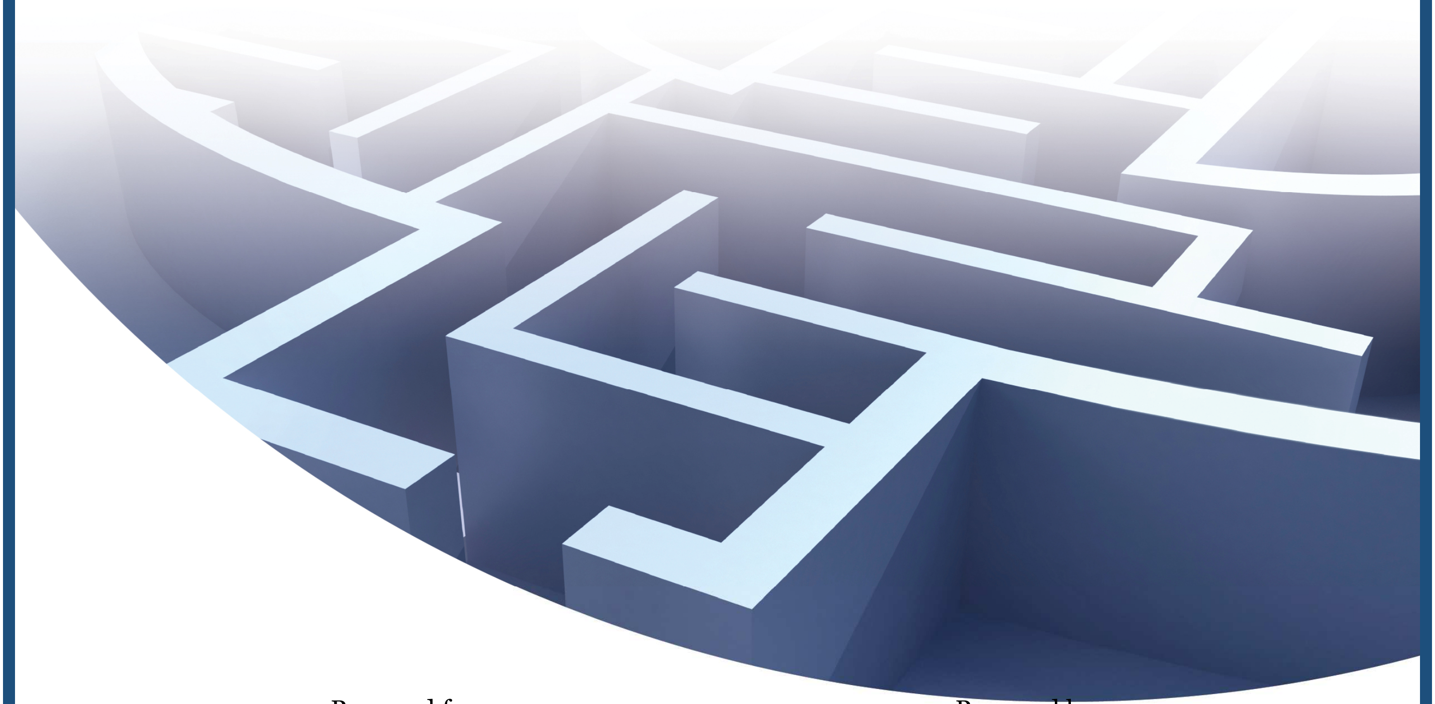
Crossbeam Systems, Inc.

X-Series Platform with XOS v9.9.0 on X60 and X80-S Chassis Hardware Version: CPM-9600, APM-9600, NPM-9610, and NPM-9650

Security Target

Evaluation Assurance Level (EAL): EAL4+
Document Version: 0.10



Prepared for:

crossbeam

Crossbeam Systems, Inc.
80 Central Street
Boxborough, MA 01719
United States of America

Phone: +1 (978) 318-7500

http://www.crossbeam.com

Prepared by:

Corsec

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy, Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
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 TOE is the Crossbeam X-Series Platform with XOS v9.9.0 on X60 and X80-S Chassis, and will hereafter be referred to as the TOE throughout this document. The TOE is a platform for consolidating and managing multiple security applications on a single platform. The platform provides the capability for multiple levels of redundancy and failover via the use of hot-swappable hardware modules. All inter-module communications are consolidated to a common backplane.

Three chassis are included for this evaluation: the X80-S-AC, X80-S-DC, and X60. The X80 chassis can hold up to fourteen blades, while the X60 chassis can hold up to seven. The two X80 chassis are identical except that the X80-S-AC uses AC power adapters, whereas the X80-S-DC uses DC power adapters.

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), 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 Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and 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	Crossbeam Systems, Inc. X-Series Platform with XOS v9.9.0 on X60 and X80-S Chassis Security Target
ST Version	Version 0.10
ST Author	Corsec Security, Inc.
ST Publication Date	2012-06-26
TOE Reference	Crossbeam X-Series Platform with XOS v9.9.0 on X60 and X80-S Chassis (kit 8) Hardware Version: CPM-9600, APM-9600, NPM-9610, and NPM-9650

ST Title	Crossbeam Systems, Inc. X-Series Platform with XOS v9.9.0 on X60 and X80-S Chassis Security Target
FIPS[1] 140-2 Status	Level 2, Validated crypto module, Certificate No. [xxx]
Keywords	XOS, X80-S, X60, Crossbeam, security appliance consolidation

1.3 PP Conformance

This Security Target does not fully conform to any protection profile, but does claim several SFRs from the U.S.[2] Government Security Requirements for Network Devices Protection Profile, 10 December 2010, Version 1.0 (NDPP). The SFRs from the NDPP that this Security Target claims include:

- FAU_GEN.1 Audit data generation,
- FCS_CKM.1 Cryptographic key generation,
- FCS_COMM_PROT_EXT.1 Communications Protection,
- FCS_COP.1 Cryptographic operation,
- FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation),
- FIA_PMG_EXT.1 Password Management,
- FIA_UAU_EXT.5 Extended: Password-based Authentication Mechanism,
- FIA_UAU_EXT.7 Protected Authentication Feedback,
- FMT_SMF.1 Specification of management functions,
- FMT_SMR.1 Security roles,
- FPT_PTD.1 Management of TSF DATA (for reading of authentication data),
- FPT_STM.1 Reliable time stamps, and;
- FTA_TAB.1 Default TOE Access Banners.

1.4 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 X-Series platform consolidates multiple security applications onto a single multifunction device. The applications that can be installed on the Crossbeam platform include antivirus, firewall, spam filtering, Intrusion Prevention System (IPS), proxy, and web content gateways. A full list of supported applications can be found on Crossbeam's website: http://www.crossbeam.com and clicking on the Applications tab.

The platform is composed of a combination of hot-swappable modules seated on a common backplane. The modules provide processing and storage that is used to implement the functionality of the X-Series Operating System (XOS). XOS v9.9.0 provides all of the functionality described later in this section. The modules can be one of the following three types:

- Control Processor Modules (CPMs) – provide all generic system-wide functions, including a switched Ethernet control network for all slots in the chassis, all management ports, management of the system boot process, management of insertion or removal of new modules into the system, service provisioning, Redundant Array of Independent Disks (RAID) data protection, management

[1] FIPS – Federal Information Processing Standard

[2] U.S. – United States

of alarms, system health monitoring, and statistical reporting. Both X-Series platforms support up to two CPMs per chassis for redundancy.

- Network Processor Modules (NPMs) – provide network connectivity, handle traffic flows into and out of the system, and make load-balancing decisions. X60 platforms can support up to two NPMs, while the X80-S supports up to four. Multiple NPMs can provide failover in the event that one of the NPMs suffers a failure.
- Application Processor Modules (APMs) – host security applications and provide application-level processing of traffic flows. All traffic is load balanced among APMs by the NPM. Incoming traffic is received from the NPMs, and outgoing traffic is returned to the NPMs. The X60 supports up to five APMs, while the X80-S supports up to ten. Multiple APMs can provide failover for applications. Applications are loaded from storage on the CPM, so an APM running one application can be switched to run a different, more critical application immediately when a failure occurs.

The CPM communicates to the other modules via a dual-redundant, private, switched control plane. The CPM contains the switching elements with all point-to-point connections from each of the other modules connecting through the backplane connector. All modules run on independent blades that are inserted into the chassis backplane.

The TOE uses flows to provide load balancing for Virtual Application Processors (VAPs). A VAP is the application operating environment running on an APM, consisting of the OS, the system software, and the application installed and running on the APM. Flows are rules that define the path that information takes once it reaches the TOE. The path is the series of APMs that information flows through, and the order that each VAP is visited. Paths can define serial information flows where traffic must return from one APM before being forwarded to the next, and parallel information flows where traffic is sent to multiple APMs simultaneously.

Flows are provided by physical interfaces, circuits, and logical interfaces:

- Physical interfaces are the actual ports on the NPM that receive traffic from external entities.
- Circuits provide the path that packets follow from the physical interfaces to the VAP groups. A VAP group is a collection of VAPs configured with identical policies and running the same application. Circuits can also connect VAPs within a VAP group and different applications in separate VAP groups.
- Logical interfaces have one or more physical interfaces mapped to them. The logical interface can move to a different physical interface in the event of a link failure. Logical interfaces are used to represent a single VLAN or a range of VLANs associated with one or more physical interfaces.

