Extreme Networks, Inc.
ExtremeXOS Network Operating System v12.3.6.2

Security Target

Evaluation Assurance Level: EAL3+
Document Version: 0.9

Prepared for:

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, CA 95051

Phone: +1 408 579 2800
http://www.extremenetworks.com

Prepared by:

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

Phone: +1 703 267 6050
http://www.corsec.com

Table of Contents

Table of Figures

List 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 Extreme Networks ExtremeXOS Network Operating System v12.3.6.2 (EXOS), and will hereafter be referred to as the TOE throughout this document. The TOE is a software-only operating system (OS) that runs on the BlackDiamond 8500/8800/8900 series switch and all Summit model switches. The switches and EXOS are produced by Extreme Networks, Inc. The BlackDiamond and Summit switches are network switching appliances, designed to provide network traffic management and control.

1.1 Purpose

This ST is divided into nine sections, as follows:

- 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), ST 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 and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 – ST and TOE References

ST Title	Extreme Networks, Inc. ExtremeXOS Network Operating System v12.3.6.2 Security Target
ST Version	Version 0.9
ST Author	Corsec Security, Inc.
ST Publication Date	3/12/2012
TOE Reference	Extreme Networks ExtremeXOS Network Operating System v12.3.6.2
Keywords	Modular Switching Products, Modular OS, Ethernet Network

1.3 TOE Overview

The TOE is network switching software, designed to provide network traffic management and control. The TOE runs on network switch appliances. It is a software-only TOE.

The TOE is a full-featured operating system that is designed specifically for the Extreme Networks BlackDiamond and Summit network switches. The TOE is limited to the EXOS version 12.3.6.2. The BlackDiamond and Summit network switches are a required component of the TOE environment. The TOE is designed to protect and transfer user data across a network reliably and in a timely fashion.
The TOE includes the following features:

- Virtual routers: This capability allows a single physical switch to be split into multiple virtual routers. This feature separates the traffic forwarded by a virtual router from the traffic on a different virtual router. Each virtual router maintains a separate logical forwarding table, which allows the virtual routers to have overlapping address spaces. Because each virtual router maintains its own separate routing information, and switch ports can belong to one and only one virtual router, packets arriving at a port on one virtual router can never be switched to the ports on another.
- Load Sharing: Load sharing supports an increase in bandwidth and resiliency by using a group of ports to carry traffic in parallel between systems. This feature allows the switch to use multiple ports as a single logical port.

1.3.1 TOE Environment

The TOE runs on the following hardware appliances:

- BlackDiamond 8500/8800/8900 Series Switch
- Summit X150 Series
- Summit X250e Series
- Summit X350 Series
- Summit X450 Series
- Summit X450a Series
- Summit X450e Series
- Summit X650 Series
- SummitStack

The BlackDiamond switches are referred to as “chassis” switches because they are designed to be physically upgradeable or extendable (i.e., new cards and interfaces can be added, etc.), while the Summit switches are referred to as “fixed” switches since they are generally not designed to be physically upgradeable. While the Summit switches generally consist of a mainboard and daughterboard that implement all ports, interfaces, and functionality, the BlackDiamonds are composed of:

- a Management Switch Module (MSM), which provides the management plane and switch plane, or a Management Module (MM), which provides just the management plane
- a Switch Fabric (SF) module, which provides the switch fabric if an MM (rather than an MSM) is present

- several I/O[1] modules (IOB[2]s), which provide the network interfaces (copper, Fibre Channel, etc.)
- a control plane, which provides Gigabit Ethernet (GigE) connectivity between each of the modules

The TOE relies on the switches to include a hardware clock and provides a reliable time stamp.

By default, the memory buffer and the NVRAM[3] in the switch (on which the TOE runs) are configured to store the generated audit records. The TOE shall use a Syslog server in the IT environment to store the generated audit records.

1.4 TOE Description

The TOE is the ExtremeXOS Network Operating System v12.3.6.2. It is a software only TOE that performs switching and security functions. The TOE provides logical connections for management of network traffic flow and for management access.

The TOE consists of custom-written application software that provides the switching and other product-specific functionality, running on a customized Linux operating system.

1.4.1 Architecture

The BlackDiamond and Summit switches run essentially the same software. The software images for each are compiled from the same source code, but features unusable on specific models are not compiled into the software image for that model. Each BlackDiamond runs a uniquely compiled software image, while all of the Summit appliances run the same software image. Figure 1 below provides a diagram showing the high-level architecture and deployment posture.

