National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

iboss, Inc.

FireSphere 14600_FIPS and FireSphere 7960_FIPS

Report Number: CCEVS-VR-10663-2016
Dated: 15 April 2016
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Acknowledgements

Validation Panel

Jerome F. Myers, Ph.D.
The Aerospace Corporation
Columbia, MD

Jay P. Vora
The MITRE Corporation
Annapolis Junction, MD

Kelly A. Hood
The Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

Kenji Yoshino
InfoGard Laboratories, Inc.
San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report documents the NIAP validators' assessment of the CCEVS evaluation of the FireSphere 14600_FIPS and FireSphere 7960_FIPS Target of Evaluation (TOE).

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

The TOE is classified as a Network Device and is designed to sit within or at the edge of a private network in order to analyze and filter data passing to or from the private network. Any security related functional capabilities of the product not included in the scope of this evaluation, specifically intrusion detection and intrusion prevention capabilities, were not evaluated.

This table identifies components in the Operational Environment that support the operation of the TOE:

Component	Description
Syslog Server	The TOE supports outgoing (client) audit log connections supporting RFC 3164 tunneled over TLS implementing RFC 5425. The available TLS protocols are described below in the 'TLS/HTTPS Connections' description box.
Serial Connection (Local Management)	Serial connection client for local administration: • RS-232 connection
Web Browser(s) (Remote/Local Management)	The TOE requires one of the following known compatible browsers that have been tested with the TOE: IE 10, Chrome 29, Firefox 22, and Safari 6.
Trusted Updates	The TOE's IT environment must support outgoing TCP connections to the iboss update server (https://pudsus1.ibossconnect.com) for trusted updates.

TLS/HTTPS Connections

The TOE requires incoming TLS/HTTPS connections for the web interface, and optionally supports outgoing TLS tunnels for syslog and LDAP, with the following protocol prerequisites:

TOE Hardware	**Functionality**	**TLS Versions**	**Ciphersuites**
7960	LDAP	1.1 (RFC4346) 1.2 (RFC5246)	TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256
7960	Syslog	1.1 (RFC4346) 1.2 (RFC5246)	TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256
7960	HTTPS	1.1 (RFC4346) 1.2 (RFC5246)	TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256
7960	Trusted Update (pudsus1.ibossconnect.com)	1.1 (RFC4346) 1.2 (RFC5246)	TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256
7960	SMTP	1.1 (RFC4346) 1.2 (RFC5246)	TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256
14600	LDAP	1.0 (RFC2246) 1.1 (RFC4346) 1.2 (RFC5246)	TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
14600	HTTPS	1.1 (RFC4346 1.2 (RFC5246)	TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256
14600	Trusted Update (pudsus1.ibossconnect.com)	1.1 (RFC4346 1.2 (RFC5246)	TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256
7960 and 14600	Intra-TSF Communication	1.1 (RFC4346) 1.2 (RFC5246)	TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256

SMTP Mail Server (Optional)	The TOE optionally supports outgoing mail connections using SMTP and implementing RFC 3207.
LDAP Authentication Server (Optional)	The TOE optionally supports outgoing (client) external authentication server connections using LDAP implementing RFC 4510 tunneled over TLS.
NTP Time Server (Optional)	The TOE optionally supports connections to the time.nist.gov NTP server using NTPv4 and implementing RFC 5905.

Table 1: Operational Environment Components

2 Identification of the TOE

Table 2 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE), the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	FireSphere 14600_FIPS and FireSphere 7960_FIPS
Protection Profile	• Protection Profile for Network Devices, Version 1.1, 08 June 2012 • Security Requirements for Network Devices Errata #3, 3 November 2014
Security Target	iboss FireSphere Security Target, Version 0.8, March 22, 2016
Dates of Evaluation	August 26, 2015 – March 25, 2016
Conformance Result	Pass
Common Criteria Version	Version 3.1 Revision 3, July 2009
Common Evaluation Methodology (CEM) Version	Version 3.1, Revision 3, July 2009
Evaluation Technical Report	16-3460-R-0005 V1.3

(ETR)	
Sponsor/Developer	iboss, Inc.
Common Criteria Testing Lab (CCTL)	InfoGard Laboratories, Inc.
CCTL Evaluators	Kenji Yoshino
CCEVS Validators	Jerome F. Myers, Ph.D. Jay P. Vora Kelly A. Hood

Table 2: Product Identification

3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the International interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all international interpretations with effective dates on or before August 26, 2015.