The TOE is primarily configured and managed with an XOS Command Line Interface (CLI) that administrators access via Secure Shell (SSH). The CLI offers a robust set of commands that can be used to manage all portions of the TOE. XOS also provides a Unix CLI that is excluded from the TOE boundary and inaccessible in the CC-approved mode of operation.

The TOE offers multiple layers of redundancy. The CPM, NPM, and APM modules can be configured to provide failover when an individual module fails. Modules are hot-swappable and can be replaced as needed to ensure a working configuration. A backup instance of the TOE can be brought online to provide redundancy in the event of a catastrophic failure that brings down the entire TOE. Configurations are synchronized across multiple instances of the TOE via Virtual Router Redundancy Protocol (VRRP).

The TOE can hold up to two CPMs, one active and one standby. The active CPM performs all CPM tasks, while the standby sits ready to take over in the event of a failure of the active CPM. CPMs exchange periodic heartbeat messages to detect a failure. If the active CPM detects a catastrophic module failure and crashes, or if the secondary CPM detects that the active CPM is no longer operational, the standby CPM takes over as active and resets the previously active CPM in an attempt to bring it back online. The CPMs swap control network Internet Protocol (IP) addresses during failover to make the process transparent to the other modules on the system.

The TOE can hold up to four NPMs, with the capability to define redundant interfaces. Redundant interfaces allow administrators to define backup interfaces in the event that the primary interface fails. Backup interfaces can exist on the same NPM, or on a different NPM for more robust failover.

The TOE can hold up to 10 APMs, each with its own VAP. The TOE supports the capability to configure VAP groups. These VAP groups provide redundancy and allow for increased throughput, as traffic can be load balanced between the VAPs in a VAP group. If an APM fails, then the other VAPs in the VAP group can take over the load for the failed APM immediately.

The TOE can failover entirely to another instance of the TOE in the same failover group[3]. A failover group is a grouping of one or more Virtual Routers (VRs). A VR is a collection of circuits and associated VAP groups spread across multiple instances of the TOE with the same group Identifier (ID). Rather than synchronize configurations across TOE instances in real time, administrators set up VRs using similar VAP groups and circuits and the same group ID on each TOE instance. This allows each instance of the TOE to be utilized at all times, rather than leaving one instance idle until a failover occurs.

Figure 1 shows the details of the deployment configuration of the TOE for single-box high availability deployments. Figure 2 shows the details of the deployment configuration of the TOE for dual-box high availability deployments. Both deployment configurations have been tested as part of the CC evaluation[4].

[3] This is called dual-box high availability. Failover of individual blades to backup blades is referred to as single-box high availability.

[4] The high availability functionality provided by FPT_FLS.1(b) and FRU_FLT.1(b) is not available when the TOE is deployed in the single-box high availability configuration.

