Big Switch Networks

Big Cloud Fabric 4.7.0

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 0.8

Prepared for:

Big Switch Networks
3965 Freedom Circle
Suite 300
Santa Clara, CA 95054
United States of America

Phone: +1 650 322 6510
www.bigswitch.com

Prepared by:

Corsec Security, Inc.
13921 Park Center Road
Suite 460
Herndon, VA 20171
United States of America

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

Table of Contents

List of Tables

List of Figures

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is a Software-Defined Network (SDN) software bundle that includes the BCF network management application and the BCF proprietary and trademarked NW[1] OS[2], Switch Light. The TOE provides centralized network management, network scalability and resilience, and automation for data centers.

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 functionality 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 (PP), 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 below shows the ST and TOE references.

Table 1 – ST and TOE References

ST Title	Big Switch Networks Big Cloud Fabric 4.7.0 Security Target
ST Version	Version 0.8
ST Author	Corsec Security, Inc.
ST Publication Date	October 5, 2018

[1] NW – Network

[2] OS – Operating System

TOE Reference	Big Switch Networks Big Cloud Fabric 4.7.0
FIPS[3] 140-2 Status	Level 1, FIPS 140-2 validated cryptographic modules, OpenSSL FIPS Object Module v2.0.10, CMVP[4] certificate #1747 and Bouncy Castle FIPS Object Module BC-FJA v1.0.0, CMVP certificate #2768.

1.3 Product Overview

The Product Overview[5] provides a high-level description of the TOE. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

The TOE is Big Switch Networks Big Cloud Fabric 4.7.0 software and is an SDN that provides network scalability and resilience, centralized network management and automation for data centers, and reduced costs due to the disaggregation of network device hardware and software through the use of brite-box[6] switches. BCF provides Layer 2 (L2) switching, Layer 3 (L3) routing, and higher layer services through service insertion and chaining.

BCF is installed on a Clos architecture switching fabric comprised of dual BCF Controllers configured in a High Availability (HA) cluster, and leaf-spine switches as shown in Figure 1 below. The HA cluster provides redundancy for continued network management and traffic forwarding in the event of a controller failure. The leaf-spine architecture optimizes bandwidth between switch ports within the data center by creating a high-capacity fabric using multiple spine switches that interconnect the edge ports on each leaf switch. This design provides consistent latency and minimizes the hops between servers in different racks. The fabric design is modular and scalable; leaf switches can be added to increase the number of switch edge ports, whereas fabric bandwidth can be increased by adding more spine switches.

The fabric traffic is separated into control, management, and data networks. Control network traffic includes the configurations and policies pushed from the BCF Controller to the switches running Switch Light OS. Control network traffic is secured using SSH[7] and TLS[8] v1.2. The management network traffic includes traffic between the BCF Controller and the management console, RADIUS[9] server, and Operational Environment (OE) components. Management network traffic is secured using HTTPS, SSH, and TLSv1.2. Data network[10] traffic includes production data between the leaf and spine switches. Production data from other networks in the data center or the internet can only ingress and egress the TOE via a leaf switch. This includes external production data from other networks, internal or external to the data center, or the Internet.

The TOE supports a multi-tenant model. A tenant is a logical router that provides L3 routing and L2 switching services. There are two types of tenants: a tenant that contains segments[11] and a specialized tenant, system tenant, which interconnects other tenants within the fabric but does not contain segments. A segment's logical

[3] FIPS – Federal Information Processing Standard
[4] CMVP – Cryptographic Modules Validation Program
[5] The Product Overview content is taken from the *BCF User Guide* and the *BCF Leaf-Spine Clos Fabric for Data Centers* datasheet.
[6] Brite-box – vendor branded switches that are shipped without an embedded network operating system.
[7] SSH – Secure Shell
[8] TLS – Transport Layer Security
[9] RADIUS – Remote Dial-In User Service
[10] The data network is also referred to as the data plane.
[11] Segment – An L2 network consisting of logical ports and endpoints. Defines the default broadcast domain boundary.

ports are identified by membership rules based on switch, interface, and VLAN[12]. Segments can be interconnected within the tenant by enabling the segment interface for each segment. A segment contains endpoints and can include switch interface or interface groups for connections to external devices and networks. Multi-tenant access control is applied through L3 access control policies, which provide tenant inter-segment and intra-segment routing, and System tenant inter-tenant routing.

The switches are physically connected into a Clos fabric. L2 traffic is forwarded on a physical or defined logical interface. By default, within a tenant, all links forward L2 traffic and route L3 traffic unless a policy is applied to the switch.

The BCF Controller provides centralized management of the network fabric. From the management console, a TOE administrator configures tenants and segments, and defines policies. The BCF Controller automates the management and configuration of the fabric, including updates to BSN's Switch Light OS, distribution of policies, topology updates and link state change notifications, and the addition or removal of nodes within the fabric. The management console exposes a web-based GUI[13], CLI[14], and REST[15] APIs[16]. The REST APIs can be used for automation and integration. The Zero Touch Fabric (ZTF) feature uses the Open Network Install Environment (ONIE) boot loader to automate switch installation and configuration.

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 TOE, and defining the specific evaluated configuration.

The TOE is software-only and includes the BCF v4.7.0 application software and the BCF proprietary network operating system, Switch Light OS v4.7.0.

BCF 4.7.0 runs on BSN's BCF Controller appliances with Intel Xeon E5-2620 v3 2.40 GHz[17] processors. Each BCF Controller runs the Ubuntu OS 16.04, BCF v4.7.0 application, HTTP[18] server Nginx v1.11, OpenJDK[19] 8, OpenSSL v1.0.2g with FIPS Object Module v2.0.10, and Bouncy Castle with FIPS Object Module BC-FJA v1.0.0 cryptographic libraries. BCF leaf and spine switches are brite-box switches with 12 or 24 core Intel Xeon processors. Each switch includes Switch Light OS v4.7.0, ONIE bootloader, and the OpenSSL v1.0.1t cryptographic library with FIPS Object Module v2.0.10 . The leaf and spine switches form a 10Gb[20] / 40Gb network fabric providing L2 switching and L3 routing. Load balancing is performed across the fabric.

Designed for data centers and multi-tenant environments, the TOE implements several key security features:

[12] VLAN – Virtual Local Area Network
[13] GUI – Graphical User Interface
[14] CLI – Command Line Interface
[15] REST – Representational State Transfer
[16] API – Application Program Interface
[17] GHz – Gigahertz
[18] HTTP – Hyper Text Transport Protocol
[19] OpenJDK – Open Java Development Kit
[20] Gb – Gigabyte

- Role Management – TOE users are assigned to either read-only or admin roles. TOE users in the admin role can add, delete, modify, or view TSF[21] data. TOE users in the read-only role can only view TSF data.
- Centralized fabric management via the Web GUI, CLI, and REST APIs. TOE users in the admin and read-only role can access the BCF Controller via the Web GUI or the CLI, either locally or remotely. ZTF functionality uses the ONIE bootloader to automate switch installation and configuration.
- Network Isolation – TOE management, control, and production data network traffic traverses three physically separated networks. The management network includes traffic between the management console and the BCF Controller, between the BCF Controller and RADIUS server, and between the BCF Controller and NTP server. The control plane includes traffic between the BCF Controller and the spine switches, and between the BCF Controllers and the leaf switches. The production data network includes traffic between leaf-spine switches.
- Tenant Isolation – A tenant is a logical router, which establishes an L3 boundary with other tenants. A tenant can have logical segments, which establish L2 boundaries within the tenant. A tenant can be connected to another tenant via an intermediary tenant, a system tenant.
- Access Control – Access control policies are pushed down to the switches from the BCF Controller. Access to the BCF Controller can be controlled by specific protocols, and in the case of SSH, access can be allowed only from IP[22] addresses or subnetworks. Switch policies control access to the ingress interface on each switch.
- Multiple authentication mechanisms – Both local and RADIUS authentication are supported and can be configured to authenticate TOE user credentials entered at the Web GUI and CLI.
- High availability and secure failover – Dual BCF Controllers are configured in a HA cluster. If the Active BCF Controller fails, the Standby BCF Controller becomes active. If both controllers fail, data traffic continues to be forwarded based on network information at the time of the failure.
- Auditing – System level events are recorded to a local system log file; GUI actions and CLI commands, including configuration changes and REST API requests, are recorded to the audit log.
- Secure Communications – The TOE secures a trusted path between the BCF Controller and the RADIUS server using TLSv1.2. The communication between the BCF Controller and the management console is secured using HTTPS for Web GUI sessions and REST API messages and SSH for CLI sessions. RPC[23] traffic between the two BCF Controllers is protected by TLSv1.2. OpenFlow[24] communications between the BCF Controller and switches is protected by TLS v1.2. The TOE leverages FIPS 140-2 validated cryptographic modules, OpenSSL FIPS Object Module v2.0.10 and Bouncy Castle FIPS Object Module BC-FJA v1.0.0 for establishing secure communications.

[21] TSF – TOE Security Function

[22] IP – Internet Protocol

[23] RPC – Remote Procedure Call

[24] OpenFlow is a communications protocol that allows remote administration of an L3 switch's packet forwarding table.

