Blue Coat Systems, Inc.

ProxySG SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1

Security Target

Evaluation Assurance Level: EAL4+
Document Version: 1.3

Prepared for:

Blue Coat Systems, Inc.
420 N. Mary Avenue
Sunnyvale, CA 94085

Phone: +1 (408) 220-2200
Email: usinfo@bluecoat.com
http://www.bluecoat.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033

Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2009-08-11	Christopher Lockard	Initial draft.
0.2	2009-12-06	Bill Shanahan	Updates based on Blue Coat feedback and further internal review.
0.3	2010-03-02	Bill Shanahan	Changed platform information to include 4 platforms.
0.4	2010-06-02	Bill Shanahan Amy Nicewick	Updated document based on feedback from Blue Coat.
0.5	2010-08-26	Matthew Williams	Updated document based on feedback from Blue Coat and OR#1.
0.6	2010-09-28	Matthew Williams	Updated Table 19 and SFRs to reflect SkyUI functionality.
0.7	2011-06-03	Matthew Williams	Removed SkyUI functionality, added CAC authentication, clarified SSH timeout claims, added SG510.
0.8	2011-07-29	Shashi Karanam	Updated TOE Title, TOE reference, accelerator cards, and cryptographic algorithms information. Updated Corsec's address.
0.9	2011-08-04	Shashi Karanam	Updated TOE Title, TOE reference, and physical scope section.
1.0	2011-09-27	Shashi Karanam	Updated the ProxySG build number.
1.1	2011-12-14	Jerrod Schultz	Updated document references
1.2	2012-01-27	Greg Milliken	Updated document references.
1.3	2012-02-15	Ian Hall	Updated Document references. Aligned Table 18 to match with the guidance documents in section 1.4.1.2.

Table of Contents

Table of Figures

Table of Tables

1 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 SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1, 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 Wide Area Network (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 contains the following sections to provide mapping of the Security Environment to the Security Requirements that the TOE meets in order to remove, diminish or mitigate the defined threats:

- 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, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security 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 (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) 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.
- TOE 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 SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target and TOE References

Table 1 - ST and TOE References

ST Title	Blue Coat Systems, Inc. ProxySG SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1 Security Target
ST Version	Version 1.3
ST Author	Corsec Security, Inc. Matt Williams
ST Publication Date	2012-02-15
TOE Reference	Blue Coat ProxySG SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1.5.4, build 77833.
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 ProxySG SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1 appliances (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, SG600, SG810, SG900 and SG9000 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 capacity, performance, and scalability options, as depicted below in Table 2.

Table 2 – Platform Comparison

	SG510	SG600	SG810	SG900	SG9000
Concurrent Users	200-Unlimited	450-Unlimited	2500-Unlimited	3500-Unlimited	Unlimited
Storage	2x80GB – 2x320 GB SATA	1x250GB[1] – 2x250GB SATA[2]	2x73GB – 4x300GB SCSI[3] Ultra 320	2x500 GB – 4x1TB SAS	8x500GB – 10x500GB SAS[4]

[1] GB – Gigabyte

Memory	2GB	4GB	2-6GB	6-16GB	8-16GB
Throughput	• 2x10/100/1000 Base-T card (dual GigE) • 2x10/100/1000 Base SX card (dual GigE Fibre) • 4x10/100/1000 Base T (quad GigE with passthru)	• 2x1000 Base-T card • 1x1000 Base-T card	• 2x10/100/1000 Base-T card (dual GigE) • 2x10/100/1000 Base SX card (dual GigE Fibre) • 4x10/100/1000 Base T (quad GigE with passthru)	2x 1000 Base-T (bridged pair)	4x1000 Base-T (1x management, 1x auxilliary, 1 bridged pair)
Enclosure	1U x 19"	1U[5] x 19"	1U x 19"	1U x 19"	4U x 19"

Figure 1 shows the details of the deployment configuration of the TOE:

[2] SATA – Serial Advanced Technology Attachment
[3] SCSI – Small Computer System Interface
[4] SAS – Serial Attached SCSI
[5] U – Unit

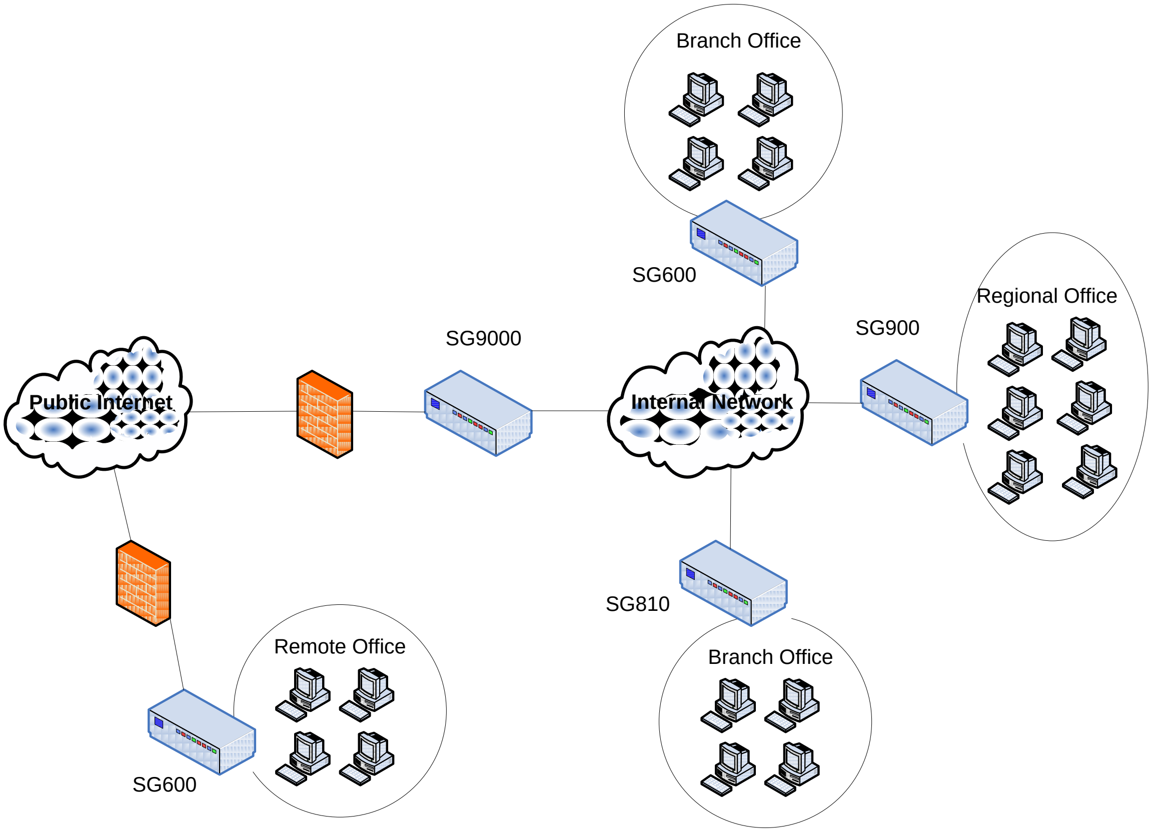


Figure 1 - Deployment Configuration of the TOE

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: Application Delivery Network (ADN) and Proxy. The ADN edition appliances offer a subset of the Proxy's services and 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 ADN edition)
- Instant Messaging (AOL[6], MSN[7]/Windows LIVE Messenger, and Yahoo!) (not included with ADN edition)
- Common Internet File System (CIFS)
- Real-Time Streaming Protocol (RTSP)
- Microsoft Media Streaming (MMS)
- Messaging Application Programming Interface (MAPI)

[6] AOL – America Online

[7] MSN – The Microsoft Network

- Transmission Control Protocol (TCP) tunnelling protocols (e.g., Secure Shell (SSH), IMAP[8], POP3[9], SMTP[10])
- Telnet
- Domain Name System (DNS)

Control is achieved by enforcing a configurable policy (Proxy SFP[11]) 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 TOE Concepts

The following paragraphs depict a brief description of the TOE components and functionality.