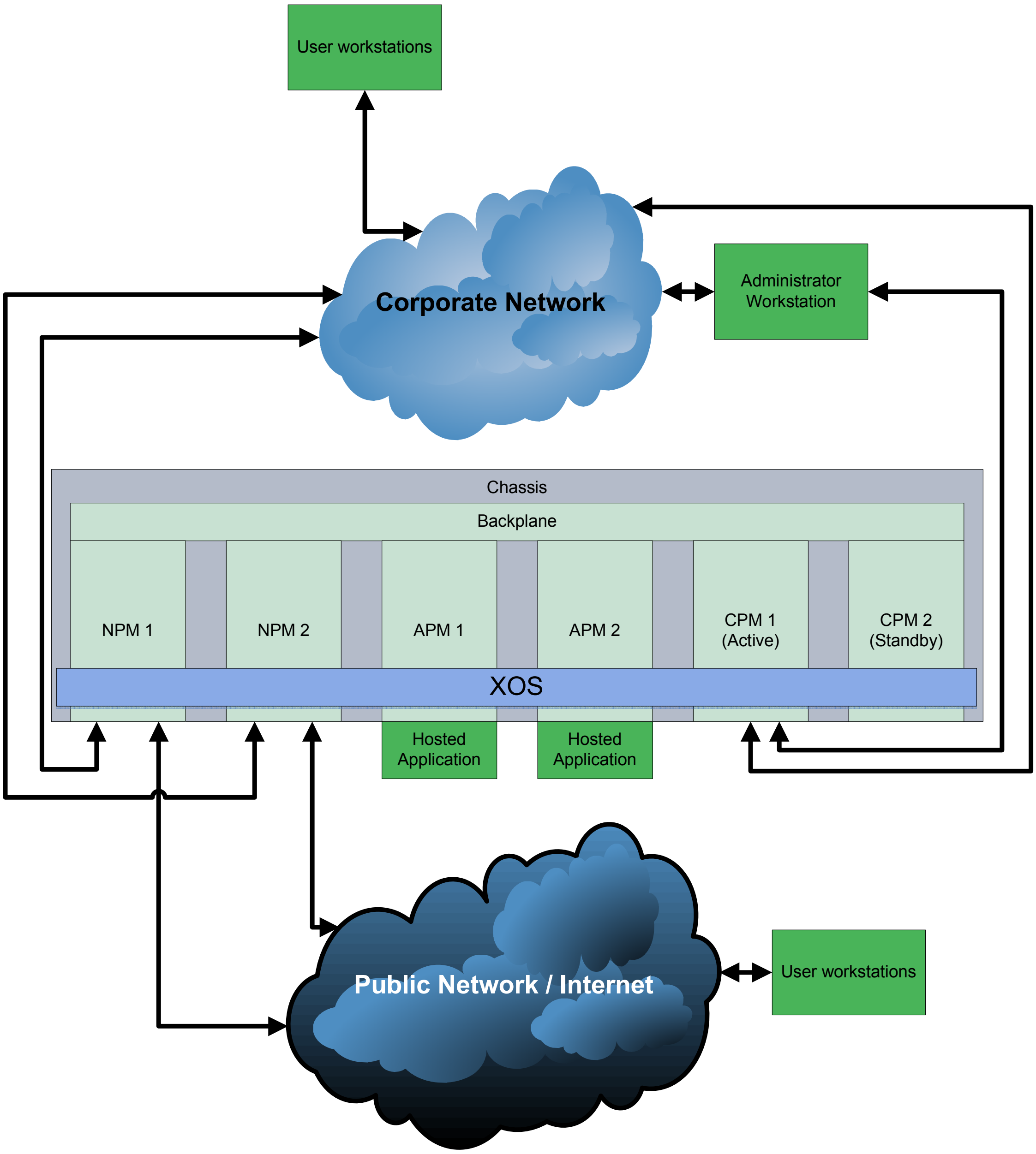


Figure 1 – Single-Box Deployment Configuration of the TOE

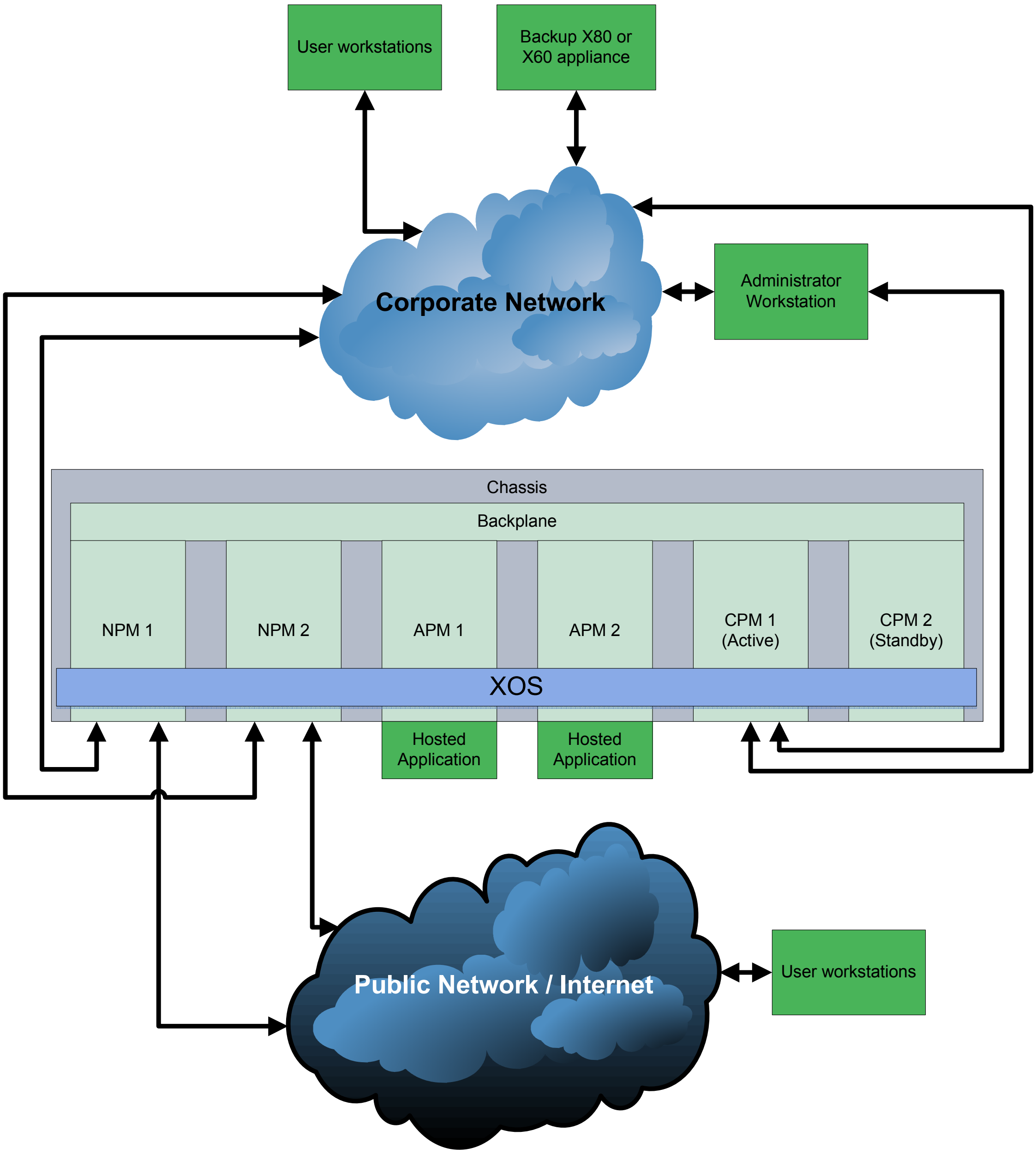


Figure 2 – Dual-Box Deployment Configuration of the TOE

1.4.1 TOE Environment

The TOE is a platform for consolidation of security applications designed to run on X60 or X80-S hardware. The TOE OS is included within the installation image and installed as part of the process of installing the TOE software.

The TOE needs the following environmental components in order to function properly:

- cables, connectors, and switching and routing devices that allow all of the TOE and environmental components to communicate with each other,

- power and cooling for the system hardware,
- an administrator workstation with an SSH client.

The TOE is intended to be deployed in a secure data center that protects physical access to the TOE. The TOE is intended to be managed by administrators operating under a consistent security policy.

The TOE is meant to host security applications on APMs. Traffic intended for these applications should be directed to the TOE so that it can be forwarded to the appropriate application. Additionally, administrators must install security applications onto the TOE in order to fully utilize the TOE for its intended function.

In order for total system failover to work properly in a dual-box high availability deployment, a backup instance of the TOE must be present on the same network as the TOE.

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.5.1 Physical Scope

Figure 3 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

The TOE is installed on custom hardware as depicted in the figure below. The TOE can be deployed in a variety of places within the network topology depending on the applications installed on the APMs. The essential physical components for the proper operation of the TOE in the evaluated configuration are

- the XOS software,
- CPM blades,
- APM blades,
- NPM blades,
- Carrier-grade X60 and X80-S chassis.

The XOS software version 9.9.0 is comprised of several Linux kernels, described in Table 2 below:

Table 2 – XOS Kernels

Module	VAP	Linux Kernel(s)	Architecture	Virtualized
CPM	n/a	2.6.18-164.2.1	x86_64	No
APM	xsve	2.6.18-164.2.1	x86_64	Yes
APM	xslinux_v5_64	2.6.18-164.2.1	x86_64	No

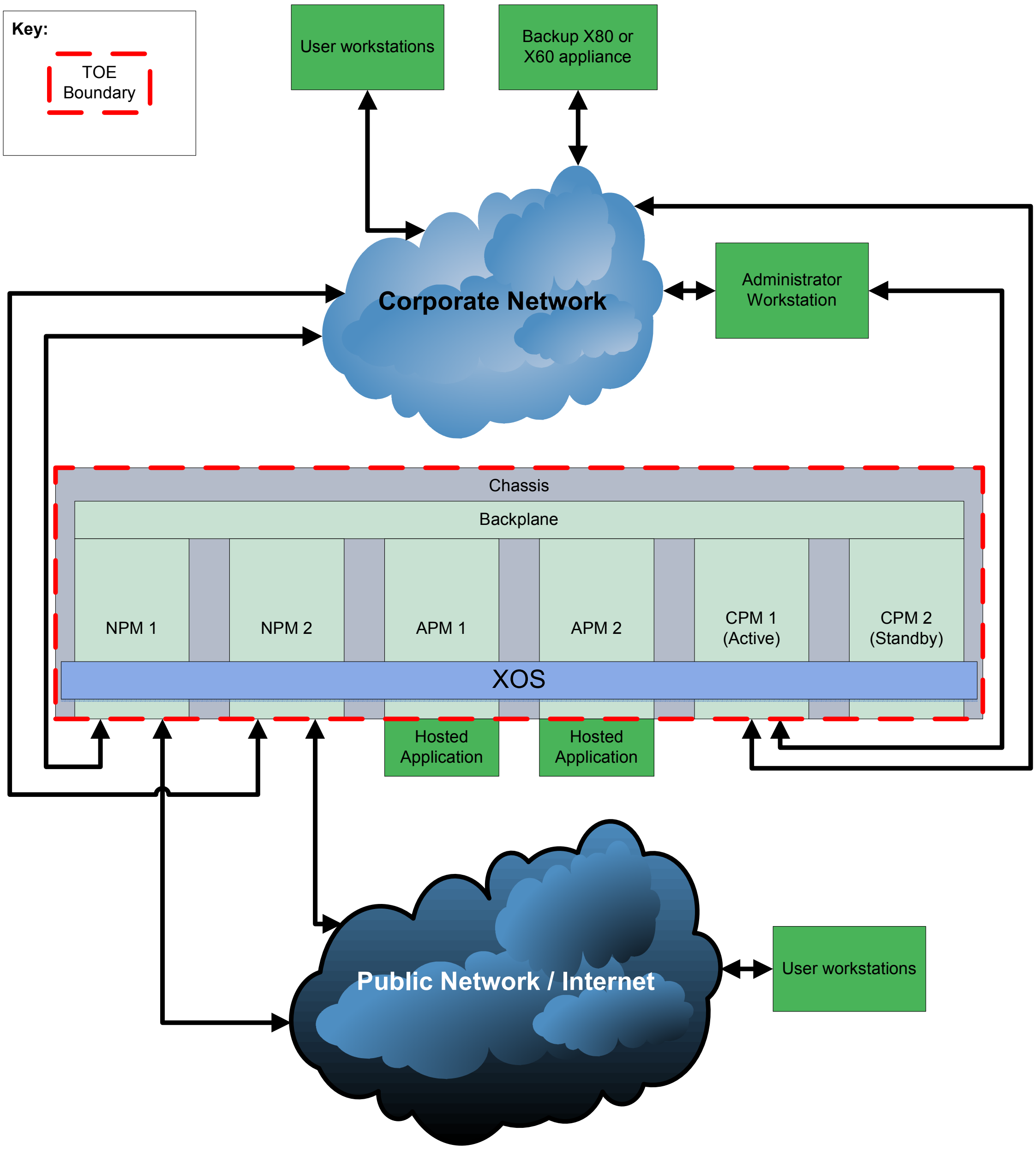


Figure 3 – Physical TOE Boundary

1.5.1.1 TOE Software and Hardware

The TOE is a combination of hardware and software. The software (excluding applications running on the APM, which are excluded from the TOE) and hardware are both purpose built and are included with the purchase of the TOE. Additional APM, NPM, and CPM modules can be purchased separately for inclusion in the TOE chassis. Slots on the X-Series platform are designed to hold specific modules. Please refer to the Crossbeam XOS Configuration Guide for more details.

1.5.1.2 Guidance Documentation

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

- Crossbeam XOS Configuration Guide
- Crossbeam XOS Command Reference Guide
- Crossbeam XOS 9.9.0 Release Notes
- Crossbeam Multi-System High Availability Configuration Guide
- X60 Platform Hardware Installation Guide
- X80-S Platform Hardware Installation Guide

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functionality (TSF)
- Resource Utilization,
- TOE Access.

1.5.2.1 Security Audit

The TOE generates audit records for administrator actions and system-level events. Audit records contain a time stamp, an event type field, and a brief description of the event. The description describes the subject and outcome of the event. Authorized administrators can review audit records from a CLI, which can be used to search and filter the results.

1.5.2.2 Cryptographic Support

The TOE implements a FIPS 140-2 validated cryptographic module that provides cryptographic services for securing management traffic.

1.5.2.3 User Data Protection

The TOE controls traffic via a set of flow rules. These flow rules comprise a Flow Security Functional Policy (SFP) that is used primarily to load balance between the APMs on the TOE. Traditional routing functionality is not provided by the TOE's Flow SFP.

1.5.2.4 Identification and Authentication

The TOE requires identification and authentication credentials from administrators before presenting any of the TOE management capabilities. Administrators are required to use a password that meets industry standard strength requirements, and can configure additional complexity rules as needed. Passwords have an expiration lifetime and must be changed at the end of that lifetime. The TOE obscures visual feedback when administrators are authenticating at the login prompt.

1.5.2.5 Security Management

The TOE offers a CLI that administrators can use to configure and manage TOE settings and the Flow SFP. Each administrator and command is assigned a permission level. The administrator's permission level must be greater than or equal to the permission level of any command for the command to execute successfully. Authorized administrators are capable of altering permission levels for administrators and commands.