[1] I/O – Input/Output

[2] IOB – Input/Output Blade; Also called Input/Output Module

[3] NVRAM – Non-volatile random access memory

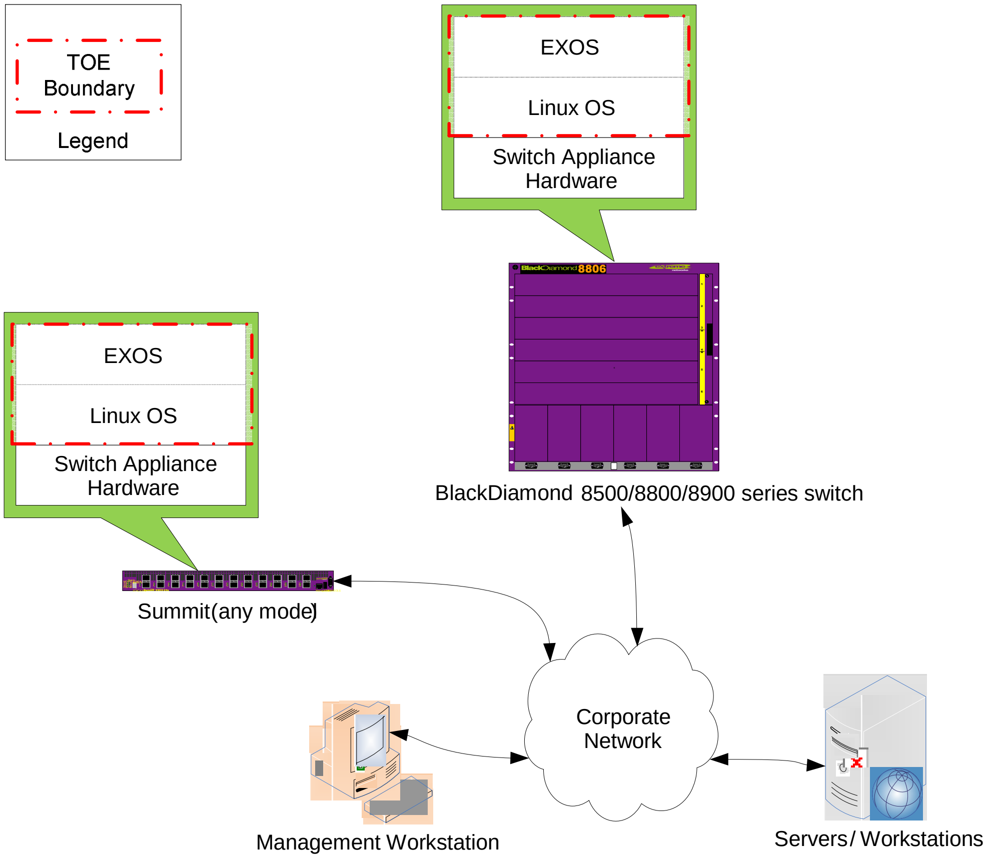

Figure 1 – BlackDiamond and Summit Switches High-Level Architecture

On the BlackDiamond, EXOS runs on the MM or MSM (whichever is present). When the IOBs boot up, they load their software images from the EXOS software running on the MM or MSM. The boot process of the BlackDiamond and Summit switches can be generalized by the following steps:

1. EXOS kernel boots from flash memory (on the mainboard on the Summit, or on the MM or MSM on the BlackDiamond)

2. EXOS kernel loads the EXOS Process Monitor (EPM)[4]

3. EPM loads and monitors all other required processes

After EXOS has successfully booted, the management interfaces are available (and can be dynamically enabled or disabled as desired).

As an Ethernet switch, the core product functionality primarily focuses on switching packets to their intended destinations as quickly as possible.

[4] EPM is the root of all EXOS processes. EPM performs active monitoring of all EXOS processes.

1.4.2 Physical Boundaries

This section identifies the hardware and software components of the product that are in the TOE. Section 1.3.1 identifies the hardware and software components that the TOE relies upon and that are part of the IT[5] environment.

There are no hardware components that are part of the TOE. The TOE runs on the hardware appliances listed in Section 1.3.1.

The following software component constitutes the entire TOE:

- ExtremeXOS Network Operating System v12.3.6.2

EXOS is based on a MontaVista Linux real-time operating system (which is based on Linux kernel v2.4). Figure 2 below shows the physical boundary of the TOE.

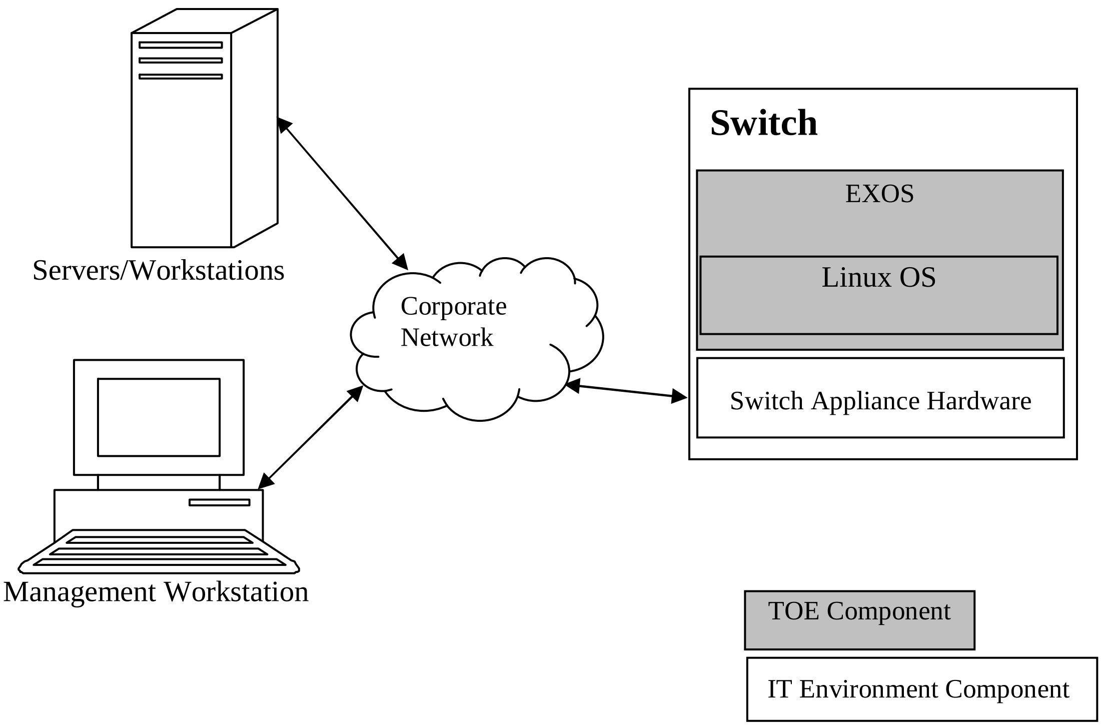

Figure 2 – EXOS Physical Boundaries

1.4.2.1 Guidance Documentation

The TOE includes the following guidance:

- ExtremeXOS Concepts Guide, Software Version 12.3, published June 2009, part number 100339-00 Rev.01
- ExtremeXOS Command Reference Guide, Software Version 12.3, published June 2009, part number 100340-00 Rev.01

[5] IT – Information Technology

1.4.3 Logical Boundaries

The logical boundaries of the TOE include the security functions of the TOE interfaces. The TOE logically supports the following security functions:

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

1.4.3.1 Security Audit

The TOE collects audit data on security-relevant user actions and provides an interface for reviewing the audit logs. Audit information generated by the system includes date and time of the event, user identifier (ID) that caused the event to be generated, computer where the event occurred, and other event-specific data. The TOE provides a reliable time stamp, relying on the hardware appliance to include a hardware clock. The ability to review all audit records is available to all users; however, users with the User role will see sanitized forms of certain audit records (for example, login and logout records will have the usernames removed).