1.3.1.1 Administrative Access

Administrative access to the TOE is provided by the ProxySG's serial port and Ethernet port. Administrators 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. Administrators can also access the CLI using SSH over an Ethernet connection. Administrators access the Java Management Console (JMC) using HTTPS over an Ethernet connection 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 (ADN 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 (ADN or Proxy)

[8] IMAP – Internet Message Access Protocol
[9] POP3 – Post Office Protocol version 3
[10] SMTP – Simple Mail Transfer Protocol
[11] SFP – Security Functional Policy

- 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 ADN Settings (optional), traffic types to be intercepted, and initial policy

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

- Front Panel configuration method (not permitted in the evaluated configuration)
- Automatic registration with the Director management application (not permitted in the evaluated configuration)
- 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[12] using the configured administrative credentials
- log on to the JMC through HTTP[13] or HTTPS

After first-time configuration is completed, the administrator must log in to the TOE via the ProxySG CLI or JMC 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 authorised administrator defines information flow policy rules, which comprise the Proxy SFP.

These rules can require authentication of End Users. An authorised 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 Appliance Content Policy Language Reference, Version SGOS 6.1.x*.

[12] Telnet access to the CLI is disabled by default and not included in the evaluated configuration

[13] HTTP access to the JMC is disabled by default and not included in the evaluated configuration

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 LAN.

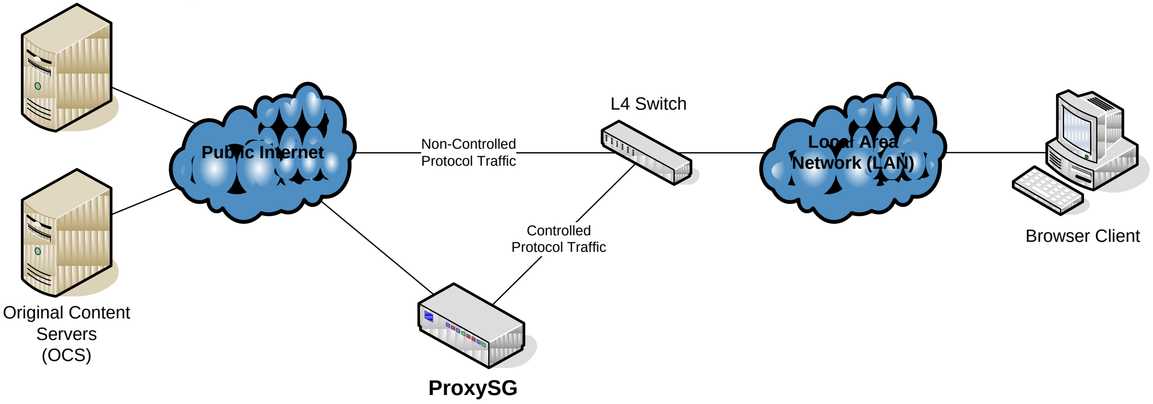


Figure 2 – Transparent Forward (Gateway) Proxy Deployment

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.

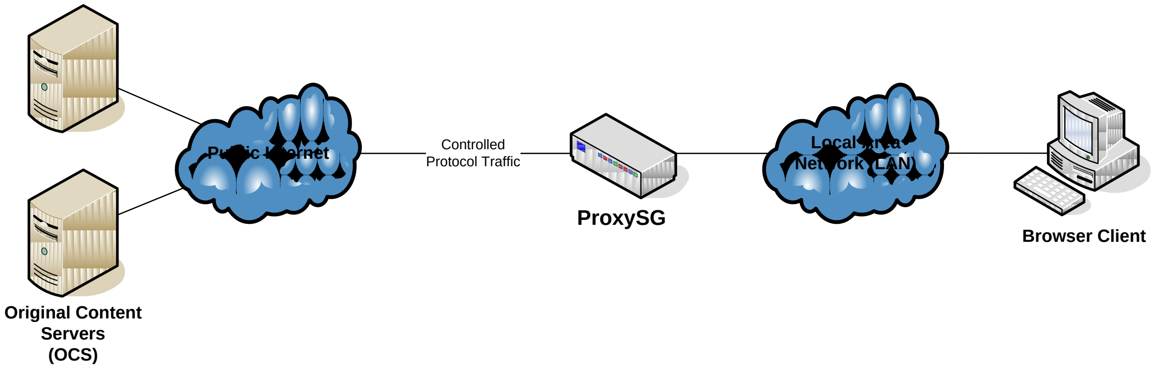


Figure 3 – Explicit Forward (Gateway) Proxy Deployment

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 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.

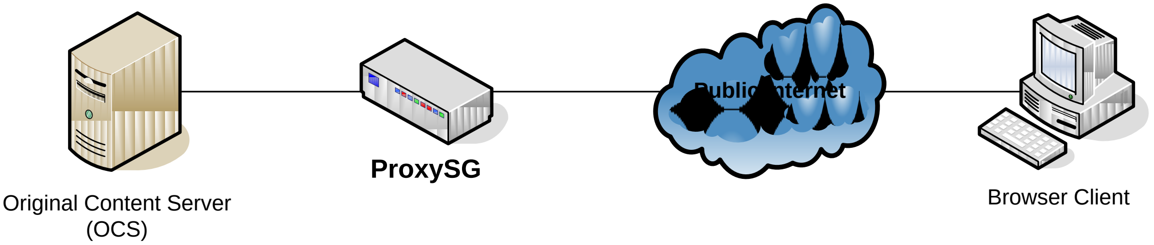


Figure 4 – Reverse (Server) Proxy Deployment

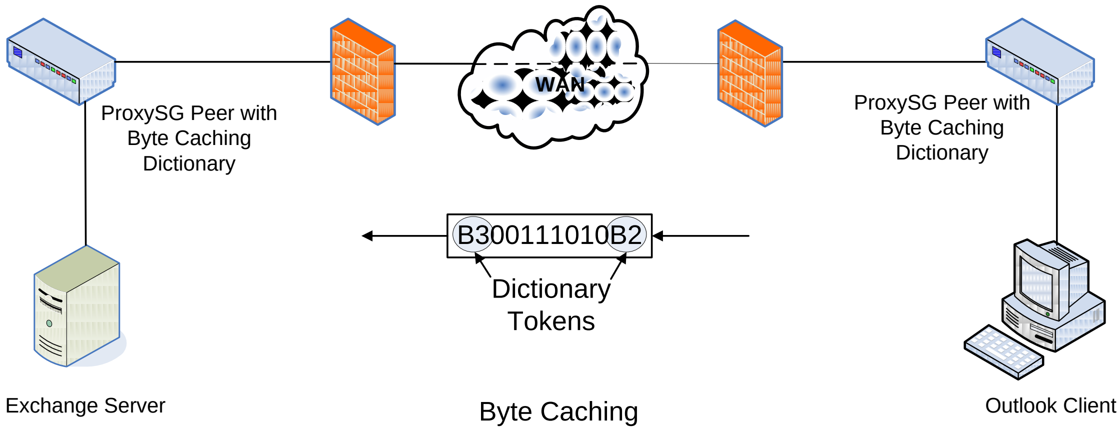
In the Reverse Proxy deployment, a ProxySG is associated with an OCS web server (as depicted in Figure 4 above). The ProxySG can cache and deliver pictures and other non-variable content rapidly, offloading those efforts from the OCS. This frees the OCS to perform application-based services (such as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

1.3.1.6 WAN Optimization

The ProxySG's ADN implements byte caching[14] 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[15] to provide acceleration for the WAN. Figure 5 (below) shows a typical WAN Optimization deployment for email exchange across a WAN.

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

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


ProxySG Peer with Byte Caching Dictionary
WAN
ProxySG Peer with Byte Caching Dictionary
B300111010B2
Dictionary Tokens
Exchange Server
Outlook Client

Byte Caching Dictionary

B0 = 00110110
B1 = 10111011
B2 = 01010100
B3 = 11010010

Figure 5 - WAN Optimization Deployment

The components required for an ADN implementation include ADN nodes in branch offices and data centres that can be authenticated and authorised, and an optional ADN manager to provide routing information and control access to the ADN network. 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 centre 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 centre 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.