1.5.2.6 Protection of the TSF

The TOE provides high availability features for module failover and full system failover. Failover allows the TOE to provide a complete set of functionality in the event of partial or total system failure. Passwords are not stored in plaintext on the TOE. The TOE provides reliable time stamps for its own use.

1.5.2.7 Resource Utilization

The TOE provides high availability features for module failover and full system failover. Failover allows the TOE to provide a complete set of functionality in the event of partial or total system failure.

1.5.2.8 TOE Access

The TOE presents a login banner warning against unauthorized access to administrators and users logging into the TOE.

1.5.3 Product Physical/Logical Features and Functionality not included in the TOE

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

- Unix command line interface,
- Applications installed on APMs,
- SNMP v1 and v2c,
- Greenlight Element Manager (GEM),
- Crossbeam X-Series Management System (XMS).

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; PP claim (none); Parts 2 and 3 Interpretations of the Common Evaluation Methodology (CEM) as of 2011-04-14 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None.
Evaluation Assurance Level	EAL4+ augmented with Flaw Remediation (ALC_FLR.2).

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[5] 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 low skill level, limited resources to alter TOE configuration settings or 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 or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)
- Environmental factors that could affect the operation of the TOE.

All are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[6] and 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.CRITICAL_FAILURE	An unidentifiable threat may cause the TOE to experience a failure of a crucial component that prevents users and administrators from being able to access TOE functionality.
T.INTERCEPT	An unauthorized person or IT entity may be able to view or modify management traffic that is sent between remote administrators and the TOE.
T.MEDIAT	An unauthorized person may send information through the TOE that results in the exploitation of resources on the TOE or the systems the TOE is meant to protect.
T.NO_AUDIT	An attacker may perform security-relevant operations on the TOE without being held accountable for it.
T.UNAUTH	A user or administrator may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.

[5] IT – Information Technology

[6] TSF – TOE Security Functionality

3.2 Organizational Security Policies

This Security Target defines no OSPs.

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 5 – Assumptions

Name	Description
A.LOCATE	The TOE is located within a controlled access facility.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NETCON	The TOE environment provides the network connectivity required to allow the TOE to perform its intended function.
A.NOEVIL	The administrators who manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.
A.NTP	The TOE environment should provide protection to ensure that Network Time Protocol (NTP) information communicated from an NTP source to the TOE cannot be modified by an attacker.
A.ROBUST_ENVIRONMENT	The operational environment is at least as robust as the TOE.

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 6 – Security Objectives for the TOE

Name	Description
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and security attributes, ensuring that TOE administrators with the appropriate privileges and only those TOE administrators may exercise such control.
O.AUDIT	The TOE must maintain a record of security-relevant events that occur on the TOE, and make that record available for review by TOE administrators.
O.AUTHENTICATE	The TOE must require administrators to authenticate before gaining access to the TOE interfaces.
O.ENCRYPT	The TOE must protect the confidentiality of its dialogue with authorized remote administrators. Confidentiality is provided by encryption of management traffic.
O.FAIL_SECURE	The TOE will provide mechanisms to allow for secure failure and recovery.
O.MEDIAT	The TOE must mediate the flow of all information between clients and APMs.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

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

Table 7 – IT Security Objectives

Name	Description
OE.NTP	NTP Servers providing time information to the TOE are on the local network and inaccessible to non-administrators.
OE.ROBUST_ENVIRONMENT	The operational environment that supports the TOE for enforcement

Name	Description
	of its security objectives is at least the same level of robustness as the TOE.
OE.TRAFFIC	The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.

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 8 – Non-IT Security Objectives

Name	Description
NOE.MANAGE	Sites deploying the TOE provide competent TOE administrators who ensure the system is used securely.
NOE.NOEVIL	Sites using the TOE ensure that the TOE administrators are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.
NOE.PHYSICAL	The TOE is used in a physically secure site that protects it from interference and tampering by untrusted subjects.

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 9 identifies all extended SFRs implemented by the TOE.

Table 9 – Extended TOE Security Functional Requirements

Name	Description
FCS_COMM_PROT_EXT.1	Communications Protection
FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)
FIA_PMG_EXT.1	Password Management
FIA_UAU_EXT.5	Extended: Password-based Authentication Mechanism
FIA_UAU_EXT.7	Protected Authentication Feedback
FPT_PTD.1	Management of TSF Data (for reading authentication data)

5.1.1 Communications Protection

Family Behaviour

This family defines the requirements for protecting remote management sessions between the TOE and an authorized administrator. This family describes the types of protection that will be applied to the traffic (IPSec, SSH, or TLS).

Component Leveling

Figure 4 – Communication Protection family decomposition

FCS_COMM_PROT_EXT.1 Communication Protection specifies the protections required for management sessions with the TOE.

Management: FCS_COMM_PROT_EXT.1

- Management of certificates used to establish IPSec and TLS sessions.

Audit: FCS_COMM_PROT_EXT.1

- Establishment of a cryptographic session.

FCS_COMM_PROT_EXT.1 Communications Protection

Hierarchical to: No other components

FCS_COMM_PROT_EXT.1.1

The TSF shall protect communications using [selection: IPsec, SSH] and [selection: TLS/HTTPS, no other protocol].

Dependencies: No dependencies

5.1.2 Extended: Cryptographic Operation (Random Bit Generation)

Family Behaviour

This family defines the requirements for random bit generation by a Pseudo-Random Number Generator (PRNG). This family specifies the allowed PRNG algorithms and specifies a minimum of 64 bits of entropy for any seeds used in the creation of random numbers.

Component Leveling

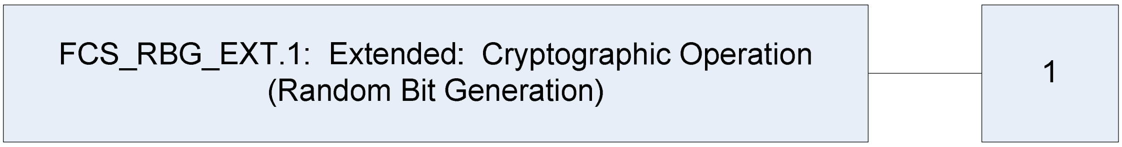

FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)
1

Figure 5 – Extended: Cryptographic Operation (Random Bit Generation) family decomposition

FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation) specifies the requirements for PRNGs used by the TOE.

Management: FCS_RBG_EXT.1

- No management activities foreseen.

Audit: FCS_RBG_EXT.1

- Errors resulting from the failure of a continuous random number generation test.

FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)
Hierarchical to: No other components

FCS_RBG_EXT.1.1

The TSF shall perform all random bit generation (RBG) services in accordance with [selection, choose one of: NIST Special Publication 800-90 using [selection: Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES), Dual_EC_DRBG (any)]; FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES] seeded by an entropy source that accumulated entropy from at least one independent TSF-hardware-based noise source.

FCS_RBG_EXT.1.2

The deterministic RBG shall be seeded with a minimum of [selection, choose one of: 128 bits, 256 bits] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

Dependencies: No dependencies

5.1.3 Password Management

Family Behaviour

This family defines the requirements for password strength on the TOE. These requirements also specify that passwords must have a maximum lifetime, and new passwords must have a minimum of four characters different from the previous password. Maximum passwords have no limit on complexity or length and can be settable by an administrator, but minimum requirements include the use of at least:

- one upper-case letter,
- one lower-case letter,
- one number,
- one special character (such as !, @, #, $, etc.), and;
- eight characters in total length.

Component Leveling

Figure 6 – Password Management family decomposition

FIA_PMG_EXT.1 Password Management specifies the requirements for passwords enforced by the TOE.

Management: FIA_PMG_EXT.1

- Management of password requirements.

Audit: FIA_PMG_EXT.1

- There are no auditable events foreseen.

FIA_PMG_EXT.1 Password Management
Hierarchical to: No other components
FIA_PMG_EXT.1.1

The TSF shall provide the following password management capabilities for administrative passwords:

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”);
2. Minimum password length shall settable by the Security Administrator, and support passwords of 8 characters or greater;
3. Passwords composition rules specifying the types and number of required characters that comprise the password shall be settable by the Security Administrator.
4. Passwords shall have a maximum lifetime, configurable by the Security Administrator.
5. New passwords must contain a minimum of 4 character changes from the previous password.

Dependencies: No dependencies

5.1.4 Extended: Password-based Authentication Mechanism

Family Behaviour

This family ensures that the TOE provides at a minimum a local, password-based authentication mechanism for administrators and allows other authentication methods to be specified. This family also ensures that administrators with expired passwords acquire new passwords before they are allowed to log into the TOE again.

Component Leveling

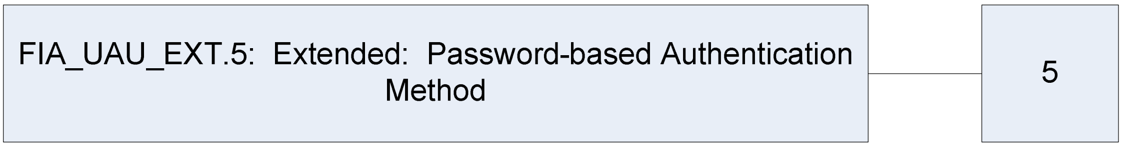

FIA_UAU_EXT.5: Extended: Password-based Authentication Method
5

Figure 7 – Extended: Password-based Authentication Mechanism family decomposition

FIA_UAU_EXT.5 Extended: Password-based Authentication Mechanism specifies the requirements for authentication mechanisms used by the TOE.

