

# National Information Assurance Partnership



## Common Criteria Evaluation and Validation Scheme Validation Report

### Sourcefire 3D System

(Sourcefire Defense Center: models DC750, DC1500, and DC3500

Sourcefire 3D Sensor licensed for IPS: models 3D500, 3D1000, 3D2000,  
3D7110, 3D7120, 3D8120, 3D8130, 3D8140, and 3D8250;

Sourcefire Virtual Defense Center,

Sourcefire Virtual 3D Sensor licensed for IPS)

Version 4.10.2.4 (SEU 568)

**Report Number: CCEVS-VR-VID10502-2012**

**Dated: May 23, 2012**

**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**

**Mr. Daniel P. Faigin, CISSP**

*The Aerospace Corporation, El Segundo California*

**Dr. Patrick Mallett**

*The MITRE Corporation, McLean, Virginia*

## **Common Criteria Testing Laboratory**

**Mr. Deepak Somesula**

*Cygnacom Solutions, McLean, Virginia*

Much of the material in this report was extracted from evaluation material prepared by the CCTL. The CCTL team deserves credit for their hard work in developing that material. Many of the product descriptions in this report were extracted from the Sourcefire 3D System, Version 4.10.2.4 (SEU 568) Security Target.

## Table of Contents

<b>1</b>	<b><i>Executive Summary</i></b> .....	<b>6</b>
<b>2</b>	<b><i>Identification</i></b> .....	<b>8</b>
<b>3</b>	<b><i>Security Policy</i></b> .....	<b>9</b>
<b>3.1</b>	<b>Security Audit Functions</b> .....	<b>9</b>
<b>3.2</b>	<b>Identification and Authentication Functions</b> .....	<b>9</b>
<b>3.3</b>	<b>Security Management Functions</b> .....	<b>10</b>
<b>3.4</b>	<b>Protection of Security Functions</b> .....	<b>11</b>
<b>3.5</b>	<b>TOE Access Functions</b> .....	<b>11</b>
<b>3.6</b>	<b>System Data Collection Functions</b> .....	<b>11</b>
<b>3.7</b>	<b>System Data Analysis and Reaction Functions</b> .....	<b>12</b>
<b>3.8</b>	<b>System Data Review, Availability and Loss Functions</b> .....	<b>13</b>
<b>3.9</b>	<b>Summary</b> .....	<b>13</b>
3.9.1	Security functional Requirements.....	13
3.9.2	Operational Environment Objectives.....	16
<b>4</b>	<b><i>Assumptions and Clarification of Scope</i></b> .....	<b>18</b>
<b>4.1</b>	<b>Usage Assumptions</b> .....	<b>18</b>
<b>4.2</b>	<b>Assumptions</b> .....	<b>18</b>
<b>4.3</b>	<b>Clarification of Scope</b> .....	<b>19</b>
<b>5</b>	<b><i>Architectural Information</i></b> .....	<b>22</b>
<b>6</b>	<b><i>Documentation</i></b> .....	<b>29</b>
<b>6.1</b>	<b>Guidance Documentation</b> .....	<b>29</b>
<b>6.2</b>	<b>Security Target (ST)</b> .....	Error! Bookmark not defined.
<b>6.3</b>	<b>Development (ADV) Evidence Documentation</b> .....	Error! Bookmark not defined.
<b>6.4</b>	<b>Life-Cycle (ALC) Evidence Documentation</b> .....	Error! Bookmark not defined.
<b>6.5</b>	<b>Testing (ATE) and Vulnerability Analysis (AVA) Documentation</b> Error! Bookmark not defined.	Error! Bookmark not defined.
<b>6.6</b>	<b>Evaluation Technical Report (ETR)</b> .....	Error! Bookmark not defined.
<b>7</b>	<b><i>IT Product Testing</i></b> .....	<b>31</b>
<b>7.1</b>	<b>Developer Testing</b> .....	<b>31</b>
7.1.1	Overall Test Approach and Results: .....	31
7.1.2	Depth and Coverage .....	32
7.1.3	Results .....	32
<b>7.2</b>	<b>Evaluator Independent Testing</b> .....	<b>32</b>
7.2.1	Execution the Developer’s Functional Tests .....	32
7.2.2	Team-Defined Functional Testing .....	33
7.2.3	Vulnerability/Penetration Testing .....	34

<b>8</b>	<b><i>Evaluated Configuration</i></b> .....	<b>36</b>
<b>9</b>	<b><i>Results of Evaluation</i></b> .....	<b>39</b>
<b>10</b>	<b><i>Validators Comments/Recommendations</i></b> .....	<b>41</b>
<b>11</b>	<b><i>Security Target</i></b> .....	<b>42</b>
<b>12</b>	<b><i>Glossary</i></b> .....	<b>43</b>
<b>12.1</b>	<b>Acronyms</b> .....	<b>43</b>
<b>12.2</b>	<b>Terminology</b> .....	<b>45</b>
<b>13</b>	<b><i>Bibliography</i></b> .....	<b>55</b>

## List of Figures

Figure 1: TOE: Boundary - Sourcefire 3D System with Defense Center.....	26
Figure 2: TOE: Boundary - Sourcefire 3D System with Virtual Defense Center .....	27
Figure 3: TOE: Boundary - Sourcefire 3D System using a stand-alone 3D Sensor with IPS.....	28
Figure 4: A Virtual Defense Center managing a 3D2000_32 Sensor deployed in passive mode and a Virtual 3D Sensor deployed in inline mode .....	37
Figure 5: A DC1500 Defense Center managing a 3D8140_64 Sensor deployed in inline mode and a Virtual Sensor deployed in passive mode .....	38
Figure 6: A standalone 3D2000 Intrusion Sensor deployed in inline mode.....	38

