National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report
Sourcefire 3D System Version 5.2.0.1

Report Number: CCEVS-VR-VID10537-2014

Dated: August 6, 2014

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 Team

Paul A. Bicknell CISM, CISSP
Bradford O'Neill
The MITRE Corporation, Bedford, MA

Common Criteria Testing Laboratory

Rory Saunders
COACT, Inc., Columbia, Maryland

Table of Contents

List Of Tables

List of Figures

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Sourcefire 3D System, provided by Sourcefire, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the COACT, Inc. Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in August 2014. The information in this report is largely derived from the associated test reports, all written by COACT, Inc. The evaluation team determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements set forth in the Network Device Protection Profile (NDPP Errata 2) Version 1.1 along with the Extended Firewall Protection Profile.

The Target of Evaluation (TOE) is identified as the Sourcefire 3D System:

Defense Center (DC)	DC 750
	DC1500
	DC3500

Devices	3D7010
	3D7020
	3D7030
	3D7110
	3D7115
	3D7120
	3D7125
	3D8120
	3D8130
	3D8140
	3D8250
	3D8260
	3D8270
	3D8290
	3D9900

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4), as interpreted by the assurance activities contained in the NDPPv1.1 Errata 2, hereafter referred to as NDPP. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation test report and the assurance activities report are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes, and reviewed the individual work units of the ETR and the Assurance Activity reports for the NDPP assurance activities. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Sourcefire 3D System Security Target Version 1.0 and analysis performed by the Validation Team.

2. Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 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 Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1 - Evaluation Identifiers

Item	Identifier	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme	
TOE	Sourcefire 3D System 5.2.0.1	
	Defense Center (DC)	DC750
		DC1500
		DC3500
	Devices	3D7010
		3D7020
		3D7030
		3D7110
		3D7115
		3D7120
		3D7125
		3D8120
		3D8130
		3D8140
		3D8250
		3D8260
		3D8270
		3D8290
		3D9900
Protection Profile	*Security Requirements for Network Devices, Version 1.1, 13 January 2013 [NDPP Errata 2]* *Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall, Version 1.0, 19 December 2011 [TFFW]*	
Security Target	Sourcefire 3D System Security Target, Version 1.0, June 12, 2014	
Evaluation Technical Report	Sourcefire 3D System Evaluation Technical Report, August 4, 2014, Document No. F1-0614-003	

Item	Identifier
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Sourcefire Inc.
Developer	Sourcefire Inc.
Common Criteria Testing Lab (CCTL)	COACT, Inc., Columbia, MD
CCEVS Validators	Paul Bicknell, The MITRE Corporation CISM, CISSP Bradford O'Neill, The MITRE Corporation

3. Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

3.1 TOE Introduction

The TOE combines the security of a network intrusion protection system with access controls based on network attributes such as addresses, ports, protocols, and more. The TOE monitors incoming and outgoing network traffic and performs real-time traffic analysis and logging. All packets on the monitored network are scanned, decoded, preprocessed and compared against a set of rules to determine whether inappropriate traffic is being sent over the network. The system generates alerts or blocks the traffic when deviations of the expected network behavior are detected or when there is a match to a known attack pattern.

In addition, the TOE also provides stateful inspection filtering capability, hereafter referred to as access control. Access control is a policy-based feature that allows administrators to inspect and log the traffic that can enter, exit, or travel within the monitored network. An access control policy determines how the system handles traffic on the network. Administrators can include access control rules in an access control policy to further define how traffic is handled. For example, administrators can specify a rule action, such as to permit, deny, log, or inspect matching traffic with an intrusion policy.

3.2 Physical Boundaries

The TOE is a physical network rack-mountable appliance that supports modules that serve to offer a wide range of network ports varying in number, form factor (copper or fiber optic), processor power, disk space (e.g., 40 – 400 GB) and memory performance (e.g., 1 – 12 GB). The list of applicable series and devices is provided in section 1.1.

The TOE can be configured to rely on and utilize a number of other components in its operational environment.

- Management Workstation – The TOE supports CLI and web access and as such an administrator would need a terminal emulator or SSH client (supporting SSHv2) or web browser (supporting HTTPS such as Firefox 22.0 or later, or Internet Explorer 9 and 10) to utilize those administrative interfaces.

- Audit server – TOE can be configured to deliver audit records to an external log server (HTTP server).

- Authentication servers – The TOE can be configured to utilize external authentication servers.

- Certificate Authority (CA) server – The TOE can be configured to utilize digital certificates, e.g., for HTTPS connections.

- NTP server – The TOE can be configured to obtain time from a trusted time source.

- SMTP (E-mail) server – The TOE can be configured to send e-mail to alert specified users.