Management: FIA_UAU_EXT.5

- There are no management activities foreseen.

Audit: FIA_UAU_EXT.5

- There are no auditable events foreseen.

FIA_UAU_EXT.5 Extended: Password-based Authentication Mechanism

Hierarchical to: No other components

FIA_UAU_EXT.5.1

The TSF shall provide a local password-based authentication mechanism, [selection: [*assignment: other authentication mechanism(s)*], none] to perform user authentication.

FIA_UAU_EXT.5.2

The TSF shall ensure that users with expired passwords are [selection: required to create a new password after correctly entering the expired password, locked out until their password is reset by an administrator].

Dependencies: No dependencies

5.1.5 Protected Authentication Feedback

Family Behaviour

This family ensures that the TOE provides either obscured feedback or no feedback to users when authentication at the local console is in progress.

Component Leveling

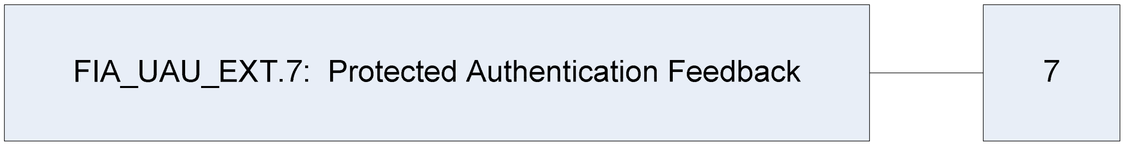


Figure 8 – Protected Authentication Feedback family decomposition

FIA_UAU_EXT.7 Protected Authentication Feedback specifies the requirements for feedback of a user's password when the user is authenticating.

Management: FIA_UAU_EXT.7

- There are no management activities foreseen.

Audit: FIA_UAU_EXT.7

- There are no auditable events foreseen.

FIA_UAU_EXT.7 Protected Authentication Feedback
Hierarchical to: No other components
FIA_UAU_EXT.7.1

The TSF shall provide only obscured feedback to the user while the authentication is in progress at the local console.

Dependencies: No dependencies

5.1.6 Management of TSF Data (for reading of authentication data)

Family Behaviour

This family ensures that passwords stored on the TOE are not stored in plaintext.

Component Leveling

FPT_PTD.1: Management of TSF Data (for reading of authentication data)
1

Figure 9 – Management of TSF Data (for reading of authentication data) family decomposition

FPT_PTD.1 Management of TSF Data (for reading of authentication data) requires the TOE to obfuscate passwords stored on the TOE.

Management: FPT_PTD.1

- There are no management activities foreseen.

Audit: FPT_PTD.1

- There are no auditable events foreseen.

FPT_PTD.1 Management of TSF Data (for reading of authentication data)
Hierarchical to: No other components
FPT_PTD.1.1
The TSF shall prevent reading of the plaintext passwords.
Dependencies: No dependencies

5.2 Extended TOE Security Assurance Components

There are no extended SARs defined for this ST.

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 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 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 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.
- Some claims were pulled from the (NDPP) and were left as-is to follow the conventions within that document.

6.2 Security Functional Requirements

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

Table 10 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FAU_SAR.3	Selectable audit review		✓		
FCS_CKM.1	Cryptographic key generation		✓		
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COMM_PROT_EXT.1	Communications Protection	✓			
FCS_COP.1	Cryptographic operation		✓		
FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)	✓			
FDP_IFC.1	Subset information flow control		✓		
FDP_IFF.1	Simple security attributes		✓		
FIA_PMG_EXT.1	Password Management				

Name	Description	S	A	R	I
FIA_UAU.2	User authentication before any action				
FIA_UAU_EXT.5	Extended: Password-based Authentication Mechanism	✓	✓		
FIA_UAU_EXT.7	Protected Authentication Feedback				
FIA_UID.2	User identification before any action				
FMT_MOF.1	Management of security functions behavior	✓	✓		
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialization	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_FLS.1(a)	Failure with preservation of secure state		✓		✓
FPT_FLS.1(b)	Failure with preservation of secure state		✓		✓
FPT_PTD.1	Management of TSF Data (for reading of authentication data)				
FPT_STM.1	Reliable time stamps				
FRU_FLT.1(a)	Degraded fault tolerance		✓		✓
FRU_FLT.1(b)	Degraded fault tolerance		✓		✓
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) [*all administrator actions, access list events, flows, software events*].

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 (if applicable), 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 other audit relevant 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 [*CLI administrators with sufficient permissions (default level 0)*] with the capability to read [*all audit information*] 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

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1

The TSF shall provide the ability to apply [*searching and filtering*] of audit data based on [*a keyword string*].

Dependencies: FAU_SAR.1 Audit review

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 [*the cryptographic key generation algorithm as listed in Table 11*] and specified cryptographic key sizes [*the key sizes listed in Table 11*] that meet the following: [*the standards listed in Table 11*].

Table 11 – Cryptographic Key Generation

Key Generation Method	Cryptographic Key Size	Standards
PRNG	128 bit, 168 bit, 256 bit	ANSI X9.31

Dependencies: FCS_COP.1 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_COMM_PROT_EXT.1 Communications Protection
Hierarchical to: No other components.
FCS_COMM_PROT_EXT.1.1

The TSF shall protect communications using [SSH] and [no other protocol].

Dependencies: No dependencies

FCS_COP.1 Cryptographic operation
Hierarchical to: No other components.
FCS_COP.1.1

The TSF shall perform [*encryption and decryption of remote administrator sessions*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms listed in Table 12*] and cryptographic key sizes [*the cryptographic key sizes listed in Table 12*] that meet the following: [*the list of standards in Table 12*].

Table 12 – Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Symmetric encryption and decryption	Advanced Encryption Standard (AES)	128, 192, 256	FIPS 197 (certificate #1877 and #1878)
	Triple-Data Encryption Standard (DES)	168	FIPS 46-3 (certificate #1220 and #1221)

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Asymmetric encryption and decryption	Rivest, Shamir, Adelman (RSA)	1024, 1536, 2048, 3072, 4096	FIPS 186-2 for Sign/Verify (certificate #958 and #961)
Message digest	Secure Hashing Algorithm (SHA)	160, 224, 256, 384, 512	FIPS 180-2 (certificate #1650 and #1651)
Message authentication	Hashed Message Authentication Code (HMAC)	160, 224, 256, 384, 512	FIPS 198 (certificate #1121 and #1122)
Digital signature verification	Digital Signature Algorithm (DSA)	1024	FIPS 186-2 (certificate #587 and #590)
Random number generation	American National Standards Institute (ANSI) X9.31 Pseudo-Random Number Generator (PRNG)	N/A	X9.31 (certificate #983 and #986)

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

FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)
Hierarchical to: No other components
FCS_RBG_EXT.1.1

The TSF shall perform all random bit generation (RBG) services in accordance with [FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES] seeded by an entropy source that accumulated entropy from at least one independent TSF-hardware-based noise source.

FCS_RBG_EXT.1.2

The deterministic RBG shall be seeded with a minimum of [256 bits] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

Dependencies: No dependencies

6.2.3 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 [*Flow SFP*] on [

Subjects:

1. *User workstations sending network traffic to a VAP group on the TOE*

Information:

1. *Transmission Control Protocol (TCP)/IP traffic*

Operations:

1. *load-balance*
2. *drop*
3. *allow*
4. *pass-to-master*
5. *pass-to-vap*
6. *broadcast*
7. *bypass-tcp-flow-setup-validation*
8. *direction*
9. *skip-port-protocol*
10. *generate-reversed-flow*
11. *source-addr*
12. *destination-addr*
13. *source-port*
14. *destination-port*
15. *protocol*
16. *domain*
17. *incoming-circuit-group*
18. *timeout*
19. *trace*
20. *activate*
21. *show*

].

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 [*Flow SFP*] based on the following types of subject and information security attributes: [

Subject security attributes:

1. *Source IP address*
2. *Source port number*
3. *Domain*

Information security attributes:

1. *Source IP address*
2. *Source port number*
3. *Destination IP address*
4. *Destination port number*
5. *Protocol*

].

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: [

1. *Flow rules are applied in order of priority (highest to lowest).*
2. *If a flow rule is defined that matches the subject or information attributes, apply the relevant action (as listed in* Table 16*).*
3. *If no flow rules are defined, or none match the criteria defined, use the default flow rule:*
    a. *The IP Flow Rule action will be set to broadcast when the IP address subnet is set to a broadcast address. Secondary actions are set to default and the priority is 21.*
    b. *For other IP addresses, the action is to load balance, using the IP address as the destination address. Secondary actions are set to default and the priority is 21.*
    c. *When using the IP address with increment-per-vap, the original address is sent to VAP index 1. The next IP address in sequential order is sent to VAP index 2, and so on. The flow is not load balanced. Secondary actions are set to default, timeout is set to auto, and the priority is 21.*
    d. *When using the IP address with increment-per-vap, the IP flow rule action is set to broadcast for packets with a broadcast address. Otherwise, the default flow-rule is used. Priority is 21.*

].