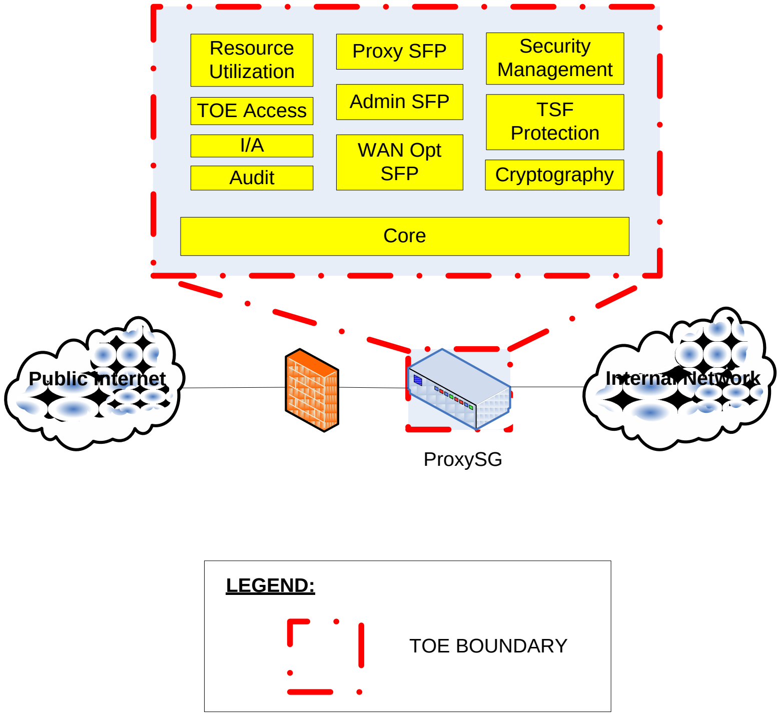


Figure 6 – TOE Boundary

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 and Hardware

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:

- ProxySG 510/810-5
- ProxySG 510/810-10, 510/810-20, 510/810-25 with a Cavium CN1010 PCI-Extended (PCI-X) card, or a BCM5825 PCI-Extended (PCI-X) card
- ProxySG 600-10, 600-20, 600-35 with a Cavium CN501 Security Macro Processor
- ProxySG 900-10, 900-20, 900-30, 900-45 with a Cavium CN1610 Security Macro Processor
- ProxySG 9000-10, 9000-20 with a Cavium CN1620 PCI-Express (PCI-e) card

For all the above appliance models, the appliance type can be either Mach5 edition (For example, ProxySG 510-5-M5) for WAN optimization, or Proxy edition (For example, ProxySG 510-5-PR) for Proxy and WAN optimization features. No additional hardware or environmental components are required for the TOE to function in the evaluated configuration.

1.4.1.2 Guidance Documentation

The following guides are required reading and part of the TOE:

- Blue Coat Systems SGOS Administration Guide, Version SGOS 6.1.x, 231-03113, SGOS 6.1.1-08/2011
- Blue Coat SGOS 6.1.x Release Notes, SGOS 6.1.5.2, 12/20/2011
- Blue Coat Systems ProxySG Appliance Command Line Interface Reference, version SGOS 6.1.x, 231-03035, SGOS 6.1.3-07/2011
- Blue Coat Systems ProxySG Appliance Content Policy Language Reference, version SGOS 6.1.x, 231-03019, SGOS 6.1.1-07/2011
- Blue Coat Systems ProxySG Appliance SGOS 6.1.x Upgrade/Downgrade Feature Change Reference, Version SGOS 6.x, 231-03034, SGOS 6.1.1.-09/2010
- Blue Coat Systems ProxySG Appliance Visual Policy Manager Reference, SGOS Version 6.x, 231-03015, SGOS 6.1.1-09/2010
- ProxySG Quick Start Guide SG600 Series, 231-03048, Rev A.0
- ProxySG Quick Start Guide: SG900 Series, 231-03109, Rev B.0
- ProxySG Quick Start Guide ProxySG 210 ProxySG 510 ProxySG 810 ProxySG 9000 Series, 231-03122, Rev B.3
- Blue Coat 510/810 Series FIPS Compliant Tamper Evident Faceplate and Label Installation Guide, 231-02995, A-0
- Blue Coat ProxySG 600 Series FIPS Compliance Guide: Tamper Evident Panel and Label Installation, 231-03160, A.0
- Blue Coat ProxySG 900 Series FIPS Compliance Guide: Tamper Evident Panel and Label Installation, 231-03161, B.0

- Blue Coat ProxySG 9000 Series FIPS Compliant Tamper Evident Shutter and Label Installation Guide, 231-03063, A.1
- Blue Coat Using FIPS Mode on the ProxySG, 231-03154, March 2011
- Blue Coat Systems ProxySG Appliance SGOS 6.x Upgrade/Downgrade Guide, SGOS Version 6.x, N/A[18], Version 6.1.1-(09/2010)
- Blue Coat Systems, Inc. ProxySG SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1 Guidance Supplement v0.5

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 Administrators and 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[19] are provided for convenience, and custom log formats can be defined using W3C[20]. 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 access 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.

[18] N/A – Not Applicable

[19] NCSA – National Center for Supercomputing Applications

[20] W3C – World Wide Web Consortium

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 SSH CLI or JMC. TLS[21] 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 can be encrypted using a public key from an external certificate, which is associated with a private key, and digitally signed using an external SSL certificate guaranteed by a Certificate Authority (CA). The TOE uses SSL, CA, and external certificates that conform to the x.509 v3 standard. These certificates are used to guarantee the integrity and authenticity of signed audit logs as well as to authenticate and secure communications between itself and OCSs, other ProxySGs, and between end users. Cryptographic operations are performed by a FIPS 140-2-validated cryptographic module, certificate #XXX.

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 authorised 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 Appliance Content Policy Language Reference, Version SGOS 6.1.x.*

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[22] 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,

[21] TLS – Transport Layer Security

[22] URL – Uniform Resource Locator

restrict traffic for specified URLs to authorised 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 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 byte 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 authorised 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.

If FIPS-compliant Common Access Card (CAC) or Personal Identity Verification (PIV) card authentication is required, only the LDAP and Certificate realms will be permitted in realm sequencing. For details on this and other CAC authentication requirements, see the Blue Coat Systems Common Access Card (CAC) Solutions Guide, SGOS 6.1.2.

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[23] 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.

[23] IT – Information Technology

The time can be synchronized to Coordinated Universal Time manually through the configuration settings. Administrators are assumed 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 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 reset. If the time since the last activity time exceeds the inactivity-timeout value, the End User is logged out.

1.4.3 Product Physical/Logical Features and Functionality not included in the TSF

Features and functionalities that are not part of the evaluated configuration of the TSF are:

- ProxyClient
- Remote management over Telnet
- Front panel configuration
- Remote management over HTTP
- XML authentication realm
- Session Monitor
- Unauthenticated access to the VPM
- 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 (PP), 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 3 - CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 extended; CC Part 3 conformant; Parts 2 and 3 Interpretations from the Interpreted CEM[24] as of 2010/02/01 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL4+ augmented with ALC_FLR.2

[24] CEM – Common Criteria Evaluation Methodology

3 Security Problem

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 three categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a basic 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 wilfully hostile to the TOE.)
- Agents or processes working either on behalf of attackers or autonomously: They may or may not have knowledge of the public or proprietary TOE configuration settings/parameters and typically take the form of bots or botnets designed to exploit common vulnerabilities or deny others access to IT products and services.

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 4 – 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.HEALTH	TOE users may perform actions that compromise the health of the TOE.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorised access to data or TOE resources.
T.NACCESS	An unauthorised person or external IT entity may be able to view or

	modify data that is transmitted between the TOE and a remote authorised external entity.
T.UNAUTHORISED_ACCESS	A user may gain access to security data on the TOE for which they are not authorised according to the TOE security policy through the improper use of valid credentials.
T.RESOURCE	TOE users or attackers may cause network connection resources to become overused and therefore unavailable.