Figure 1 shows the details of the evaluated configuration of the TOE. The controller and leaf-spine switch hardware appliances are outside the TOE boundary and are depicted with gray shadows. Data plane traffic enters and exits the TOE boundary via leaf switches. Rack 1 and Rack 2 in the diagram represent the external devices respectively that forward traffic to or receive traffic from the leaf switches.

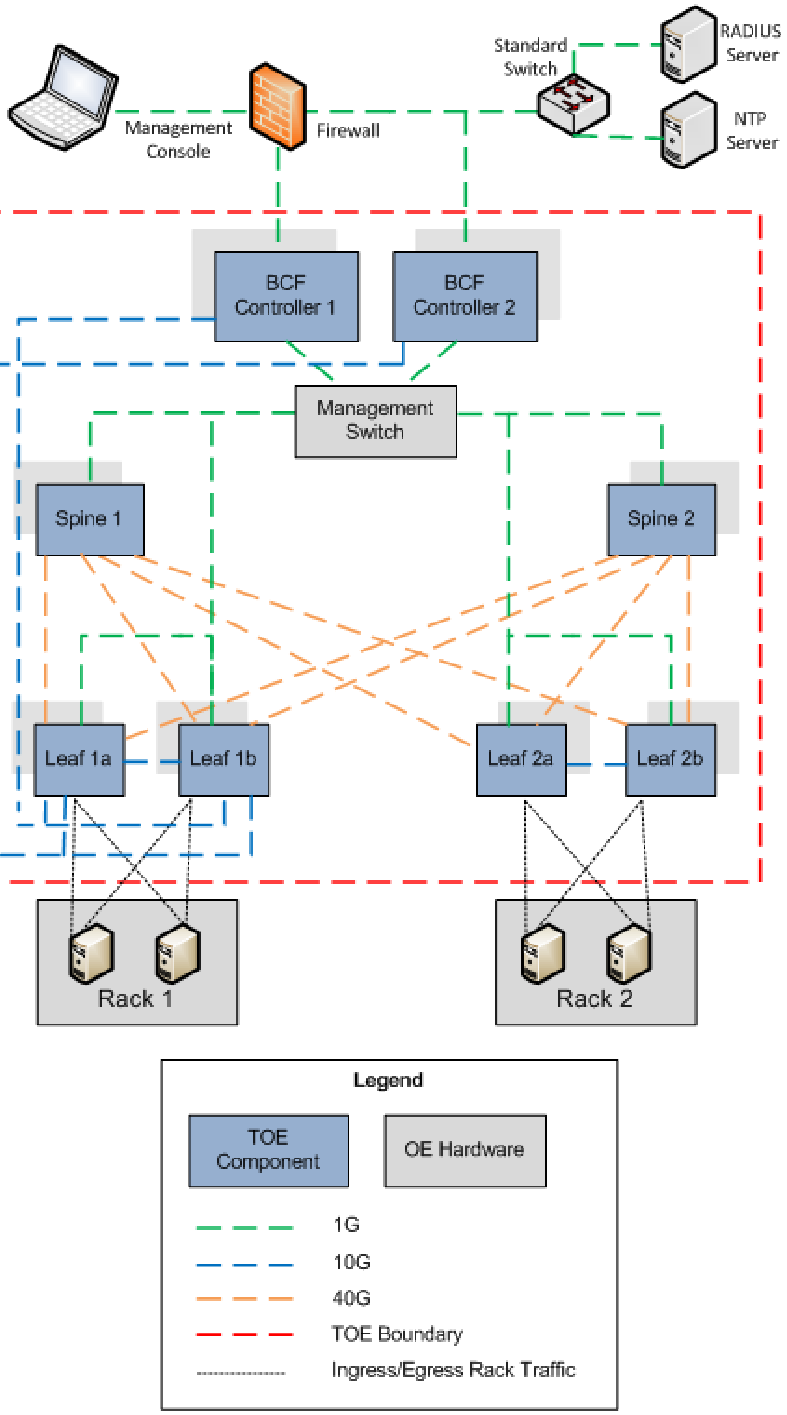


Figure 1 – Evaluated Configuration of the TOE

1.4.1 Brief Description of the Components of the TOE

The TOE is available as a downloadable software binary image or preinstalled on a BCF Controller, and includes the BCF v4.7.0 application and the Switch Light OS v4.7.0. The software binary is uniquely versioned as 4.7.0.

NOTE: The CC evaluation has been performed using the method of downloading the TOE from the BSN Customer Portal (and not on preinstalled TOE software).

1.4.2 TOE Environment

The TOE is intended to be deployed in a secure data center that protects physical access to the TOE.

The TOE relies on non-TOE hardware and software for its essential operation. Though this hardware and software is necessary for the TOE's operation, it is not part of the TOE. The following non-TOE hardware/software is required for essential operation of the TOE:

- non-TOE hardware
  - BCF Controller appliances (2) - BCF-CTLR-HWB-PRP / Intel Xeon E5-2620 v3 2.40GHz
  - Spine switches (2) - Dell S6010-ON / Intel Xeon 12/24
  - Leaf switches (4) - Dell S4048-ON / Intel Xeon 12/24 or Dell S6010-ON / Intel Xeon 12/24
  - Communication racks (2) – contain the endpoint devices
  - OE Switch (1) – Dell S3048-ON
  - Management console (1) – laptop or workstation used to manage the TOE and OE servers
  - RADIUS server (1)
  - NTP server (1)
  - Firewall (1)

- non-TOE software
  - Management console OS
  - Nginx v1.1
  - ONL[25]
  - ONIE
  - Open JDK 8
  - OpenStack Compute Platform[26]
  - VMWare[27] Compute Platform[28]
  - Ubuntu OS 16.04 kernel 4.4.0
  - Web browsers: Chrome 37.x, Internet Explorer 10.x, Safari 7.x, Firefox 32.x, and later versions of each web browser

[25] ONL – Open Network Linux

[26] OpenStack Compute Platform is a cloud operating system on a rack component

[27] VMware – Virtual Machine ware

[28] VMWare Compute Platform is a VMWare cloud on a rack component

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

The TOE provides other security features that are out of the scope of the TOE. These features are not included in the TOE and will not be evaluated, and therefore there is no assurance level associated with them. The features not included in the TOE are the following:

- Rate limiters between the data plane and the control plane to protect against overwhelming the BCF Controller
- Service Insertion - firewalls and intrusion protection systems inserted in the data plane
- sFlow packet generation and forwarding (sFlow configuration is included)
- Remote logging of Syslog events

1.5 TOE Description

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

1.5.1 Physical Scope

The TOE is comprised of the BCF v4.7.0 application and the Switch Light OS v4.7.0 network operating system. BCF v4.7.0 runs on the BCF Controllers, and Switch Light OS v4.7.0 runs on two spine switches and four leaf switches. The customer loads the TOE binary on the Active BCF Controller and then installs the BCF v4.7.0 application on the Active BCF Controller and the Standby BCF Controller. After the BCF Controllers are configured, the switches are configured and the Switch Light OS is pushed down to them when they first boot up.

1.5.1.1 TOE Software

The TOE installation media, BCF-4.7.0-FIPS-Controller-Appliance-2018-05-24.iso, includes the installation files, the BCF 4.7.0 application software and the Switch Light OS v4.7.0. The software components are deployed as follows:

- BCF 4.7.0 on each BCF Controller – One instance
- Switch Light OS – One instance pushed to the two spine switches and to the four leaf switches

The downloadable TOE software, and installation and guidance documentation, are downloaded from the BSN Customer Portal (https://www.bigswitch.com/support). The customer accesses the portal by authenticating with the username and password credentials sent from BSN via email.

1.5.1.2 Guidance Documentation

The documentation is in .pdf format and is downloaded from the BSN Customer Portal. The following guides are required reading and part of the TOE:

- *Big Switch Networks Big Cloud Fabric 4.7 CLI Reference Guide; RELEASE DATE: May 24, 2018; Document Version 1.0, May 24, 2018*
- *Big Switch Networks Big Cloud Fabric 4.7 Deployment Guide; RELEASE DATE: May 24, 2018; Document Version 1.0, May 24, 2018*
- *Big Switch Networks Big Cloud Fabric 4.7 GUI Guide; RELEASE DATE: May 24, 2018; Document Version 1.0, May 24, 2018*

- *Big Switch Networks Big Cloud Fabric 4.7 Hardware Compatibility List; RELEASE DATE: May 24, 2018; Document Version 1.0, May 24, 2018*
- *Big Switch Networks Big Cloud Fabric 4.7 Hardware Guide; RELEASE DATE: May 24, 2018; Document Version 1.0, May 24, 2018*
- *Big Switch Networks Big Cloud Fabric 4.7.0 Release Notes; RELEASE DATE: May 24, 2018; Document Version 1.3, July 11, 2018*
- *Big Switch Networks Big Cloud Fabric 4.7 REST API Guide; RELEASE DATE: May 24, 2018; Document Version 1.0, May 24, 2018*
- *Big Switch Networks Big Cloud Fabric 4.7 System Messages Guide; RELEASE DATE: May 24, 2018; Document Version 1.0, May 24, 2018*
- *Big Switch Networks Big Cloud Fabric 4.7 User Guide; RELEASE DATE: May 24, 2018; Document Version 1.0, May 24, 2018*
- *Freeradius Installation and Setup (Ubuntu) 2017-Dec-20*
- *Big Switch Networks Big Cloud Fabric 4.7.0 Guidance Documentation Supplement v0.7*

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 Section 6 and Section 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 TSF
- TOE Access
- Trusted Path/Channels

1.5.2.1 Security Audit

Log records are generated for system events and user actions initiated from the Web GUI and the CLI, and REST API calls. The identity of a user is associated with a user generated event. TOE users in the admin and read-only role can view the audit data via the Web GUI and via CLI show commands. Log data is stored on the BCF Controller and on the RADIUS server. Log data sent to the RADIUS server is protected from unauthorized modification. See Section 6.2.1 for a list of audit events.