# 1 Executive Summary

This Validation Report (VR) documents the evaluation and validation of the product Sourcefire 3D System (Sourcefire Defense Center: models DC750, DC1500, and DC3500; Sourcefire 3D Sensor licensed for IPS: models 3D500, 3D1000, 3D2000, 3D7110, 3D7120, 3D8120, 3D8130, 3D8140, and 3D8250; Sourcefire Virtual Defense Center, Sourcefire Virtual 3D Sensor licensed for IPS) Version 4.10.2.4 (SEU 568).

This VR is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The Target of Evaluation (TOE) is an Intrusion Detection System, which consists of the Sourcefire Defense Center and Sourcefire 3D Sensor licensed for IPS appliances, Sourcefire Virtual Defense Center, Sourcefire Virtual 3D Sensor licensed for IPS and Sourcefire 3D System Version 4.10.2.4 (SEU 568) software.

The TOE combines open-source and proprietary technology that is used to monitor incoming (and outgoing) network traffic, from either inside or outside a firewall. All packets on the monitored network are scanned, decoded, processed and compared against a set of rules to determine whether inappropriate traffic, such as system attacks, is being passed over the network. The system then notifies a designated TOE administrator of these attempts. The system generates these alerts when deviations of the expected network behavior are detected and when there is a match to a known attack pattern.

**Note:** The evaluation team did not evaluate the Sourcefire supplied rule sets that are bundled with the TOE for suitability to task—only that the tests included in the rule sets work correctly.

The Sourcefire 3D Sensor is based on an enhanced version of Snort, which is an open source IDS. Snort is used to read all the packets on the monitored network, and then analyze them against the rule set that has been created by the TOE administrators. The Sourcefire-modified Snort, version 2.9.2 is included in the TOE.

The TOE provides the following security functionality: auditing of security relevant events; TOE user account administration; TOE user identification and authentication; security role based access control to management functions; trusted communication between components; display of TOE access information; and system data collection, analysis, review, availability and loss.

**Note:** The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

The TOE is intended for use in computing environments where there is a low-level threat of malicious attacks. The assumed level of expertise of the attacker for all the threats is unsophisticated.

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed on 23 May 2012. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is Common Criteria

version 3.1 R3 [CC] Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL 2 augmented with ALC\_FLR.2 from the Common Methodology for Information Technology Security Evaluation, Version 3.1 R3, [CEM].

The evaluation and validation are consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site [www.niap-ccevs.org](http://www.niap-ccevs.org). The Security Target (ST) is contained within the document *Sourcefire 3D System Security Target (Sourcefire Defense Center: models DC750, DC1500, and DC3500; Sourcefire 3D Sensor licensed for IPS: models 3D500, 3D1000, 3D2000, 3D7110, 3D7120, 3D8120, 3D8130, 3D8140, and 3D8250; Sourcefire Virtual Defense Center; Sourcefire Virtual 3D Sensor licensed for IPS) Version 4.10.2.4 (SEU 568)*.

## 2 Identification

<b>Target of Evaluation:</b>	Sourcefire 3D System (Sourcefire Defense Center: models DC750, DC1500, and DC3500; Sourcefire 3D Sensor licensed for IPS: models 3D500, 3D1000, 3D2000, 3D7110, 3D7120, 3D8120, 3D8130, 3D8140, and 3D8250; Sourcefire Virtual Defense Center, Sourcefire Virtual 3D Sensor licensed for IPS) Version 4.10.2.4 (SEU 568))
<b>Assurance level:</b>	EAL2 augmented with ALC_FLR.2
<b>Evaluated Software and Hardware:</b>	<p><i>Sourcefire 3D System Version 4.10.2.4 (SEU 568) consisting of the following components:</i></p> <ul style="list-style-type: none"><li>• <i>The Sourcefire 3D Sensor licensed for IPS models 3D500, 3D1000, 3D2000, 3D7110, 3D7120, 3D8120, 3D8130, 3D8140, and 3D8250</i></li><li>• <i>The Sourcefire Defense Center models DC750, DC1500, and DC3500</i></li><li>• <i>The Sourcefire Virtual 3D Sensor license for IPS</i></li><li>• <i>The Sourcefire Virtual Defense Center</i></li></ul>
<b>Developer:</b>	Sourcefire, Inc.
<b>CCTL:</b>	CygnCom Solutions 7925 Jones Branch Dr., Suite 5400 McLean, VA 22102-3321
<b>Evaluators:</b>	Deepak Somesula
<b>Validation Scheme:</b>	National Information Assurance Partnership CCEVS
<b>Validators:</b>	Mr. Daniel P. Faigin, Dr. Patrick W Mallett
<b>CC Identification:</b>	Common Criteria for Information Technology Security Evaluation, Version 3.1 R3, July 2009
<b>CEM Identification:</b>	Common Methodology for Information Technology Security Evaluation, Version 3.1 R3, July 2009



### **3 Security Policy**

The TOE's security policy is expressed in the security functional requirements identified in Section 6.1 of the ST. Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements.

The TOE provides the security features described in the following sections.