FDP_IFF.1.3

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

FDP_IFF.1.4

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

FDP_IFF.1.5

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

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

6.2.4 Class FIA: Identification and Authentication

FIA_PMG_EXT.1 Password Management

Hierarchical to: No other components

FIA_PMG_EXT.1.1

The TSF shall provide the following password management capabilities for administrative passwords:

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")");
2. Minimum password length shall be settable by the Security Administrator, and support passwords of 8 characters or greater;
3. Passwords composition rules specifying the types and number of required characters that comprise the password shall be settable by the Security Administrator.
4. Passwords shall have a maximum lifetime, configurable by the Security Administrator.
5. New passwords must contain a minimum of 4 character changes from the previous password.

Dependencies: No dependencies

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 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_EXT.5 Extended: Password-based Authentication Mechanism

Hierarchical to: No other components

FIA_UAU_EXT.5.1

The TSF shall provide a local password-based authentication mechanism, [none] to perform user authentication.

Application Note: In the above component text, none refers to the lack of alternative authentication mechanisms. The TOE provides only password-based authentication of users. The SFR is written this way to conform to the SFR as written in the NDPP.

FIA_UAU_EXT.5.2

The TSF shall ensure that users with expired passwords are [required to create a new password after correctly entering the expired password].

Dependencies: No dependencies

FIA_UAU_EXT.7 Protected Authentication Feedback

Hierarchical to: No other components

FIA_UAU_EXT.7.1

The TSF shall provide only obscured feedback to the user while the authentication is in progress at the local console.

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 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 [enable, disable, modify the behaviour of] the functions [*basic commands, enabling system management, configure and manage VAP groups, configure and manage flow provisioning, configure interfaces for VAP groups, configure and manage multi-system high availability, manage configuration files, advanced commands, display configuration settings, using swatch scripts, and troubleshooting*] to [*administrators with a sufficient permission level*].

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

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1

The TSF shall enforce the [*Flow SFP*] to restrict the ability to [change_default, query, modify, delete, [*create*]] the security attributes [*Flow SFP rules*] to [*administrators with a sufficient permission level*].

Dependencies: FDP_IFC.1 Subset information flow control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1

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

FMT_MSA.3.2

The TSF shall allow the [*administrators with a sufficient permission level*] 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_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: [*management of security attributes, management of security functions behaviour*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*CLI administrators with a permission level of 0 to 15, Crypto Officer*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.2.6 Class FPT: Protection of the TSF

FPT_FLS.1(a) Failure with preservation of secure state

Hierarchical to: No other components.

FPT_FLS.1.1(a)

The TSF shall preserve a secure state when the following types of failures occur: [*failure of an APM, NPM, or CPM*].

Dependencies: No dependencies.

FPT_FLS.1(b) Failure with preservation of secure state

Hierarchical to: No other components.

FPT_FLS.1.1(b)

The TSF shall preserve a secure state when the following types of failures occur: [*failure of critical system services or components*].

Dependencies: No dependencies.

FPT_PTD.1 Management of TSF Data (for reading of authentication data)

Hierarchical to: No other components

FPT_PTD.1.1

The TSF shall prevent reading of the plaintext passwords.

Dependencies: No dependencies

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_FLT.1(a) Degraded fault tolerance
Hierarchical to: No other components.
FRU_FLT.1.1(a)

The TSF shall ensure the operation of [*all TOE functionality*] when the following failures occur: [*failure of a CPM, NPM, or APM*].

Dependencies: FPT_FLS.1(a) Failure with preservation of secure state

FRU_FLT.1(b) Degraded fault tolerance
Hierarchical to: No other components.
FRU_FLT.1.1(b)

The TSF shall ensure the operation of [*failover capabilities*] when the following failures occur: [*failure of critical system services or components*].

Dependencies: FPT_FLS.1(b) Failure with preservation of secure state

6.2.8 Class FTA: TOE Access

FTA_TAB.1 Default TOE Access Banners
Hierarchical to: No other components
FTA_TAB.1.1

Before establishing a **user/administrator** session, the TOE shall display **a Security Administrator-specified advisory notice and consent warning message** regarding unauthorized use of the TOE.

6.2.9 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 13 – Assurance Requirements summarizes the requirements.

Table 13 – 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.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM 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_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

7 TOE Summary 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 14 – 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
	FAU_SAR.3	Selectable audit review
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COMM_PROT_EXT.1	Communications Protection
	FCS_COP.1	Cryptographic operation
	FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)
User Data Protection	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Identification and Authentication	FIA_PMG_EXT.1	Password Management
	FIA_UAU.2	User authentication before any action
	FIA_UAU_EXT.5	Extended: Password-based Authentication Mechanism
	FIA_UAU_EXT.7	Protected Authentication Feedback
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles

TOE Security Function	SFR ID	Description
Protection of the TSF	FPT_FLS.1(a)	Failure with preservation of secure state
	FPT_FLS.1(b)	Failure with preservation of secure state
	FPT_PTD.1	Management of TSF Data (for reading of authentication data)
	FPT_STM.1	Reliable time stamps
Resource Utilization	FRU_FLT.1(a)	Degraded fault tolerance
	FRU_FLT.1(b)	Degraded fault tolerance
TOE Access	FTA_TAB.1	Default TOE Access Banners

7.1.1 Security Audit

The TOE records audit records for all administrator actions, access list events, flows, and software events:

- "All administrator actions" refers to any action an administrator performs via the CLI,
- "Access list events" refers to any event related to the access list that controls connectivity to the CPM. Control can govern access from networks, individual hosts, or allowed protocols.
- "Flows" refers to any event related to the flows that direct traffic to the APMs for load balancing.
- "Software events" refers to system events and operation problems generated by APMs and NPMs

The TOE audit records contain the following information:

Table 15 – Audit Record Contents

Field	Content
Time stamp	The date and time the event was recorded.
Type	What type of event (i.e. command, alarm, etc.).
Subject	The individual or entity responsible for the event.
Outcome	The results of the action that caused the event.

Administrators can review audit records via the CLI. Each CLI command is assigned a permission value from zero to fifteen. By default, all show commands have a value of 0, meaning any administrator can view the audit records by default. Administrators can later change the permissions for each show command so that only administrators with a certain access level can review audit records. By combining the show log commands with grep and search commands, administrators can perform string searching and filtering of audit records.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1, FAU_SAR.3.

7.1.2 Cryptographic Support

The TOE provides encryption and decryption of management traffic SSH sessions. All cryptography is performed by a FIPS 140-2-validated cryptographic module. ANSI X9.31 PRNG output is produced by /dev/urandom, which is seeded by at least 256 bits of entropy.

TOE Security Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM.4, FCS_COMM_PROT_EXT.1, FCS_COP.1, FCS_RBG_EXT.1.

7.1.3 User Data Protection

The TOE implements an administrator-defined Flow SFP (composed of a set of flow rules) that is used to determine how to process each network traffic flow that enters the NPMs and is destined for a VAP group. Each flow rule contains an action and a set of packet-matching criteria. The packet-matching criteria are used to apply each rule to a subset of all traffic entering the NPMs, such as those containing a certain destination port. A description of the actions can be found in Table 16.

Each IP flow rule additionally has an associated priority level. The priority level differentiates rules with overlapping criteria. Priority values can range from 0 to 31. Only priorities with range 10-20 and 25-30 are configurable. The rest are for system-use only. Flow rules are applied in order from highest-to-lowest. By default no rules are defined and no traffic can traverse the TOE.

Table 16 – Flow SFP Actions

Action	Description
load-balance	The NPM load-balances the IP flows that match the packet-matching criteria.
drop	The NPM drops all IP packets that match the packet-matching criteria.
allow	The NPM allows all IP packets that match the packet-matching criteria to pass through the VAP group and proceed to their destination IP addresses.
pass-to-master	The NPM passes the IP packets that match the packet-matching criteria to the master VAP in the VAP group.
pass-to-vap	The NPM passes the IP packets that match the packet-matching criteria to the specified VAP in the VAP group.
broadcast	The NPM broadcasts the IP packets that match the packet-matching criteria to every VAP in the VAP group.
direction	Applies an action only to IP traffic flowing in the specified direction (inbound to or outbound from the VAP group).
skip-port-protocol	Excludes the source-port number, destination-port number, and protocol number from the packet matching criteria for the flow rule.
generate-reversed-flow	Enables bi-directional IP-flow matching, meaning that criteria can be configured for both source and destination IP addresses and port numbers.
source-addr	Applies a flow rule's action only to IP packets that meet the specified source IP address.

Action	Description
destination-addr	Applies a flow rule's action only to IP packets that meet the specified destination IP address.
source-port	Applies a flow rule's action only to IP packets that meet the specified source port.
destination-port	Applies a flow rule's actions only to IP packets that meet the specified destination port.
protocol	Applies a flow rule's action only to IP packets that meet the specified protocol.
domain	Applies a flow rule's action only to IP packets that meet the specified domain.
incoming-circuit-group	Applies the flow rule's action only to IP packets that meet the specified incoming circuit group.
timeout	Sets an interval for how long an IP flow can remain idle before the NPM deletes the IP flow from the Active Flow Table.
trace	Enables or disables packet tracing for IP packets that match conditions defined in the packet matching criteria for the VAP group IP flow rule.
bypass-tcp-flow-setup-validation	Bypasses TCP validation during flow setup. Typically bypass should be set when the topology prevents a flow's bidirectional symmetry (through the chassis). When bypassed, TCP sequence numbers will be updated and FIN and RST sequence numbers will be validated before flow removal.
show	Displays the current configuration settings for the system-level IP flow rules that is being configured.
activate	Activates or deactivates (using no) the system-level IP flow rule that is being configured.