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 5 - 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 pages delivered via controlled protocols.
P.ADMIN	Only authorised 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 unauthorised content types via controlled protocols on the External Network.
P.FILTERED_URLS	End Users shall not access unauthorised 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.PASS_TRAFFIC	The TOE shall enforce the WAN Optimization SFP on traffic passing from the internal network to the external network.
P.POST_TYPE	End Users shall not post unauthorised content types to the External Network using controlled protocols.

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.

Table 6 – 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 authorised persons.
A.INSTALL	The TOE 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.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 7 - Security Objectives for the TOE

Name	Description
O.ALERT	The TOE must alert the administrator of changes in TOE health.
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.
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.PASS_TRAFFIC	The TOE must pass traffic from the internal network to the external network as defined by the WAN Optimization SFP.
O.PROTECT	The TOE must have the capability to protect management traffic from unauthorised reading or modification.
O.QUOTA	The TOE must be able to place quotas on network connection resources.
O.REMOVE_ACTIVE	The TOE must be able to remove active content from HTML pages delivered via a controlled protocol as defined by the Proxy SFP.
O.SCREEN_TYPE	The TOE must disallow controlled protocol traffic of given content types as defined by the Proxy SFP.
O.SCREEN_URL	The TOE must disallow controlled protocol traffic for given URLs as defined by the Proxy SFP.
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.

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 8 - IT Security Objectives

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

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 and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 9 - Non-IT Security Objectives

Name	Description
NOE.ADMIN	The administrator must be non-malicious and competent, and must follow all guidance.
NOE.ENVIRON	The physical environment must be suitable for supporting a computing device in a secure setting.

5 Extended Components

This section defines the extended SFRs and extended 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 10 identifies all extended SFRs implemented by the TOE.

Table 10 - Extended TOE Security Functional Requirements

Name	Description
FIA_ PCR_EXT.1	Password controlled role
FRU_ARP_EXT.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_ PCR_EXT.1: Password controlled role was modelled after the CC family FIA_UAU: User authentication. The extended component FIA_ PCR_EXT.1: Password controlled role was modelled after the CC component FIA_UAU.6: Re-authenticating.

5.1.1.1 Password Controlled Role (FIA_PCR_EXT)

Family Behaviour

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

Component Levelling

Figure 7 – FIA_PCR_EXT Password Controlled Role family decomposition

FIA_ PCR_EXT.1 Password controlled role provides the capability to authenticate an authorised user to another role.

Management: FIA_ PCR_EXT.1

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

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

Audit: FIA_ PCR_EXT.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_PCR_EXT.1 Password Controlled Role
Hierarchical to: No other components
Dependencies: No dependencies
This component will provide authorised administrators the capability to authenticate as a new role.

FIA_ PCR_EXT.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 authentication actions taken*].

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 FRU_ARP_EXT: Health check alarms was modelled after the CC family FAU_ARP: Security audit automatic response. The extended component FRU_ARP_EXT.1: Health check alarms was modelled after the CC component FAU_ARP.1: Security alarms.

5.1.2.1 Health Check Alarms (FRU_ARP_EXT)

Family Behaviour

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

Component Levelling

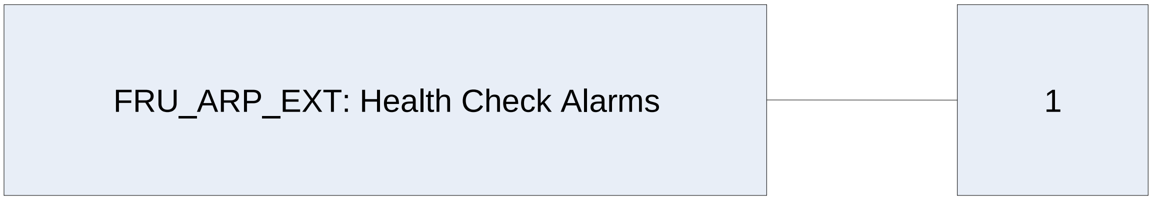


Figure 8 – FRU_ARP_EXT Health check alarms family decomposition

FRU_ARP_EXT.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: FRU_ARP_EXT.1

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

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

Audit: FRU_ARP_EXT.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.

FRU_ARP_EXT.1 Health check alarms

Hierarchical to: No other components

Dependencies: No dependencies

FRU_ARP_EXT.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.
- Extended Functional and Assurance Requirements are identified using "_EXT" at the end of the family name.
- 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 11 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 11 - TOE Security Functional Requirements

Name	Description	S	A	R	I
EXT_FRU_ARP.1	Health check alarms		✓		
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		✓		
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_IFC.1(b)	Subset information flow control		✓		✓
FDP_IFF.1(a)	Simple security attributes		✓		✓
FDP_IFF.1(b)	Simple security attributes		✓		✓
FIA_AFL.1	Authentication failure handlings	✓	✓	✓	
FIA_PCR_EXT.1(a)	Password controlled role		✓		✓
FIA_PCR_EXT.1(b)	Password controlled role		✓		✓
FIA_UAU.1	Timing of authentication		✓	✓	
FIA_UAU.2	User authentication before any action			✓	
FIA_UAU.5	Multiple authentication mechanism		✓	✓	
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			✓	
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				
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		✓	✓	

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

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

Application Note: Although the TOE does perform auditing at the basic level for JMC password-based authentication attempts, certificate-based authentication attempts are not logged in this version of the TOE.

- [*Communication errors with external IT devices; and*
- *All actions resulting from the Proxy SFP*].

Table 12 - Basic-Level Auditable Events

Component	Level	Auditable Event
FAU_SAR.1	Basic	Reading of information from the audit records
FAU_STG.1	Basic	All deletion attempts on 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_ACC.1	Basic	All requests to establish a Privileged Administrative role over the selected TOE interface.
FDP_ACF.1	Basic	All requests to perform an operation on an object covered by the Administrative Access SFP
FDP_IFC.1(a)	Basic	All attempts by external IT entities to send controlled protocol traffic through the TOE.
FDP_IFC.1(b)	Basic	All hosts sending controlled data traffic to one another through the TOE
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_PCR_EXT.1(a)	Basic	All authentication requests to the new role
FIA_PCR_EXT.1(b)	Basic	All authentication requests to the new role at the serial console

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(a)	Basic	All re-authentication attempts as an End-User
FIA_UAU.6(b)	Basic	All re-authentication attempts as an Administrator
FIA_UAU.7(a)	Basic	All authentication attempts in progress over the CLI management interfaces
FIA_UAU.7(b)	Basic	All authentication attempts in progress over the JMC.
FIA_UID.1(a)	Basic	All use of the user identification mechanisms, including the user identity provided
FIA_UID.1(b)	Basic	All use of the user identification mechanisms on behalf of the Serial Console
FIA_UID.2	Basic	All use of the user identification mechanisms, including the user identity provided
FMT_MOF.1	Basic	All modifications in the behaviour of the functions in the TSF
FMT_MSA.1(a)	Basic	All modifications to the security attributes
FMT_MSA.1(b)	Basic	All modifications to the security attributes
FMT_MSA.2	Minimal	All offered and rejected values for a security attribute
FMT_MSA.3(a)	Basic	Modifications of the default setting of permissive or restrictive rules All modifications of the initial values of security attributes
FMT_MSA.3(b)	Basic	Modifications of the default setting of permissive or restrictive rules All modifications of the initial values of security attributes
FMT_MSA.3(c)	Basic	Modifications of the default setting of permissive or restrictive rules All modifications of the initial values of security attributes
FMT_MTD.1(a)	Basic	All modifications to the values of TSF data
FMT_MTD.1(b)	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

Component	Level	Auditable Event
FRU_ARP_EXT.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
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 [*Administrators, 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 13 - Cryptographic Key Generation Standards

Key Generation Type	Algorithm and Key Size	Standards (Certificate #)
Random Number Generator (RNG)	N/A	NIST SP[25] 800-90 (FIPS certificate #153)
Rivest, Shamir, and Adelman (RSA)	1024, 1536, 2048	ANSI X9.31 (FIPS 186-2) (FIPS certificate #956)

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* –

[25] SP – Special Publication

see table below] and cryptographic key sizes [*cryptographic key sizes* – **see table below**] that meet the following: [*list of standards* – **see table below**].