4 Security Policy

This section contains product features and denotes which are within the logical boundaries of the TOE. The following Security Functions are supported by the TOE:

- Audit
- Cryptography
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

The TOE contains the following unevaluated functionality:

- All Intrusion Prevention System (IPS) functions (anomaly and signature based detection)
- Behavioral sandboxing (signature-less detection)
- Auto-Quarantine
- CISO Command Center
- Threat Intelligence Cloud

4.1 Audit

The TOE's auditable events include start-up and shutdown of the audit functions, all administrative actions, and the events listed in Table 7 in Section 6 of the ST.

Code to generate audit logs is implemented within critical sections of the 14600 and the 7960 to produce audit logs based upon user interaction, automated processes, or manual interaction with the system. In the case of the 14600, audit data is transmitted to the 7960. From the 7960 audit logs are then written in a standardized fashion to the configured remote syslog server utilizing syslog4j which utilizes an RFC 3164 protocol tunneled over TLS according to RFC 5425. The audit messages are sent from the 14600 to the 7960, as well as from the 7960 to the remote syslog server, over the Trusted Channel utilizing TLS. The format of the message transmitted to syslog is Date/time of event, the type of event, and a textual description of the event that occurred.

4.2 Cryptographic Operations

The TOE implements CAVP validated cryptographic algorithms for random bit generation, encryption/decryption, authentication, and integrity protection/verification. These algorithms are used to provide security for the TLS protocol.

The TSF contains the Red Hat OpenSSL user space library that provides confidentiality and integrity services for authentication and for protecting communications with Trusted IT Entities. The crypto algorithms certified are as follows:

- Firesphere OpenSSL Version 8.2.0.0 (Firmware)
  - AES (Cert #3902)
  - SHA-1, 256 (Cert #3215)
  - HMAC SHA-1, 256 (Cert #2532)
  - CTR_DRBG (AES-256) (Cert #1118)
  - RSA (Cert #1987)
- Firesphere Java Version 7.1.0.0 (Firmware)
  - AES (Cert #3562)
  - SHA-1, 256 (Cert #2931)
  - HMAC SHA-1, 256(Cert #2269)
  - RSA (Cert #1831)

Cryptographic Key Generation

The TOE generally fulfills all of the NIST SP 800-56Br1 requirements for pair-wise key establishment using integer factorization cryptography, with the exception of Initialization Vector derivation. The TOE uses the shared secret to derive the initialization vector according to the TLSv1, TLSv1.1, and TLSv1.2 specified KDF.

Zeroization

The TSF zeroizes all plaintext secret and private cryptographic keys and CSPs once they are no longer required. Plaintext keys are protected by the TSF's limited administrative interface which disallows read access to the underlying file system.

The TSF stores hashes (SHA-256) of user passwords. Password hashes are not considered plaintext Critical Security Parameters (CSPs) and therefore not subject to zeroization requirements.

The TSF zeroizes persistent CSPs whenever a file containing CSPs is modified or deleted by reading the size of the file in bytes and overwriting with zeros that amount. The file is then truncated to a length of 0 and overwritten with new data if modified.

The TSF maintains the following secret and private keys in volatile memory (RAM):

- TLS pre-master secret & TLS master secret
- TLS Session Keys
- CTR_DRBG (AES-256) primitives *V* and *Key*
- HTTP administrative session cookie (JSESSIONID)

The TSF zeroizes volatile secret and private keys when power is removed[1].

When the user invokes a "Reset to factory defaults," the TSF performs a zeroization of all persistent CSPs, followed by a system reboot to zeroize all volatile CSPs.

