support is provided by a FIPS 140-2-valiated cryptographic module in the TOE. The FIPS 140-2 certification for the TOE has been issued by the National Institute of Standards and Technology, certificate #XXX.

Comment [MSOffice2]: To the Evaluator: The FIPS certificate number will be added when the module has completed FIPS 140-2 certification.

TOE Security Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM.4, FCS_COP.1(a), FCS_COP.1(b).

7.1.3 Administrative Access SFP

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

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

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

7.1.4 Proxy SFP

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

TOE Security Functional Requirements Satisfied: FDP_IFC.1(a), FDP_IFF.1(a)

7.1.5 WAN Optimization SFP

The WAN Optimization security function defines how the TOE performs byte caching and acceleration techniques such as compression and object caching on data being transmitted through the TOE. The TOE enforces the WAN Optimization SFP on specified TOE subjects, objects, and operations. The architecture of the TOE ensures that all operations between the specified objects and subjects are regulated by the TOE based upon the criteria defined in the WAN Optimization SFP. The object attributes include source IP address, destination IP address, source port, destination port, subnet address, and proxy service type. All data traversing the TOE between the internal network and the external network undergoes WAN Optimization, unless this has been disabled for the specified traffic.

TOE Security Functional Requirements Satisfied: FDP_IFC.1(b), FDP_IFF.1(b)

7.1.6 Identification and Authentication

ProxySG users are identified by their usernames and in the evaluated configuration authentication is via passwords. Authentication is tied to the session, either the Administrative session or the End User session.

7.1.6.1 Administrator Authentication

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

When a browser connects to the Management Console port, the user is directed to enter a username and password. The management console GUI provides access to the setup functions as well as the operational administrative functions.

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

The Privileged Administrator role (the only way to make configuration or policy changes) is also subject to authentication. To assume the Privileged Administrator role on the CLI, an authenticated Administrator must execute the "enable" command, which challenges for a password. Administrator-role users authenticate as Privileged Administrators by supplying the "enable" password that is part of system configuration. Ordinary administrators authenticate to the "enable" command with their associated password from the local user list (access to the "enable" command by ordinary administrators is controlled by policy). The Privileged Administrator role is assumed by any user logging in to the Management Console with the administrator username and password, or when the configured policy grants read/write access. The "enable" command is not required.

7.1.6.2 End User Authentication

End Users establish a session with the ProxySG when the user agent in use establishes a TCP/IP connection with the ProxySG 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 employing. Once authenticated, additional requests made using the same session (TCP/IP connection) will be considered authenticated.

If an End Users attempts to authenticate, but an authentication error occurs (such as an external server failure), the TOE will check the error against an administrator-defined authentication error list. If the error matches an error on the list, the End User will be allowed to proceed unauthenticated. Otherwise, the authentication fails. If the End User is permitted to continue unauthenticated, the End User will have no username, group information, or surrogate credentials. Policy that uses the user, group, domain, or attribute conditions does not match.

In the evaluated configuration, the ProsySG supports all available authentication modes: automatic, proxy, proxy-IP, origin, origin-IP, origin-cookie, origin-cookie-redirect, origin-IP-redirect, SG2, form-IP, form-cookie, form-cookie-redirect, and form-IP-redirect. These modes designate what kind of challenge is issued (proxy, origin, or origin-redirect), and the type of surrogate credentials used, if applicable (IP, cookie, or connection).

Proxy-style challenges are sent from proxy servers to clients that are explicitly proxied. Origin-style challenges are sent from origin content servers (OCS), or from proxy servers impersonating an OCS. Form-style challenges are presented to collect the user's credentials.

IP surrogate credentials authenticate the user based on the IP address of the client. Cookie surrogate credentials use a cookie constructed by the ProxySG as a surrogate. Connection surrogate credentials use the TCP/IP connection to authenticate the user.

7.1.6.3 Automatic Account Lockout

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

TOE Security Functional Requirements Satisfied: FIA_ADM_PCR.1(a), FIA_ADM_PCR.1(b), FIA_AFL.1, FIA_UAU.1, FIA_UAU.2, FIA_UAU.5, FIA_UAU.6(a), FIA_UAU.6(b), FIA_UAU.7(a), FIA_UAU.7(b), FIA_UID.1(a), FIA_UID.1(b), FIA_UID.2

7.1.7 Security Management

ProxySG security is managed by administrators, who have varying degrees of authority to review and modify the configuration of the security attributes of TOE. Levels of administrative authority are based on the credentials used to authenticate and (for "ordinary" administrators) any associated policies defined in the Administrative Access SFP (refer to paragraph 7.1.6.1 for details regarding authentication methods for the various administrators). All administrators are allowed to review such attributes as credentials, audit settings, network settings, and policies. Privileged Administrators can also modify the TOE configuration and define Administrative Access SFP and the Proxy SFP rules. CLI users that authenticate using the configured "enable" password at the "enable" command challenge are granted full read/write privileges, while those administrators defined by the local user list that are allowed Privileged access are granted privileges based on policy.