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

7.1.4 Identification and Authentication

The TOE requires successful identification and authentication of administrators before allowing access to any management functionality of the CLI. Administrators authenticate at a login prompt with a username and password. The TOE obscures visual feedback for passwords while the user or administrator is typing it at the login prompt. The TOE requires all passwords to be at least eight characters with at least one upper-case and lower-case letter, one number, and one special character. The TOE stores usernames and passwords locally.

Administrators can also define additional rules for passwords strength. Administrators are able to specify the lifetime for each password. After the lifetime is reached, the password expires and must be changed by the user or administrator during their next login. New passwords must have at least four character changes from the previous password.

TOE Security Functional Requirements Satisfied: FIA_PMG_EXT.1, FIA_UAU.2, FIA_UAU_EXT.5, FIA_UAU_EXT.7, FIA_UID.2.

7.1.5 Security Management

The TOE presents a CLI to administrators that can be used to configure and manage the TOE and the policy that is used to control traffic flows. Additionally, a variety of commands can be used to manage, configure, and troubleshoot the various services available on the TOE, such as high availability and VAP groups.

Upon successful authentication, administrators are granted a permission level that can be from 0 to 15. Each CLI command also is assigned a permission level from 0 to 15, or Crypto Officer. Administrators can only execute CLI commands if the administrator's permission is greater than or equal to the permission level assigned to the command, except for Crypto Officers who can access all available commands. By default all "show" commands are assigned permission level 0, while all other commands are assigned permission level 15. Administrators can modify the permission level of each command with the "configure privilege level" command.

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

7.1.6 Protection of the TSF and Resource Utilization

The X80-S can support up to 4 NPMs, 10 APMs, and 2 CPMs, while the X60 can support up to 2 NPMs, 5 APMs, and 2 CPMs. These components can be configured for redundancy, allowing for complete failover of each component to a backup in the event of a module failure. Additionally, XOS provides full platform failover in the case of a critical system error that brings down the entire X80-S or X60 platform. The TOE maintains a secure state during failover by regularly synchronizing critical security data necessary for the proper function of the TOE to the backup module. After a failure occurs, the backup module can immediately be brought up to provide the complete set of TOE functionality. For platform failover, the backup X-Series must be manually configured to handle the failover, as no data is synchronized to the backup platform.

The TOE obscures all stored passwords with a SHA-2 hash.

The TOE generates time stamps from a system clock for use on audit messages. The system time is set from a hardware clock during startup. The time can be set by an administrator or an NTP server.

TOE Security Functional Requirements Satisfied: FPT_FLS.1(a), FPT_FLS.1(b), FPT_PTD.1, FPT_STM.1, FRU_FLT.1(a), FRU_FLT.1(b).

7.1.7 TOE Access

The TOE presents a login banner to administrators and users who have successfully authenticated, warning about unauthorized access. This banner is configurable by an administrator.

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, 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, policies, and assumptions to the security objectives are 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 17 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.CRITICAL_FAILURE The TOE may experience a failure of a crucial component that prevents users and administrators from being able to access TOE functionality.	O.FAIL_SECURE The TOE will provide mechanisms to allow for secure failure and recovery.	O.FAIL_SECURE counters this threat by ensuring that the TOE can recover securely from a critical failure.
T.INTERCEPT An unauthorized person or IT entity may be able to view or modify management traffic that is sent between remote administrators and the TOE.	O.ENCRYPT The TOE must protect the confidentiality of its dialogue with authorized remote administrators. Confidentiality is provided by encryption of management traffic.	O.ENCRYPT counters this threat by ensuring that remote management sessions are protected by FIPS 140-2 compliant encryption.
T.MEDIAT An unauthorized person may send information through the TOE that results in the exploitation of resources on the TOE or the systems the TOE is meant to protect.	O.MEDIAT The TOE must mediate the flow of all information between clients and APMs.	O.MEDIAT counters this threat by ensuring that information flowing through the TOE is directed to APMs in an appropriate order so that all security applications required to run are applied to the traffic.
T.NO_AUDIT An attacker may perform security-relevant operations on the TOE without being held accountable for it.	O.AUDIT The TOE must maintain a record of security-relevant events that occur on the TOE, and make that record available for review by TOE administrators.	O.AUDIT counters this threat by ensuring that an audit trail of security-relevant events is preserved. O.AUDIT ensures that accurate time stamps are provided for all audit records, allowing the order of events to be preserved.
T.UNAUTH A user or administrator may gain access to security data on the TOE, even though the user is not	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and	O.ADMIN counters this threat by ensuring that access to TOE security data is limited to those administrators authorized to

Threats	Objectives	Rationale
authorized in accordance with the TOE security policy.	security attributes, ensuring that TOE administrators with the appropriate privileges and only those TOE administrators may exercise such control.	access the management functions of the TOE.
	O.AUDIT The TOE must maintain a record of security-relevant events that occur on the TOE, and make that record available for review by TOE administrators.	O.AUDIT counters this threat by ensuring that unauthorized attempts to access the TOE are recorded.
	O.AUTHENTICATE The TOE must require administrators to authenticate before gaining access to the TOE interfaces.	O.AUTHENTICATE counters this threat by ensuring that administrators are identified and authenticated prior to gaining access to TOE security data.
	O.ENCRYPT The TOE must protect the confidentiality of its dialogue with authorized remote administrators. Confidentiality is provided by encryption of management traffic.	O.ENCRYPT counters this threat by ensuring that management sessions are encrypted, reducing the risk of a remote administrator's session being hijacked.

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

This Security Target defines no OSPs.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 18 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.LOCATE The TOE is located within a controlled access facility.	NOE.PHYSICAL The TOE is used in a physically secure site that protects it from interference and tampering by untrusted subjects.	NOE.PHYSICAL upholds this assumption by ensuring that physical security is provided within the TOE environment sufficient to protect the TOE from interference and tampering by untrusted entities.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the	NOE.MANAGE Sites deploying the TOE provide competent TOE administrators who ensure the system is used	NOE.MANAGE upholds this assumption by ensuring that competent individuals are assigned to manage the TOE.

Assumptions	Objectives	Rationale
information it contains.	securely.	
A.NETCON The TOE environment provides the network connectivity required to allow the TOE to perform its intended function.	OE.TRAFFIC The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.	OE.TRAFFIC upholds this assumption by ensuring that the environment provides the TOE with the appropriate network configuration to perform its intended function.
A.NOEVIL The administrators who manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.	NOE.NOEVIL Sites using the TOE ensure that the TOE administrators are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.	NOE.NOEVIL upholds this assumption by ensuring that sites deploying the TOE provide administrators that are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.
A.NTP The TOE environment should provide protection to ensure that Network Time Protocol (NTP) information communicated from an NTP source to the TOE cannot be modified by an attacker.	OE.NTP NTP Servers providing time information to the TOE are on the local network and inaccessible to non-administrators.	OE.NTP upholds this assumption by ensuring that NTP information remains on the local protected network.
A.ROBUST_ENVIRONMENT The operational environment is at least as robust as the TOE.	OE.ROBUST_ENVIRONMENT The operational environment that supports the TOE for enforcement of its security objectives is at least the same level of robustness as the TOE.	OE.ROBUST_ENVIRONMENT upholds this assumption by ensuring that the TOE is only installed in an operational environment that is at least as robust as the TOE. The TOE is intended to be protected from an attacker with enhanced-basic attack potential, therefore all elements in the environment the TOE depends on for enforcement of its security objectives are also assumed to protected against attackers with an enhanced-basic attack potential. These elements could include network devices, client machines, and boundary protection devices (such as firewalls, IDS, etc.).

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

Several extended requirements have been pulled from the Security Requirements for NDPP. These requirements were added to this security target to enhance the security claims already made and to demonstrate how this ST meets SFRs from the NDPP. Claiming SFRs from the NDPP provides assurance that the TOE addresses several of the security concerns of the United States government and any other entities with similar security needs.

8.4 Rationale for Extended TOE Security Assurance Requirements

No extended SARs have been defined for this ST.