#### ***3.1 Security Audit Functions***

The TOE is able to audit the use of the 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 TOE users once they are authenticated. Auditable actions include changes to the IDS rules and viewing/modifying the audit records of both the system access and the IDS event log.

Defense Centers, Virtual Defense Centers, and 3D Sensors with IPS log read-only auditing information for user activity in the Sourcefire 3D System audit log. The Virtual 3D Sensor with IPS, having no administrative GUI, does not record information to the audit log.

The audit data is protected by the access control mechanisms of the database and OS of the TOE components and by the TOE management interface. Only users with the Administrator Role or a Custom User Role with the "Operations -> Monitoring -> Audit" Permission have access to the audit records. Users having the Administrator Role or a Custom User Role with the "Operations -> Monitoring -> Audit" Permission can view and sort the audit records. Suppression lists may be configured during installation and maintenance to limit the events recorded.

When the available audit storage is exhausted, the TOE automatically overwrites the oldest audit events. This ensures that the availability of the most recent audit events is limited only by the size of the audit trail. It is the responsibility of the administrator to perform periodic backups of the audit data (via the WebUI backup function) to prevent loss of data.

Security Audit depends on the Operational Environment to provide reliable time for the audit records. It depends on an Email Server in the Operational Environment to provide warnings to administrators when the audit records are overwritten. It also depends on the Operational Environment to provide a secure communications path between the TOE and the external servers.

#### ***3.2 Identification and Authentication Functions***

The TOE requires all users to provide unique identification and authentication data before any access to the system is granted. User identification and authentication is done by the TSF through username/password authentication or optionally through the use of an

external authentication server for configurations that include a Defense Center or Virtual Defense Center. The appliance based Defense Center supports both LDAP and RADIUS; the Virtual Defense Center supports user authentication by an external LDAP server only.

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 level(s) of authorization (roles) for TOE users. The user account also contains a password strength check attribute. If selected the user's password must be at least eight alphanumeric characters of mixed case and must include at least one numeric character. It cannot be a word that appears in a dictionary or include consecutive repeating characters. The strength check applies only to user authentication done by the TOE for access to the management GUI; it does not apply to user authentications done by an external LDAP or RADIUS server.

Identification and Authentication depends on the Operational Environment to provide an external authentication server if that feature is configured. It also depends on the Operational Environment to provide a secure communications path between the TOE and the external authentication server.

### ***3.3 Security Management Functions***

The TOE provides a web-based (using HTTPS) management interface for all run-time TOE administration, including the IDS 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.

All users of the TOE have access to TSF data and management functions and therefore are considered administrators for the purposes of this evaluation. The pre-defined roles for TOE users are:

- “**Administrator**” Role: this role can perform all management, maintenance and analysis functions on the TOE.
- “**Maintenance**” Role: this role can view and manage status, security audit events, system time, and the reporting functionality of the product, and can also perform system level maintenance related actions.
- “**Intrusion Event Analyst**” Role: this role can view, analyze, review, and delete intrusion events and can also create incidents and generate reports.
- “**Intrusion Event Analyst (Read Only)**” Role: this role has read-only access to IPS analysis features, including intrusion event views, incidents, and reports.
- “**Policy and Response Administrator**” Role: this role can create, modify, and implement intrusion policies and intrusion rules for the IDS.

TOE users may also be assigned to one or more **Custom User Roles** that have been created by the Administrator. These Custom User Roles can be defined to have more restricted access to the WebUI management functions than the pre-defined roles.

The Custom User Roles can be used to give a user the permission, with a password, to gain temporarily the privileges of another user role. This allows administrators to substitute one user for another during an absence, or to track more closely the use of advanced user privileges,

The TOE also provides a command line interface, the use of which must be restricted. This interface is only used for Security Management when creating or modifying Audit Suppression Lists.

Security management relies on a management console in the Operational Environment with a properly configured Web Browser to support the web-based management interfaces.

### ***3.4 Protection of Security Functions***

The TOE ensures that data transmitted between separate parts of the TOE are protected from disclosure or modification. This protection is ensured through strong encryption during both setup and the transition of data. The TOE uses OpenSSL Version 0.9.8q and can be configured for Internet Protocol Version 6 (IPv6) Internet Layer protocol or IPv4 for packet-switched internetworks.

**Note:** The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

### ***3.5 TOE Access Functions***

The TOE enhances the functionality of user session establishment by displaying a warning banner upon user login.

### ***3.6 System Data Collection Functions***

The TOE has the ability to set rules to govern the collection of data regarding potential intrusions. While the TOE 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 TOE administrators complete control over the types of traffic that will be monitored.

**Note:** The evaluation team did not evaluate the Sourcefire supplied rule sets that are bundled with the TOE for suitability to task—only that the tests included in the rule sets work correctly

System Data Collection depends on the Operational Environment to provide reliable timestamps for the collected data records. It also depends on the Operational Environment to provide a physically secure communications path between the TOE and the external time server.

### ***3.7 System Data Analysis and Reaction Functions***

To analyze the data collected by the (Virtual) 3D Sensors with IPS, the TOE uses policies, signatures, statistical analysis, decoders, and preprocessors.

Sourcefire provides default intrusion policies for both passive and inline deployments. Administrators can tune policies by enabling or disabling preprocessor options and rules. Tuning preprocessor options and rule sets allows configuration, at a very granular level, of how the system processes and inspects the traffic on the network. Sourcefire 3D System Version 4.10.2.4 has the capability of constructing intrusion policies in building blocks, called policy layers. By editing a company-wide policy layer, all intrusion policies that incorporate that policy layer can be updated instantly.