Table 14 - Cryptographic Operation

Algorithm	Standard	Software Implementation Certificate Number	Hardware Accelerator Card		
			Appliance	Card	Certificate Number
Symmetric Key Algorithms					
AES: ECB[26], CBC[27], OFB[28], CFB[29]-128 bit mode for 128-, 192-, and 256-bit key sizes	FIPS 197	1875	510	CN1010	105
				BCM5825	397
			600	CN501	105
			810	CN1010	105
				BCM5825	397
			900	CN1610	1265
			9000	CN1620	1265
Triple-DES[30]: ECB, CBC, CFB-64, OFB mode for keying option 1 (3 different keys)	FIPS 46-3	1218	510	CN1010	217
				BCM5825	435
			600	CN501	217
			810	CN1010	217
				BCM5825	435
			900	CN1610	895
			9000	CN1620	895
Asymmetric Key Algorithms					
RSA PKCS[31]#1 sign/verify – 1024-, 1536-, 2048-bit	ANSI X9.31 (FIPS 186-2)	956	N/A		
Hashing Functions					
SHA[32]-1	FIPS 180-2	1648	N/A		
SHA-224, SHA-256, SHA-384, SHA-512	FIPS 180-2	1648	N/A		
Message Authentication Code (MAC) Functions					

[26] ECB – Electronic Codebook
[27] CBC – Cipher Block Chaining
[28] OFB – Output Feedback
[29] CFB – Cipher Feedback
[30] DES – Data Encryption Standard
[31] PKCS – Public Key Cryptography Standard
[32] SHA – Secure Hash Algorithm

Algorithm	Standard	Software Implementation Certificate Number	Hardware Accelerator Card		
			Appliance	Card	Certificate Number
HMAC[33] with SHA-1	FIPS 198	1120	N/A		
HMAC with SHA-224, SHA-256, SHA-384, SHA-512	FIPS 198	1120	N/A		

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 JMC**.

Table 15 - Cryptographic Operations Part 2

Algorithm	Standard	Software Implementation Certificate Number	Hardware Accelerator Card		
			Appliance	Card	Certificate Number
Symmetric Key Algorithms					
AES: ECB[34], CBC[35], OFB[36], CFB[37]-128 bit mode for 128-, 192-, and 256-bit key sizes	FIPS 197	1875	510	CN1010	105
				BCM5825	397
			600	CN501	105
			810	CN1010	105
				BCM5825	397
			900	CN1610	1265
			9000	CN1620	1265
Triple-DES[38]: ECB, CBC, CFB-64, OFB mode for	FIPS 46-3	1218	510	CN1010	217
				BCM5825	435

[33] HMAC – Hash-Based Message Authentication Code
[34] ECB – Electronic Codebook
[35] CBC – Cipher Block Chaining
[36] OFB – Output Feedback
[37] CFB – Cipher Feedback
[38] DES – Data Encryption Standard

Algorithm	Standard	Software Implementation Certificate Number	Hardware Accelerator Card		
			Appliance	Card	Certificate Number
keying option 1 (3 different keys)			600	CN501	217
			810	CN1010	217
				BCM5825	435
			900	CN1610	895
			9000	CN1620	895
Asymmetric Key Algorithms					
RSA PKCS[39]#1 sign/verify – 1024-, 1536-, 2048-bit	ANSI X9.31 (FIPS 186-2)	956	N/A		
Hashing Functions					
SHA[40]-1	FIPS 180-2	1648	N/A		

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

[39] PKCS – Public Key Cryptography Standard
[40] SHA – Secure Hash Algorithm

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 Administrative 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 to the CLI via SSH or the Serial port. 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 on the CLI via SSH or the Serial port. 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*[41]
3. *Establish an administrative session via the JMC: evaluate (with admin.access=WRITE) the <admin> layers of the configured policy rules according to the CPL specification and permit execution of the*

[41] 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_PCR_EXT.1.1(a).

resulting action is "allow," otherwise, evaluate (with admin.access=READ) 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.

].

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*].

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*

].

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*[42] *type*
10. *Request method (the requested operation)*
11. *Any part of an HTTP request other than the body (e.g. header fields*[43]*)*
12. *HTTP response header fields*
13. *HTTP response body*

].

FDP_IFF.1.2(a)

[42] MIME – Multipurpose Internet Mail Extensions

[43] 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).

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*].

FDP_IFF.1.4(a)

The TSF shall explicitly authorise an information flow based on [*no additional rules*].

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: [

1) Subject attributes:

1. none

2) Information attributes:

1. Source IP address or subnet

2. Destination IP address or subnet

3. Source Port

4. Destination Port

5. *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_PCR_EXT.1(a) Password Controlled Role

Hierarchical to: No other components.

FIA_PCR_EXT.1.1(a)

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

Dependencies: No dependencies

FIA_PCR_EXT.1(b) Password Controlled Role

Hierarchical to: No other components.

FIA_PCR_EXT.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 [*an administrator-configurable number of*] 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 an administrator-configurable interval of time.*

].

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 **JMC** 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 JMC access*
5. *Common Access Card (CAC)/Personal Identity Verification (PIV) microprocessor Integrated Circuit Card (ICC) and password for JMC access*
6. *RSA public key authentication for SSH access to the CLI*
7. *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 JMC,*
   a. *verification of the configured console username and password,*
   b. *verification of the administrator's CAC/PIV certificate and LDAP password, or*
   c. *verification of Administrative Access SFP policy rules*
   d. *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~~ [*obscured visual feedback*] to the **JMC** 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 **JMC** 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 16*].

Table 16 - Authorised 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.
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 JMC using the configured console username and password. • The user authenticates to the JMC 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 Utilization

FRU_ARP_EXT.1 Health check alarms

Hierarchical to: No other components.

FRU_ARP_EXT.1.1The TSF shall take [*one of the following notification actions: email, event logging, SNMP*[44] *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

[44] SNMP – Simple Network Management Protocol

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**, except for SSH sessions between a Blue Coat Director appliance and a subjugated ProxySG,** 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 EAL4 augmented with ALC_FLR.2. Table 17 - Assurance Requirements summarizes the requirements.

Table 17 - Assurance Requirements

Assurance Requirements	
Class ALC : Life Cycle Support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM[45] Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: Basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

6.4 TOE Security Assurance Measures

EAL4+ was chosen to provide a comprehensive level of independently assured security. This section of the Security Target maps the assurance requirements of the TOE for a CC EAL4+ 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.

