National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Sourcefire, Incorporated

Sourcefire Intrusion Detection System
(NS 500, NS 1000, NS 2000, NS 2100, NS 3000, MC 1000, and MC 3000)

Report Number: **CCEVS-VR-05-0102**
Dated: **03 June 2005**
Version: **0.2**

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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Victoria A. Ashby
The MITRE Corporation
McLean, VA

Royal Purvis, Sr.
Jeffrey Gilliatt
Mitretek
Fair Oaks, VA

Common Criteria Testing Laboratory

Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

The evaluation of the Sourcefire Intrusion Detection System (SFIDS) was performed by Science Applications International Corporation (SAIC) in the United States and was completed on 3 June 2005.

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 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1). In addition, the TOE has been evaluated for conformance to the US Government Intrusion Detection System System Protection Profile, Version 1.4, February 4, 2002, as updated by PP0097. Security Functional Requirements (SFRs) from the Common Criteria for IT Security Evaluation (Version 2.1) Part 2 have been extended by additional IDS-specific SFRs included in the PP updated by PP0097.

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 technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the Sourcefire Intrusion Detection System product by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. 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 SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 2) have been met.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by SAIC.

1.1 Interpretations

This evaluation used the Common Criteria for Information Technology Security Evaluation Parts 2 and 3, Version 2.1, August 1999, ISO/IEC 15408-2. International interpretations issued subsequent to Version 2.1 were included in the evaluation. The International interpretations applicable to this evaluation are as follows:

Interp ID	Interp Title	Resulting Change
RI-3		Addition made to ACM_CAP.2 reflected in ST and ETR section.
RI-43		Updates made to ASE_OBJ in ETR.
RI-51		Updates made to ADO_IGS and AVA_VLA in ST and in ETR sections.
RI-65		ST has text in section 8.4 explaining why new dependencies introduced by this RI are satisfied.
RI-84		ASE_REQ ETR work unit changed
RI-85		ASE_REQ ETR work units changed

1.2 Threats to Security

The following are threats identified in the PP and the ST for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

TOE Threats

T.COMINT An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

T.NOHALT An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

T.FACCNT Unauthorized attempts to access TOE data or security functions may go undetected.

1.3 IT System Threats

The following identifies threats to the IT System that may be indicative of vulnerabilities in or misuse of IT resources.

T.SCNCFG Improper security configuration settings may exist in the IT System the TOE monitors.

T.SCNMLC Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.

T.SCNVUL Vulnerabilities may exist in the IT System the TOE monitors.

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

T.MISUSE Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

T.INADVE Inadvertent activity and access may occur on an IT System the TOE monitors.

T.MISACT Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

T.EXPOSE An improperly configured IT environment may allow unauthorized users to gain access to the TSF.

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) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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:	The Sourcefire Network Sensor version 3.2.3 software is embedded in the following products: NS 500, NS 1000, NS 2000, NS 2100, and NS 3000 models of Intrusion Detection Sensors. The Management Console version 3.2.3 software is embedded in the following products: MC1000, and MC3000 models of the Sourcefire Management Console..
Protection Profile	*US Government Intrusion Detection System System Protection Profile,* Version 1.4, February 4, 2002, *(IDSSPP*), as updated by PP-0097.
ST:	*Sourcefire Intrusion Detection System Security Target*,

Item	Identifier
	Version 1.3, 20 May 2005
Evaluation Technical Report	*Evaluation Technical Report for Sourcefire Intrusion Detection System,* Version 1.0, May 20, 2005
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, ISO/IEC 15408-2.
Conformance Result	CC Part 2 Extended with IDS SFRs conformant, CC Part 3 conformant
Sponsor	Sourcefire, Incorporated
Developer	Sourcefire, Incorporated
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validator	Vicky Ashby, The MITRE Corporation
	Royal Purvis, Sr and Jeffrey Gilliat, Mitretek

3 Security Policy

The TOE provides the following security functions: Security Audit, Identification and Authentication, Security Management, Protection of Security Functions, System Data Collection, System Data Analysis, and System Data Review, Availability, and Loss. Each is discussed in more detail as follows:

- **Security Audit -** SFIDS is able to audit the use of administration/management functions of the IDS. This audit is separate from the IDS functionality (recording network traffic), and relates specifically to the management functions of the TOE. This function records attempts to access the system itself, such as successful and failed authentication, as well as the actions taken by the user once authenticated. Auditable actions include changes to the IDS rules and viewing or deleting the audit records.