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

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

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

7.1.8 Protection of the TSF

The TOE provides reliable timestamp information for its own use. The TOE software retrieves the timestamp from the hardware clock, which is set during installation of the appliance. The order of the audit records can be determined by the value of the timestamps.

The time can be synchronized to Coordinated Universal Time manually through the configuration settings. Administrators are assumed to be trusted and competent, and may change the system time whenever necessary.

TOE Security Functional Requirements Satisfied: FPT_STM.1.

7.1.9 Resource utilisation

The TOE enforces administrator-defined quotas on the number and duration of network connections and bandwidth utilization. The TSF enforces configured maximum quotas on the number of connections, number of failed requests, and number of warnings that defined classes of traffic can use over a specified interval. This enables attack detection by the TSF, reducing the effects of Distributed Denial of Service and port scanning attacks. The TSF prevents attacks such as these by limiting the number of simultaneous TCP connections from each client IP address. The TSF will either not respond to connection attempts from a client at its limit, or it will reset the connection.

The TSF also enforces configured minimum and maximum quotas on bandwidth usage that defined classes of traffic can use at the same time. All classes are assured of the receiving at least the minimum quota of bandwidth configured, if the bandwidth is available. A class can never receive more than the configured maximum quota.

The TOE can also be configured to send alerts to notify the TOE administrator of changes in the health status of the TOE. The TSF periodically tests the health status of the TOE, thereby determining its availability to the network. Health checks test for network connectivity, target responsiveness, and basic functionality of the upstream system or service. Health checks are run on external resources, such as forwarding hosts, SOCKS gateways, Dynamic Real-Time Rating (DRTR) services, authentication servers, DNS servers, and ICAP or Websense off-box services. If the health check for an individual host fails, the TSF can select a healthy host to take over, or report the failure to an administrator, or both. When notifications are configured, the TSF may send email, event log notifications, or SNMP traps to the TOE administrator. Notifications can be configured globally, for all health checks, or explicitly, for specific checks.

TOE Security Functional Requirements Satisfied: EXT_FRU_ARP.1, FRU_RSA.1, FRU_RSA.2.

7.1.10 TOE Access

The TOE restricts the number of concurrent sessions that belong to the same End User by policy. If an End User exceeds the number of concurrent sessions permitted, the TOE will log the user off of one or more sessions, depending on the number permitted.

The TOE will also terminate an End User session after an administrator-defined interval of inactivity. Each time a login is completed, the inactivity-timeout value is updated. If the time since the last activity time exceeds the inactivity-timeout value, the End User is logged out.

TOE Security Functional Requirements Satisfied: FTA_MCS.2, FTA_SSL.3.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target extends Part 2 and conforms to Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, version 3.1. The extended SFRs contained within this ST are FIA_ADM_PCR.1(a) and FIA_ADM_PCR.1(b). These were included to define the security functionality provided by the use of the "enable" command and the setup password in administrator authentication on the Serial Console and CLI.

There are no protection profile claims for this Security Target.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Table 19 demonstrates the mappings between the threats, polices, and assumptions to the security objectives is complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

Table 19 - Mapping of Security Objectives to Threats, Policies, and Assumptions

Objectives / Threats Policies Assumptions	O.AUDIT	O.AUTHENTICATE	O.MANAGE	O.REMOVE_ACTIVE	O.SCREEN_TYPE	O.SCREEN_URL	O.TIMESTAPMP	O.VALIDATED_CRYPTO	O.PROTECT	O.QUOTA	O.ALERT	O.PASS_TRAFFIC	OE.NETWORK	OE.ADMIN	OE.ENVIRON	OE.PASSWORD
THREATS																
T.EXTERNAL_NETWORK				✓	✓	✓										
T.MASQUERADE		✓														
T.UNAUTHORIZED_ACCESS		✓	✓					✓	✓							
T.NACCESS								✓	✓							
T.RESOURCE										✓	✓					
T.HEALTH										✓	✓					
POLICIES																

Objectives / Threats Policies Assumptions	O.AUDIT	O.AUTHENTICATE	O.MANAGE	O.REMOVE_ACTIVE	O.SCREEN_TYPE	O.SCREEN_URL	O.TIMESTAPMP	O.VALIDATED_CRYPTO	O.PROTECT	O.QUOTA	O.ALERT	O.PASS_TRAFFIC	OE.NETWORK	OE.ADMIN	OE.ENVIRON	OE.PASSWORD
P.ACTIVE_CONTENT				✓												
P.ADMIN		✓	✓													
P.AUDIT	✓						✓									
P.CONTENT_TYPE					✓											
P.FILTERED_URLS						✓										
P.MANAGE			✓													
P.NON_ANONYMOUS		✓														
P.POST_TYPE					✓											
P.PASS_TRAFFIC												✓				
ASSUMPTIONS																
A.ENVIRON															✓	
A.INSTALL														✓		
A.NETWORK													✓			
A.NO_EVIL_ADMIN														✓		
A.PASSWORD																✓