1.4.3.2 User Data Protection

The TOE enforces a Switch Traffic Flow control policy which restricts access to the network. The TOE provides an Administrator the ability to define access rules on the traffic received by the TOE. The access control lists consist of access rules and are used to perform packet filtering and forwarding decisions on incoming traffic.

1.4.3.3 Identification and Authentication

The TOE requires users to provide unique identification and authentication data before any administrative access to the system is granted. The TOE provides the ability to define levels of authority and access for users, providing administrative flexibility. The TOE does not require identification and authentication for information flow through the switch.

The TOE supports local authentication via usernames and passwords. Administrators can configure a password policy for the product, specifying the password complexity and composition requirements and the allowed number of failed authentication attempts before lockout occurs.

1.4.3.4 Security Management

The TOE is managed through the following management interfaces, which can be dynamically enabled or disabled as desired.

- Command Line Interface (CLI)
- ScreenPlay Web GUI[6] ("Flash interface")
- Remote Manage interface
- XML[7]/WebServices interface

[6] GUI – Graphical User Interface

[7] XML – eXtensible Markup Language

The CLI is accessible through a remote console, as well as a local terminal console (a management console) via a serial port. Through this interface all management can be performed, including user management and the configuration of the switch functions.

The Web GUI, called "ScreenPlay", consists of Adobe Flash web applications that are served to users connecting to the switch via HTTPS[8]. ScreenPlay provides a subset of the full configuration functionality available via the CLI.

The XML/Web Services interface is accessible via HTTPS. It allows arbitrary external programs to administer the switch (assuming that they are properly authenticated) by exposing the switch's management functions as XML-based WebServices APIs[9].

The Remote Manage is accessible via SNMP[10] v1, v2, and v3 protocol for remote reporting and remote management of the switch. In the CC-evaluated configuration, the use of SNMP v1 and v2 are excluded.

The Time Stamp interface is accessible via the kernel of the operating system. It allows for a reliable source of synchronizing the internal clock of the EXOS through the hardware of the client machine.

There are two types of administrative users in the system: Administrator (fully privileged administrators) and User (restricted or "non-privileged" users). Users only have read-only access (no changes are allowed), and certain data is sanitized for display to them (such as usernames in certain audit logs, as described above). By default two predefined users: "admin" and "user" are created. At installation time, the administrator can also choose to enable a "failsafe" user account, which allows recovery of the system if all of the other accounts get locked out.

1.4.3.5 Protection of the TSF

The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is that users must authenticate before any administrative operations can be performed on the system, whether those functions are related to the management of user accounts or the configuration of traffic flows. Another protection mechanism is that all functions of the TOE are confined to the TOE itself. The TOE is completely self-contained, and therefore maintains its own execution domain.

1.4.3.6 TOE Access

An administrator can configure the TOE to display a warning banner at the beginning of each login prompt of each session.

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

The following features/functionalities are not included in the evaluated configuration:

- Use of an external TACACS+ server
- Use of an external RADIUS server
- SNMP Protocol v1, and v2
- Cryptographic operations
- Telnet

[8] HTTPS – Secure HTTP, where HTTP stands for Hypertext Transport Protocol

[9] API – Application Programming Interface

[10] SNMP – Simple Network Management Protocol; SNMP version 1 and 2 are not included in the evaluated configuration. SNMP v3 is used for authentication purposes and is not being used to claim any cryptographic functionality.

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 2 – 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 [conformant]; CC Part 3 [conformant]; PP claim (none); Parts 2 and 3 Interpretations from the CEM as of 2009/12/14 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL3+ Augmented with Flaw Remediation (ALC_FLR.2)

3 Security Problem

The TOE security environment describes the security aspects of the intended environment in which the TOE is to be used and the manner in which it is expected to be employed. The statement of TOE security environment defines the following:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions made on the operational environment and the method of use intended for the product

The TOE is intended to be used in environments where the TOE components can be physically protected from tampering and where necessary information will be available via other network components (e.g. routers).

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 following threats are applicable:

Table 3 – Threats

Name	Description
T.MEDIATE	An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
T.NOAUDIT	A user may not be accountable for his actions due to his actions not being recorded or due to an administrator not reviewing the audit records.
T.NOMGMT	An authorized administrator is not able to manage the TOE security functions and data which results in the TOE being configured in an insecure manner.
T.PRIV	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data, inappropriately changing the configuration data for TOE security functions.

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.

There are no OSPs defined for this ST.

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 4 – Assumptions

Name	Description
A.AUDREV	The TOE administrators will periodically review the audit records generated by the TOE.
A.FLOW	The TOE will be placed in a network infrastructure such that information to be controlled will always flow through the TOE.
A.GENPUR	The TOE does not have the ability to run general purpose applications and does not host public data.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.EXCLUSIVE	All administrative interfaces are not accessible to non-administrators and only administrators have access to the administrative interfaces to ensure the network is secure.

4 Security Objectives

This section defines the security objectives of the TOE and its supporting environment. Security objectives, categorized as either IT security objectives or non-IT security objectives, reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified. All of the identified threats and organizational policies are addressed under one of the categories below.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 5 – Security Objectives for the TOE

Name	Description
O.ACCESS	The TOE must allow only authorized users and processes (applications) to access protected TOE functions and data.
O.ACCOUNT	The TOE must provide user accountability for information flows through the TOE and for authorized administrators' use of security functions related to audit.
O.ADMIN	The TOE must provide services that allow effective management of its functions and data.
O.AUDIT	The TOE must provide a means to record an audit trail of security-related events, with accurate dates and times.
O.IDAUTH	The TOE must require that all administrative users be identified and authenticated prior to obtaining administrative access.
O.MEDIATE	The TOE will mediate the flow of information from users on a connected network to users on another connected network as defined by administrator-configured policies/routing information.
O.PROTECT	The TOE must protect itself from unauthorized access to its functions and data.

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 6 – IT Security Objectives

Name	Description
OE.IDAUTH	The TOE operating environment shall provide the ability to uniquely identify and authenticate remote users.
OE.PROTECT	The TOE operating environment shall provide the ability to protect the data in transit from unauthorized modifications.