- **Identification and Authentication -** SFIDS requires users to provide unique identification and authentication data (passwords) before any access to the system is granted. The TOE provides five levels of authority for users: Administrator, Rules, Data, Maintenance, and Restrictive Data. An Administrator has complete control over the TOE, and can manage user accounts, create/modify and implement IDS

rules, and view or delete the audit records. A user with Rules authority can create or modify IDS rules and has the ability to implement the rules on the system, but can not view or modify the audit records. Data users can view/manage/delete the IDS (or System) event trail. Restrictive Data users have the same abilities as Data users for any sensor to which that user is granted access.

- **Security Management -** SFIDS provides a web-based (using https) management interface for all administration, including the IDS rule set, user accounts and roles, and audit functions.

- **Protection of Security Functions** – SFIDS protects the security functions it provides through a variety of mechanisms. One of the primary protections is that users must authenticate before any administrative operations can be performed on the system, including creating new rules or viewing the IDS data. The IDS collection portion of the SFIDS is protected on the monitored network by "hiding" the fact it is there. This is done primarily by using a non-TCP/IP network stack on the SFIDS, which prevents it from being accessed as a network device on the network. Also, the rule set is protected doubly as the system is configured to not accept any management requests or input from the monitored network. The TOE protects the ability to continue recording data by periodically clearing the stored event logs, starting with the oldest records first. This assures there is always adequate disk space to record current and new data that has been found to match the current rule set.

- **System Data Collection –** In accordance with the IDSSPP as updated by PP0097, SFIDS has the ability to set rules to govern the collection of data regarding potential intrusions. While SFIDS contains default rules to detect currently known vulnerabilities and exploits, new rules can be created to detect new vulnerabilities as well as specific network traffic, allowing the administrator complete control over the types of traffic that will be monitored.

- **System Data Analysis** – In accordance with the IDSSPP as updated by PP0097, SFIDS uses signatures and preprocessors to analyze the data collected by snort. Signatures are patterns of traffic that can be used to detect potential attacks or exploits. Since many attacks or exploits require several network connections to work, the IDS also provides the ability to detect these more complex patterns through preprocessors that are included in the TOE. The TOE embodies signatures and preprocessors in rules that can be designed and exercised by the TOE. The administrator can manage the signature identification capabilities by adding and editing rules to respond to the latest exploits. Also, based upon results of analysis, the administrator can trigger alarms for notification of a problem.

- **System Data Review** – In accordance with the IDSSPP as updated by PP0097 , IDS Event data can only be viewed by authorized users (Administrator and Data roles). The data stores of the raw collection data are constantly monitored and if

they become too full, new records will replace the oldest records to prevent active/current data loss.

4 Assumptions

The following secure usage assumptions about the intended environment of the TOE are identified in the Security Target:

Intended Usage Assumptions

A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.

A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.

Physical Assumptions

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

Personnel Assumptions

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.NOTRST The TOE can only be accessed by authorized users.

5 Organizational Security Policies

The following organizational security policies that apply to the TOE and to the intended environment of the TOE are identified in the Security Target:

P.DETECT Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

P.MANAGE The TOE shall only be managed by authorized users.

P.ACCESS All data collected and produced by the TOE shall only be used for authorized purposes.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

P.INTGTY Data collected and produced by the TOE shall be protected from modification.

P. PROTCT The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

6 Architectural Information

The TOE consists of two possible configurations. The first, shown in Figure 1, has one or more Sourcefire appliances running the Sourcefire Linux Version 3.2.0 operating system, the Sourcefire Network Sensor Version 3.2.3 application for products NS 500, NS 1000, NS 2000, NS 2100, and NS 3000. The second, shown in Figure 2, has one or more Sourcefire appliances running SFLinux and the Network Sensor application, with the product numbers listed above, and one hardware appliance running SFLinux, and Sourcefire Management Console Version 3.2.3 for products MC 1000 and MC 3000.

The TOE also requires services from the IT environment. These services are as follows:

- A properly-configured web browser for user access to the Network Sensor and Management Console appliances,
- Network services for sending email,
- SNMP service to monitor the target network(s), and
- A separate network for remote access.

Note that the networks being monitored and those that allow communication between the Network Sensor and Management Console and associated user management web browsers are necessarily different. All networks, except those being monitored, are assumed to be protected from unauthorized access.