1.5.2.2 Cryptographic Support

The Cryptographic Support functionality utilizes the FIPS-validated cryptographic libraries, OpenSSL FIPS Object Module v2.0.10 and Bouncy Castle FIPS Object Module BC-FJA v1.0.0 on the BCF Controller, and OpenSSL FIPS Object Module v2.0.10 on the BCF switches. See Table 10 and Table 11 for the cryptographic services and provided by the TOE. The TOE generates and replaces keys, encrypts and decrypts data, and provides digital signatures, random number generation, and secure communications. The cryptographic operations which secure communications are as follows:

- TLSv1.2
    - BCF Controller – BCF Controller

  - BCF Controller – Spine Switches
  - BCF Controller – Leaf Switches
- EAP-TTLS[29]
  - BCF Controller – RADIUS server
- HTTPS[30] (Web GUI)
  - BCF Controller – Management Console
- SSH (CLI)
  - BCF Controller – Management Console
  - BCF Controller – Leaf Switches
  - BCF Controller – Spine Switches

1.5.2.3 User Data Protection

The User Data Protection functionality enforces the BCF Controller Information Flow Control SFP [31] for management and control plane traffic and the BCF Switch Information Flow Control SFP for control and production data traffic. The Information Flow SFPs control access by defining what traffic is allowed on the BCF Controller and switch interfaces.

1.5.2.4 Identification and Authentication

The Identification and Authentication functionality requires all users to identify and authenticate before gaining access to any TOE functionality. User credentials are obscured when logging in to the Web GUI and not displayed when entered at the CLI. The TOE supports two authentication mechanisms: password-based authentication and RADIUS authentication. The user name, password, and role membership are stored on the BCF Controller and the RADIUS server.

1.5.2.5 Security Management

The Security Management functionality provides the capability for administrators to manage the security functionality, TSF data, and security attributes provided by the TOE. The TOE provides two roles, admin and read-only. A TOE user associated with the admin role has full administrative capabilities to manage the TOE and is referred to as a TOE administrator. A TOE user associated with the read-only role has management capabilities limited to viewing TSF data and is referred to as a read-only user.

1.5.2.6 Protection of the TSF

The Protection of the TSF functionality ensures that the TOE maintains a secure state in the event of a failure of one or both BCF Controllers. If the Active BCF Controller fails, the Standby BCF Controller takes over after all switches report loss of connectivity to the previously Active BCF Controller. The TOE continues to forward data plane traffic based on the forwarding tables in place at the time when either one BCF Controller fails or both BCF Controllers fail. If both BCF Controllers fail, no changes can be made to forwarding tables and no new switches can be added to the fabric.

The TOE also ensures that TSF data is protected from disclosure or modification when transferred internally between the TOE components on the following appliances in the control plane:

- BCF Controller – BCF Controller
- BCF Controller – Spine Switches

[29] EAP-TTLS – Extensible Authentication Protocol-Tunneled Transport Layer Security

[30] HTTPS – HyperText Transport Protocol Secure (HTTP over TLS)

[31] SFP – Security Function Policy

- BCF Controller – Leaf Switches

1.5.2.7 TOE Access

The TOE Access functionality ensures that TOE user sessions can be terminated by the TOE user.

1.5.2.8 Trusted Path/Channels

The Trusted Path/Channels functionality ensures that communications between the TOE and trusted IT products is protected from modification or disclosure. The TOE provides trusted channels using TLSv1.2 for communications between the BCF Controller and the RADIUS server. For trusted path communications between the BCF Controller and the management console, two secure protocols are supported: HTTPS for web-based traffic and SSH for CLI terminal sessions.

2. Conformance Claims

This section and Table 2 provide the identification for any CC, 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, Release 5, April 2017; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2017/04/04 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ 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 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. The threat agents are listed below.

- 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 read-only users (users in the read-only role): They have general knowledge of how the TOE operates and are granted limited permissions to view TOE TSF data.

- TOE administrators (users in the admin role): 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 administrators are trusted to be benevolent and to perform their duties without malicious intent or actions.

All users are assumed to have a low level of motivation. The IT assets requiring protection are the TSF and user data saved on or transitioning through the TOE and the hosts on the protected network. Both the confidentiality and integrity of the TSF data must be protected. Removal, diminution, and mitigation of the threats are through the security objectives identified in Section 4.
Table 3 below list the applicable threats.

Table 3 – Threats

Name	Description
T.DATA_COMPROMISE	An attacker who is not a TOE user may read, modify, or destroy security critical TOE data stored on the TOE or being transmitted between physically separated parts of the TOE.
T.INTERCEPT	The TOE may communicate with remote IT entities in the operating environment. An attacker who is not a TOE user may attempt to access these entities to intercept these communications in order to read or modify critical TSF data.
T.UNAUTHORIZED	A read-only TOE user may gain unauthorized administrative access to TSF data on the TOE or to TSF 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 Security Target.

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. Table 4 lists the specific conditions that 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.NETCON	The TOE environment provides the network connectivity required to allow the TOE to provide secure routing and switching functions. This includes the use of a firewall to prevent access from non-trusted entities.
A.PHYSICAL	The TOE and OE components (BCF controllers, switches, routers, communication racks, cables, and servers) are located within a controlled access facility. The management console from which the TOE is accessed is also located within a controlled access facility. The management console is located within a separate controlled-access facility.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.
A.TRUSTED_ADMIN	The users who manage the TOE are TOE administrators. TOE administrators and read-only users are non-hostile, appropriately trained, and follow all guidance.

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 listed in Table 5 below.

Table 5 – 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 data, ensuring that only authorized TOE administrators may exercise such control.
O.AUDIT	The TOE must record security relevant events and associate each event with the identity of the user that caused the event. The TOE must provide authorized administrators with the ability to review the audit trail.
O.AUTHENTICATE	The TOE must be able to identify and authenticate TOE users prior to allowing access to TOE TSF-mediated functions and data.
O.FAIL_SECURE	The TOE must protect its functions and TSF data to ensure its SFRs are enforced and capabilities intact in the event of a controller failure.
O.PROTECT	The TOE must ensure the integrity and confidentiality of TSF data by protecting itself from unauthorized modifications and access to its functions and data.
O.TRAFFIC	The TOE must route or switch traffic only as defined by the information flow SFP.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 6 below lists the IT security objectives that are to be satisfied by the environment.

Table 6 – IT Security Objectives

Name	Description
OE.NETWORK	The TOE and the supporting OE components (BCF Controllers, switches, routers, cables, communication racks, management console, and servers) must be implemented such that the TOE is appropriately located within the network to perform its intended function. The NTP server should be located within a separate network than that of the management console component. Firewalls must be implemented to restrict external access from outside the internal network where the TOE resides.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.

4.2.2 Non-IT Security Objectives

Table 7 below lists the non-IT environment security objectives that 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.ADMIN	TOE administrators and read-only users are appropriately trained and trusted to be non-hostile and to follow and apply all guidance documentation.
OE.PHYSICAL	The TOE and its required OE components, except the management console must be located in a physically secured room or data center with the appropriate level of physical access control and physical protections (e.g., badge access, fire control, locks, alarms, etc.). The management console must be located within a separate controlled-access facility.

5. Extended Components

There are no extended components.