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 decoders and preprocessors that are included in the TOE. The TOE embodies signatures, decoders, and preprocessors in rules that can be designed and exercised by the TOE.

The TOE administrators can manage the signature identification capabilities by adding and editing rules to respond to the latest exploits. In addition, based upon results of analysis, the TOE administrators can trigger alarms for the notification of a problem.

Sourcefire 3D System Version 4.10.2.4 includes a limited capability to detect and block rate-based denial-of-service (DoS) and distributed denial of service (DDoS) attacks through statistical analysis. Rate-base attack prevention identifies abnormal traffic patterns and attempts to minimize the impact of that traffic on legitimate service requests. Sourcefire's IPS functionality, without the use of a TCP proxy function, can detect hosts attempting to initiate or receive a configured number of connection attempts in a given time period, as well as hosts that have already established or received a configured number of connections in a given time period.

The Snort engine is used to read all the packets on the monitored network, and then analyze them against the rule set that has been created by the TOE administrators.

When a decoder, a preprocessor or statistical analysis identifies anomalous behavior, or when signature matches are found, they can either be logged for later use or set to trigger an alarm and immediately notify a specific person of critical events via email alerts. This is part of the configuration of active signatures and intrusion policies. The TOE can also be configured to enable logging to syslog facilities or send event data to an SNMP Trap Server.

If the 3D Sensor with IPS is deployed inline and traffic flows through a pair of interfaces on the sensor, the detection engine of the sensor can block possible intrusions by dropping suspicious traffic or replace harmful content in a packet if specified to do so by an intrusion policy.

However, no actions to drop or replace traffic when a possible intrusion has been detected will be taken if any the following conditions hold true:

- Passive deployment of 3D Sensors with IPS.

- Automatic application bypass feature is on and the bypass threshold time configured has been exceeded.
- The PEP feature has been configured to drop or fastpath network traffic.

**Note:** The PEP feature is only available on the 3D7000 and 3D8000 Series models of the sensor appliance.

System Data Analysis relies on the Operational Environment to support the notification of administrators via email and (optionally) SNMP (v2 or v3) and syslog alarms. It also depends on the Operational Environment to provide a secure communications path between the TOE and the external servers. System Data Analysis has a dependency on the Operational Environment to provide the user with updated rules and signature information that can then be input manually.

### ***3.8 System Data Review, Availability and Loss Functions***

IDS event logs can only be viewed by authorized TOE users (users with the Administrator or Intrusion Event Analyst Roles or a Custom User Role with the “Analysis & Reporting -> IPS -> Intrusion Events” Permission). 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. It is the responsibility of the administrator to perform periodic backups of the event data (via the WebUI backup function) to prevent loss of data.

System Data Review Availability and Loss depends on an Email Server in the Environment to provide warnings to administrators when the data records are overwritten. It also depends on the Operational Environment to provide a secure communications path between the TOE and the external email server.

## ***3.9 Summary***

### **3.9.1 SECURITY FUNCTIONAL REQUIREMENTS**

A summary of the SFRs for the TOE follows. Note that \_EXT in the SFR ID indicates extended requirements.

#### **1. FAU\_GEN.1: Audit data generation**

The TOE generates an audit record of the following auditable events:

- a. Start-up and shutdown of the audit functions;
- b. All auditable events for the basic level of audit; and
- c. Access to the System and access to the TOE and system data

The TOE records at least the following information: date and time of the event, type of event, subject identity, the outcome (success or failure) of the event and additional information depending on the event type, within each audit record.

#### **2. FAU\_SAR.1: Audit review**

The TOE provides users with the Administrator Role or a Custom User Role with the appropriate permissions, the ability to read all audit information.

3. **FAU\_SAR.2: Restricted audit review**

Unless a user has been granted read-access, the TOE prohibits access to the audit records.

4. **FAU\_SAR.3: Selectable audit review**

The TOE provides the ability to sort the audit data based on date and time, subject identity, type of event, and success or failure of related event.

5. **FAU\_SEL.1: Selective audit**

The TOE allows events to be included or excluded from the audit record based on: event type, IP address, message, subsystem, and username.

6. **FAU\_STG.2: Guarantees of data availability**

The TOE protects the stored audit records from unauthorized deletion.

The TSF is able to detect unauthorized modifications to the audit records.

When the available audit storage is exhausted, the TOE automatically overwrites the oldest audit events. This ensures that the availability of the most recent audit events is limited only by the size of the audit trail.

7. **FAU\_STG.4: Prevention of audit data loss**

The TOE overwrites the oldest stored audit records and sends an alarm if the audit trail storage is full.

8. **FIA\_ATD.1: User attribute definition**

User account information is stored in the TOE and contains the following attributes:

- User Name.
- Authentication Data (password).
- Authorizations (user roles).
- Use External Authentication Method.
- Force Password Reset on Login.
- Password Strength Check.
- Max Number of Failed Logins.
- Password Expiration.
- Days until Expiration Warning.
- Restrict Deletion Rights
- Command Line Interface Access

9. **FIA\_UAU\_EXT.1: Timing of authentication**

Each user must be successfully authenticated either by the TOE or by an authentication service (LDAP or RADIUS) in the Operational Environment invoked by the TOE before the TOE allows any actions aside from entry of the user's login data.

**10. FIA\_UID.1: Timing of identification**

Each user must be successfully identified before the TOE allows any actions aside from entry of the user's login data.