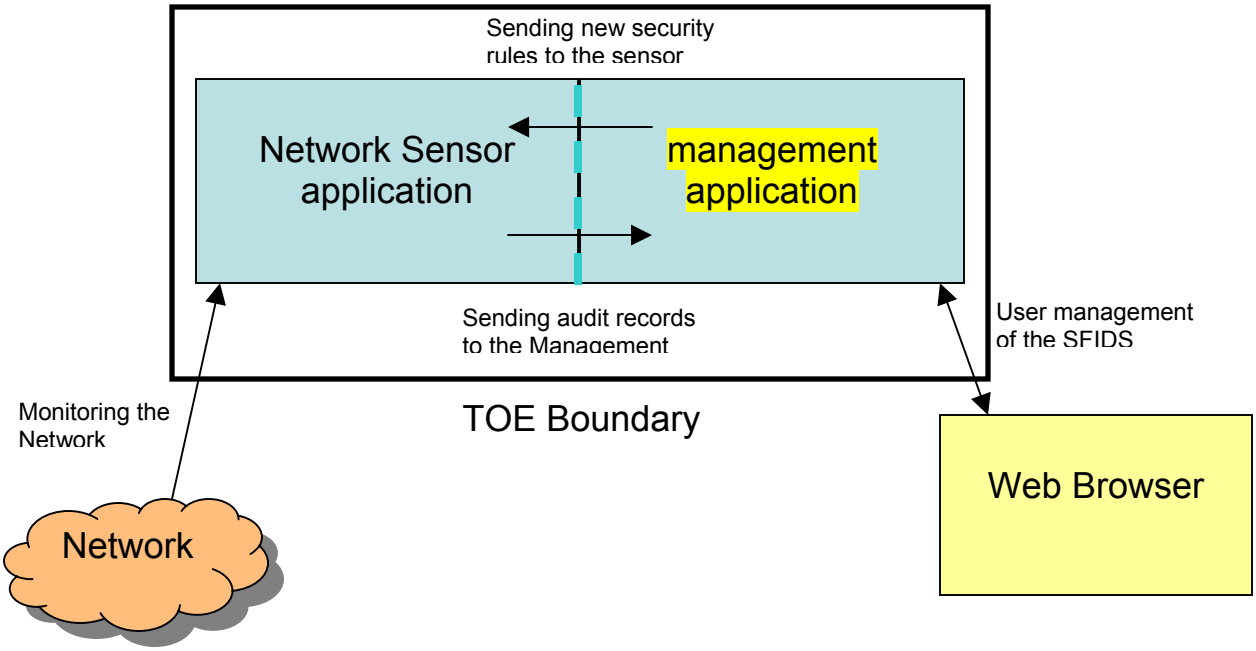

Figure 1 – SFIDS without separate Management Console appliance

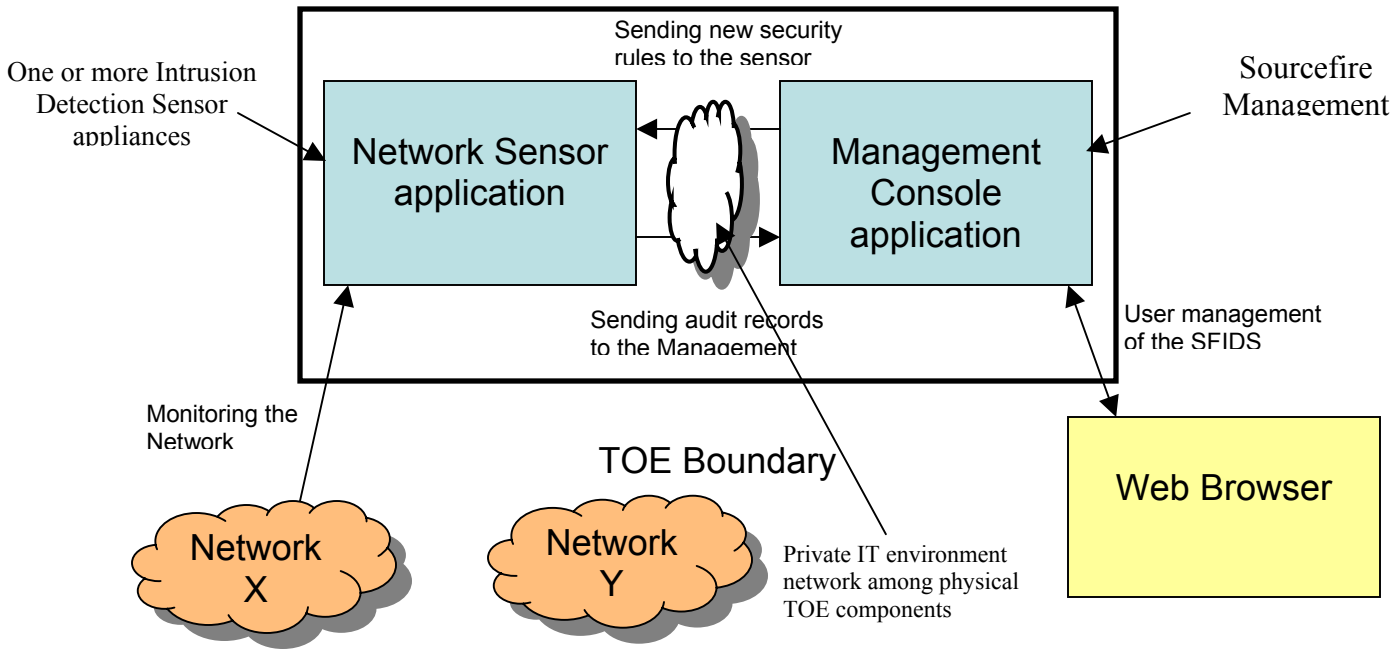

Figure2: SFIDS with separate Sourcefire Management Console appliance

7 Documentation

Design Documentation

Document	Version	Date
Sourcefire Intrusion Detection System High Level Design: Sensor	0.9	03/03/05
Sourcefire Intrusion Detection System High Level Design: Management Console	0.9	02/03/05
Sourcefire Intrusion Detection System Functional Specification: Management Console	1.1	05/18/05
Sourcefire Intrusion Detection System Functional Specification: Network Sensor	1.1	05/18/05

Guidance Documentation

Document	Version	Date
Sourcefire Management Console User Guide	V3.2.3	
Sourcefire Network Sensor User Guide	V3.2.3	

Configuration Management Documentation

Document	Version	Date
Sourcefire Intrusion Detection System Configuration Management Plan	0.5	04/27/05

Delivery and Operation Documentation

Document	Version	Date
Sourcefire Intrusion Detection System Delivery Procedures, Draft	0.4	06/17/03

Test Documentation

Document	Version	Date
Sourcefire ISM v3.2 Test Procedures	0.8	05/16/05
Sourcefire ISM v3.2 QA Test Plan	0.4	04/21/05
Sourcefire ISM v3.2.3 Test Results	1.0	04/21/05

Vulnerability Assessment Documentation

Document	Version	Date
Sourcefire Intrusion Detection System SOF for Authentication System	1.2	08/11/04

Document	Version	Date
Sourcefire Intrusion Management System Vulnerability Analysis	0.7	09/08/04

Security Target

Document	Version	Date
Sourcefire Intrusion Detection System Security Target	1.4	May 19, 2005

8 IT Product Testing

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

Developer Testing

The vendor provided a complete set of test results for analysis. The test procedures were a mix of manual and automatic. The automatic test procedures used Mercury's Quality Center to allow automation of tests using the web browser-based interface. The test procedures were run once for the Network Sensor application and once for the Management Console application.