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 [*italicized and <u>underlined text within brackets</u>*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 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_GEN.2	*User Identity Association*				
FAU_SAR.1	*Audit review*		✓		
FCS_CKM.1	*Cryptographic key generation*		✓		
FCS_CKM.4	*Cryptographic key destruction*		✓		
FCS_COP.1	*Cryptographic operation*		✓		
FDP_IFC.1(a)	*Subset information flow control (BCF Controller)*		✓		✓
FDP_IFC.1(b)	*Subset information flow control (BCF Switch)*		✓		✓
FDP_IFF.1(a)	*Simple security attributes (BCF Controller)*		✓		✓
FDP_IFF.1(b)	*Simple security attributes (BCF Switch)*		✓		✓
FIA_UAU.2	*User authentication before any action*				
FIA_UAU.5	*Multiple authentication mechanisms*		✓		
FIA_UAU.7	*Protected authentication feedback*		✓		
FIA_UID.2	*User authentication before any action*				
FMT_MSA.1(a)	*Management of security attributes (BCF Controller)*	✓	✓		✓
FMT_MSA.1(b)	*Management of security attributes (BCF Switch)*	✓	✓		✓
FMT_MSA.3(a)	*Static attribute initialization (BCF Controller)*	✓	✓		✓
FMT_MSA.3(b)	*Static attribute initialization (BCF Switch)*	✓	✓		✓
FMT_SMF.1	*Specification of management functions*		✓		
FMT_SMR.1	*Security roles*		✓		
FPT_FLS.1	*Failure with preservation of secure state*		✓		
FPT_ITT.1	*Basic internal TSF data transfer protection*	✓			
FTA_SSL.4	*User-initiated termination*				
FTP_ITC.1	*Inter-TSF trusted channel*	✓	✓		
FTP_TRP.1	*Trusted path*	✓	✓		

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.
Dependencies: FPT_STM.1 Reliable time stamps

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. [
Audit events:
- *commands entered from the CLI*
- *configuration changes made from the CLI, REST API and Web GUI*
- *REST API requests including those created by Web GUI and CLI actions*
- *system log events*
- *user and administrator login*
- *failed login authentication attempts*
- *password reset*

].

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, [*remote address, task id, session id, action, message, method, uri*[32]*, code, command arguments*].

Application Note: The startup and shutdown of the audit function is implied when the controller starts up or shuts down. In this case, the user, remote address, task id, and session id fields are not included as they are not applicable to the controller startup or shutdown event. Additionally, an audit record is generated when an admin enables or disables AAA Accounting from the GUI, CLI, or REST API interfaces.

Application Note: The system log events do not contain the task_id and session_id fields.

Application Note: The user and administrator login, failed login attempts, and password reset events do not contain the action and message fields.

FAU_GEN.2 User identity association

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

[32] URI – Uniform Resource Identifier

FAU_SAR.1 Audit review

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1

The TSF shall provide [*admin users*] with the capability to read [*the contents of the audit file, and system log data*] 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.

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*cryptographic key generation using a deterministic random bit generator*] and specified cryptographic key sizes [*listed in* Table 9] that meet the following: [*none*].

Table 9 – Keys Generated by the TOE

FIPS Module	Key Type	Key Sizes
OpenSSL FIPS Object Module v2.0.10	AES[33]	128
	RSA	2048
BCJ-FA	AES	128
	RSA	2048

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*by replacing old keys with zeroes*] that meets the following: [*none*].

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation],
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1

[33] AES – Advanced Encryption Standard

The TSF shall perform [*the cryptographic operations listed in Table 10 – OpenSSL Cryptographic Services* and *Table 11 – Bouncy Castle Cryptographic Services*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms listed in Table 10 and Table 11*] and cryptographic key sizes [*the cryptographic key sizes listed in Table 10 and Table 11*] that meet the following: [*the standards and the CAVP certificate numbers listed in Table 10 and Table 11*].

Table 10 – OpenSSL Cryptographic Services

Cryptographic Operation	Cryptographic Algorithm	Key / Digest Size (bits)	Validation #
Symmetric Cipher Encryption / Decryption	AES CTR	128	3264
Message Digest	SHA[34]-1 SHA-2	160 256	2702
Key Exchange	ECDHE[35]	2048	Vendor affirmed, allowed in FIPS mode
Digital Signature Generation	RSASSA[36] PKCS[37]V.1.5 RSASSA PSS[38]	2048/SHA256 2048/SHA256	1664
Digital Signature Verification	RSASSA PKCSV.1.5 RSASSA PSS	2048/SHA256 2048/SHA256	1664

Table 11 – Bouncy Castle Cryptographic Services

Cryptographic Operation	Cryptographic Algorithm	Key / Digest Size (bits)	Validation #
Symmetric Cipher Encryption / Decryption	AES GCM[39]	128	3756
Message Digest	SHA-1 SHA-2	160 256	3126
Key Exchange	ECDHE	2048	Vendor affirmed, allowed in FIPS mode
Digital Signature Verification	RSASSA PKCS V.1.5 RSASSA PSS	2048/SHA256 2048/SHA256	1932

Application Note: The TOE uses RSASSA PSS for digital signatures when used for X.509 certificates per RFC 4055. Within the TLS and SSH context, the TOE uses RSASSA PKCSv1.5 for digital signatures as explained in RFC 5246 and RFC 4253 respectively.

[34] SHA – Secure Hash Algorithm
[35] ECDHE – Elliptic Curve Diffie-Hellman Ephemeral
[36] RSASSA – Rivest, Shamir, Adleman Signature Signing Algorithm
[37] PKCS – Public Key Cryptography Standards
[38] PSS – Probabilistic Signature Scheme
[39] GCM – Galois Counter Mode

6.2.3 Class FDP: User Data Protection

FDP_IFC.1(a) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1(a) BCF Controller

The TSF shall enforce the [*BCF Controller Information Flow Control SFP*] on
[
Subject: BCF Controller Interfaces
Information: control plane traffic
Operations: allow, deny traffic
that cause controlled information to flow to and from controlled subjects covered by the SFP
].

FDP_IFC.1(b) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1(b) BCF Switch

The TSF shall enforce the [*BCF Switch Information Flow Control SFP*] on
[
Subject: BCF Switch Interfaces
Information: data plane traffic
Operations: allow, deny (and option to log) L2 and L3 traffic
that cause controlled information to flow to and from controlled subjects covered by the SFP
].

FDP_IFF.1(a) Simple security attributes

Hierarchical to: No other components.

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

FDP_IFF.1.1(a) BCF Controller

The TSF shall enforce the [*BCF Controller Information Flow Control SFP*] based on the following types of subject and information security attributes:
[

- *Subject - BCF Controller Interfaces with security attributes:*
  - *IP address or subnet*
- *Information – Control Plane network packets with security attributes:*
  - *protocol*

].

FDP_IFF.1.2(a) BCF Controller

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

[*If the configured policies allow the information flow based on a combination of subject security attributes and information security attributes, then the network packets are allowed to flow*].

FDP_IFF.1.3(a) BCF Controller

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

FDP_IFF.1.4(a) BCF Controller

The TSF shall explicitly authorize an information flow based on the following rules: [*no explicit authorization rule*s].

FDP_IFF.1.5(a) BCF Controller

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

FDP_IFF.1(b) Simple security attributes

Hierarchical to: No other components.

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

FDP_IFF.1.1(b) BCF Switch

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

[

- *Subject – BCF Switch Interfaces with security attributes:*
  - *rule number*
  - *protocol*
  - *next-hop*
  - *source:*
    - *segment interface*
    - *tenant interface*
    - *tenant name*
    - *segment IP address*
    - *port*
  - *destination:*
    - *tenant name*
    - *segment name*
    - *IP address*
    - *port*
- *Information – Data Plane network packets and the security attributes:*
  - *source IP address*
  - *destination IP address*
  - *logical segment ports*
  - *protocol*

].

FDP_IFF.1.2(b) BCF Switch

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

[

- *For a tenant interface,*
  if the configured policies allow the information flow based on a combination of subject security attributes and information security attributes, then the network packets are allowed to flow.
- *For a segment interface,*
  if segment interface is defined and if the configured policies allow the information flow based on a combination of subject security attributes and information security attributes, then the network packets are allowed to flow.

- *For a system tenant interface,*
  if the tenant interfaces are defined on the system tenant and if the configured policies allow the information flow based on a combination of subject security attributes and information security attributes, then the network packets are allowed to flow.

].

FDP_IFF.1.3(b) BCF Switch

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

FDP_IFF.1.4(b) BCF Switch

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

FDP_IFF.1.5(b) BCF Switch

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

6.2.4 Class FIA: Identification and Authentication

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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.

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_UAU.5.1

The TSF shall provide [*password-based, RADIUS authentication*] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [*local password-based authentication mechanism, and RADIUS authentication mechanism*].

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1

The TSF shall provide only [*obscured characters at the Web GUI and no visible characters at the CLI*] to the user while the authentication is in progress.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies

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.

6.2.5 Class FMT: Security Management

FMT_MSA.1(a) Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1(a) BCF Controller

The TSF shall enforce the [*BCF Controller Information Flow Control SFP*] to restrict the ability to [*query, modify, delete*] the security attributes [*in the administratively defined information flow policies, listed in Table 12*] *to [the roles and operations listed in Table 12].*

Table 12 – Security Attributes Management (BCF Controller)

Role	Operation	BCF Controller Information Security Attributes
admin	query, modify, delete	*subnet, protocol*
read-only	query	

FMT_MSA.1(b) Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1(b) BCF Switch

The TSF shall enforce the [*BCF Switch Information Flow Control SFP*] to restrict the ability to [*query, modify, delete*] the security attributes [*in the administratively defined information flow policies listed in Table* 13] *to* [*the roles and operations listed in Table* 13].