8.2.1 Security Objectives Rationale Relating to Threats

Table 20 - Threats:Objectives Mapping

Threats	Objectives	Rationale
T.EXTERNAL_NETWORK A user or process on the Internal Network may access or post content on the External Network that has been deemed inappropriate or potentially harmful to the Internal Network.	O.REMOVE_ACTIVE The TOE must be able to remove active content from HTML pages delivered via a controlled protocol as defined by the Proxy SFP.	O.REMOVE_ACTIVE ensures that active content on HTML pages is removed prior to being delivered to the Internal Network, thereby minimizing the risk of attack to the Internal Network.
	O.SCREEN_TYPE The TOE must disallow controlled protocol traffic of given content types as defined by the Proxy SFP.	O.SCREEN_TYPE ensures that controlled protocol traffic of the specified content type(s) is disallowed, thereby minimizing the risk of Internal Network users accessing the External Network for non-approved activities.
	O.SCREEN_URL The TOE must disallow controlled protocol traffic for given URLs as defined by the Proxy SFP.	O.SCREEN_URL ensures that controlled protocol traffic from the specified URL(s) is disallowed, thereby minimizing the risk of Internal Network users accessing the External Network for non-approved activities.
T.MASQUERADE A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.AUTHENTICATE The TOE must require the Administrator to authenticate before gaining access to the administrative interfaces of the TOE, and End Users to authenticate if their controlled protocol traffic matches a Proxy SFP rule which requires authentication.	O.AUTHENTICATE ensures that Administrators and End Users supply login credentials (including strong passwords) before being granted access to services or information, thereby reducing the risk of access by masquerading.
T.UNAUTHORIZED_ACCESS A user may gain access to security data on the TOE for which they are not authorized according to the TOE security policy.	O.AUTHENTICATE The TOE must require the Administrator to authenticate before gaining access to the administrative interfaces of the TOE, and End Users to authenticate if their controlled protocol traffic matches a Proxy SFP rule which requires authentication.	O.AUTHENTICATE ensures that users supply login credentials (including strong passwords) before being granted access to any security-related information, thereby reducing the risk of unauthorized access.

Threats	Objectives	Rationale
	O.MANAGE The TOE must provide secure management of the system configuration, the Administrative Access SFP, the WAN Optimization SFP, and the Proxy SFP.	O.MANAGE provides the capability for an administrator to properly configure the management mechanisms of the TOE designed to mitigate this threat.
	O.VALIDATED_CRYPTO The TOE shall provide cryptographic functions for its own use. These functions will be provided by a FIPS 140-2 validated cryptographic module.	O.VALIDATED_CRYPTO ensures that data is protected from unauthorized access, thereby ensuring that the security data on the TOE is protected from unauthorized access.
	O.PROTECT The TOE must have the capability to protect management traffic from unauthorized reading or modification.	O.PROTECT ensures that the TOE is capable of protecting the management data transmitted through the TOE from unauthorized access, thereby ensuring that security data that is transmitted is protected from unauthorized access.
T.NACCESS An unauthorized person or external IT entity may be able to view or modify data that is transmitted between the TOE and a remote authorized external entity.	O.VALIDATED_CRYPTO The TOE shall provide cryptographic functions for its own use. These functions will be provided by a FIPS 140-2 validated cryptographic module.	O.VALIDATED_CRYPTO ensures that the TOE provides cryptographic functionality such as encryption and certificate authentication, ensuring that data that is transmitted through the TOE is cannot be accessed.
	O.PROTECT The TOE must have the capability to protect management traffic from unauthorized reading or modification.	O.PROTECT ensures that the TOE has the capability to protect management traffic from unauthorized access, thereby ensuring that no unauthorized person or external entity may view or modify the data.
T.RESOURCE TOE users or attackers may cause network connection resources to become overused and therefore unavailable.	O.QUOTA The TOE must be able to place quotas on network connection resources.	O.QUOTA ensures that the TOE is capable of placing administrator-defined quotas on the network connection resources, thereby ensuring that those resources do not become unavailable.
	O.ALERT The TOE must alert the administrator of changes in TOE health.	O.ALERT ensures that the TOE alerts the administrator of changes in TOE health status, thereby ensuring that the network connection resources do not become unavailable.