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 19 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT The TOE must maintain a record of security-relevant events that occur on the TOE, and make that record available for review by TOE administrators.	FAU_GEN.1 Audit data generation	FAU_GEN.1 supports this objective by requiring the TOE to produce audit records for all administrator actions, access list events, flows, and software events.
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and security attributes, ensuring that TOE administrators with the appropriate privileges and only those TOE administrators may exercise such control.	FAU_SAR.1 Audit review	FAU_SAR.1 supports this objective by requiring the TOE to make the recorded audit records available for TOE administrators to review.
O.AUDIT The TOE must maintain a record of security-relevant events that occur on the TOE, and make that record available for review by TOE administrators.	FAU_SAR.1 Audit review	FAU_SAR.1 supports this objective by requiring the TOE to make the audit records available for review.
	FAU_SAR.3 Selectable audit review	FAU_SAR.3 supports this objective by allowing administrators to perform string searching and filtering of the audit

Objective	Requirements Addressing the Objective	Rationale
		records.
O.ENCRYPT The TOE must protect the confidentiality of its dialogue with authorized remote administrators. Confidentiality is provided by encryption of management traffic.	FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 supports this objective by ensuring that a FIPS 140-2 validated cryptographic module is available to generate cryptographic keys for use in encrypting management traffic.
	FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4 supports this objective by ensuring that a FIPS 140-2 validated cryptographic module is available to destroy cryptographic keys when they are no longer being used.
	FCS_COMM_PROT_EXT.1 Communications Protection	FCS_COMM_PROT_EXT.1 supports this objective by ensuring that management sessions are encrypted via SSH.
	FCS_COP.1 Cryptographic operation	FCS_COP.1 supports this objective by ensuring that a FIPS 140-2 validated cryptographic module is available to apply encryption to management traffic.
	FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)	FCS_RBG_EXT.1 supports this objective by ensuring the proper function of random number generators used to enforce cryptographic services.
O.MEDIAT The TOE must mediate the flow of all information between clients and APMs.	FDP_IFC.1 Subset information flow control	FDP_IFC.1 supports this objective by defining the subjects, objects, and operations that the TOE can control to implement the Flow SFP.
	FDP_IFF.1 Simple security attributes	FDP_IFF.1 supports this objective by defining the attributes that the Flow SFP can use to control traffic and by defining the rules of the Flow SFP.
O.AUTHENTICATE The TOE must require administrators to authenticate before gaining access to the TOE interfaces.	FIA_PMG_EXT.1 Password Management	FIA_PMG_EXT.1 supports this objective by requiring administrators to use strong passwords, reducing the risk of an attacker gaining access to an administrator's account.
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and	FIA_UAU.2 User authentication before any action	FIA_UAU.2 supports this objective by ensuring that TOE administrators are authenticated before any other TSF-mediated

Objective	Requirements Addressing the Objective	Rationale
security attributes, ensuring that TOE administrators with the appropriate privileges and only those TOE administrators may exercise such control.		actions are performed.
O.AUTHENTICATE The TOE must require administrators to authenticate before gaining access to the TOE interfaces.	FIA_UAU.2 User authentication before any action	FIA_UAU.2 supports this objective by requiring all TOE administrators to authenticate before any other TSF-mediated actions are performed.
	FIA_UAU_EXT.5 Extended: Password-based Authentication Mechanism	FIA_UAU_EXT.5 supports this objective by requiring passwords to be replaced after expiration.
	FIA_UAU_EXT.7 Protected Authentication Feedback	FIA_UAU.7 supports this objective by preventing an attacker from looking at an authorized administrator's screen during login to steal login credentials.
	FIA_UID.2 User identification before any action	FIA_UID.2 supports this objective by ensuring that TOE administrators are identified before any other TSF-mediated actions are performed.
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and security attributes, ensuring that TOE administrators with the appropriate privileges and only those TOE administrators may exercise such control.	FIA_UID.2 User identification before any action	FIA_UID.2 supports this objective by ensuring that TOE administrators are identified before any other TSF-mediated actions are performed.
	FMT_MOF.1 Management of security functions behavior	FMT_MOF.1 supports this objective by specifying the functions of the TOE that can be managed, and describing the permission levels required to access those functions.
	FMT_MSA.1 Management of security attributes	FMT_MSA.1 supports this objective by allowing authorized TOE administrators to manage the Flow SFP security attributes.
O.MEDIAT The TOE must mediate the flow of all information between clients and APMs.	FMT_MSA.1 Management of security attributes	FMT_MSA.1 supports this objective by ensuring that only authorized administrators are able to modify security attributes related to the Flow SFP.
O.ADMIN The TOE must include a set of functions that allow efficient	FMT_MSA.3 Static attribute initialization	FMT_MSA.3 supports this objective by defining permissive default values for the Flow SFP.

Objective	Requirements Addressing the Objective	Rationale
management of its functions and security attributes, ensuring that TOE administrators with the appropriate privileges and only those TOE administrators may exercise such control.		
O.MEDIAT The TOE must mediate the flow of all information between clients and APMs.	FMT_MSA.3 Static attribute initialization	FMT_MSA.3 supports this objective by ensuring that the Flow SFP has a permissive default policy that can be changed only by an authorized administrator.
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and security attributes, ensuring that TOE administrators with the appropriate privileges and only those TOE administrators may exercise such control.	FMT_SMF.1 Specification of management functions	FMT_SMF.1 supports this objective by specifying the management capabilities of the TOE.
	FMT_SMR.1 Security roles	FMT_SMR.1 supports this objective by defining the permission levels available to administrators.
O.FAIL_SECURE The TOE will provide mechanisms to allow for secure failure and recovery.	FPT_FLS.1(a) Failure with preservation of secure state	FPT_FLS.1a supports this objective by ensuring that the TOE can enter a secure state after the failure of a module.
O.FAIL_SECURE The TOE will provide mechanisms to allow for secure failure and recovery.	FPT_FLS.1(b) Failure with preservation of secure state	FPT_FLS.1b supports this objective by ensuring that the TOE can enter a secure state after the failure of a critical system service or component.
O.AUTHENTICATE The TOE must require administrators to authenticate before gaining access to the TOE interfaces.	FPT_PTD.1 Management of TSF Data (for reading of authentication data)	FPT_PTD.1 supports this objective by preventing the reading of plaintext passwords, increasing the level of complexity required to illicitly obtain a password.
O.AUDIT The TOE must maintain a record of security-relevant events that occur on the TOE, and make that record available for review by TOE administrators.	FPT_STM.1 Reliable time stamps	FPT_STM.1 supports this objective by ensuring that the TOE can provide reliable time stamps for its own use. The time stamps allow the TOE to place events in the order that they occur.
O.FAIL_SECURE The TOE will provide mechanisms to allow for secure failure and recovery.	FRU_FLT.1(a) Degraded fault tolerance	FRU_FLT.1a supports this objective by ensuring that the TOE can recover from the failure of a module.
	FRU_FLT.1(b)	FRU_FLT.1b supports this

Objective	Requirements Addressing the Objective	Rationale
	Degraded fault tolerance	objective by ensuring that the TOE can recover from the failure of a critical system service or component.
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and security attributes, ensuring that TOE administrators with the appropriate privileges and only those TOE administrators may exercise such control.	FTA_TAB.1 Default TOE Access Banners	FTA_TAB.1 supports this objective by displaying an access banner warning against unauthorized access.

8.5.2 Security Requirements Rationale for Refinement

This Security Target defines refinements to FTA_TAB.1: Default TOE Access Banners. These refinements were made to meet the requirement as written in the NDPP.

8.5.3 Security Assurance Requirements Rationale

EAL4+ was selected because it is best suited to addressing 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 still 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 chosen to give greater assurance of the developer's on-going flaw remediation process.

8.5.4 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 20 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 20 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FCS_CKM.1	FCS_COP.1	✓	
	FCS_CKM.4	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COMM_PROT_EXT.1	None	Not applicable	

SFR ID	Dependencies	Dependency Met	Rationale
FCS_COP.1	FCS_CKM.4	✓	
	FCS_CKM.1	✓	
FCS_RBG_EXT.1	None	Not applicable	
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	
	FMT_MSA.3	✓	
FIA_PMG_EXT.1	None	Not applicable	
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_EXT.5	None	Not applicable	
FIA_UAU_EXT.7	None	Not applicable	
FIA_UID.2	None	Not applicable	
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
	FDP_IFC.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	Not applicable	
FMT_SMR.1	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.
FPT_FLS.1(a)	None	Not applicable	
FPT_FLS.1(b)	None	Not applicable	
FPT_PTD.1	None	Not applicable	
FPT_STM.1	None	Not applicable	
FRU_FLT.1(a)	FPT_FLS.1(a)	✓	
FRU_FLT.1(b)	FPT_FLS.1(b)	✓	
FTA_TAB.1	None	Not applicable	

9 Acronyms

This section defines the acronyms used throughout this document.

9.1 Acronyms

Table 21 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
APM	Application Processor Module
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CPM	Control Processor Module
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
HMAC	Hashed Message Authentication Code
HTTPS	Secure Hypertext Transfer Protocol
ID	Identifier
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
NDPP	U.S. Government Security Requirements for Network Devices Protection Profile, 10 December 2010, Version 1.0
NPM	Network Processor Module
NTP	Network Time Protocol
OS	Operating System
PP	Protection Profile
PRNG	Pseudo-Random Number Generator
RAID	Redundant Array of Independent Disks
RSA	Rivest, Shamir, Adelman (cryptographic algorithm)
SAR	Security Assurance Requirement

Acronym	Definition
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA	Secure Hashing Algorithm
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
U.S.	United States
VAP	Virtual Application Processor
VLAN	Virtual Local Area Network
VR	Virtual Router
VRRP	Virtual Router Redundancy Protocol
XMS	X-Series Management System
XOS	X-Series Operating System

Prepared by:
Corsec Security, Inc.

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

Phone: (703) 2676050
Email: info@corsec.com
http://www.corsec.com