**11. FMT\_MOF.1: Management of security functions behavior**

The TOE restricts the ability to modify the system data collection, analysis and reaction and audit data generation functions of the TOE by user role.

**12. FMT\_MTD.1: Management of TSF data**

The TOE restricts the management functions of the TOE by user role.

**13. FMT\_SMF.1 Specification of Management Functions**

The TOE is capable of performing security management functions through the TOE user interfaces.

**14. FMT\_SMR.1: Security roles**

The TOE maintains the following user roles:

- Administrator
- Maintenance
- Intrusion Event Analyst
- Intrusion Event Analyst (Read Only)
- Policy and Response Administrator
- Custom User Role(s)

**15. FPT\_ITT.1: Basic internal TSF data transfer protection**

The TOE protects data from disclosure and modification when it is transmitted between the (Virtual) Defense Center and the (Virtual) 3D Sensor(s) with IPS by using a secure, SSL-encrypted TCP tunnel.

**16. FTA\_TAB.1: Default TOE access banners**

The TOE has the capability to display a warning message regarding unauthorized use of the TOE on the user login screen.

**17. IDS\_SDC\_EXT.1: System Data Collection**

The TOE is able to collect network traffic information from targeted IT System resource(s).

The TOE collects and records the following network traffic information: date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; Protocol Source address Destination address.

**18. IDS\_ANL\_EXT.1: Analyzer analysis**

The TOE uses signatures, decoders and preprocessors to analyze the network data collected.

**19. IDS\_RCT\_EXT.1: Analyzer react**

When an intrusion is detected, the TOE is able to send an alarm to a designated email administrative address, an external syslog server, and/or an external trap server.

When an intrusion is detected, the TOE is able to drop or replace packets containing suspicious network traffic according to the administrator-configured rules for inline deployment of (Virtual) 3D Sensors with IPS. The TOE will take no actions for sensors passively configured.

**20. IDS\_RDR\_EXT.1: Restricted Data Review**

The TOE provides only users with the Administrator Role or a Custom User Role with the appropriate permissions with the capability to read all captured IDS data from the system data

**21. IDS\_STG\_EXT.1: Guarantee of System Data Availability**

The TOE protects the stored audit records from unauthorized modification and deletion.

When the available system storage is exhausted, the TOE automatically overwrites the oldest system event data.

**22. IDS\_STG\_EXT.2: Prevention of System data loss**

The TSF will overwrite the oldest stored system data and send an alarm if the storage capacity has been reached.

**3.9.2 OPERATIONAL ENVIRONMENT OBJECTIVES**

The TOE's operating environment must satisfy the following objectives.

1. Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.
2. Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
3. Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner that is consistent with IT security.
4. Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.
5. The TOE is interoperable with the IT System it monitors.
6. The Operational Environment will provide reliable timestamps to the TOE.
7. The Operational Environment will provide mechanisms to notify responsible personnel of a possible problem.



8. The Operational Environment must provide a mechanism to establish a trusted communications path, which provides for the protection of the data from modification or disclosure while being exchanged between TOE components and external entities.
9. The Operational Environment must provide an authentication service for user identification and authentication that can be invoked by the TSF to control a user's logical access to the TOE.

**Note:** This objective is only applicable when the TOE is configured to use an external LDAP or RADIUS authentication service.

10. The Operational Environment must ensure that all packets coming in to the physical ports of the VMware hosts are transmitted unchanged to the virtual ports in the VMware environment.

**Note:** Customers are responsible for using a VMware version that is not subject to vulnerabilities and for patching their VMware server accordingly as vulnerabilities are identified.

## 4 Assumptions and Clarification of Scope

### 4.1 Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL 2 assurance requirements:

- AGD\_OPE.1 Operational user guidance
- AGD\_PRE.1 Preparative procedures
- ALC\_CMC.2 Use of a CM system
- ALC\_CMS.2 Parts of the TOE CM coverage
- ALC\_DEL.1 Delivery procedures

### 4.2 Assumptions

#### **TOE Intended Usage Assumptions:**

- The administrators must make sure that the Defense Center and 3D Sensors with IPS have full access to the networks and external servers in the Operational Environment.
- Administrators must make sure that they use the administrative functions of the WebUI and the CLI to modify the TOE configuration in response to any Operational Environment changes.
- To ensure that network traffic does not bypass the IPS functionality of the 3D Sensors with IPS, the customer must choose the appropriate sensor model for their network and administrators must follow the guidelines in the user guidance for optimal deployment of the sensors. The customer must choose a 3D Sensor model that matches or exceeds the traffic bandwidth of the network segment it monitors.

#### **TOE Physical Assumptions:**

- Access to the Defense Center and the 3D Sensors with IPS must be physically restricted (i.e., located within controlled access facilities, which will prevent unauthorized physical access)
- All packets coming in to the physical ports of the VMware hosts are transmitted unchanged to the virtual ports in the VMware environment.

#### **TOE Personnel Assumptions:**

- Administrators of the TOE must be carefully selected and be properly trained to manage the TOE and ensure the security of the information it contains.
- Only required personnel should have user accounts on the system and they must protect their authentication information (username and password).