Threats	Objectives	Rationale
T.HEALTH TOE users may perform actions that compromise the health of the TOE.	O.QUOTA The TOE must be able to place quotas on network connection resources.	O.QUOTA ensures that the TOE is capable of placing administrator-defined quotas on the network connection resources, thereby ensuring that those resources remain available.
	O.ALERT The TOE must alert the administrator of changes in TOE health.	O.ALERT ensures that the TOE alerts the administrator of changes in TOE health status, thereby enabling the administrator to take action to repair the condition.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

Table 21 - Policies:Objectives Mapping

Policies	Objectives	Rationale
P.ACTIVE_CONTENT The TOE shall provide a means to remove active content (e.g. Java, JavaScript, ActiveX) in HTML pages delivered via controlled protocols.	O.REMOVE_ACTIVE The TOE must be able to remove active content from HTML pages delivered via a controlled protocol as defined by the Proxy SFP.	O.REMOVE_ACTIVE ensures that active content delivered from the External Network is removed as defined by the Proxy's policies, minimizing the risk of this type of exploit
P.ADMIN Only authorized individuals shall have the ability to perform administrative actions on the TOE.	O.AUTHENTICATE The TOE must require the Administrator to authenticate before gaining access to the administrative interfaces of the TOE, and End Users to authenticate if their controlled protocol traffic matches a Proxy SFP rule which requires authentication	O.AUTHENTICATE ensures that administrators enter credentials before access to the administrative interfaces of the TOE is granted.
	O.MANAGE The TOE must provide secure management of the system configuration, the Administrative Access SFP, the WAN Optimization SFP, and the Proxy SFP.	O.MANAGE ensures that only administrators are given credentials allowing access to the administrative functions of the TOE.

Policies	Objectives	Rationale
P.AUDIT The TOE shall record events of security relevance at the "basic level" of auditing. The TOE shall record the resulting actions of the Proxy SFP.	O.AUDIT The TOE must record events of security relevance at the "basic level" of auditing. The TOE must record the resulting actions of the Proxy SFP.	O.AUDIT ensures that events of the appropriate security relevance are recorded at the appropriate level.
	O.TIMESTAMP The TOE must provide a timestamp for use by the TOE.	O.TIMESTAMP ensures that timestamps are provided for use in the audit records.
P.CONTENT_TYPE End Users shall not access unauthorized content types via controlled protocols on the External Network.	O.SCREEN_TYPE The TOE must disallow controlled protocol traffic of given content types as defined by the Proxy SFP.	O.SCREEN_TYPE ensures that End Users are prevented from accessing forbidden content types via controlled protocols by disallowing such traffic.
P.FILTERED_URLS End Users shall not access unauthorized URLs via controlled protocols on the External Network.	O.SCREEN_URL The TOE must disallow controlled protocol traffic for given URLs as defined by the Proxy SFP.	O.SCREEN_URL ensures that End Users are prevented from accessing forbidden URLs via controlled protocols by disallowing such traffic.
P.MANAGE The TOE shall provide secure management of the system configuration, the Proxy SFP, the WAN Optimization SFP, and the Administrative SFP.	O.MANAGE The TOE must provide secure management of the system configuration, the Administrative Access SFP, the WAN Optimization SFP, and the Proxy SFP.	O.MANAGE ensures that the TOE provides a mechanism by which it can be securely managed.
P.NON_ANONYMOUS Access to some resources via controlled protocols on the External Network may be restricted to particular End Users.	O.AUTHENTICATE The TOE must require the Administrator to authenticate before gaining access to the administrative interfaces of the TOE, and End Users to authenticate if their controlled protocol traffic matches a Proxy SFP rule which requires authentication	O.AUTHENTICATE ensures that End Users authenticate to the system before being allowed access to controlled protocol traffic (if required by the Proxy SFP rules).

Policies	Objectives	Rationale
P.POST_TYPE End Users shall not post unauthorized content types to the External Network using controlled protocols.	O.SCREEN_TYPE The TOE must disallow controlled protocol traffic of given content types as defined by the Proxy SFP.	O.SCREEN_TYPE ensures that End Users cannot post unauthorized content types (as defined by the Proxy SFP rules) to the External Network via controlled protocols.
P.PASS_TRAFFIC The TOE shall enforce the WAN Optimization SFP on traffic passing from the internal network to the external network.	O.PASS_TRAFFIC The TOE must pass traffic from the internal network to the external network as defined by the WAN Optimization SFP.	O.PASS_TRAFFIC ensures that traffic that passes from the internal network to the external network is controlled by the WAN Optimization SFP.

Every policy is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives enforce all defined policies.

8.2.3 IT Environment Security Objectives Rationale Relating to Assumptions

Table 22 - Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.ENVIRON The TOE is located in an environment that provides physical security, uninterruptible power, air conditioning, and all other conditions required for reliable operation of the hardware. Physical access to the appliance is restricted to authorized persons.	OE.ENVIRON The physical environment must be suitable for supporting a computing device in a secure setting.	OE.ENVIRON ensures that the TOE IT environment is suitable to ensure the proper, secure, and on-going functioning of the TOE.
A.INSTALL The ProxySG device has been installed and configured according to the appropriate installation guides.	OE.ADMIN The Administrator must be non-malicious and competent, and must follow all guidance.	OE.ADMIN reduces the risk of security vulnerabilities by ensuring that the administrator responsible for the ProxySG device installed and configured the device according to the documented guidance.