OE.TIME	The TOE will have access to a hardware clock from the TOE environment.
OE.SYSLOG	The TOE operating environment will include a syslog server to provide storage for audit records.

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 7 – Non-IT Security Objectives

Name	Description
OE.AUDREV	The TOE administrators will be trained to periodically review the audit records generated by the TOE.
OE.FLOW	The network infrastructure in which the TOE is placed must be installed, administered and operated in a manner that ensures all information to be controlled flows through the TOE.
OE.GENPUR	The TOE will not execute general purpose applications and the TOE does not host public data.
OE.MANAGE	Authorized administrators are trained, non-hostile and follow all administrator guidance.
OE.PHYS	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.ADMIN	The administrator must not be careless, negligent, or willfully hostile; must be appropriately trained; and must follow all guidance.

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.

5.1 Extended TOE Security Functional Components

There are no extended TOE security functional components defined for this evaluation.

5.2 Extended TOE Security Assurance Components

There are no extended TOE security assurance components defined for this evaluation.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE.

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. Assignment and selection operations are used within this ST. These operations are performed as described in Part 2 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 beginning of the short 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 8 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 8 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FDP_IFC.1	Subset information flow control		✓		
FDP_IFF.1	Simple security attributes		✓		
FIA_AFL.1	Authentication failure handling	✓	✓		
FIA_ATD.1	User attribute definition		✓		
FIA_SOS.1	Verification of secrets		✓		
FIA_UAU.1	Timing of authentication		✓		
FIA_UID.1	Timing of identification		✓		
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation		✓		
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		

FPT_STM.1	Reliable time stamps		✓		
FTA_TAB.1	Default TOE access banners				

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:

a) Start-up and shutdown of the audit functions;
b) All auditable events, for the [*not specified*] level of audit; and
c) [authentication attempts *FIA_UID.1 & FIA_UAU.1) and administrative actions (FMT_MSA.1, FMT_MSA3, FMT_MTD.1)*].

FAU_GEN.1.2
The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no additional information*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review
Hierarchical to: No other components.

FAU_SAR.1.1
The TSF shall provide [administrator, user[11]] with the capability to read [*all auditable events*] from the audit records.

FAU_SAR.1.2
The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

[11] The user role will see sanitized forms of certain audit records (for example, login and logout records will have the usernames removed.

6.2.2 Class FDP: User Data Protection

FDP_IFC.1 Subset information flow control
Hierarchical to: No other components.

FDP_IFC.1.1

The TSF shall enforce the [*Switch Traffic Flow SFP*[12]] on [
subjects: *IT entities sending and receiving information through the TOE,*
information: network traffic; and,
operations: switching and routing of information].

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1 Simple security attributes
Hierarchical to: No other components.

FDP_IFF.1.1

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

[a. *subject security: attributes:*
- *the presumed address*

b. *information security attributes:*
- *presumed address of the source subject;*
- *presumed address of the destination subject;*
- *IP*[13] *protocol field;*
- *TCP*[14]*/UDP*[15] *source port (DHCP*[16]*, NTP*[17]*, etc.);*
- *TCP/UDP destination port (DHCP, NTP, etc);*
- *TCp flags;*
- *ICMP*[18] *message type;*
- *ICMP code field;*
- *ICMP-type;*
- *Source Service Advertising Protocol (SAP);*
- *Destination SAP;*
- *Snap Type;*
- *IP Type of Service (TOS) field;*
- *Fragments;*
- *Virtual Local Area Network (VLAN) ID*
- *Ethernet packet type (e.g., IP, IPv6, 8021.Q);*
- *Ethernet source Media Access Control (MAC) address;*

[12] SFP – Security Function Policy

[13] IP – Internet Protocol

[14] TCP – Transport Control Protocol

[15] UDP – User Datagram Protocol

[16] DHCP - Dynamic Host Configuration Protocol

[17] NTP – Network Time Protocol

[18] ICMP – Internet Control Message Protocol

- *Ethernet destination MAC address;*
- *TOE interface on which traffic information arrives and depart]*.

FDP_IFF.1.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[*a) A virtual circuit has been established between the inbound TOE interface and some other interface (in which case the information is forwarded to the associated outbound TOE interface) AND all of the information security attribute values are unambiguously permitted by the Access Control List (ACL) rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by an authorized administrator*

OR

b) The presumed destination address of the information identifies a subject associated with an outbound TOE interface (in which case the information is forwarded to the identified outbound TOE interface) AND all of the information security attribute values are unambiguously permitted by the ACL rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by an authorized administrator.

OR

c) The presumed destination address of the information identifies a subject that is not associated with any TOE interface AND the TOE has been configured to broadcast traffic when it doesn't recognize the presumed address of the destination subject (in which case the information is broadcast out all TOE interfaces that are not configured as part of a virtual circuit) AND all of the information security attribute values are unambiguously permitted by the ACL rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by an authorized administrator].

FDP_IFF.1.3

The TSF shall enforce the [*no additional information flow rules*].

FDP_IFF.1.4

The TSF shall explicitly authorize an information flow based on the following rules: [*no additional information flow rules*].

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: [*no additional denial information flow rules*].

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

6.2.3 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1

The TSF shall detect when [*an administrator configurable positive integer within* [*the range of 1-10*]] unsuccessful authentication attempts occur related to [*user's attempts or processes (application) attempts to establish a new session*].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [*terminate the session or if configured by the administrator, disable user account if attempting to establish a new session]*. A session includes SSH and non-SSH session components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [*user identity, authentication data, and role*].

Dependencies: No dependencies

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [*the following administrator configurable conditions:*

a) Minimum password length between 8 and 32 characters

b) Password must not be one of the previous 5 passwords recorded

c) Password includes at least 2 characters from each of the following sets:

1. *Uppercase characters (A-Z)*
2. *Lowercase characters (a-z)*
3. *Numeric characters (0-9)*
4. *Non-alphanumeric characters [(‘(‘, ‘!’, ‘@’, ‘#’, ‘$’, ‘%’, ‘^’, ‘*’, ‘)’)].*

Dependencies: No dependencies

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1

The TSF shall allow [*switch traffic flow subject to TOE policies*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2

The TSF shall require each 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_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1

The TSF shall allow [*switch traffic flow subject to TOE policies*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2

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

Dependencies: No dependencies

6.2.4 Class FMT: Security Management

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1

The TSF shall enforce the [*Switch Flow Traffic Flow SFP*] to restrict the ability to [*query, modify, delete, [create]*] the security attributes [*ACL rules on the switch*] to [*Administrators*].