### ***4.3 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 (EAL 2 in this case).
2. This evaluation only covers the specific version of the product identified in this document, and not any earlier or later versions released or in process.
3. As with all EAL 2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, 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.
4. The following are not included in the Evaluation Scope:
  - Real-Time Network Awareness (RNA) – RNA is a separate product that requires additional licensing
  - Vulnerability Assessment (VA) - VA requires integration with Nmap and is only applicable with RNA license
  - Network Behavior Analysis (NBA) – NBA requires an RNA license
  - Collection of data from NetFlow devices– requires Cisco NetFlow and an RNA license
  - Adaptive IPS – uses information from RNA
  - Real-Time User Awareness (RUA) – RUA is a separate product that requires additional licensing
  - NAC and Network Usage Control (NUC) – requires RUA license
  - Intrusion Agents - Requires an existing installation of Snort
  - Estreamer Application Programming Interface (API) - Estreamer integration requires custom programming
  - Security Enhancement Updates (SEU) – The updates may include binary updates to the TOE software, which will take the product out of the evaluated configuration when installed
  - A Master Defense Center (MDC) – requires a multiple Defense Center configuration
  - The High Availability feature - requires a multiple Defense Center configuration
  - IPS for Crossbeam Systems Security Switches (software-only sensors)

- Switched Stack System Interconnect (“stack”) configuration (installation of an additional chassis using a stack cable)
  - Integration with and remediation of traffic to firewalls, routers, and other external devices, including:
    - Integration with Cisco PIX and Checkpoint firewalls
  - Integration with and remediation of traffic to external 3rd-party products, including:
    - Sending alerts through trouble ticket systems
    - Interfaces with the patch management systems
  - Xen Hypervisor platforms for virtual components.
  - Integration with Checkpoint OPSEC™ Suspicious Activity Monitor (SAM), including sending OPSEC alerts and use of OPSEC responses
  - Defense Center database access using an external third-party client
5. The Operational Environment needs to provide the following capabilities:
- The Web Browser for the Defense Center, Virtual Defense Center and 3D Sensor with IPS Management Interfaces. Only the following were tested for Sourcefire 3D System Version 4.10.2.4:
    - Firefox Version 7
    - Microsoft Internet Explorer Version 7.0
    - Microsoft Internet Explorer Version 8.0
  - The protected network(s) used for communications between the TOE components
  - The network(s) that are to be monitored
  - Network Authentication Services
  - A trusted DNS Server
  - An external NTP Server
  - An external Email Server
  - An optional external Syslog Server
  - An optional external SNMP Trap Server
  - An optional external LDAP or RADIUS Authentication Server
  - The platforms for the Virtual Defense Center and Virtual 3D Sensor with IPS including the platform hardware, the underlying platform operating system and the VMware ESX implementation

The ST provides additional information on the assumptions made and the threats countered.

**Note:** The evaluation team did not evaluate the Sourcefire supplied rule sets that are bundled with the TOE for suitability to task—only that the tests included in the rule sets work correctly

**Note:** The cryptographic functions used by the TOE are not FIPS certified. Correctness of the encryption mechanisms used by the TOE is by Vendor Assertion.

**Note:** Customers are responsible for using a VMware version that is not subject to vulnerabilities and for patching their VMware server accordingly as vulnerabilities are identified.

**Note:** The following TOE components were used in testing:

- Virtual Defense Center
- DC1500 Defense Center
- Virtual Sensor
- 3D2000 Sensor (32-bit SFLinux)
- 3D7120 Sensor (64-bit SFLinux)
- 3D8140 Sensor (64-bit SFLinux)

Because of their identical functionality and behavior, not every 3D Sensor appliance from each category of 3D Sensors was used in evaluator testing.

**Note:** The sensors were located in the same physical location as the Defense Center in the testing scenarios. This is equivalent to deployment scenarios where the sensors are in multiple physical locations because the same SSL-encrypted communications channel is used between the sensors and Defense Center, except that it is transmitted over a VPN in the multi-site scenario.

## 5 Architectural Information

The Sourcefire 3D Sensor is based on an enhanced version of Snort, which is an open source IDS. Snort (as modified and included in the TOE) is used to read all the packets on the monitored network, and then analyzes them against the rule set that has been created by the TOE administrators.

A detection engine is the mechanism on a Sourcefire 3D Sensor that is responsible for analyzing the traffic on the network segment where the sensor is connected. A detection engine has two main components:

- An **interface set**, which can include one or more sensing interfaces
- A **detection resource**, which is a portion of the sensor's computing resources

Depending on which components are licensed on the sensor, Sourcefire 3D Sensors can support three types of detection engines:

- Intrusion Prevention System (IPS)
- Real-Time Network Awareness (RNA)
- Real-Time User Awareness (RUA)

Only the IPS detection engine is included in the scope of this evaluation.

Each 3D Sensor with IPS, both virtual and appliance-based, uses rules, decoders, and preprocessors to look for the broad range of exploits that attackers have developed. Sourcefire 3D Sensors that are licensed to use IPS are packaged with a set of intrusion rules developed by the Sourcefire Vulnerability Research Team (VRT). The TOE administrators can choose to enable rules that would detect the attacks most likely to occur on the monitored network. Custom intrusion rules and policies can also be created for a customer's operating environment.

**Note:** The evaluation team did not evaluate the Sourcefire supplied rule sets that are bundled with the TOE for suitability to task—only that the tests included in the rule sets work correctly

When a (Virtual) 3D Sensor with IPS identifies a possible intrusion, it generates an intrusion event, which is a record of the date, time, the type of exploit, and contextual information about the source of the attack and its target. For packet-based events, a copy of the packet or packets that triggered the event is also recorded.