Random Bit Generation

The TOE utilizes the CTR_DRBG (AES 256) mode of SP800-90A for generating TLS certificates and the sensitive-settings encryption key. The module gathers entropy from the 3rd party RDRAND entropy source. The TSF forces RDRAND to re-seed 4 times while gathering seed data for the DRBG and assumes that the DRBG is seeded with at least 256-bit of entropy.

TLS

The TSF implements the server and client side of TLSv1.1, and TLSv1.2 according to RFCs 4346, and 5246 respectively. The TSF also implements the client side of TLSv1 according to RFC 2246. The TSF does not include any client-side extensions such as TLS client certificate authentication.

The TSF supports the following TLS cipher suites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_ SHA256

HTTPS

The TSF implements the server side of the HTTPS protocol according to RFC 2818 by using a TLS connection in place of a TCP connection. The TSF listens on port 443 for HTTPS connections. The TSF uses HTML over HTTPS to present the administrative users with a secure management interface. The TSF uses TLS to provide a secure connection between the TSF and the administrator; however, HTTP is used to maintain the administrator's session. The management interface performs administrator authentication.

[1] This method of zeroization meets the NSA CSS Storage Device Declassification Manual for the zeroization of DRAM and SRAM.

4.3 User Data Protection

The TOE ensures that data will not be reused when processing network packets by clearing all bytes after processing. This is performed by using the system call memset and writing zeros to all fields. This ensures that the previous contents are immediately overwritten.

4.4 Identification and Authentication

The TSF provides local console and the HTTPS web GUI to administer the TSF.

When a user connects to the console interface, the TSF prompts the user for a username and password. The TSF echoes asterisk characters back to the local console while the user is entering their password while connecting to the 7960. The 14600 does not echo any characters when the user is entering their password. If the username/password combination matches an authorized administrator's credentials, the user is granted access to the command line interface.

When a user connects to the HTTPS interface, the TSF prompts the user for a username and password. The TSF presents the user's browser with an HTML Password field to indicate that the characters should not be echoed back; however, displaying or hiding the password is outside of the control of the TSF. If the username/password match an authorized administrator's credentials, the user is granted access to the HTTPS interface.

The TSF requires passwords to be 15 to 32 characters, and allows administrators to configure this minimum length. The TSF supports passwords containing lowercase, uppercase, and numeric ASCII characters. The TSF also allows the following special characters to be used in passwords: !@#$%^&*()

The TOE uses Linux iptables to restrict incoming and outgoing traffic to ensure that the TSF only provide warning banners via HTTPS, layer-2 Ethernet functionality (ARP), and Domain Name Resolution (i.e. DNS) to unauthorized users.

4.5 Security Management

The TSF implements two security management interfaces, a limited local console and a HTML based GUI. Regardless of interface, the TSF does not allow any administrative actions to be performed prior to authentication of the administrative user. The HTML based GUI allows an administrator to initiate a TOE update that fetches an update file from an internet-based server and performs a digital signature check before installing.

The TSF maintains the role of Authorized Administrator. The Authorized Administrator is able to administer the TOE locally and remotely.

When LDAP is used for authentication, the administrative interface makes the LDAP call directly, and maps the LDAP group to a set of TOE permissions. The TOE connects to the configured LDAP authentication server using the LDAP protocol over TCP/IP and TLS (LDAPS).

4.6 Protection of the TSF

The restrictive management interfaces do not provide the user with commands to view pre-shared keys, symmetric keys, passwords, and private keys.

The TOE implements a database of administrative users that have administrative (HTTPS and console) access, including their roles and permissions.

The TSF contains a real-time clock to maintain the time between updates from the NTP server and provide time to other TSF security functions. The real-time clock is considered reliable, because the TSF security functions that utilize the time only utilize an accuracy of one second.

The TSF performs an RSA 2048 with SHA-256 signature verification of any candidate update image. The TSF verifies that the image is signed by the iboss certificate. This certificate is persistently stored in the TOE file system (i.e. hard-coded). If the signature check fails, the TSF will not install the update.

Upon power-up, the TSF performs a SHA-256 of the kernel, all executables, and all interpreted files. The TSF also performs a known answer test on each cryptographic algorithm. The TSF then begins normal operation, if all of the executables are unchanged and the cryptographic algorithms are operating correctly.