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1

The TSF shall enforce the [*Switch Traffic Flow SFP*] to provide [*permissive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

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

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

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [*perform operations identified in column 1 of* Table 9] the [*list of TSF data identified in column 2 of* Table 9] to [*Administrator*].

Table 9 – Management of TSF Data

Operation	TSF data
modify	switch configuration
query, modify, delete, [create]	user accounts
modify	system time
modify	the number of failed logins before terminating a session or disabling an account
modify	Password restrictions policy

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

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

- modify switch configuration
- manage user accounts
- modify the system time
- manage ACL rules
- terminate process
- modify the number of failed logins before terminating a session or disabling an account
- modify the password restrictions policy
- management and configuration of the information flow policies and routing policies

].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*Administrator and User*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.2.5 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

6.2.6 Class FTA: TOE Access

FTA_TAB.1 Default TOE access banners
Hierarchical to: No other components.

FTA_TAB.1.1

Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

Dependencies: No dependencies

6.3 Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 3 components as specified in Part 3 of the Common Criteria with ALC_FLR.2. No operations are applied to the assurance components.

Table 10 – Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC : Life Cycle Support	ALC_CMC.3 Authorization controls
	ALC_CMS.3 Implementation representation CM[19] coverage
	ALC_DEL.1 Delivery Procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_FLR.2 Flaw Reporting Procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural 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.2 Vulnerability analysis

[19] CM – Configuration Management

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 11 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
User Data Protection	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UID.1	Timing of identification
Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of TOE Security Functions	FPT_STM.1	Reliable time stamps
TOE Access	FTA_TAB.1	Default TOE access banners

7.1.1 Security Audit

The TOE provides fully configurable audit record generation capability for all actions performed by authorized administrators and authorized users on the system.

The TOE generates audit records for the following auditable events:

- Start-up and shutdown of the audit functions (via log records that indicate that the system is booting and shutting down)
- Authentication attempts (login and logout on all management interfaces)

- All administrative actions including management and configuration of the information flow policies and routing policies.

Audit records can be generated for all of the commands issued using the CLI and Web GUI. The use of the XML/Web Services and SNMP interfaces can also be audited.
The administrator can configure where the audit event messages are sent/stored upon generation. Audit records can be sent to more than one location (target). Not all event messages are sent to every enabled target. Each target receives only the messages for which it is configured. Storage filtering can be based on message content and type. The records can be sent to the following locations:

- Console display
- Current remote session
- Internal memory buffer, which can contain 200 to 20,000 messages (1000 by default)
- NVRAM, where the messages remain after a reboot
- Remote syslog host
- Primary MSM/MM for BlackDiamond or primary node for Summit
- Backup MSM/MM for BlackDiamond or backup node for Summit

The memory buffer and NVRAM can only contain a limited number of messages, so the oldest message is lost when a new message arrives when the buffer is full.

In the evaluated configuration, a copy of the audit records must be sent to the syslog host for persistent storage and to maintain a history of events worthy of forensic analysis. The TOE protects the audit records stored in the memory buffer until a copy is sent to a syslog host and the TOE environment protects the audit records that are sent for historical purposes.

Each audit record will include the date and time of the event, type of event, subject identity (host ID or username), and the outcome (success or failure) of the event. The CLI commands provide the capability for the administrator to configure various aspects of the switch's system audit log messages. The log messages contain configuration and fault information pertaining to the device. The log messages can be formatted to contain various items of information, such as:

- the timestamp when the event occurred
- the severity level of the event (critical, error, warning, notice, info, debug-summary, debug-verbose, and debug-data)
- the component or functional area where the event tool place
- a message that details the event.

The ability to review all audit records is available to users with the administrator or user role. However, the entities with the user role will see sanitized forms of certain audit records (for example, login and logout records will have the usernames removed).

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1

7.1.2 User Data Protection

The TOE enforces a Switch Traffic Flow control policy restricting access to the network and providing the administrator with the ability to define access rules on the traffic received by the TOE. The Switch Traffic Flow control policy is enforced upon all IT entities sending and receiving information through the TOE, network traffic and switching and routing of information.

The Switch Traffic Flow control policy allows combinations of network traffic attributes to be used to dictate allowable information flows between IT entities respective of the current operational environment. The Switch Traffic Flow control policy enforcement is based on the following security attributes:

- presumed address of the source subject;
- presumed address of the destination subject;
- IP protocol field;
- TCP/UDP source port (DHCP, NTP, etc);
- TCP/UDP destination port (DHCP, NTP, etc)
- TCP flags;
- ICMP message type;
- ICMP code field;
- ICMP-type;
- Source SAP;
- Destination SAP;
- Snap Type;
- IP TOS field;
- Fragments;
- VLAN ID
- Ethernet packet type (e.g., IP, IPv6, 802.1Q);
- Ethernet source MAC address;
- Ethernet destination MAC address;
- TOE interface on which traffic information arrives and depart

The TOE permits an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- A virtual circuit has been established between the inbound TOE interface and some other interface (in which case the information is forwarded to the associated outbound TOE interface) **AND all of the information security attribute values are unambiguously permitted by the ACL rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by an authorized administrator.**

OR

- The presumed destination address of the information identifies a subject associated with an outbound TOE interface (in which case the information is forwarded to the identified outbound TOE interface) **AND all of the information security attribute values are unambiguously permitted by the ACL rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by an authorized administrator.**

OR

- The presumed destination address of the information identifies a subject that is not associated with any TOE interface AND The TOE has been configured to broadcast traffic when it doesn't recognize the presumed address of the destination subject (in which case the information is broadcast out all TOE interfaces that are not configured as part of a virtual circuit) **AND all of the information security attribute values are unambiguously permitted by the ACL rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by an authorized administrator.**

Access Control Lists (ACLs) consist of access rules and are used to perform packet filtering and forwarding decisions on incoming traffic. For example, each packet arriving on an ingress port is compared to the ACL applied to that port and is either permitted or denied. ACLs apply to all traffic. For example, if you deny all the traffic to a port, no traffic, including control packets, such as Open Shortest Path First (OSPF) or Routing Information Protocol (RIP), will reach the switch and the adjacency will be dropped. The administrator must explicitly allow those types of packets (if desired).