The Sourcefire 3D Sensor licensed for IPS is an appliance-based component of the TOE and includes both software and hardware. 3D Sensors with IPS can be deployed either inline, where "live" traffic passes through the appliance, or passively, in which case traffic is being only monitored. When used inline, IPS can block malicious code and attacks in real-time so that the 3D Sensor with IPS is used as an intrusion prevention device.

In a passive deployment, the sensing interfaces connected to the network are configured in stealth mode so that, to other devices on the network, the sensor itself does not appear to be connected to the network at all. A benefit of passive deployment is that almost all of

the sensor bandwidth and computational power are devoted to monitoring traffic, reconstructing datagrams and streams, normalizing packets, detecting anomalies, and sending alerts of possible intrusions. Moreover, because the sensor is deployed out of band and operates in stealth mode, attackers are unlikely to know of its existence, which renders it less of a target for attacks. However, in a passive deployment the 3D Sensor with IPS can only perform passive intrusion detection and send alerts when it detects malicious traffic packets, but it cannot affect the flow of network traffic.

Both the inline and passive deployments are included in the evaluated configuration.

In addition, 3D Sensors with IPS run decoders and preprocessors against detected network traffic to normalize traffic and detect malicious packets. If the 3D Sensor with IPS is deployed inline on the network and creates what is called an inline detection engine, the 3D Sensor with IPS can be configured to drop or replace packets that are known to be harmful.

PEP is an optional feature available only for the 3D8120, 3D8130, 3D8140 and 3D8250 (8000 Series) and 3D7110 and 3D7120 (7000 Series) models of the sensor appliance. PEP allows users to create policies that drop or fastpath (send through the sensor without analysis) network traffic for user specified targets. PEP and fast path rules can be created to block, analyze, or send traffic directly through these sensors with no further inspection. The PEP feature therefore allows the user to override the normal collection and analysis functions of the sensor.

An additional option only available on the 7000 and 8000 Series sensors is the Enable Fail-Safe option. The Enable Fail-Safe option is only available on inline interface configurations. When enabled, traffic is allowed to bypass detection and continue through the sensor. The 7000 and 8000 Series sensors monitor internal traffic buffers and bypass detection engines if those buffers are full.

The 8000 Series and 7000 Series sensors cannot be run stand-alone and must be managed and licensed with a Defense Center. These sensors have a Limited WebUI, which is accessed in the same manner as the Defense Center WebUI except that user authorization cannot be done by an external authentication server. Detection engines and interface sets cannot be managed from the WebUI of the 7000 Series and 8000 Series sensors. The user accounts for access to the Limited WebUI are kept separately from the Defense Center user accounts. The only user role for access to the Limited WebUI is “Administrator”.

The Sourcefire Virtual 3D Sensor licensed for IPS is a software-only version of the Sourcefire 3D Sensor licensed for IPS that runs within a VMware virtual environment. The Virtual 3D Sensor with IPS runs on any platform that supports VMware’s ESX/ESXi Version 4.1 or higher hypervisor. Virtual 3D Sensors with IPS differ from the appliance-based 3D Sensors with IPS by the following features and limitations:

- Appliance-based versions of the 3D Sensor with IPS can inspect traffic going into and out of a VMware virtual environment, but they cannot inspect traffic that passes between two or more virtual machines (VMs). The Virtual 3D Sensor with IPS, on the other hand, can monitor the network activity between any two VMs.
- The IPS feature for a Virtual 3D Sensor is licensed through a Defense Center (appliance-based or virtual). An IPS feature license for a Virtual 3D Sensor must

be added to the managing Defense Center to process and store IPS events from the Virtual 3D Sensor with IPS.

- There is no embedded graphical user interface (WebUI) on the Virtual 3D Sensor with IPS. It must be managed with a Defense Center (appliance-based or virtual). However, virtual sensors do have a command line interface (CLI) which contains a controlled set of management commands and options that is used for off-line installation, configuration and maintenance of the virtual sensors.
- The Virtual 3D Sensor with IPS does not record user events to an audit log itself. It depends on its controlling Defense Center for all audit functionality.
- There is no event storage on a Virtual 3D Sensor with IPS; a Defense Center (appliance-based or virtual) must be used to store the events from the sensor.
- There is no backup and restore on a Virtual 3D Sensor; a Defense Center (appliance-based or virtual) must be used for backup and restoration.
- The Virtual 3D Sensor with IPS has a limit of three detection engines, a maximum rate of 250 Mbps per detection engine, and three detection resources.

The Sourcefire Defense Center is an appliance-based component of the TOE and includes both software and hardware. The Sourcefire Defense Center provides a centralized management interface for the Sourcefire 3D System. The Defense Center is used to manage the full range of sensors that are a part of the Sourcefire 3D System, and to aggregate, analyze, and respond to the threats they detect on the monitored network. A Defense Center can manage from 3 to 100 sensors depending on the appliance model.

In a Sourcefire 3D System deployment that includes (Virtual) 3D Sensors with IPS and a Defense Center, the sensors transmit events and sensor statistics to the Defense Center where the aggregated data can be viewed.

The Sourcefire Virtual Defense Center is a software-only version of the Sourcefire Defense Center that runs within a VMware virtual environment. Virtual Defense Center can manage both physical and virtual sensors. Virtual Defense Centers differ from the appliance-based Defense Centers only by the following features and limitations:

- A Virtual Defense Center can store up to 10 million intrusion events and 10 million flow events.
- A Virtual Defense Center provides the ability to manage up to 25 3D Sensors.
- A Virtual Defense Center does not support RADIUS authentication.
- A Virtual Defense Center cannot be used as a Master Defense Center but it can be managed by a Master Defense Center. Note: A Master Defense Center is not included in the evaluated configuration.