- SNMP server – The TOE can be configured to issue and received SNMP traps. Note that the TOE supports SNMPv3. Note that SNMP cannot be used for management.

- DNS server – The TOE supports domain name service in the network.

4. Security Policy

This section summaries the security functionality of the TOE:

4.1 Security Audit

The TOE is designed to be able to generate audit logs for a wide range of security relevant events. The TOE is configured in the evaluated configuration to send the logs to a designated syslog server.

4.2 Cryptographic Support

The TOE includes cryptographic functions that provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and asymmetric key generation features in support of higher level cryptographic protocols including TLSv1, HTTPS, and SSHv2.

The TOE algorithms were validated through the Cryptographic Algorithm Validation Program (CAVP). The certificate numbers are provided below.

Table 2 - Supported Cryptographic Algorithms

Algorithms	Standards	Certificate Numbers
Asymmetric Key Generation		
• Domain parameter generation	NIST Special Publication 800-56B NIST Special Publication 800-57	1227
• Random number generation	See RBG below	
Encryption/Decryption		
• AES (128, 192, and 256 bits) in CBC mode	FIPS PUB 197 NIST SP 800-38A	2575
Cryptographic Signature Services		
• RSA Digital Signature Algorithm (rDSA) (modulus 2048)	FIPS PUB 186-2	1322
Cryptographic Hashing		
• SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 (digest sizes 160, 224, 256, 384 and 512 bits)	FIPS PUB 180-3	2174
Keyed-hash Message Authentication		
• HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 (message digest sizes 160, 224, 256, 384, and 512 bits)	FIPS PUB 198-1 FIPS PUB 180-3	1598
Random Bit Generation (RBG)		
• RBG with independent software-based noise source of 128 bits	FIPS PUB 140-2 Annex C: X9.31 Appendix 2.4 using AES	1227

4.3 User Data Protection

The TOE performs a wide variety of network filtering and IDS/IPS functions, passing network traffic among its various physical and logical network connections. While implementing applicable network protocols associated with network traffic storing and forwarding, the TOE is designed to ensure that it doesn't inadvertently reuse data found in network traffic pool.

4.4 Stateful Traffic Filtering

The TOE provides access control and intrusion protection to the monitored network. The TOE can process the standard network protocols such as ICMPv4, ICMPv6, IPv4, IPv6, TCP, and UDP and provide filtering based on network attributes such as addresses, ports, transport protocols, and more. Administrators can define what action is applied to a network packet when its attributes match the corresponding rule. In addition, the TOE maintains session state tables to track establishing connections and can dynamically allow packets that belong or in response to an existing, allowed connections. Finally, network packets that are invalid according to the standard RFCs are dropped.

4.5 Identification and Authentication

TOE requires users (i.e., administrators) to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers both a locally connected console and serial as well as network accessible interfaces (SSHv2 and HTTPS) for remote interactive administrator sessions.

The TOE supports the local (i.e., on device) definition of administrators with usernames and passwords. All authorized TOE users must have a user account with security attributes that control the user's access to TSF data and management functions. These security attributes include user name, password, and roles for TOE users.

4.6 Security Management

The TOE provides a web-based (using HTTPS) management interface for all TOE administration, including the access control rule sets, user accounts and roles, and audit functions. The ability to manage various security attributes, system parameters and all TSF data is controlled and limited to those users who have been assigned the appropriate administrative role.

The TOE also provides a command line interface (CLI) and shell access to the underlying operating system of the TOE components. The shell access must be restricted to off-line installation, pre-operational configuration, and maintenance and troubleshooting of the TOE. The CLI provides only a subset of the management functions provided by the web GUI and is only available on the Devices. The use of the web GUI is highly recommended over the CLI.

Security management relies on a management workstation in the operational environment with a properly supported web browser or SSH client to access the management interfaces.

4.7 Protection of theTSF

The TOE implements a number of features design to protect itself to ensure the reliability and integrity of its security features. It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability) or can utilize a trusted time server in the operational environment.

The TOE ensures that data transmitted between separate parts of the TOE are protected from disclosure or modification. This protection is ensured by transmission of data between the TOE components over a secure, TLS-protected tunnel.

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

4.8 TOE Access

The TOE can be configured to display an informative advisory banner when an administrator establishes an interactive session and subsequently enforce an administrator-defined inactivity timeout value after which the inactive session will be terminated. The administrators can also terminate their own interactive sessions when needed.

4.9 Trusted Path / Channels

The TOE protects interactive communication with administrators using SSHv2 for CLI access or HTTPS for web GUI access. The TOE protects communication with network peers, such as a log server, using HTTPS connections. All the underlying algorithms for the specified security protocols are FIPS-certified.

5. Assumptions

The assumptions state the specific conditions that are expected to be met by the development environment, operational environment, and/or administrators.