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

7.1.3 Identification and Authentication

The TOE requires users to provide unique identification and authentication data before any administrative access to the system is granted. The TSF permits traffic flow through the switch as allowed by the switch traffic flow SFP for unidentified and unauthenticated subjects. The TOE can detect unsuccessful user authentication attempts and will deny the new session if the number of consecutive unsuccessful authentication attempts meets or surpasses the number specified by the administrator. The TOE can also be configured to disable a user account if the number of consecutive unsuccessful authentication attempts meets or surpasses the number specified by the administrator when a user is attempting to establish a new session (includes both SSH and non-SSH interfaces). The default administrator account and failsafe accounts are never locked out.

The TOE is, by default, configured with two accounts, user and administrator, and can have a total of 16 user accounts.

The TOE maintains a list of user security attributes for each user which include user identity (username), authentication data (password) and role. The TOE limits the number of user accounts to 16. In addition, the TOE also maintains the following information related to user accounts: password expiry date, number of successful login attempts, and number of failed login attempts.

The TOE provides the capability to enforce strong password restrictions for all users or for specific users as configured by an administrator. An administrator can set any or all of the following password restriction parameters and the TOE will enforce these restrictions.

- Minimum password length between 8 and 32 characters;
- Password must not be one of the previous passwords recorded (checks new password against the previous 5 passwords recorded);
- Password includes at least 2 characters from each of the following sets:
  - Uppercase characters (A-Z)
  - Lowercase characters (a-z)
  - Numeric characters (0-9)
  - Non-alphanumeric characters [('(', '!', '@', '#', '$', '%', '^', '*', ')')].

The TOE handles authentication failure in different ways on different interfaces:

- CLI: users can re-try logging in through the serial console or via a remote console; this is subjected to a set number of retry login attempts based on a value configured by an administrator, after which the user triggers a lockout if too many fail attempts are performed Web GUI, SNMP, and XML/Web Services: User logins through these system are subjected to a set number of retry login attemps based on a value configured by an administrator, after which the user is disconnected if too many fail attempts are performed

TOE Security Functional Requirements Satisfied: FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UID.1.

7.1.4 Security Management

The TOE is managed through a Command Line Interface (CLI). This interface is accessible through remote sessions, as well as a local terminal console (a management console). Through this interface all management can be performed, including user management and the configuration of the switch functions.

The TOE supports two roles: User and Administrator. Below is the description for each role.

User: A user has viewing access to all manageable parameters, with the exception of the User account database and the Simple Network Management Protocol (SNMP) community strings. A user-level account can change the password assigned to the account name and use the ping command to test device accessibility. The ping command is used to test for connectivity to a specific host. The ping command is available for both the user and administrator privilege level.

Administrator: The system must have at least one administrator account; the command will fail if an attempt is made to delete the last administrator account on the system. Administrators are allowed access to all Switch functions, (i.e. configuration commands) and can view and change all switch parameters. They can also add and delete users and change the password associated with any account name. You must have administrator privileges to change passwords for accounts other than your own, view accounts that have been created, delete user accounts.

The CLI is accessible through a remote console, as well as a local terminal console (a management console) via a serial port. Through this interface all management can be performed, including user management and the configuration of the switch functions**.** Only administrators will be given accounts on the appliance and must provide unique identification and authentication data in order to access the TOE and its management functions.

The Web GUI, called "ScreenPlay", consists of Adobe Flash web applications that are served to users connecting to the switch via HTTPS. ScreenPlay provides a subset of the full configuration functionality available via the CLI.

The XML/Web Services interface is accessible via HTTPS. It allows arbitrary external programs to administer the switch (assuming that they are properly authenticated) by exposing the switch's management functions as XML-based WebServices APIs.

The Time Stamp interface is accessible via the kernel of the operating system. It allows for a reliable source of synchronizing the internal clock of the EXOS through the hardware of the client machine.

Only authorized administrators have the ability to modify ACLs. Permissive default values are provided for security attributes that are used to enforce the SFP. If no action is specified in the ACL rule, the packet is permitted by default.

Only authorized administrators can perform the operations identified in Table 9 using the CLI, Web GUI, XML/Web Services, or SNMP interfaces.

The TOE provides an interface to perform all of the security management functions identified in the Section 6.2.4.

TOE Security Functional Requirements Satisfied: FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

7.1.5 Protection of the TSF

The TOE provides a reliable time stamp using the hardware clock that is located in the IT environment.

TOE Security Functional Requirements Satisfied: FPT_STM.1.

7.1.6 TOE Access

The TOE shall be configured to display a logon banner (showing an administrator-configured message) when any user attempts to access the management interfaces of the system.

TOE Security Functional Requirements Satisfied: FTA_TAB.1.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, version 3.1 revision 3.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat and assumption that compose the Security Target. Sections 8.2.1, and 8.2.2 demonstrate that 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 12 displays the mapping of threats to objectives.