4.7 TOE Access

The administrator can access the TSF via the local console (serial) or remotely via HTTPS. The TSF displays a configurable advisory and consent message when an administrator accesses the local console or HTTPS interface. The administrator can terminate a console or HTTPS session by logging out. The TSF terminates local console and HTTPS sessions after a configurable period of inactivity. The TSF immediately terminates local sessions if the period of inactivity expires. The TSF computes the time from the last activity to the current request upon receipt of each HTTPS request. If the time difference exceeds the inactivity timer, the TSF does not process the request and terminates the session.

4.8 Trusted Path/Channels

The TOE uses TLS to provide a trusted communication channel between itself and all authorized IT entities that are logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data. The TOE permits the TSF, or the authorized IT entities to initiate communication via the trusted channel. The TOE permits remote administrators to initiate communication via the trusted path. The TOE requires the use of the trusted path for administrator authentication and all remote administration actions.

The TOE also utilizes TLS to protect intra-TSF communication.

5 TOE Security Environment

5.1 Secure Usage Assumptions

The following assumptions are made about the usage of the TOE:

A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all admin guidance in a trusted manner.

5.2 Threats Countered by the TOE

The TOE is designed to counter the following threats:

T.ADMIN_ERROR	An authorized administrator may incorrectly install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

5.3 Organizational Security Policies

The TOE enforces the following OSPs:

P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

5.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PP and performed by the evaluation team).
2. This evaluation covers only the specific device models and software version identified in

this document, and not any earlier or later versions released or in process.

3. The evaluation of security functionality of the product was limited to the functionality specified in the NDPP. Any additional security related functional capabilities of the product were not covered by this evaluation. The FireSphere product contains the following unevaluated functionality:
    - All Intrusion Prevention System (IPS) functions (anomaly and signature based detection)
    - Behavioral sandboxing (signature-less detection)
    - Auto-Quarantine
    - CISO Command Center
    - Threat Intelligence Cloud
4. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

6 Architectural Information

The TOE is classified as a Network Device for Common Criteria purposes. The TOE is made up of hardware and software components.

6.1 Architecture Overview

The TOE consists of the following:

Hardware:

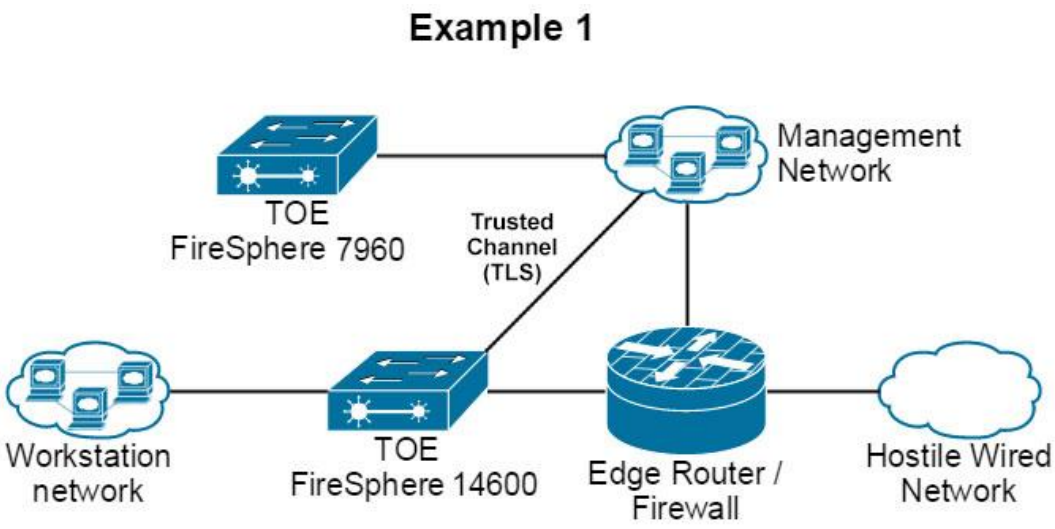
- The combination of FireSphere 7960_FIPS and FireSphere 14600_FIPS

Firmware:

- Firesphere 14600_ FIPS Server Software: Version 8.2.0.10
- Firesphere 7960_FIPS Server Software: Version 8.2.0.10

The guidance documentation that is part of the TOE is listed in ST Section 9: “References”, within Table 11: “TOE Guidance Documentation”.