SAIC and the developer consider the detailed test configuration to be proprietary information. However, the Evaluation Team has included a description of the vendor's test configurations in the ETR, Part 2.

The evaluation team analyzed the vendor test procedures to ensure adequate coverage and to determine if the interfaces between subsystems were behaving as expected. This analysis was confirmed during Evaluation Team independent testing.

Evaluation Team Independent Testing

The evaluation team installed the TOE in the evaluated configuration using the developer's test lab at the developer's site. This tested the installation, generation, and start-up procedures to determine, in accordance with ADO_IGS.1.1E, that those procedures result in a secure configuration. Some issues were noted during installation. Updates to the vendor documentation have corrected those issues.

The Evaluation Team chose to run a subset all of the tests that the developer performed on the TOE that they had installed. The subset was chosen to ensure adequate coverage for all security functional requirements. The Evaluation Team determined that the developer's actual test results matched the vendor's expected results for the chosen subset.

The Evaluation Team added specific team tests to extend the developer's tests and to answer specific questions not addressed by the developer's tests. These Evaluation Team tests concentrated on TOE audit generation and password strength, leading to increased understanding of both areas.

Some issues were noted during the Evaluation Team Independent testing. Updates to the vendor documentation and the Network Sensor and Management Console application software have corrected these issues.

Evaluation Team Penetration Testing

For its penetration tests, the Evaluation Team used a combination of open-source vulnerability documentation, and a set of test procedures proposed by the penetration test team to identify penetration test cases based on the developer's vulnerability assessment documentation. The Evaluation Team used the developer's test configuration to successfully perform its penetration tests.