Table 13 – Security Attributes Management (BCF Switch)

Role	Operation	BCF Switch Information Security Attributes
admin	query, modify, delete	*rule number, protocol, next-hop group, source (segment interface, tenant interface, tenant name, segment IP address, port), destination (tenant name, segment name, IP address, port)*
read-only	query	

FMT_MSA.3(a) Static attribute initialization

Hierarchical to: No other components.

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

FMT_MSA.3.1(a) BCF Controller

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

FMT_MSA.3.2(a) BCF Controller

The TSF shall allow the [*no one*] to specify alternative initial values to override the default values when an object or information is created.

Application Note: The TOE provides blank access lists by default for each protocol. This statement means that it cannot be accessed by external entities.

FMT_MSA.3(b) Static attribute initialization

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1(b) BCF Switch

The TSF shall enforce the [*BCF Switch Information Flow Control SFP*] to provide [*__restrictive__*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(b) BCF Switch

The TSF shall allow the [*no one*] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No Dependencies

FMT_SMF.1.1

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

- *Manage User Accounts*
- *Enable Secure Control Plane (Enable FIPS mode)*
- *Configure and Manage the following:*
  - *Fabric Switches*
  - *Interface Groups*
  - *Tenants, Segments, and Endpoints*
  - *BCF Information Control Policy Lists*
  - *NTP Server*
  - *RADIUS Integration*
  - *Authentication Settings and Services*
  - *Logging and Audit*

].

FMT_SMR.1 Security roles

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1

The TSF shall maintain the roles [*read-only, admin*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Application Note: The REST API allows the read-only user to list the available roles and the users that belong to them, while this capability is prohibited via the CLI and GUI.

Application Note: The REST API allows the read-only user to review his login history, while this capability is prohibited via the CLI and GUI.

6.2.6 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [*Failure of the Active BCF Controller or failure of both the Active BCF Controller and the Standby BCF Controller*].

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_ITT.1.1

The TSF shall protect TSF data from [*disclosure and modification*] when it is transmitted between separate parts of the TOE.

6.2.7 Class FTA: TOE Access

FTA_SSL.4 User-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_SSL.4.1

The TSF shall allow user-initiated termination of the user's own interactive session.

6.2.8 Class FTP: Trusted Path/Channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_ITC.1.1

The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2

The TSF shall permit [*the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [*RADIUS authentication*].

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_TRP.1.1

The TSF shall provide a communication path between itself and [*remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [*modification or disclosure*].

FTP_TRP.1.2

The TSF shall permit [*remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for [*Initial user authentication, authentication of TOE read-only and admin users, and communications between the BCF Controller and the external management console.]*].

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2+ augmented with ALC_FLR.2.

Table 14 summarizes these requirements.

Table 14 – 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.2 Use of a CM[40] system
	ALC_CMS.2 Parts of the TOE CM Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

[40] CM – Configuration Management

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 Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 15 lists the security functionality and their associated SFRs.

Table 15 – TOE Security Functionality

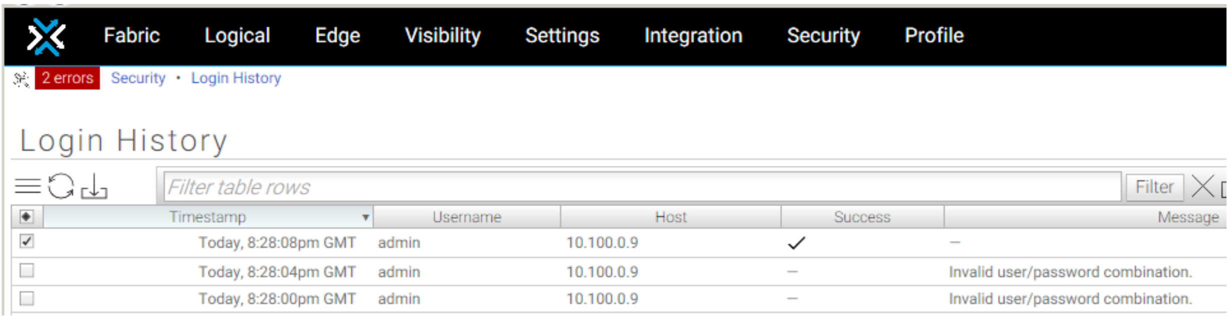
TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit review
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_IFC.1(a)	Subset information flow control (BCF Controller)
	FDP_IFC.1(b)	Subset information flow control (BCF Switch)
	FDP_IFF.1(a)	Simple security attributes (BCF Controller)
	FDP_IFF.1(b)	Simple security attributes (BCF Switch)
Identification and Authentication	FIA_UAU.2	User authentication before any action
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User authentication before any action
Security Management	FMT_MSA.1(a)	Management of security attributes (BCF Controller)
	FMT_MSA.1(b)	Management of security attributes (BCF Switch)
	FMT_MSA.3(a)	Static attribute initialization (BCF Controller)
	FMT_MSA.3(b)	Static attribute initialization (BCF Switch)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_FLS.1	Failure with preservation of secure state

	FPT_ITT.1	Basic internal TSF data transfer protection
TOE Access	FTA_SSL.4	User-initiated termination
Trusted Path/Channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

7.1.1 Security Audit

Log records are generated for the following: startup and shutdown of the audit functions, user actions initiated from the Web GUI, commands entered at the CLI, and REST API requests sent to the BCF Controller. Audit events are written to the */var/log/floodlight/audit.log file*. The identity of a user is associated with a user generated event. User authentication attempts, including successful and failed logins, are associated with a user's ID and are logged. Fabric switches can be configured to send audit data to the Active and Standby BCF Controllers. For the evaluated configuration, the audit function is configured from the GUI or CLI, as local. The audit function is started by starting up the controller and stopped by shutting down the controller. Configuring or removing the AAA Accounting settings also results in an audit record. See Section 6.2.1 for a list of audit events.

A user with the admin role views the audit.log file from the CLI. The **`show logging audit`**[41] command displays the short-term history of the CLI commands and REST API requests issued to the controller. The **`show logging audit`** command with keyword ***`complete`*** displays the complete history of the audit.log. An administrator can view filtered audit.log file login information from the GUI by selecting **Security** > **Login History** from the Menu bar as shown in Figure 2 below.



	Timestamp	Username	Host	Success	Message
☑	Today, 8:28:08pm GMT	admin	10.100.0.9	✓	–
□	Today, 8:28:04pm GMT	admin	10.100.0.9	–	Invalid user/password combination.
□	Today, 8:28:00pm GMT	admin	10.100.0.9	–	Invalid user/password combination.

Figure 2 - GUI Login History

Each audit record is made up of multiple fields, described in Table 16 below. The Login History fields that are also available from the GUI are notated in the "Field" or "Event" column followed by "(GUI)". The GUI indicates a successful login attempt with a checkmark and an unsuccessful attempt with a message.

[41] Commands are rendered in **`bolded Courier New`** type and ***`keywords`*** are in bolded and in **italics**.

Table 16 – Log Files and Records

Audit Record Fields Common to All Audit File Events /var/log/floodlight/audit.log		
Field	Description	
@timestamp (GUI)	Date and time of the event	
User (GUI)	The TOE user (or process ID that caused the event)	
remote_address (GUI)	IP[42] address	
task_id	"Session@"sessionid	
session_id	Unique session identifier (hexadecimal)	
type	All audit events have type value, "logs"	
TSF Event Fields		
Event*	Event Action**	Fields (Value)
login	Session.Create	**action** **message**
login failure (GUI)	Session.Fail	**method** Authentication Authorization
password reset	RestAuditFilter.request	**action** **message** **uri** Note: The Yang path value differs for a password reset by an admin user (…/core/aaa/local-user) and a password reset by a read-only user (…/core/aaa/change-password-local-user).
command	cli.command	**cmd_args**
rest api req • REST requests • all configuration changes • startup/shutdown	RestAuditFilter.request	**uri** **code** **method**
* The Event is the type of activity. ** The Event Action value is found in the action or message fields following "AUDIT EVENT". This field also indicates the outcome of the event (success or failure)		

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, and FAU_SAR.1

7.1.2 Cryptographic Support

The TOE uses FIPS-validated cryptographic modules and all cryptographic support claims involve the use of FIPS-approved algorithms. The BCF Controller implements OpenSSL v1.0.2g with FIPS Object Module v2.0.10 (certificate #1747) and Bouncy Castle with FIPS Object Module BC-FJA v1.0.0 (certificate #2768). The switches implement OpenSSL v1.0.1t with FIPS Object Module v2.0.10 (certificate #1747).

[42] IP – Internet Protocol

The dual BCF Controllers, and the BCF Controllers and switches, mutually authenticate using X.509 certificates issued by a third-party Certificate Authority (CA). The TOE uses the ECDHE_RSA and RSA ciphers from FIPS Object Module v2.0.10 and FIPS Object Module BC-FJA v1.0.0 libraries to generate the X.509 certificate asymmetric public-private key pairs. BCF supports PEM[43] certificates. Symmetric keys for encryption and decryption are generated by AES-GCM.