Table 12 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.MEDIATE An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.	O.MEDIATE The TOE will mediate the flow of information from users on a connected network to users on another connected network as defined by administrator-configured policies/routing information.	O.MEDIATE counters this threat by mediating the flow of information from users on a connected network to users on another connected network.
T.NOAUDIT A user may not be accountable for his actions due to his actions not being recorded or due to an administrator not reviewing the audit records.	O.ACCOUNT The TOE must provide user accountability for information flows through the TOE and for authorized administrators' use of security functions related to audit.	O.ACCOUNT counters this threat by providing user accountability for information flows through the TOE and for authorized administrators' use of security functions related to audit.
	OE.AUDREV The TOE administrators will be trained to periodically review the audit records generated by the TOE.	OE.AUDREV counters this threat by providing a means to record and audit trail of security-related events, with accurate dates and times.
	OE.SYSLOG The TOE operating environment will include a syslog server to provide storage for audit records.	OE. SYSLOG counters this threat by ensuring that the operating environment will provide a syslog server to provide a sufficient amount of persistent storage for the audit events.
	OE.TIME The TOE will have access to a hardware clock from the TOE environment.	OE.TIME counters this threat by ensuring that the operating environment will provide a hardware clock used by the TOE to provide a reliable time stamp

		when generating the audit records.
	O.AUDIT The TOE must provide a means to record an audit trail of security-related events, with accurate dates and times.	O.AUDIT counters this threat by providing a means to record and audit trail of security-related events, with accurate dates and times.
T.NOMGMT An authorized administrator is not able to manage the TOE security functions and data which results in the TOE being configured in an insecure manner.	O.ADMIN The TOE must provide services that allow effective management of its functions and data.	O.ADMIN counters this threat by requiring the TOE to provide management services that allow administrators to manage the security functions and data.
T.PRIV An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data, inappropriately changing the configuration data for TOE security functions.	O.ACCESS The TOE must allow only authorized users and processes (applications) to access protected TOE functions and data.	O.ACCESS counters this threat by only allowing authorized users and processes (applications) to access protected TOE functions and data.
	O.IDAUTH The TOE must require that all administrative users be identified and authenticated prior to obtaining administrative access.	O.IDAUTH counters this threat by ensuring that all users and administrators must be authenticated and identified before allowing use of the TOE or its resources.
	OE.IDAUTH The TOE operating environment shall provide the ability to uniquely identify and authenticate remote users.	OE.IDAUTH counters this threat by providing the technology to identify and authenticate all remote users and administrators before allowing use of the TOE or its resources.
	O.PROTECT The TOE must protect itself from unauthorized access to its functions and data.	O.PROTECT counters this threat by requiring the TOE to protect itself from unauthorized access to its functions and data.
	OE.PROTECT The TOE operating environment shall provide the ability to protect the data in transit from unauthorized modifications.	The OE.PROTECT objective ensures that the data in transit is protected from unauthorized inspection or tampering by individuals or applications.

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 Assumptions

Table 13 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.AUDREV The TOE administrators will periodically review the audit records generated by the TOE.	OE.AUDREV The TOE administrators will be trained to periodically review the audit records generated by the TOE.	OE.AUDREV satisfies this assumption by requiring that training provided to the TOE administrators will include instructions to periodically review the audit records.
A.FLOW The TOE will be placed in a network infrastructure such that information to be controlled will always flow through the TOE.	OE.FLOW The network infrastructure in which the TOE is placed must be installed, administered and operated in a manner that ensures all information to be controlled flows through the TOE.	OE.FLOW satisfies this assumption by ensuring that the network infrastructure in which the TOE is installed, administered and operated ensures that all information to be controlled flows through the TOE.
A.GENPUR The TOE does not have the ability to run general purpose applications and does not host public data.	OE.GENPUR The TOE will not execute general purpose applications and the TOE does not host public data.	OE.GENPUR satisfies this assumption by ensuring that the TOE will not execute general purpose applications or host public data.
A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	OE.PHYS Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.	OE.PHYS satisfies this assumption by ensuring that those responsible for the TOE ensure that those parts of the TOE critical to security policy are protected from any physical attack.
A.NOEVIL The authorized administrators are competent, not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by TOE documentation.	OE.MANAGE Authorized administrators are trained, non-hostile and follow all administrator guidance.	OE.MANAGE satisfies this assumption by ensuring that authorized administrators are non-hostile and follow all administrator guidance.
A.EXCLUSIVE All administrative interfaces are not accessible to non-administrators and only administrators have access to the administrative interfaces to ensure the network is secure.	OE.ADMIN The administrator must not be careless, negligent, or willfully hostile; must be appropriately trained; and must follow all guidance.	OE.ADMIN upholds this assumption by ensuring that administrators are willfully not hostile and properly trained to not grant users without privileges to access administrative interfaces.

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 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target.

8.3.1 Security Functional Requirements Rationale

Table 14 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE must allow only authorized users and processes (applications) to access protected TOE functions and data.	FIA_AFL.1 Authentication Failure Handling	FIA_AFL.1 supports this objective by ensuring that the TOE will detect an administrator specified number of unsuccessful authentication attempts related to a user's attempt or processes (applications) attempt to logon during the current session and will terminate the current session when this number has been met or surpassed.
	FIA_ATD.1 User attribute definition	FIA_ATD.1 supports this objective by ensuring that the TOE will maintain a list of security attributes belonging to individual users.
	FIA_SOS.1 Verification of secrets	FIA_SOS.1 supports this objective by ensuring that the TOE is capable of enforcing strict password policies related to the composition of the password, password length, and password history/reuse.
	FIA_UAU.1 Timing of authentication	FIA_UAU.1 supports this objective by ensuring that the TOE will require each user to be successfully authenticated before allowing any actions on behalf of the user, except for switch traffic flow allowed by TOE policies.
	FIA_UID.1 Timing of identification	FIA_UID.1 supports this objective by ensuring that the TOE will require that each user be successfully identified before allowing any actions on behalf of the user, except for switch traffic flow allowed by TOE policies.
	FMT_MSA.1 Management of security attributes	FMT_MSA.1 supports this objective by restricting the ability to modify security attributes to administrators.
	FMT_MTD.1 Management of TSF data	FMT_MTD.1 supports this objective by ensuring that the TOE will restrict the ability to perform the operations identified in Table 9.
	FMT_SMR.1 Security roles	FMT_SMR.1 supports this objective by associating authorized users with roles, to access protected TOE functions and data.
O.ACCOUNT The TOE must provide user accountability for information flows through the TOE and for authorized administrators'	FAU_GEN.1 Audit data generation	FAU_GEN.1 supports this objective by providing an audit trail listing all security-relevant user and administrator actions on the TOE and on the information passing through the TOE.