Table 3 - TOE Assumptions

Assumption Name	Assumption Definition
A.CONNECTIONS**	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.
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 administrator guidance in a trusted manner.

* - NDPP

** - TFFW

6. Documentation

The following documentation was used as evidence for the evaluation of the Sourcefire 3D System.

6.1 Design Documentation

- Sourcefire 3D System Security Target, Version 1.0, June 12, 2014
- Entropy Design Document for Sourcefire 3D System 5.2, November 26, 2013 (PROPRIETARY)

6.2 Guidance Documentation

- CC Version 5.2.0.1 Supplemental User Guide for Sourcefire 3D System, Version 2.0, April 30, 2014
- Sourcefire 3D System Installation Guide Version 5.2, June 19, 2013
- Sourcefire 3D System User Guide Version 5.2, June 19, 2013

7. IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Sourcefire 3D Version 1.0 Test Report, August 4, 2014, Document No. F1-0614-001 (proprietary).

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

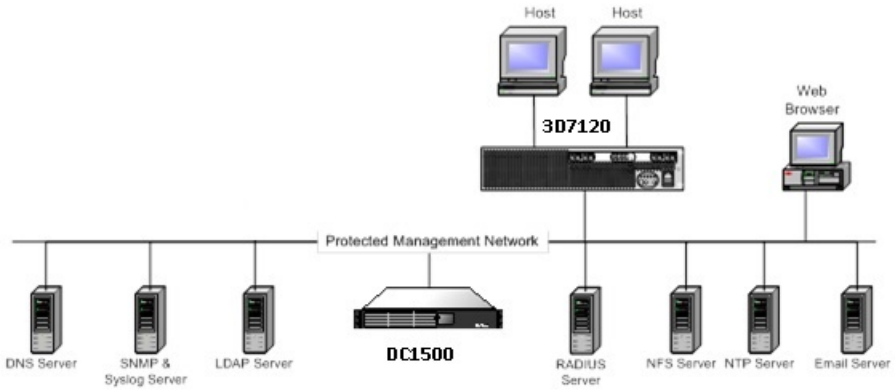
7.2 Evaluation Team Testing

The evaluation team verified the product according the CC Version 5.2.0.1 Supplemental User Guide for Sourcefire 3D System, Version 2.0, April 30, 2014 document and performed the tests and documentation analysis as specified in the NDPP and TFFW.

8. Evaluated Configuration

The evaluated test configuration was defined in the security target. The test configuration in the CCTL test lab is shown below.

Figure 1 - Evaluated Test Configuration



9. Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR and the Assurance Activities Report. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Sourcefire 3D System TOE to be Part 2 extended, and meets the SARs contained the PP.

The following evaluation results are extracted from the proprietary Evaluation Technical Report and Assurance Activities Report provided by the CCTL, and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Sourcefire 3D System products that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally the evaluator performed an assessment of the assurance activities specified in the Security Requirements for NDPP and TFFW.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each assurance activity. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the NDPP and TFFW related to the examination of the information contained in the TSS.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each assurance activity. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally the evaluator performed the assurance activities specified in the NDPP and TFFW related to the examination of the information contained in the operational guidance document.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each assurance activity. The evaluation team found that the TOE was identified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each assurance activity. The evaluation team ran the set of tests specified by the assurance activities in the NDPP and TFFW and recorded the results in a Test Report.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team applied each assurance activity. The evaluation team performed a public search for vulnerabilities and did not discover any public issues with the TOE.

9.7 Summary of the Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

10. Validator Comments / Recommendations

The validators did not have any specific additional comments or recommendations.

11. Annexes

Not applicable

12. Security Target

Sourcefire 3D System Security Target, Version 1.0,12 June 2014

13. Glossary

The following definitions are used throughout this document:

Common Criteria Testing Laboratory (CCTL). An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.

Conformance. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.

Evaluation. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology as interpreted by the supplemental guidance in the NDPP Assurance Activities to determine whether or not the claims made are justified.

Evaluation Evidence. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.

Target of Evaluation (TOE). A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.

Validation. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.

Validation Body. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14. Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 4, dated: September 2012.
2. Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 4, dated: September 2012.
3. Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 4, dated: September 2012
4. Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology*, Version 3.1, Revision 4, dated: September 2012.
5. Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.
6. COACT, Inc. Sourcefire 3D Evaluation Technical Report, August 4, 2014, Document No. F1-0614-003 (Proprietary)
7. COACT, Inc. Test Report – Sourcefire 3D System Test Report, Version 1.0, August 4, 2014, Document No. F1-0614-001 (Proprietary)
8. Sourcefire 3D System Security Target, Document Number: Version 1.0, June 12, 2014

End of Document