[45] CM – Configuration Management

Table 18 - Assurance Measures Mapping to TOE Security Assurance Requirements (SARs)

Assurance Component	Assurance Measure
ALC_CMC.4	Blue Coat ProxySG SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1 - Configuration Management Document
ALC_CMS.4	Blue Coat ProxySG SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1 - Configuration Management Document
ALC_DEL.1	Blue Coat ProxySG SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1 - Secure Delivery Document
ALC_DVS.1	Blue Coat ProxySG SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1 - Life Cycle Document
ALC_LCD.1	Blue Coat ProxySG SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1 - Life Cycle Document
ALC_TAT.1	Blue Coat ProxySG SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1 - Life Cycle Document
ALC_FLR.2	Blue Coat ProxySG SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1 - Flaw Remediation Document
ADV_ARC.1	Blue Coat ProxySG SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1 - Development and Architecture Document
ADV_FSP.4	Blue Coat ProxySG SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1 - Development and Architecture Document
ADV_IMP.1	Blue Coat ProxySG SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1 - Development and Architecture Document
ADV_TDS.3	Blue Coat ProxySG SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1 - Development and Architecture Document

Assurance Component	Assurance Measure
AGD_OPE.1	Blue Coat Systems SGOS Administration Guide, Version SGOS 6.1.x, 231-03113, SGOS 6.1.1-08/2011 Blue Coat SGOS 6.1.x Release Notes, SGOS SGOS 6.1.5.2, 12/20/2011 Blue Coat Systems ProxySG Appliance Command Line Interface Reference, version SGOS 6.1.x, 231-03035, SGOS 6.1.3-07/2011 Blue Coat Systems ProxySG Appliance Content Policy Language Reference, version SGOS 6.1.x, 231-03019, SGOS 6.1.1-07/2011 Blue Coat Systems ProxySG Appliance SGOS 6.1.x Upgrade/Downgrade Feature Change Reference, Version SGOS 6.x, 231-03034, SGOS 6.1.1.-09/2010 Blue Coat Systems ProxySG Appliance Visual Policy Manager Reference, SGOS Version 6.x, 231-03015, SGOS 6.1.1-09/2010 Blue Coat 510/810 Series FIPS Compliant Tamper Evident Faceplate and Label Installation Guide, 231-02995, A-0 Blue Coat ProxySG 600 Series FIPS Compliance Guide: Tamper Evident Panel and Label Installation, 231-03160, A.0 Blue Coat ProxySG 900 Series FIPS Compliance Guide: Tamper Evident Panel and Label Installation, 231-03161, B.0 Blue Coat ProxySG 9000 Series FIPS Compliant Tamper Evident Shutter and Label Installation Guide, 231-03063, A.1 Blue Coat Using FIPS Mode on the ProxySG, 231-03154, March 2011 Blue Coat Systems, Inc. ProxySG SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1 Guidance Supplement v0.5
AGD_PRE.1	ProxySG Quick Start Guide SG600 Series, 231-03048, Rev A.0 ProxySG Quick Start Guide: SG900 Series, 231-03109, Rev B.0 ProxySG Quick Start Guide ProxySG 210 ProxySG 510 ProxySG 810ProxySG 9000 Series, 231-03122, Rev B.3 Blue Coat Systems ProxySG Appliance SGOS 6.x Upgrade/Downgrade Guide, SGOS Version 6.x, N/A, Version 6.1.1-(09/2010)
ATE_COV.2	Blue Coat ProxySG SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1 - Tests: Coverage, Depth
ATE_DPT.1	Blue Coat ProxySG SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1 - Tests: Coverage, Depth
ATE_FUN.1	Blue Coat ProxySG SG510, SG600, SG810, SG900, and SG9000 running SGOS v6.1 - Test: Functional Tests

6.4.1 ALC_CMC.4: Production support, acceptance procedures, and automation

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 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_CMS.4: Problem tracking CM coverage

The Configuration Management document details the TOE configuration items that are controlled by the configuration management system.

6.4.3 ALC_DEL.1: Delivery Procedures

The Secure 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.

6.4.4 ALC_DVS.1: Identification of Security Measures

The Life Cycle Document provides a description of the secure development procedures implemented by Blue Coat to protect against TOE modification during product development.

6.4.5 ALC_LCD.1: Developer Defined Life Cycle Model

The Life Cycle Document provides a description of the secure development procedures implemented by Blue Coat to protect against TOE modification during product developments.

6.4.6 ALC_FLR.2: Flaw Reporting Procedures

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.

6.4.7 ALC_TAT.1: Well-Defined Development Tools

The Life Cycle Document outlines tools and techniques used by Blue Coat to generate the TOE.

6.4.8 ADV_ARC.1: Security Architecture Description

The Developement and Architecture Document provides a description of the architecture-oriented features of domain separation, TSF self-protection, and non-bypassability of the security functionality.

6.4.9 ADV_FSP.4: Complete Functional Specification

The Development and Architecture Document 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 Functional Specification (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.

6.4.10 ADV_IMP.1: Implementation Representation of the TSF

The Development and Architecture Document provides the Implementation Representation, which is a mapping to the source code modules that make up the TOE.

6.4.11 ADV_TDS.3: Basic Modular Design

The Development and Architecture Document provides the Basic Modular Design, which is a design specification that refines the TSF functional specification into the major constituent parts (subsystems) and minor constituent parts (modules) of the TSF for a relatively simple TOE. The basic modular design identifies the basic structure of the TSF, the major and minor 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.

6.4.12 AGD_OPE.1: Operational User Guidance

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.

6.4.13 AGD_PRE.1: Preparative Procedures

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.

6.4.14 ATE_COV.2: Analysis of Coverage

The Coverage Analysis demonstrates that testing is performed against the functional specification. The Coverage Analysis demonstrates that all TSFI[48]s in the FSP have been tested.

6.4.15 ATE_DPT.1: Testing: Basic Design

The Depth Analysis demonstrates the level of detail to which the TSF has been tested by the developer. Testing of the TSF is based upon increasing depth of information derived from the security architecture description and the architectural design.

[48] TSFI – Target of Evaluation (TOE) Security Functional Interface

6.4.16 ATE_FUN.1: Functional Testing

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 Specification

This section presents information to detail how the TOE meets the functional 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 19 - Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Administrative Access SFP	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
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
Identification and Authentication	FIA_PCR_EXT.1(a)	Password controlled role
	FIA_PCR_EXT.1(b)	Password controlled role
	FIA_AFL.1	Authentication failure handlings
	FIA_UAU.1	Timing of authentication
	FIA_UAU.2	User authentication before any action
	FIA_UAU.5	Multiple authentication mechanism
	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
Protection of the TSF	FPT_STM.1	Reliable timestamps
Proxy SFP	FDP_IFC.1(a)	Subset information flow control

	FDP_IFF.1(a)	Simple security attributes
Resource utilisation	FRU_ARP_EXT.1	Health check alarms
	FRU_RSA.1	Maximum quotas
	FRU_RSA.2	Minimum and maximum quotas
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
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
	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
TOE Access	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.3	TSF-initiated termination
WAN Optimization SFP	FDP_IFC.1(b)	Subset information flow control
	FDP_IFF.1(b)	Simple security attributes

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[49]. These records are stored in the Event 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 Event Log can be displayed using the administrative interfaces; this function is restricted to Administrators and 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 Event Log and the Access Log are protected against unauthorised 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 SSH CLI and JMC. This data is

[49] Use of the “advanced-url” command is not logged by the TOE.

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[50] primary and alternate secret, the LDAP search password, and the content filter download passwords.

The TOE uses x.509 v3 certificates in its implementation of Public Key Infrastructure (PKI). X.509 specifies a standard format for public key certificates, which are used by the ProxySG in the form of SSL/TLS certificates, CA certificates, and external certificates. These certificates provide a mechanism by which users and devices can be authenticated to one another, and public keys are exchanged. The ProxySG uses PKI to authenticate the identities of OCSs, other ProxySGs, and administrators; and to exchange public keys used to encrypt data flowing between the ProxySG and OCSs, other ProxySGs, and between end users wishing to communicate privately over the organization's intranet via WAN Optimization or proxied TLS.

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 JMC. 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 a NIST SP 800-90 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.
The TOE destroys cryptographic keys in accordance with FIPS 140-2 zeroization requirements.

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

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.

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 authorised administrators to enforce a very flexible policy using the ProxySG CPL. Using CPL, an authorised 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 caching and acceleration techniques such as compression and object caching, byte-caching, and

compression 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 JMC, the user is directed to enter a username and password. JMC obscures the password by displaying asterisks instead of the actual password as it is typed. The GUI[51] 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

[51] GUI – Graphical User Interface

any user logging in to the JMC with the administrator username and password, or when the configured policy grants read/write access. The "enable" command is not required.

TOE appliances consumed by the United States Department of Defence (DoD) must meet Homeland Security Presidential Directive (HSPD)-12 requirements regarding the use of FIPS 201 validated CAC authentication for administrators connecting to management functionality of the TOE. Additionally, other agencies may require FIPS 201 validated PIV II card authentication.