The FIPS Object Module BC-FJA v1.0.0 on the BCF Controller and the FIPS Object Module v2.0.10 on the switches use ECDHE-RSA-AES128-GCM-SHA256 algorithms for secure TLSv1.2 communications between the control plane devices below:

- Active/Standby BCF Controllers (RPC communications to support HA)
- Active/Standby BCF Controllers and spine switches
- Active/Standby BCF Controllers and leaf switches

The SSH connections for management plane and control plane communications are supported between the following using the FIPS Object Module v2.0.10 on the BCF Controllers and switches:

- Management console (CLI) and Active/Standby BCF Controller
- BCF Controller and leaf switches
- BCF Controller and spine switches

The TOE provides the following secure TLS v1.2 communications between the BCF Controller and the management plane devices using the FIPS Object Module v2.0.10:

- Active/Standby BCF Controllers and the management console (HTTPS – HTTP[44] over TLSv1.2)
- Active BCF Controller and RADIUS server (EAP-TTLS)

The Bouncy Castle FIPS Object Module BC-FJA v1.0.0 algorithms are used to secure communications using TLSv1.2 as follows:

- RPC communications between the BCF Controllers to support HA
- OpenFlow and HTTPS (HTTP/TLSv1.2) communications between the BCF Controller and switches.

TLSv1.2 and SSH make use of encryption and decryption, digital signature verification, hashing, and MAC[45] functionality provided by the cryptographic libraries. The TOE achieves key destruction by replacing old keys with zeroes.

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

7.1.3 User Data Protection

There are two BCF information flow policies: the BCF Controller Information Flow Control SFP and the BCF Switch Information Flow Control SFP. By default, until a policy is defined for the interface, L2 traffic is forwarded on a physical or defined logical interface, and L3 traffic is routed on a defined logical interface.

[43] PEM – Privacy Enhanced Mail
[44] HTTP – Hypertext Transfer Protocol
[45] MAC – Message Authentication Code

The BCF Controller Information Flow Control SFP is applied to the BCF Controllers ingress interfaces which connect to the management network and to the control network, and its subnets. Information flow across the interface and to the subnets is determined by a combination of the following attributes: source IP address, destination IP address, logical segment ports and protocol. Protocols can be allowed or denied by specifying the following keywords: `api` (for REST/API access), `gui` (for web-based access), `ssh` (for a secure terminal session), and `snmp` (for network management messages). In the case of SSH, access can also be restricted to specific IP addresses or subnets.

The BCF Switch Information Flow Control SFP applies to data network traffic. These policies are applied to ingress tenant interfaces, segment interfaces, and to system tenant interfaces. The policies contain one or more rules and are applied to the specified ingress interfaces of the tenant logical router and its logical segments. A combination of interface security attributes, including rule number, allow or deny the flow of information across the interface and to a tenant or segment. See Section 6.2.3, for the complete list of BCF Switch interface security attributes. Packet security attributes include the following: source IP address, destination IP address, logical segment ports, and protocol. Traffic is assigned to an L2 segment by defining membership rules that specify the logical ports that should be included in the segment. A membership rule is based on the switch, interface, and VLAN, or on the interface group. Traffic within each segment remains local unless an interface is defined on the tenant logical router. An interface group membership rule assigns traffic to a given segment if the traffic is seen by any switch using the specified interface group with the designated VLAN tag or an untagged VLAN. Traffic is routed between tenants only if the tenants' interfaces are defined on the system tenant.

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

7.1.4 Identification and Authentication

BCF supports local password-based and RADIUS authentication. The authentication mechanism and authentication order can be set to local only, local then remote, remote then local, or remote. In the evaluated configuration, the authentication order is set to remote then local; RADIUS is the primary method of authentication and local is the secondary method. User and role credentials are stored on the RADIUS sever for remote authentication, and on the BCF Controller for local authentication.

TOE users access the BCF GUI from a supported browser on the management console by entering the IP address of the Active BCF Controller's management interface. A TOE user can also enter the IP address of the Standby BCF Controller's management interface, but only limited functionality is available. From the login screen, the TOE user enters their user name and password and each password character is obscured as it is entered.

A TOE user can also access the BCF CLI using an SSH terminal session. From the CLI, the TOE user enters their username and password credentials at the command prompt. The password characters are not displayed as they are entered. The username and password for REST API calls are included in the initial login message, which is protected by HTTPS over TLSv1.2.

For login attempts from the GUI, the CLI, and the REST API, the credentials entered are compared with the credentials stored locally or those stored remotely on the RADIUS server. All TOE users must be successfully identified and authenticated prior to performing any other TSF-mediated actions.

The TOE is installed with the default admin user account, which is associated with the admin role. The admin user's password is set during the initial setup of the BCF Controller. A recovery password is configured during installation and can be used to recover a lost admin password.

TOE Security Functional Requirements Satisfied: FIA_UAU.2, FIA_UAU.5, FIA_UAU.7, and FIA_UID.2

7.1.5 Security Management

The TOE provides two preconfigured roles, admin and read-only, and no new roles can be added. The role name is case sensitive. TOE users are assigned to either the admin role or the read-only role. A user in the admin role is a TOE administrator with full TSF administration capabilities. TOE administrator has the capabilities to manage users defined locally in the BCF Controller only (not from the RADIUS server). A user in the read-only role is a TOE read-only user with privileges for viewing TSF data.

The TOE is managed from a remote or local management console via the CLI or the Web GUI application. The CLI and Web GUI are REST clients, and CLI and GUI actions are formatted as REST messages. TOE users access the Web GUI from a supported browser on the management console by entering the IP address of the Active BCF Controller's management interface. TOE users enter the IP address to access the Standby BCF Controller's management interface. A TOE user can monitor fabric configuration and activity from the Standby BCF Controller.

A mode restricts access to the set of CLI commands. There are three modes: login, enable, and config. The admin role provides root privileges with access to all modes. The read-only role provides login mode privileges with access to most show commands. Login mode commands are available immediately after login. In login mode, a TOE read-only user can access all show commands except for **`show config`** and **`show test`**. In login mode, a TOE administrator enters the `enable` command to enter enable mode, or **`configure`** to enter config mode. In enable mode, an administrator has access to additional commands to manage the network devices. In config mode, a TOE administrator has access to configuration commands. Submodes allow the configuration of a specific type of object and are available from config mode and are nested within other submodes.

Both TOE administrators and TOE read-only users access the BCF Controller through the management console in order to manage the TOE. From the GUI or CLI, a TOE administrator configures the BCF Controllers and NTP server, registers the fabric switches, and then configures and manages the following: fabric switches and interface groups, tenants (logical routers), segments and endpoints, information flow control policies[46], RADIUS integration, authentication, and audit. From the CLI or GUI a TOE administrator enables FIPS mode by configuring the Control Plane and configures failover from the Active to the Standby Controller.

A TOE administrator manages BCF Controller access by defining and applying policies with the interface identifier and subnet security attributes. A TOE administrator manages BCF Switch access by defining and applying policies with the following attributes: rule number, protocol, next-hop group, source attributes (segment interface, tenant interface, tenant name, segment IP address, port), destination attributes (tenant name, segment name, port). The TSF enforces restrictive default values for the security attributes defined in the BCF Controller and BCF Switch Information Flow Control SFPs. No one can override the default values when an object or information is created.

[46] The GUI is used to configure and manage the BCF Switch Information Flow Control SFP only, while the CLI is used to configure and manage both the BCF Controller Information Flow Control SFP and BCF Switch Information Flow Control SFP.

TOE Security Functional Requirements Satisfied: FMT_MSA.1(a), FMT_MSA.1(b), FMT_MSA.3(a), FMT_MSA.3(b), FMT_SMF.1, and FMT_SMR.1

7.1.6 Protection of the TSF

The TOE uses FIPS validated cryptographic modules i.e., FIPS Object Module v2.0.10 and FIPS Object Module BC-FJA v1.0.0 to secure communications between the control plane of TOE components listed below. These secure communications prevent unauthorized disclosure and modification of TSF data.

The TOE enforces mutual authentication through the exchange and verification of signed X.509 certificates and through TLS v1.2 communications in the control plane between the following devices:

- Active and Standby BCF Controllers
- Active/Standby BCF Controllers and spine switches
- Active/Standby BCF Controllers and leaf switches
- Spine switches
- Leaf switches
- Spine and leaf switches

The TOE enforces secure SSH connections between management plane and control plane communications for the following:

- Management console (CLI) and Active/Standby BCF Controller
- BCF Controller and switches

The TOE provides secure failover in the event that one or both BCF Controllers fail. Two BCF Controllers, the Active BCF Controller and the Standby BCF Controller are configured in a cluster. If the Standby BCF Controller does not receive a message within the timeout period of 30 seconds, and the Active BCF Controller is unavailable, the Standby BCF Controller is designated as the Active BCF Controller. The newly designated Active BCF Controller becomes the functioning Active BCF Controller as soon as all fabric switches report a lost connection with the previous Active BCF Controller. If both BCF Controllers fail, the fabric switches continue operating in headless mode, in which packets are still forwarded and policies are enforced, but new switches cannot connect to the fabric, policies cannot be changed, and no new provisioning events are permitted.