Assumptions	Objectives	Rationale
A.NETWORK All Proxy SFP-controlled protocol traffic between the Internal and External Networks traverses the ProxySG device; there is no other connection between the Internal and External Networks for Proxy SFP-controlled protocol traffic.	OE.NETWORK All Proxy-SFP controlled protocol traffic between the Internal and External Networks must traverse the ProxySG device.	OE.NETWORK ensures that the IT environment is configured such that no Proxy SFP-controlled protocol traffic can travel between the Internal and External Networks without traversing the ProxySG device.
A.NO_EVIL_ADMIN Administrators are non-hostile and follow all administrator guidance when using the TOE. Administration is competent and on-going.	OE.ADMIN The Administrator must be non-malicious and competent, and must follow all guidance.	OE.ADMIN ensures that the administrator is trusted, educated, competent, and has no malicious intent, thereby addressing this assumption.
A.PASSWORD Passwords for the Serial Console Administrator and End User accounts, and the "enable" passwords, are at least five characters in length, and may not be a dictionary word.	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.PASSWORD ensures that the passwords selected by users are of sufficient strength to provide the desired level of security for TOE access.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.2.4 IT Environment Security Objectives Rationale Relating to Policies

There are no IT Environment Security Objectives relating to Policies defined for this Security Target.

8.3 Rationale for Extended Security Functional Requirements

A pair of explicitly-stated authentication requirements was created to specifically address the security functionality provided by the use of the "enable" command and the setup password in administrator authentication on the Serial Console and CLI. These requirements have no dependencies since the stated requirements embody all the necessary security functions. These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

FIA_ADM_PCR.1(a) was stated explicitly (rather than use FIA_UAU.6) to specify that the re-authentication process requires verification against Privileged Administrator credentials that are different than those that were originally entered by the TOE administrator on the Serial Console. FIA_ADM_PCR.1(b) was stated explicitly

(rather than use FIA_UAU.6) to specify that the re-authentication process requires verification against the Setup Console Administrator password that is different than the password that was originally entered by the TOE administrator on the Serial Console.

An explicitly-stated resource utilization requirement was created to address the security functionality provided by the use of notifications in case of a change in status of the health of the TOE. This requirement has no dependencies since the stated requirement embodies all the necessary security functions. This requirement exhibits functionality that can be easily documented in the ADV assurance evidence, and thus does not require any additional Assurance Documentation.

EXT_FRU_ARP.1 was stated explicitly to specify that notifications will be sent out when a change of health status occurs. This requirement was modeled after FAU_ARP.1, which uses the audit records as the source of the analysis. EXT_FRU_ARP.1 uses the health check status as the source of the analysis.

8.4 Rationale for Extended TOE Security Assurance Requirements

No extended Security Assurance Requirements are defined for this Security Target.

8.5 Security Requirements Rationale

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

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 23 - Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT The TOE must record events of security relevance at the "basic level" of auditing. The TOE must record the resulting actions of the Proxy SFP.	FAU_GEN.1	This requirement supports O.AUDIT by requiring the TOE to produce audit records for system security events and for actions caused by enforcement of the Proxy SFP.
	FAU_SAR.1(a)	This requirement supports O.AUDIT by requiring the TOE to make the recorded audit records available for review.
	FAU_SAR.1(b)	This requirement supports O.AUDIT by requiring the TOE to make the recorded audit records available for review.
	FAU_STG.1	This requirement supports O.AUDIT by requiring the TOE to prevent unauthorized deletion of the audit records.
	FAU_STG.4	This requirement supports O.AUDIT by requiring the TOE to mitigate audit data loss due to hardware limitations such as disk full.

Objective	Requirements Addressing the Objective	Rationale
O.AUTHENTICATE The TOE must require the Administrator to authenticate before gaining access to the administrative interfaces of the TOE, and End Users to authenticate if their controlled protocol traffic matches a Proxy SFP rule which requires authentication.	FIA_ADM_PCR.1(a)	This requirement supports O. AUTHENTICATE by requiring a TOE administrator to enter the proper password before assuming the Privileged Administrator role.
	FIA_ADM_PCR.1(b)	This requirement supports O. AUTHENTICATE by requiring a Serial Console user to enter the "setup" password before assuming the Setup Console Administrator role (which allows bypassing the TSF).
	FIA_AFL.1	This requirement supports O. AUTHENTICATE by ensuring that users' passwords are protected from brute-force guessing.
	FIA_UAU.1	This requirement supports O. AUTHENTICATE by ensuring that the only action permitted on behalf of an unauthenticated Serial Console user is the selection of the Setup Console or the CLI on the Serial Console.
	FIA_UAU.2	This requirement supports O. AUTHENTICATE by ensuring that no action is permitted on behalf of an unauthenticated Management Console user.
	FIA_UAU.5	This requirement supports O. AUTHENTICATE by defining the authentication mechanisms for End Users, Management Console users, CLI userid, Serial Console users, and Setup Console users.
	FIA_UAU.6(a)	This requirement supports O. AUTHENTICATE by ensuring the End Users are authenticated before any other TSF-mediated actions taken on their behalf are performed. Only actions that match Proxy SFP rules not requiring identification are allowed before authentication is performed.