Under these circumstances the TOE will implement a modified HTTPS-Console service as well as specially configured Content Policy Language (CPL) during administrator authentication in order to facilitate TLS mutual authentication. This is accomplished by modifying the HTTPS-Console service so that it can be configured to validate a client certificate against a chosen Certificate Authority (CA) list. CAC authentication will take place against a Certificate realm, and administrator authorization takes place against an LDAP realm.

The authentication procedure leverages 3rd party middleware in order to facilitate two factor authentication of the user to their CAC using a Personal Identification Number (PIN). This process enables the TOE to retrieve the X.509 certificate from the microprocessor smart card

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 User 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 ProxySG 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 original content servers, 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 the 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 be automatically re-enabled 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_ PCR_EXT.1(a), FIA_PCR_EXT.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 the 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 the TOE is installed 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 hardware clock, which is set during installation of the appliance, determines the order of the audit records 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 Utilization

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 (DDoS) 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[52] 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: FRU_ARP_EXT.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 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.

[52] ICAP – Internet Content Adaptation Protocol

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_PCR_EXT.1(a), FIA_PCR_EXT.1(b), and FRU_ARP_EXT.1. 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, and the resource utilization monitoring functionality of the ProxySG device.

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. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate 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.

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.HEALTH TOE users may perform actions that compromise the health of the TOE.	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.
	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.
T.MASQUERADE A user or process may masquerade as another entity in order to gain unauthorised 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.NACCESS An unauthorised person or external IT entity may be able to view or modify data that is transmitted between the TOE and a remote authorised external entity.	O.PROTECT The TOE must have the capability to protect management traffic from unauthorised reading or modification.	O.PROTECT ensures that the TOE has the capability to protect management traffic from unauthorised access, thereby ensuring that no unauthorised person or external entity may view or modify the data.
	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 cannot be accessed.
T.UNAUTHORISED_ACCESS A user may gain access to security data on the TOE for which they are not authorised according to the TOE security policy through the improper use of valid credentials.	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 unauthorised access.
	O.MANAGE The TOE must provide secure management of the system configuration, the Administrative Access SFP, the WAN	O.MANAGE provides the capability for an administrator to properly configure the management mechanisms of the TOE designed to mitigate this

	Optimization SFP, and the Proxy SFP.	threat.
	O.PROTECT The TOE must have the capability to protect management traffic from unauthorised reading or modification.	O.PROTECT ensures that the TOE is capable of protecting the management data transmitted through the TOE from unauthorised access, thereby ensuring that security data that is transmitted is protected from unauthorised access.
	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 unauthorised access, thereby ensuring that the security data on the TOE is protected from unauthorised access.
T.RESOURCE TOE users or attackers may cause network connection resources to become overused and therefore 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.
	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.

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 authorised 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	O.AUTHENTICATE ensures that administrators enter credentials before access to the administrative interfaces of the TOE is granted.

	protocol traffic matches a Proxy SFP rule which requires authentication.	
	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.
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 unauthorised 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 unauthorised 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).
P.PASS_TRAFFIC The TOE shall enforce the WAN Optimization SFP on traffic passing from the internal network to the	O.PASS_TRAFFIC The TOE must pass traffic from the internal network to the external network as defined by	O.PASS_TRAFFIC ensures that traffic that passes from the internal network to the external network is controlled by the

external network.	the WAN Optimization SFP.	WAN Optimization SFP.
P.POST_TYPE End Users shall not post unauthorised 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 unauthorised content types (as defined by the Proxy SFP rules) to the External Network via controlled protocols.

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 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 authorised persons.	NOE.ENVIRON The physical environment must be suitable for supporting a computing device in a secure setting.	NOE.ENVIRON ensures that the TOE IT environment is suitable to ensure the proper, secure, and on-going functioning of the TOE.
A.INSTALL The TOE has been installed and configured according to the appropriate installation guides.	NOE.ADMIN The administrator must be non-malicious and competent, and must follow all guidance.	NOE.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.
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.	NOE.ADMIN The administrator must be non-malicious and competent, and must follow all guidance.	NOE.ADMIN ensures that the administrator is trusted, educated, competent, and has no malicious intent, thereby addressing this assumption.
A.PASSWORD Passwords for administrative access to the TOE and for End User accounts are at least five characters in length, and are not	OE.PASSWORD Passwords for the Administrator and End User accounts and the “enable” password will be at least five characters in length and not	OE.PASSWORD ensures that the passwords selected by users are of sufficient strength to provide the desired level of security for TOE access.

dictionary words.	be a dictionary word.	

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.

8.3 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_PCR_EXT.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_PCR_EXT.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.

FRU_ARP_EXT.1 was stated explicitly to specify that notifications will be sent out when a change of health status occurs. This requirement was modelled after FAU_ARP.1, which uses the audit records as the source of the analysis. FRU_ARP_EXT.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.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.	FTA_SSL.3 TSF-initiated termination	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.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 Audit data generation	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.
O.MANAGE The TOE must provide secure management of the system configuration, the Administrative Access SFP, the WAN Optimization SFP, and the Proxy SFP.	FMT_MTD.2 Management of limits on TSF data	This requirement supports O.MANAGE by permitting Privileged Administrators to modify the limit on the size of the audit logs.
	FMT_MTD.1(b) Management of TSF data	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.1(a) Management of TSF data	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_MSA.3(c)	This requirement supports

	Static attribute initialisation	O.MANAGE. The WAN Optimization SFP is restrictive by default.
	FMT_MSA.3(b) Static attribute initialisation	This requirement supports O.MANAGE. The Proxy SFP is restrictive by default.
	FMT_MSA.3(a) Static attribute initialisation	This requirement supports O.MANAGE. The Administrative Access SFP is restrictive by default.
	FMT_MSA.2 Secure security attributes	This requirement supports O.MANAGE by ensuring that only secure values are accepted for security attributes.
	FMT_MSA.1(b) Management of security attributes	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.1(a) Management of security attributes	This requirement supports O.MANAGE by allowing all TOE administrators to query the security attribute user group membership.
	FMT_MOF.1 Management of security functions behaviour	This requirement supports O. MANAGE by specifying which functions of the TOE can be managed, and defining who can manage those functions.
	FMT_SMR.1 Security roles	This requirement supports O.MANAGE by supporting three roles: Administrator, Privileged Administrator, and Setup Console Administrator.
	FDP_ACC.1 Subset access control	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.
	FMT_SMR.3 Assuming roles	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.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.	FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions	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.
	FIA_UID.2 User identification before any action	This requirement supports O. AUTHENTICATE by ensuring administrators are identified before any other TSF-mediated actions taken on their behalf are performed.
	FIA_UID.1(b) Timing of identification	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.1(a) Timing of identification	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_UAU.7(b) Protected authentication feedback	This requirement supports O. AUTHENTICATE by requiring that characters are not echoed when administrators type their password on the Management Console.
	FIA_UAU.7(a) Protected authentication feedback	This requirement supports O. AUTHENTICATE by requiring that characters are not echoed when administrators type their password on the CLI.
	FIA_UAU.6(b) Re-authenticating	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.6(a) Re-authenticating	This requirement supports O. AUTHENTICATE by ensuring the End Users are authenticated before any other TSF-mediated actions taken on their behalf are performed. Only actions that match Proxy SFP rules not requiring identification are allowed before authentication is performed.
	FIA_UAU.5 Multiple authentication mechanism	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.2 User authentication before any action	This requirement supports O. AUTHENTICATE by ensuring that no action is permitted on behalf of an unauthenticated Management Console user.
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_UAU.1 Timing of authentication	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.
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_ACF.1 Security attribute based access control	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.
O.PROTECT The TOE must have the capability to protect management traffic from unauthorised reading or modification.	FCS_CKM.4 Cryptographic key destruction	This requirement supports O.PROTECT by providing a method for destroying cryptographic keys, thereby ensuring that the keys are not accessed by an unauthorised person or IT entity.
O.AUDIT	FAU_SAR.1(b)	This requirement supports