The FireSphere 14600_FIPS is the centralized IDS sensor. The FireSphere 7960_FIPS is a dedicated IDS manager. The TOE configuration/boundary are summarized in the diagram below:



7 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the FireSphere 7960_FIPS and FireSphere 14600_FIPS.

7.1 Guidance Documentation

Document	Revision	Date
iboss Firesphere Guidance	1.6	March 22, 2016
Secure Web Gateway User Manual	8.2.0.10	March 22, 2016
REPORT MANAGER User Manual	8.2.0.10	March 22, 2016
Report Manager Quick Start Guide	8.2.0.10	March 22, 2016
Secure Web Gateway Quick Start Guide	8.2.0.10	March 22, 2016

7.2 Security Target

Document	Revision	Date
iboss FireSphere Security Target	08	March 22, 2016

8 IT Product Testing

This section describes the testing efforts of the Developer and the Evaluation Team.

8.1 Evaluation Team Independent Testing

The CCTL (InfoGard Laboratories, Inc.) generated the Independent Test Plan and designed the testing activities specified in the Protection Profile for Network Devices v1.1, June 8, 2012 and the Security Requirements for Network Devices Errata #3, November 3, 2014 documents, and generated automated and manual tests to execute the designed test plan.

The evaluation Team verified the product in January 20 – 22, 2016 at iboss, Inc. in San Diego according to the iboss FireSphere Security Target, Version 0.7, February 17, 2016 document and ran the tests specified in the Independent Test Plan. This testing was supplemented by testing of the trusted paths and trusted channels once patches were applied to the OpenSSL libraries. The supplemental testing was performed on March 18 – 25, 2016 at the CCTL's facility in San Luis Obispo. The testing was performed according to the iboss FireSphere Security Target, Version 0.8, March 22, 2016 which reflects the OpenSSL patches. For a detailed description of each test and the corresponding SFRs tested, please see the Independent Test Plan document for the evaluation.

8.2 Vulnerability Analysis

The evaluator performed a public domain vulnerability search on January 22, 2016 on the components that process network traffic, and are therefore susceptible to remote attacks. A few residual vulnerabilities were discovered during the evaluation but these were all addressed prior to the completion of the evaluation.

9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3.

InfoGard has determined that the TOE meets the security criteria in the Security Target, which claims compliance with the Protection Profile for Network Device Protection Profile, Version 1.1, June 8, 2012, and the Security Requirements for Network Devices Errata #3, November 3, 2014. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in March 2016.

10 Validator Comments/Recommendations

As stated in Section 6.1, the FireSphere 7960_FIPS and the FireSphere 14600_FIPS were evaluated in combination. These products are intended to be used in combination and are not considered to be in an evaluated configuration when used separately.

It should also be understood that, as stated in Section 5.4 Clarification of Scope, neither the intrusion detection nor intrusion prevention capabilities included in the product were tested during this evaluation.

11 Security Target

iboss FireSphere Security Target, Version 0.8, March 22, 2016.

12 Terms

12.1 Acronyms

ARP	Address Resolution Protocol
CC	Common Criteria
CCIMB	Common Criteria Interpretations Management Board
CLI	Command Line Interface
CSP	Critical Security Parameters
DAC	Discretionary Access Control
DRBG	Digital Random Bit Generator
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication 140-2
FTP	File Transfer Protocol
HDD	Hard Disk Drive
HTTPS	Hypertext Transfer Protocol over SSL
I/O	Input/Output
IPS	Intrusion Prevention System
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol over SSL
MIB	Management Information Base
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PP	Protection Profile
PFE	Packet Forwarding Engine
RAM	Random Access Memory
RE	Routing Engine
SF	Security Functions
SFP	Small Form-factor Pluggable
SFR	Security Functional Requirements

SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated July 2009, Version 3.1 Revision 3, CCMB-2009-07-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004.