Objective	Requirements Addressing the Objective	Rationale
	FIA_UAU.6(b)	This requirement supports O. AUTHENTICATE by ensuring that the only action permitted on behalf of an unauthenticated Serial Console user is the selection of the Setup Console or the CLI on the Serial Console.
	FIA_UAU.7(a)	This requirement supports O. AUTHENTICATE by requiring that characters are not echoed when administrators type their password on the CLI.
	FIA_UAU.7(b)	This requirement supports O. AUTHENTICATE by requiring that characters are not echoed when administrators type their password on the Management Console.
	FIA_UID.1(a)	This requirement supports O. AUTHENTICATE by ensuring the End Users are identified before any other TSF-mediated actions taken on their behalf are performed. Only actions that match Proxy SFP rules not requiring identification are allowed before identification is performed.
	FIA_UID.1(b)	This requirement supports O. AUTHENTICATE by ensuring that the only action permitted on behalf of an unidentified Serial Console user is the selection of the Setup Console or the CLI on the Serial Console.
	FIA_UID.2	This requirement supports O. AUTHENTICATE by ensuring administrators are identified before any other TSF-mediated actions taken on their behalf are performed.
	FTA_MCS.2	This requirement supports O. AUTHENTICATE by ensuring End Users may only be logged in to an administrator-defined number of sessions, ensuring that unauthenticated users do not gain access to the TOE through an unattended active session.

Objective	Requirements Addressing the Objective	Rationale
	FTA_SSL.3	This requirement supports O. AUTHENTICATE by ensuring End Users are logged off after a period of inactivity, ensuring that unauthenticated users do not gain access to the TOE through an unattended session.
O.MANAGE The TOE must provide secure management of the system configuration, the Administrative Access SFP, the WAN Optimization SFP, and the Proxy SFP.	FDP_ACC.1	This requirement supports O.MANAGE by including a policy language that enables administrators to construct rules that control the access of administrators to the administrative interfaces of the TOE. The function then enforces those rules and takes the action specified.
	FDP_ACF.1	This requirement supports O.MANAGE by supporting several attributes that can be used in the Administrative Access SFP to control access to the administrative interfaces.
	FIA_ADM_PCR.1(a)	This requirement supports O. MANAGE by requiring a TOE administrator to enter the proper password before assuming the Privileged Administrator role for accessing administrative functions.
	FIA_ADM_PCR.1(b)	This requirement supports O. MANAGE by requiring a TOE administrator user to enter the “setup” password before assuming the Setup Console Administrator role (which allows bypassing the TSF) for accessing system configuration functions on the Serial Console.
	FMT_MOF.1	This requirement supports O. MANAGE by specifying which functions of the TOE can be managed, and defining who can manage those functions.
	FMT_MSA.1(a)	This requirement supports O.MANAGE by allowing all TOE administrators to query the security attribute user group membership.

Objective	Requirements Addressing the Objective	Rationale
	FMT_MSA.1(b)	This requirement supports O.MANAGE by allowing only Privileged Administrators to modify and delete the security attributes user group membership and user password.
	FMT_MSA.2	This requirement supports O.MANAGE by ensuring that only secure values are accepted for security attributes.
	FMT_MSA.3(a)	This requirement supports O.MANAGE. The Administrative Access SFP is restrictive by default.
	FMT_MSA.3(b)	This requirement supports O.MANAGE. The Proxy SFP is restrictive by default.
	FMT_MSA.3(c)	This requirement supports O.MANAGE. The WAN Optimization SFP is restrictive by default.
	FMT_MTD.1(a)	This requirement supports O.MANAGE by permitting all TOE administrators to view the system configuration, Administrative Access SFP rules, WAN Optimization SFP rules, and Proxy SFP rules.
	FMT_MTD.1(b)	This requirement supports O.MANAGE by permitting only Privileged Administrators to modify the system configuration, Administrative Access SFP rules, WAN Optimization SFP rules, and Proxy SFP rules.
	FMT_MTD.2	This requirement supports O.MANAGE by permitting Privileged Administrators to modify the limit on the size of the audit logs.
	FMT_SMF.1	This requirement supports O.MANAGE by specifying that the TOE supports configuration of the Proxy SFP.
	FMT_SMR.1	This requirement supports O.MANAGE by supporting three roles: Administrator, Privileged Administrator, and Setup Console Administrator.