Objective	Requirements Addressing the Objective	Rationale
use of security functions related to audit.	FAU_SAR.1 Audit review	FAU_SAR.1 supports this objective by presenting the audit records in a readable format so that authorized administrators can read all audit records.
	FPT_STM.1 Reliable time stamps	FPT_STM.1: The TOE provides a reliable time stamp for use in generating audit records so that a timeline of events can be created to provide user accountability. The TOE relies upon the IT environment to provide the hardware clock.
O.ADMIN The TOE must provide services that allow effective management of its functions and data.	FMT_MSA.1 Management of security attributes	FMT_MSA.1 supports this objective by restricting the ability to modify security attributes to administrators.
	FMT_MSA.3 Static attribute initialisation	FMT_MSA.3 supports this objective by allowing administrators to specify alternative values to override the default restrictive or permissive values.
	FMT_MTD.1 Management of TSF data	FMT_MTD.1 supports this objective by ensuring that the TOE will restrict the ability to perform the operations identified in Table 9.
	FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 supports this objective by providing administrators the capability to: • modify switch configuration • manage user accounts • modify the system time • manage ACL rules • terminate process • modify the number of failed logins before terminating a session or locking an account • modify the password restrictions policy
	FMT_SMR.1 Security Roles	FMT_SMR.1 supports this objective by maintaining the roles of User and Administrator.

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT The TOE must provide a means to record an audit trail of security-related events, with accurate dates and times.	FAU_GEN.1 Audit data generation	FAU_GEN.1 supports this objective by providing an audit trail listing all security-relevant user and administrator actions on the TOE and on the information passing through the TOE. The TOE generates an audit record of all security relevant user actions which includes the date and time of the event.
	FPT_STM.1 Reliable time stamps	FPT_STM.1: The TOE provides a reliable time stamp for its own use. The TOE relies upon the IT environment to provide the hardware clock.
O.IDAUTH The TOE must require that all administrative users be identified and authenticated prior to obtaining administrative access.	FIA_UAU.1 Timing of authentication	FIA_UAU.1 supports this objective by ensuring that the TOE will require each user to be successfully authenticated before allowing any administrative actions on behalf of the user.
	FIA_UID.1 Timing of identification	FIA_UID.1 supports this objective by ensuring that the TOE will require that each user be successfully identified before allowing any administrative actions on behalf of that user.
O.MEDIATE The TOE will mediate the flow of information from users on a connected network to users on another connected network as defined by administrator-configured policies/routing information.	FDP_IFC.1 Subset information flow control	FDP_IFC.1 supports this objective by ensuring that the TOE enforces the information flow control policy on all IT entities sending network traffic and switching and routing information through the TOE.
	FDP_IFF.1 Simple security attributes	FDP_IFF.1 supports this objective by ensuring that the TOE identifies the attributes of the users sending and receiving the information in the Switch Traffic Flow SFP, as well as the attributes for the information itself. The policy is defined by the requirement saying under what conditions information is permitted to flow.
O.PROTECT The TOE must protect itself from unauthorized access to its functions and data.	FIA_AFL.1 Authentication failure handling	FIA_AFL.1 supports this objective by ensuring that the TOE will detect an administrator specified number of unsuccessful authentication attempts related to a user's attempt or processes (applications) attempt to logon during the current session and will terminate the current session when this number has been met or surpassed.

Objective	Requirements Addressing the Objective	Rationale
	FIA_ATD.1 User attribute definition	FIA_ATD.1 supports this objective by ensuring that the TOE will maintain a list of security attributes belonging to individual users.
	FIA_SOS.1 Verification of secrets	FIA_SOS.1 supports this objective by ensuring that the TOE is capable of enforcing strict password policies related to the composition of the password, password length, and password history/reuse.
	FIA_UAU.1 Timing of authentication	FIA_UAU.1 supports this objective by ensuring that the TOE requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of the user.
	FIA_UID.1 Timing of identification	FIA_UID.1 supports this objective by ensuring that the TOE requires that each user be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
	FTA_TAB.1 Default TOE access banners	FTA_TAB.1 supports this objective by allowing the administrator to configure to the TOE to display a warning message prior to the login prompt of each session.

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

8.4 Security Assurance Requirements Rationale

EAL3+ was chosen to provide a moderate level of assurance that is consistent with good commercial practices. As such minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the TOE may operate in a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL3+ the TOE will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.4.1 Requirement Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 15 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 15 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	The TOE relies upon the BlackDiamond or Summit Switch to provide a hardware clock.
FAU_SAR.1	FAU_GEN.1	✓	
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	
	FMT_MSA.3	✓	
FIA_AFL.1	FIA_UAU.1	✓	
FIA_ATD.1	None	✓	
FIA_SOS.1	None	✓	
FIA_UAU.1	FIA_UID.1	✓	
FIA_UID.1	None	✓	
FMT_MSA.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
	FDP_ACC.1 or FDP_IFC.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	✓	
FMT_SMR.1	FIA_UID.1	✓	
FPT_STM.1	None	✓	
FTA_TAB.1	None	✓	

9 Acronyms

This section describes the acronyms used in this document.

Table 16 – Acronyms

Acronym	Definition
ACL	Access Control List
API	Application Programming Interface
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
EPM	EXOS Process Manager
GigE	Gigabit Ethernet
GUI	Graphical User Interface
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
EPM	EXOS Process Manager
GigE	Gigabit Ethernet
GUI	Graphical User Interface
HTTP	Hypertext Transport Protocol
HTTPS	Secure HTTP
ICMP	Internet Control Message Protocol
I/O	Input/Output
IOB	Input/Output Blade; Input/Output Module
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
MM	Management Module
MSM	Management Switch Fabric Module
N/A	Not Applicable
NTP	Network Time Protocol
NVRAM	Non-volatile Random Access Memory
OS	Operating System

Acronym	Definition
OSP	Organizational Security Policy
OSPF	Open Shortest Path First
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
RIP	Routing Information Protocol
SAP	Service Advertising Protocol
SF	Switch Fabric
SFP	Security Function Policy
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TACACS+	Terminal Access Controller Access-Control System Plus
TCP	Transport Control Protocol
TOE	Target of Evaluation
TOS	Type of Service
TSF	TOE Security Functions
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
XML	eXtensible Markup Language
TOS	Type of Service

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