The Evaluation Team's ETR, Part 2, provides a detailed description of the tests, the results, and the effects, if any, on the information presented in the ST or other evaluation evidence.

9 Evaluated Configuration

The evaluated configuration, as described in section 6 above, consists of two possible configurations as follows:

- One or more of Sourcefire products NS 500, NS 1000, NS 2000, NS 2100, and NS 3000, which each consist of the following:.
    - A Sourcefire-supplied rack-mountable Intel-based hardware appliance appropriate to the model
    - Sourcefire Linux Version 3.2.0,
    - Sourcefire Network Sensor Version 3.2.3 application, and

- One or more of the Network Sensor models listed above, combined with one of either of products MC 1000 and MC 3000, which consist of the following:
    - A Sourcefire-supplied Intel-based hardware appliance appropriate to the model
    - Sourcefire Linux Version 3.2.0, and
    - Sourcefire Management Console Version 3.2.3

10 Results of the Evaluation

The Evaluation Team conducted the evaluation based on the Common Criteria (CC) Version 2.1 and the Common Evaluation Methodology (CEM) Version 1.0 and all applicable International Interpretations in effect.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Verdicts were not assigned to assurance classes.

Section 5, Results of Evaluation, in the Evaluation Team's ETR, Part 1, states:

> "The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST." For further details, the reader is encouraged to consult the non-proprietary ETR, Part 1, for this product.

The validation team followed the procedures outlined in the Common Criteria Evaluation and Validation Scheme (CCEVS) publication number 3 for Technical Oversight and Validation Procedures. The validation team has observed the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validation team therefore concludes that the evaluation and its results of pass are complete.

11 Validator Comments/Recommendations

In addition to the information presented in other sections of this document, the validator has the following comments:

Evaluated Configuration: The Sourcefire products listed in this Validation Report can run in three configurations: on SUN hardware, on IBM hardware, or on the configuration described here. The evaluated configuration includes only the configuration described in this Validation Report. The other two versions are NOT evaluated.

In addition, not all features included in the applications are in the evaluated configuration. Specifically, Realtime Network Awareness (RNA) is not included in the evaluated configuration.

The web browser used to configure and manage the appliances, or to review audit records, is not part of the TOE but it must be configured correctly to support the TOE. Specifically, the browser must not cache web pages displayed using one user's permissions, or those web pages will be visible to a less-privileged user.

Time Stamp: Changing the time stamp removes audit events and IDS events.

Audit: Extensive evaluation team tests on audit generation showed that audit blocks were audited on creation but not on deletion if the file containing the block information was deleted. The documentation now states that the files, once created, should be left even if empty. In addition, extensive investigation of possible TSF modifications showed that TOE has limited options that will fail when changing TSF data. The only required failure is related to login. The TSF does generate failure audit records when the user fails their attempt to login.

GUI: The Sourcefire web-based GUI provides an excellent and supportive interface for authorized users. However, some needed actions cannot be done using the GUI. For example, blocking creation of audit records from specific IP addresses is done from the command line.

Vendor Test Procedures: The vendor used Mercury's Quality Center to automate tests from the web browser interface. This allowed the test procedures to be done quickly and without key errors, while presenting results in an understandable manner.

12 Annexes

- Not applicable.

13 Security Target

The Security Target is identified as *Sourcefire Intrusion Detection System Security Target*, Version 1.4, 19 May 2005.

The document identifies the security functional requirements (SFRs)necessary for conformance to *US Government Intrusion Detection System System Protection Profile,* Version 1.4, February 4, 2002. These SFRs include both Common Criteria Part 2 SFRs and Extended SFRs that capture needed IDS security functional requirements. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 2.

14 Glossary

The following definitions are used throughout this document:

Hardware: the physical equipment used to process programs.

Intrusion Detection System (IDS): An IDS monitors an IT system for activity that may inappropriately affect the IT system's assets.

Software: the programs and associated data that can be dynamically written and modified.

Target of Evaluation (TOE) - An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

15 Bibliography

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

- *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999, Parts 1, 2, and 3.
- 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.
- *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, Version 0.6, 11 January 1997.
- *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 1.0, August 1999.
- *US Government Intrusion Detection System System Protection Profile,* Version 1.4, February 4, 2002 *(IDSSPP)*
- *Sourcefire Intrusion Detection System Security Target*, Version 1.4, 29 May 2005
- ETR Part 1 (Non-Proprietary), Version 0.1, 19 May 2005.