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.	Audit review	O.AUDIT by requiring the TOE to make the recorded audit records available for review.
	FAU_SAR.1(a) Audit review	This requirement supports O.AUDIT by requiring the TOE to make the recorded audit records available for review.
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_AFL.1 Authentication failure handlings	This requirement supports O. AUTHENTICATE by ensuring that users' passwords are protected from brute-force guessing.
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_STG.4 Prevention of audit data loss	This requirement supports O.AUDIT by requiring the TOE to mitigate audit data loss due to hardware limitations such as disk full.
O.PASS_TRAFFIC The TOE must pass traffic from the internal network to the external network as defined by the WAN Optimization SFP.	FDP_IFF.1(b) Simple security attributes	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.
	FDP_IFC.1(b) Subset information flow control	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.
O.ALERT The TOE must alert the administrator of changes in TOE health.	EXT_FRU_ARP.1 Health check alarms	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.QUOTA The TOE must be able to place quotas on network connection resources.	FRU_RSA.2 Minimum and maximum quotas	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.
	FRU_RSA.1 Maximum quotas	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.
O.TIMESTAMP The TOE must provide a timestamp for use by the TOE.	FPT_STM.1 Reliable timestamps	This requirement supports O.TIMESTAMP by ensuring that the TOE provides a timestamp for the TOE's use.
O.PROTECT The TOE must have the capability to protect management traffic from unauthorised reading or modification.	FTA_SSL.3 TSF-initiated termination	This requirement supports O.PROTECT by ensuring that unauthorised 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.	FMT_SMF.1 Specification of management functions	This requirement supports O.MANAGE by specifying that the TOE supports configuration of the Proxy SFP.
O.PROTECT The TOE must have the capability to protect management traffic from unauthorised reading or modification.	FCS_COP.1(b) Cryptographic operation	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.
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_STG.1 Protected audit trail storage	This requirement supports O.AUDIT by requiring the TOE to prevent unauthorised deletion of the audit records.
O.PROTECT The TOE must have the capability to protect management traffic from unauthorised reading or modification.	FCS_CKM.1 Cryptographic key generation	This requirement supports O.PROTECT by providing cryptographic key generation, which can be used to ensure cryptographic functionality on 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.	FCS_COP.1(b) Cryptographic operation	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.
	FCS_COP.1(a) Cryptographic operation	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_CKM.4 Cryptographic key destruction	This requirement supports O.VALIDATED_CRYPTO by providing a method for destroying cryptographic keys, thereby ensuring that the keys are not accessed by an unauthorised person or IT entity.
	FCS_CKM.1 Cryptographic key generation	This requirement supports O.VALIDATED_CRYPTO by providing cryptographic key generation, which can be used to ensure cryptographic functionality on the TOE.
O.SCREEN_URL The TOE must disallow controlled protocol traffic for given URLs as defined by the Proxy SFP.	FDP_IFF.1(a) Simple security attributes	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.
	FDP_IFC.1(a) Subset information flow control	This requirement supports O.SCREEN_URL by providing a policy language that enables authorised administrators to construct rules representing their site's information flow policy. The function then enforces those rules and takes the action specified.
O.SCREEN_TYPE The TOE must disallow controlled protocol traffic of given content types as defined by the Proxy SFP.	FDP_IFF.1(a) Simple security attributes	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.
	FDP_IFC.1(a) Subset information flow control	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.
O.REMOVE_ACTIVE The TOE must be able to remove active content from HTML pages	FDP_IFF.1(a) Simple security attributes	This requirement supports O.REMOVE_ACTIVE by supporting a wide range of

delivered via a controlled protocol as defined by the Proxy SFP.		attributes that can be used in the Proxy SFP to control the flow of information between the Internal and External Networks.
	FDP_IFC.1(a) Subset information flow control	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.
O.PROTECT The TOE must have the capability to protect management traffic from unauthorised reading or modification.	FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions	This requirement supports O.PROTECT by ensuring that unauthorised users do not gain access to the TOE through an unattended active session.

8.5.2 Security Assurance Requirements Rationale

EAL4+ was selected because it is best suited to address the stated security objectives. EAL4+ challenges vendors to use best (rather than average) commercial practices. EAL4+ allows the vendor to evaluate their product at a detailed level while benefitting from the Common Criteria Recognition Agreement. The chosen assurance level is appropriate for the threats defined in the environment.

The augmentation of ALC_FLR.2 was added to specifically address requirements from the Army Office of Information Assurance and Compliance..

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)	✓	

SFR ID	Dependencies	Dependency Met	Rationale
	FCS_COP.1(b)	✓	
	FCS_CKM.4	✓	
FCS_CKM.4	FCS_CKM.1	✓	
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(a)	✓	
FDP_IFC.1(a)	FDP_IFF.1(a)	✓	
FDP_IFF.1(a)	FDP_IFC.1(a)	✓	
	FMT_MSA.3(b)	✓	
FDP_IFC.1(b)	FDP_IFF.1(b)	✓	
FDP_IFF.1(b)	FDP_IFC.1(b)	✓	
	FMT_MSA.3(c)	✓	
FIA_PCR_EXT.1(a)	No dependencies	✓	
FIA_ PCR_EXT.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	✓	
FIA_UAU.6(b)	No dependencies	✓	
FIA_UAU.7(a)	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_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	✓	

SFR ID	Dependencies	Dependency Met	Rationale
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(a)	✓	
	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(a)	FMT_MSA.1(a)	✓	
	FMT_MSA.1(b)	✓	
	FMT_SMR.1	✓	
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	✓	
FRU_ARP_EXT.1	No dependencies	✓	
FRU_RSA.1	No dependencies	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FRU_RSA.2	No dependencies	✓	
FTA_MCS.2	FIA_UID.1(a)	✓	
FTA_SSL.3	No dependencies	✓	

9 Acronyms

The following table defines the Acronyms used in this document.

Table 25 – Acronyms

Acronym	Definition
3DES	Triple Data Encryption Standard
ADN	Application Delivery Network
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AOL	America Online
CA	Certificate Authority
CAC	Common Access Card
CBC	Cipher Block Chaining
CC	Common Criteria
CEM	Common Criteria Evaluation Methodology
CFB	Cipher Feedback
CIFS	Common Internet File System
CLI	Command Line Interface
CM	Configuration Management
CPL	Content Policy Language
CRL	Certificate Revocation List
DDoS	Distributed Denial of Service (attack)
DNS	Domain Name System
DoD	United States Department of Defence
DSA	Digital Signature Algorithm
DRTR	Dynamic Real-Time Rating
EAL	Evaluation Assurance Level
ECB	Electronic Codebook
ELFF	Extended Log File Format
FIPS	Federal Information Processing Standard
FSP	Functional Specification
FTP	File Transfer Protocol
GB	Gigabyte
GigE	Gigabit Ethernet

Acronym	Definition
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
HSPD	Homeland Security Presidential Directive
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
ICAP	Internet Content Adaption Protocol
ICC	Integrated Circuit Card
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IT	Information Technology
IWA	Integrated Windows Authentication
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MAPI	Messaging Application Programming Interface
MIME	Multipurpose Internet Mail Extensions
MMS	Microsoft Media Streaming
MSN	The Microsoft Network
NCSA	National Center for Supercomputing Applications
NTP	Network Time Protocol
OCS	Original Content Server
OFB	Output Feedback
OSP	Organizational Security Policy
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
POP3	Post Office Protocol version 3
PP	Protection Profile
RADIUS	Remote Authentication Dial-In User Service
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adelman
RTSP	Real-Time Streaming Protocol

Acronym	Definition
SAR	Security Assurance Requirement
SAS	Serial Attached SCSI
SCSI	Small Computer System Interface
SFP	Security Functional Policy
SFR	Security Functional Requirement
SGOS	(Proxy)SG Operating System
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SP	Special Publication
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Functional Interface
U	Unit
URL	Uniform Resource Locator
VPM	Visual Policy Manager
W3C	World Wide Web Consortium
WAN	Wide Area Network

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033

Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com