Objective	Requirements Addressing the Objective	Rationale
	FMT_SMR.3	This requirement supports O.MANAGE by ensuring that Serial Console users can assume the Privileged Administrator and Setup Console Administrator roles on the Serial Console only by executing the required command, and providing the appropriate password.
O.REMOVE_ACTIVE The TOE must be able to remove active content from HTML pages delivered via a controlled protocol as defined by the Proxy SFP.	FDP_IFC.1(a)	This requirement supports O.REMOVE_ACTIVE by including a policy language that enables the administrator to construct rules representing their site's information flow policy. The function then enforces those rules and takes the action specified.
	FDP_IFF.1(a)	This requirement supports O.REMOVE_ACTIVE by supporting a wide range of attributes that can be used in the Proxy SFP to control the flow of information between the Internal and External Networks.
O.SCREEN_TYPE The TOE must disallow controlled protocol traffic of given content types as defined by the Proxy SFP.	FDP_IFC.1(a)	This requirement supports O.SCREEN_TYPE by including a policy language that enables the administrator to construct rules representing their site's information flow policy. The function then enforces those rules and takes the action specified.
	FDP_IFF.1(a)	This requirement supports O.SCREEN_TYPE by supporting a wide range of attributes that can be used in the Proxy SFP to control the flow of information between the Internal and External Networks.
O.SCREEN_URL The TOE must disallow controlled protocol traffic for given URLs as defined by the Proxy SFP.	FDP_IFC.1(a)	This requirement supports O.SCREEN_URL by providing a policy language that enables authorized administrators to construct rules representing their site's information flow policy. The function then enforces those rules and takes the action specified.

Objective	Requirements Addressing the Objective	Rationale
	FDP_IFF.1(a)	This requirement supports O.SCREEN_URL by supporting a wide range of attributes that can be used in the Proxy SFP to control the flow of information between the Internal and External Networks.
O.VALIDATED_CRYPTO The TOE shall provide cryptographic functions for its own use. These functions will be provided by a FIPS 140-2 validated cryptographic module.	FCS_CKM.1	This requirement supports O.VALIDATED_CRYPTO by providing cryptographic key generation, which can be used to ensure cryptographic functionality on the TOE.
	FCS_CKM.4	This requirement supports O.VALIDATED_CRYPTO by providing a method for destroying cryptographic keys, thereby ensuring that the keys are not accessed by an unauthorized person or IT entity.
	FCS_COP.1(a)	This requirement supports O.VALIDATED_CRYPTO by providing algorithms for cryptographic operation, which can be used to encrypt and decrypt data passing through or being stored on the TOE.
	FCS_COP.1(b)	This requirement supports O.VALIDATED_CRYPTO by providing algorithms for cryptographic operation, which can be used to encrypt and decrypt data passing between the TOE and the Serial Console or remote Management Console.
O.PROTECT The TOE must have the capability to protect management traffic from unauthorized reading or modification.	FCS_CKM.1	This requirement supports O.PROTECT by providing cryptographic key generation, which can be used to ensure cryptographic functionality on the TOE.
	FCS_CKM.4	This requirement supports O.PROTECT by providing a method for destroying cryptographic keys, thereby ensuring that the keys are not accessed by an unauthorized person or IT entity.

Objective	Requirements Addressing the Objective	Rationale
	FCS_COP.1(b)	This requirement supports O.PROTECT by providing algorithms for cryptographic operation, which can be used to encrypt and decrypt data passing between the TOE and the Serial Console or remote Management Console.
	FTA_MCS.2	This requirement supports O.PROTECT by ensuring that unauthorized users do not gain access to the TOE through an unattended active session.
	FTA_SSL.3	This requirement supports O.PROTECT by ensuring that unauthorized users do not gain access to the TOE through an unattended session.
O.TIMESTAMP The TOE must provide a timestamp for use by the TOE.	FPT_STM.1	This requirement supports O.TIMESTAMP by ensuring that the TOE provides a timestamp for the TOE's use.
O.QUOTA The TOE must be able to place quotas on network connection resources.	FRU_RSA.1	This requirement supports O.QUOTA by ensuring that the TOE is capable of placing maximum quotas on the number of connections available during a specified time period.
	FRU_RSA.2	This requirement supports O.QUOTA by ensuring that the TOE places minimum and maximum quotas on the bandwidth available for use by different types of traffic.
O.ALERT The TOE must alert the administrator of changes in TOE health.	EXT_FRU_ARP.1	This requirement supports O.ALERT by ensuring that the TOE sends notifications by email, SNMP traps, or event logging whenever a change in the status of the health of the TOE occurs.
O.PASS_TRAFFIC The TOE must pass traffic from the internal network to the external network as defined by the WAN Optimization SFP.	FDP_IFC.1(b)	This requirement supports O.PASS_TRAFFIC by ensuring that the TOE conforms to the WAN Optimization SFP when passing traffic from the internal network to the external network.