TOE Security Functional Requirements Satisfied: FPT_FLS.1, FPT_ITT.1

7.1.7 TOE Access

A TOE user can terminate their TOE session from the GUI or the CLI. The termination of a user active session from the GUI or CLI results in a REST API request.

TOE Security Functional Requirements Satisfied: FTA_SSL.4

7.1.8 Trusted Path/Channels

The TOE provides a trusted path between the Active/Standby BCF Controllers and the management console. The controllers and management console exchange X.509 certificates, mutually authenticate, and establish a trusted path. HTTP communications for Web GUI access and REST API messages is protected by TLSv1.2. SSH communications is supported for CLI access. Remote admin and read-only users initiate communication from the Web GUI, CLI and REST API via the trusted path.

The TOE provides a trusted channel between the Active/Standby BCF Controllers and the RADIUS server. The controllers and RADIUS server exchange X.509 certificates, mutually authenticate, and establish a trusted channel. The BCF Controller initiates the communication with by passing the read-only and admin user credentials entered at the Web GUI, REST API, and CLI. The RADIUS server does not initiate any communications with the BCF Controller.

The TOE uses OpenSSL or BC-FJA FIPS validated modules to establish trusted path and trusted channels as described in section 7.1.2 above.

TOE Security Functional Requirements Satisfied: FTP_ITC.1, FTP_TRP.1

8. Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1, Release 5.

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 below provides a mapping of the objectives to the threats they counter.

Table 17 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.DATA_COMPROMISE An attacker who is not a TOE user may read, modify, or destroy security critical TOE data stored on the TOE or being transmitted between physically separated parts of the TOE.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that only authorized TOE administrators may exercise such control.	O.ADMIN counters this threat by ensuring that only authorized users may configure the TOE security functions.
	O.AUDIT The TOE must record security relevant events and associate each event with the identity of the user that caused the event. The TOE must provide authorized administrators with the ability to review the audit trail.	O.AUDIT counters this threat by ensuring that security related events that may indicate attempts to tamper with the TOE are recorded.
	O.AUTHENTICATE The TOE must be able to identify and authenticate TOE users prior to allowing access to TOE TSF-mediated functions and data.	O.AUTHENTICATE counters this threat by ensuring that the TOE is able to identify and authenticate read-only users prior to allowing access to TOE functions and data, and administrators prior to accessing TOE security functions and security data.
	O.FAIL_SECURE The TOE must protect its functions and TSF data to ensure its SFRs are enforced and capabilities intact in the event of a controller failure.	O.FAIL_SECURE counters this threat by ensuring SFRs are enforced in the event of a controller failure.

	O.PROTECT The TOE must ensure the integrity and confidentiality of TSF data by protecting itself from unauthorized modifications and access to its functions and data.	O.PROTECT counters this threat by providing mechanisms to protect the TOE TSF data from unauthorized access and modification.
	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT ensures that the TOE is protected from external interference or tampering.
	O.TRAFFIC The TOE must route or switch traffic only as defined by the information flow control SFP.	O.TRAFFIC ensures that information flow control policies are upheld to protect data.
T.INTERCEPT The TOE may communicate with remote IT entities in the operating environment. An attacker who is not a TOE user may attempt to access these entities to intercept these communications in order to read or modify critical TSF data.	O.PROTECT The TOE must ensure the integrity and confidentiality of TSF data by protecting itself from unauthorized modifications and access to its functions and data.	O.PROTECT counters this threat by ensuring the confidentiality and integrity of TSF data by protecting it from unauthorized access and modifications.
T.UNAUTHORIZED A read-only user may gain unauthorized administrative access to TSF data on the TOE or to TSF functions.	OE.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that only authorized TOE administrators may exercise such control.	O.ADMIN counters this threat by ensuring that only authorized administrators may access the management and security functions, and security data of the TOE.
	OE.PHYSICAL The TOE and its required OE components, except the management console, must be located in a physically secured room or data center with the appropriate level of physical access control and physical protections (e.g., badge access, fire control, locks, alarms, etc.). The management console must be located within a separate controlled-access facility.	OE.PHYSICAL counters this threat by ensuring the TOE and its required OE components and the management console are located in controlled access facilities.

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

There are no Organizational Security Policies defined for this Security Target.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 18 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 18 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.NETCON The TOE environment provides the network connectivity required to allow the TOE to provide secure routing and switching functions. This includes the use of a firewall to prevent access from non-trusted entities.	OE.NETWORK The TOE and the supporting OE components (BCF Controllers, switches, routers, cables, communication racks, management console, and servers) must be implemented such that the TOE is appropriately located within the network to perform its intended function. The NTP server should be located within a separate network than that of the management console component. Firewalls must be implemented to restrict external access from outside the internal network where the TOE resides.	OE.NETWORK satisfies the assumption that the TOE environment will provide the appropriate network connectivity to allow the TOE to perform its function securely.
A.PHYSICAL The TOE and OE components (BCF controllers, switches, routers, communication racks, cables, and servers) are located within a controlled access facility. The management console is located within a separate controlled-access facility.	OE.PHYSICAL The TOE and its required OE components, except the management console, must be located in a physically secured room or data center with the appropriate level of physical access control and physical protections (e.g., badge access, fire control, locks, alarms, etc.). The management console must be located within a separate controlled-access facility.	OE.PHYSICAL satisfies the assumption that physical security is provided within the TOE environment to provide appropriate protection to the network resources.
	OE.NETWORK The TOE and the supporting OE components (BCF Controllers, switches, routers, cables, communication racks, management console, and servers) must be implemented such that the TOE is appropriately located within the network to perform its intended function. The NTP server should be located within a separate network than that of the management console component. Firewalls must be implemented to restrict external access from outside the internal network where the TOE resides.	OE.NETWORK satisfies the assumption that the TOE environment will provide the appropriate network connectivity to allow the TOE to perform its function securely.
A.PROTECT The TOE software will be protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT satisfies the assumption that the TOE software will be protected from unauthorized modification.

A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	OE.TIME satisfies the assumption that the environment provides reliable timestamps to the TOE.
A.TRUSTED_ADMIN The users who manage the TOE are TOE administrators. TOE administrators and read-only users are non-hostile, appropriately trained, and follow all guidance.	OE.ADMIN TOE administrators and read-only users are appropriately trained and trusted to be non-hostile and to follow and apply all guidance documentation.	OE.ADMIN satisfies the assumption that the individuals assigned to manage the TOE are competent, non-hostile, appropriately trained, and follow all guidance.

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

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

8.3.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 19 below shows a mapping of the objectives and the SFRs that support them.

Table 19 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that only authorized TOE administrators may exercise such control.	FAU_SAR.1 Audit review	The requirement supports the O.ACCESS objective by ensuring that only authorized
	FAU_GEN.1 Audit Data Generation	The requirement supports the O.ADMIN objective by ensuring that the TOE generates security related events, including relevant details about the event which provide information for the management of the TSF.
	FMT_MSA.1(a) Management of security attributes (BCF Controller)	The requirement meets the O.ADMIN objective by restricting the ability to manage security attributes for the TOE to authorized roles with sufficient permissions.
	FMT_MSA.1(b) Management of security attributes (BCF Switch)	The requirement meets the O.ADMIN objective by restricting the ability to manage security attributes for the TOE to authorized roles with sufficient permissions.
	FMT_MSA.3(a)	The requirement meets the O.ADMIN objective by ensuring that the TOE

	Static attribute initialization (BCF Controller)	provides restrictive default values for security attributes and specifies alternative initial values to override the default values when an object or information is created.
	FMT_MSA.3(b) Static attribute initialization (BCF Switch)	The requirement meets the O.ADMIN objective by ensuring that the TOE provides restrictive default values for security attributes and specifies alternative initial values to override the default values when an object or information is created.
	FMT_SMF.1 Specification of management functions	The requirement supports the O.ADMIN objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the O.ADMIN objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
O.AUDIT The TOE must record security relevant events and associate each event with the identity of the user that caused the event. The TOE must provide authorized administrators with the ability to review the audit trail.	FAU_GEN.1 Audit Data Generation	The requirement supports THE O.AUDIT objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
	FAU_GEN.2 User Identity Association	The requirement supports the O.AUDIT objective by associating the TOE user identity and action for each incident history record created.
	FAU_SAR.1 Audit review	The requirement supports the O.AUDIT objective by ensuring that the TOE provides the ability to review logs.
O.AUTHENTICATE The TOE must be able to identify and authenticate TOE users prior to allowing access to TOE TSF-mediated functions and data.	FIA_UAU.2 User authentication before any action	The requirement supports the O.AUTHENTICATE objective by ensuring that users are authenticated before access to TOE TSF-mediated functions or data is allowed.
	FIA_UAU.5 Multiple authentication mechanisms	The requirement supports the O.AUTHENTICATE objective by providing multiple authentication mechanisms to support TOE user or administrator authentication.
	FIA_UID.2 User authentication before any action	The requirement supports the O.AUTHENTICATE objective by ensuring that the users are identified before access to TOE administrative functions is allowed.