Objective	Requirements Addressing the Objective	Rationale
	FDP_IFF.1(b)	This requirement supports O.PASS_TRAFFIC by ensuring that the TOE conforms to the WAN Optimization SFP when passing traffic from the internal network to the external network.

8.5.2 Security Assurance Requirements Rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.1 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 24 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 24 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1(a)	FAU_GEN.1	✓	
FAU_SAR.1(b)	FAU_GEN.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.4	FAU_STG.1	✓	
FCS_CKM.1	FCS_COP.1(a)	✓	
	FCS_COP.1(b)	✓	
	FCS_CKM.4	✓	
FCS_CKM.4	FCS_CKM.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FCS_COP.1(a)	FCS_CKM.1	✓	
	FCS_CKM.4	✓	
FCS_COP.1(b)	FCS_CKM.1	✓	
	FCS_CKM.4	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_IFC.1(a)	FDP_IFF.1(a)	✓	
FDP_IFF.1(a)	FDP_IFC.1(a)	✓	
	FMT_MSA.3	✓	
FDP_IFC.1(b)	FDP_IFF.1(b)	✓	
FDP_IFF.1(b)	FDP_IFC.1(b)	✓ ✓	
	FMT_MSA.3		
FIA_ADM_PCR.1(a)	No dependencies	✓	
FIA_ADM_PCR.1(b)	No dependencies	✓	
FIA_AFL.1	FIA_UAU.1(a)	✓	
FIA_UAU.1	FIA_UID.1(b)	✓	
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FIA_UAU.5	No dependencies	✓	
FIA_UAU.6(a)	No dependencies	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FIA_UAU.6(b)	No dependencies	✓	
FIA_UAU.7(a)	FIA_UAU.1	✓	
FIA_UAU.7(b)	FIA_UAU.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FIA_UID.1(a)	No dependencies	✓	
FIA_UID.1(b)	No dependencies	✓	
FIA_UID.2	No dependencies	✓	
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(a)	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(b)	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.2	FDP_ACC.1 or FDP_IFC.1	✓	
	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(a)	FMT_MSA.1(a)	✓	
	FMT_MSA.1(b)	✓	
	FMT_SMR.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FMT_MSA.3(b)	FMT_MSA.1(a)	✓	
	FMT_MSA.1(b)	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(c)	FMT_MSA.1(a)	✓	
	FMT_MSA.1(b)	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(a)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1(b)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.2	FMT_MTD.1(b)	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	
FMT_SMR.3	FMT_SMR.1	✓	
FPT_STM.1	No dependencies	✓	
EXT_FRU_ARP.1	No dependencies	✓	
FRU_RSA.1	No dependencies	✓	
FRU_RSA.2	No dependencies	✓	
FTA_MCS.2	FIA_UID.1(a)	✓	
FTA_SSL.3	No dependencies	✓	

9 Acronyms

Table 25 - Acronyms

Acronym	Definition
3DES	Triple Data Encryption Standard
ADN	Application Delivery Network
AES	Advanced Encryption Standard
CA	Certificate Authority
CBC	Cipher Block Chaining
CC	Common Criteria
CFB	Cipher Feedback
CIFS	Common Internet File System
CLI	Command Line Interface
CM	Configuration Management
CPL	Content Policy Language
CRL	Certificate Revocation List
DNS	Domain Name System
DSA	Digital Signature Algorithm
DOS	Disk Operating System
DRTR	Dynamic Real-Time Rating
EAL	Evaluation Assurance Level
ECB	Electronic Codebook
ELFF	Extended Log File Format

Acronym	Definition
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IMAP	Internet Message Access Protocol
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
IWA	Integrated Windows Authentication
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAPI	Message Application Programming Interface
MIME	Multipurpose Internet Mail Extensions
MMS	Microsoft Media Streaming
NCSA	National Center for Supercomputing Applications
NTP	Network Time Protocol
OCS	Original Content Server
OFB	Output Feedback

Acronym	Definition
OLE	Object Linking and Embedding
OSP	Organizational Security Policy
PKI	Public Key Infrastructure
POP3	Post Office Protocol version 3
RADIUS	Remote Authentication Dial-In User Service
RFC	Request For Comments
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adelman
RTSP	Real-time Streaming Protocol
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SGOS	SG Operating System
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TBD	To Be Determined
TSF	TOE Security Function
TSP	TOE Security Policy

Acronym	Definition
URL	Uniform Resource Locator
VPM	Visual Policy Manager
W3C	World Wide Web Consortium