O.FAIL_SECURE The TOE must protect its functions and TSF data to ensure its SFRs are enforced and capabilities intact in the event of a controller failure.	FPT_FLS.1 Failure with preservation of secure state	The requirement supports the O.FAIL_SECURE objective by ensuring that in the event of a failure of the Active BCF Controller, the second Standby BCF Controller will take its place preserving the availability of TOE functionality and data. If both BCF Controllers fail, the TOE preserves limited availability of TOE functionality and data to protect the TOE from unauthorized changes to TOE functions or network configurations.
O.PROTECT The TOE must ensure the integrity and confidentiality of TSF data by protecting itself from unauthorized modifications and access to its functions and data.	FCS_CKM.1 Cryptographic key generation	The requirement supports the O.PROTECT objective by ensuring that cryptographic keys created for use by the TOE meet recommended standards for secure generation.
	FCS_CKM.4 Cryptographic key destruction	The requirement meets the O.PROTECT objective by ensuring that cryptographic keys no longer in use by the TOE are effectively destroyed by being overwritten by new keys.
	FCS_COP.1 Cryptographic Operation	The requirement meets the O.PROTECT objective by ensuring that the TOE provides confidentiality and integrity services for the TOE by providing FIPS 140-2 validated algorithms.
	FIA_UAU.2 User authentication before any action	The requirement supports the O.PROTECT objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only authenticated users are allowed access to TOE functions.
	FIA_UAU.7 Protected authentication feedback	The requirement supports the O.PROTECT objective by obscuring a user entered password and thereby preventing an unauthorized or malicious user from using the password to gain access to the TOE.
	FIA_UID.2 User authentication before any action	The requirement supports the O.PROTECT objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only identified users are allowed access to TOE functions.
	FPT_ITT.1 Basic internal TSF data transfer protection	The requirement meets the O.PROTECT objective by providing FIPS 140-2 cryptographic operations to ensure that TSF data is protected from disclosure or

		modification when transmitted between separate parts of the TOE.
	FTA_SSL.4 User-initiated termination	The requirement satisfies the O.PROTECT objective by ensuring that a TOE user session is terminated after the TOE user logs off, thereby preventing the session from being available to a potential threat agent.
	FTP_ITC.1 Inter-TSF trusted channel	The requirement meets the O.PROTECT objective by protecting TSF data from disclosure or modification while it is transmitted between TOE and other trusted IT entities.
	FTP_TRP.1 Trusted path	The requirement meets the O.PROTECT objective by protecting TSF data from disclosure or modification while it is transmitted between the TOE and users.
O.TRAFFIC The TOE must route or switch traffic only as defined by the information flow control SFP.	FDP_IFC.1(a) Subset information flow control (BCF Controller)	The requirement meets the O.TRAFFIC objective by ensuring that the TOE enforces network device information flow control based on the implemented policy.
	FDP_IFC.1(b) Subset information flow control (BCF Switch)	The requirement meets the O.TRAFFIC objective by ensuring that the TOE enforces network device information flow control based on the implemented policy.
	FDP_IFF.1(a) Simple security attributes (BCF Controller)	The requirement meets the O.TRAFFIC objective by ensuring that the TOE enforces TOE network traffic flow based on the TSF information flow control policy and the TOE components' security attributes.
	FDP_IFF.1(b) Simple security attributes (BCF Switch)	The requirement meets the O.TRAFFIC objective by ensuring that the TOE enforces TOE network traffic flow based on the TSF information flow control policy and the TOE components' security attributes.

8.3.2 Security Assurance Requirements Rationale

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

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

8.3.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 20 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are 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	✓	Although FPT_STM.1 is not included, timestamps for the TOE are provided by the OE_TIME objective. This dependency is met.
FAU_GEN.2	FAU_GEN.1	✓	FAU_GEN.1 is claimed and meets this dependency.
	FIA_UID.1	✓	FIA_UID.2, which is hierarchical to FIA_UID.1, is claimed and meets this dependency.
FAU_SAR.1	FAU_GEN.1	✓	FAU_GEN.1 is claimed and meets this dependency.
FCS_CKM.1	FCS_CKM.4	✓	FCS_CKM.4 is claimed and meets this dependency.
	FCS_COP.1	✓	FCS_COP.1 is claimed and meets this dependency.
FCS_CKM.4	FCS_CKM.1	✓	FCS_CKM.1 is claimed and meets this dependency.
	FDP_ITC.1	✓	FDP_ITC.1 is claimed and meets this dependency.
FCS_COP.1	FCS_CKM.4	✓	FCS_CKM.4 is claimed and meets this dependency.
	FDP_ITC.1	✓	FDP_ITC.1 is claimed and meets this dependency.
	FCS_CKM.1	✓	FCS_CKM.1 is claimed and meets this dependency.
FDP_IFC.1(a)	FDP_IFF.1(a)	✓	FDP_IFF.1(a) is claimed and meets this dependency.
FDP_IFC.1(b)	FDP_IFF.1(b)	✓	FDP_IFF.1(b) is claimed and meets this dependency.

FDP_IFF.1(a)	FDP_IFC.1(a)	✓	FDP_IFC.1(a) is claimed and meets this dependency.
	FMT_MSA.3(a)	✓	FDP_MSA.3(a) is claimed and meets this dependency.
FDP_IFF.1(b)	FDP_IFC.1(b)	✓	FDP_IFC.1(b) is claimed and meets this dependency.
	FMT_MSA.3(b)	✓	FMT_MSA.3(b) is claimed and meets this dependency.
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.
FIA_UAU.5	No dependencies		
FIA_UAU.7	FIA_UAU.1	✓	Although FIA_UAU.1 is not included, FIA_UAU.2, which is hierarchical to FIA_UAU.1, is included. This satisfies this dependency.
FIA_UID.2	No dependencies		
FMT_MSA.1(a)	FMT_SMF.1	✓	FMT_SMF.1 is claimed and meets this dependency.
	FMT_SMR.1	✓	FMT_SMR.1 is claimed and meets this dependency.
	FDP_IFC.1(a)	✓	FMT_IFC.1(a) is claimed and meets this dependency.
FMT_MSA.1(b)	FDP_IFC.1(b)	✓	FDP_IFC.1(b) is claimed and meets this dependency.
	FMT_SMF.1	✓	FMT_SMF.1 is claimed and meets this dependency.
	FMT_SMR.1	✓	FMT_SMR.1 is claimed and meets this dependency.
FMT_MSA.3(a)	FMT_MSA.1(a)	✓	FMT_MSA.1(a) is claimed and meets this dependency.
	FMT_SMR.1	✓	FMT_SMR.1 is claimed and meets this dependency.
FMT_MSA.3(b)	FMT_MSA.1(b)	✓	FMT_MSA.1(b) is claimed and meets this dependency.
	FMT_SMR.1	✓	FMT_SMR.1 is claimed and meets this dependency.
FMT_SMF.1	No dependencies		
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	No dependencies		

FPT_ITT.1	No dependencies		
FTA_SSL.4	No dependencies		
FTP_ITC.1	No dependencies		
FTP_TRP.1	No dependencies		

9. Acronyms

Table 21 defines the acronyms used throughout this document.

Table 21 – Acronyms

Acronym	Definition
AAA	Authentication, Authorization, Accounting
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
BCF	Big Cloud Fabric
BC-FJA	Bouncy Castle FIPS Java API
BSN	Big Switch Network
CA	Certificate Authority
CC	Common Criteria
CAVP	Cryptographic Algorithm Validation Program
CEM	Common Evaluation Method
CLI	Command Line Interface
CM	Configuration Management
CMVP	Cryptographic Modules Validation Program
CTR	Counter
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ESX	Elastic Sky X
FIPS	Federal Information Processing Standard
Gb	Gigabyte
GCM	Galois Counter Mode
GHz	Gigahertz
GNU	GNU’s Not Unix
GUI	Graphical User Interface
HA	High Availability

Acronym	Definition
HMAC	Keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
IP	Internet Protocol
IT	Information Technology
KVM	Kernel-based Virtual Machine
L2	Layer 2
L3	Layer 3
MAC	Message Authentication Code
NW	Network
OE	Operating Environment
ONIE	Open Network Install Environment
OpenJDK	Open Java Development Kit
OpenSSL	Open Secure Sockets Layer
OS	Operating System
OSP	Organizational Security Policy
PEM	Privacy Enhanced Mail
PKCS	Public Key Cryptography Standards
POC	Proof of Concept
PP	Protection Profile
PSS	Probabilistic Signature Scheme
RADIUS	Remote Dial-in User Service
REST	Representational State Transfer
RHEL	Red Hat Enterprise Linux
RPC	Remote Procedure Call
RSA	Rivest, Shamir, Adelman
RSASSA	Rivest, Shamir, Adelman Signature Signing Algorithm
SAR	Security Assurance Requirement
SDN	Software Defined Networking
SHA	Secure Hash Algorithm
SFP	Security Function Policy

Acronym	Definition
SFR	Security Functional Requirement
SP	Special Publications
SSH	Secure Shell
ST	Security Target
TBD	To Be Determined
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
VLAN	Virtual Local Area Network
VM	Virtual Machine
ZTF	Zero Touch Fabric

Prepared by:
Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

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