Some models of the appliance-based 3D Sensor with IPS provide a local web interface (WebUI) to create intrusion policies and review the resulting intrusion events and therefore can be run stand-alone, without using a Defense Center for management.

The (Virtual) Defense Center provides the following functionality through a web-based GUI (WebUI):



- An interface that displays all the data collected by the managed 3D Sensors with IPS allowing:
  - Monitoring of the information that the sensors are reporting in relation to one another
  - Assessment of the overall activity occurring on the monitored network
- An interface to analyze and respond to the alerts generated by the sensors
- The aggregation and correlation of intrusion events, network discovery information, and sensor performance data
- The ability to create and configure rules and policies for managed sensors and push the rules and policies to the sensors
- The ability to push health policies to the sensors and monitor their health status
- TOE configuration and management capabilities including configuration and management of user accounts and auditing

The TOE consists of the components described above. The physical boundary of the TOE is:

- The Sourcefire 3D Sensor licensed for IPS appliance
- The Sourcefire Defense Center appliance

The appliance based components are installed with the Sourcefire 3D System Version 4.10.2.4 (SEU 568) software, Linux-derived operating system, MySQL database, and supporting 3rd party software as commercially available from the developer

- The Sourcefire Virtual Defense Center
- The Sourcefire Virtual 3D Sensor licensed for IPS

The virtual components consist of all software that is on the installation media including Sourcefire 3D System Version 4.10.2.4 (SEU 568) software, Linux-derived operating system, MySQL database, and supporting 3rd party software.

The TOE Boundary is depicted in the following figures.

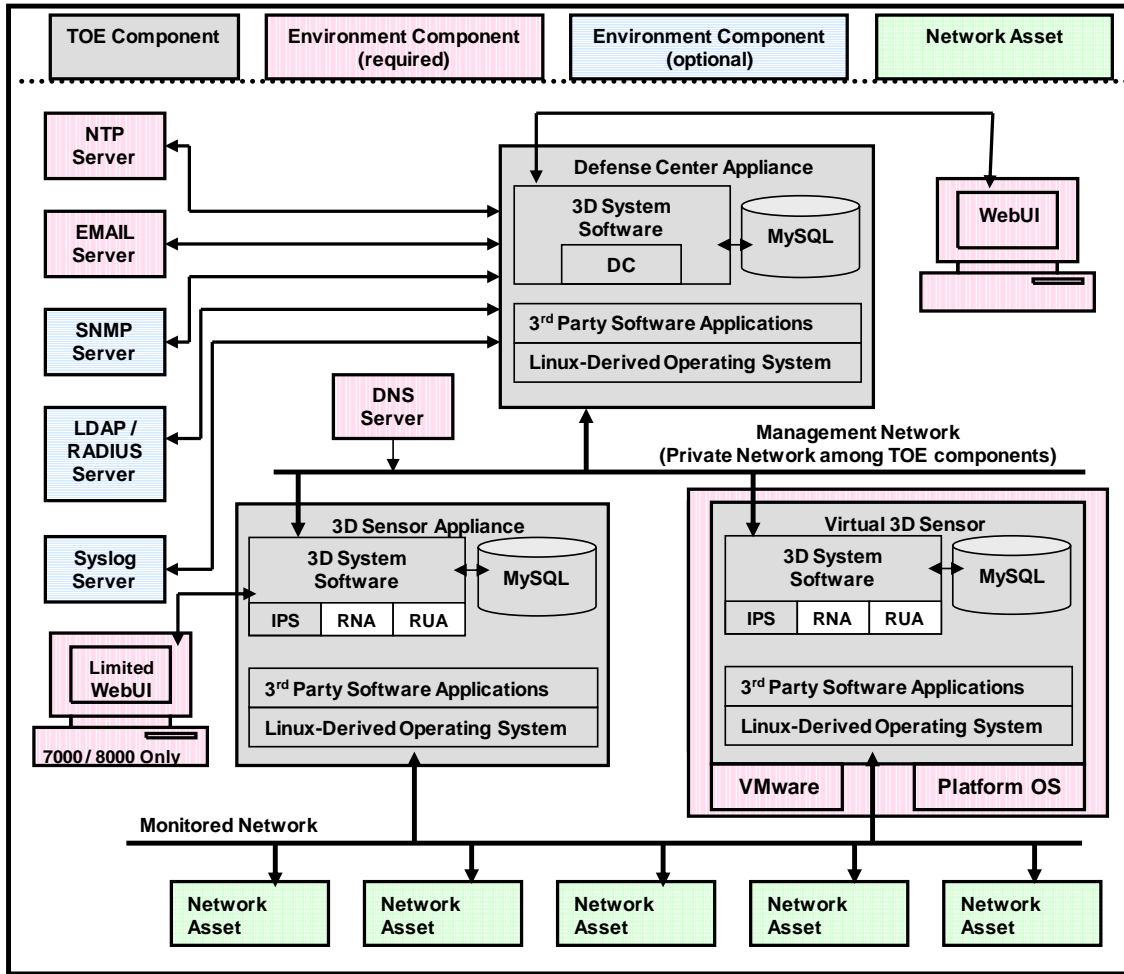


Figure 1: TOE: Boundary - Sourcefire 3D System with Defense Center

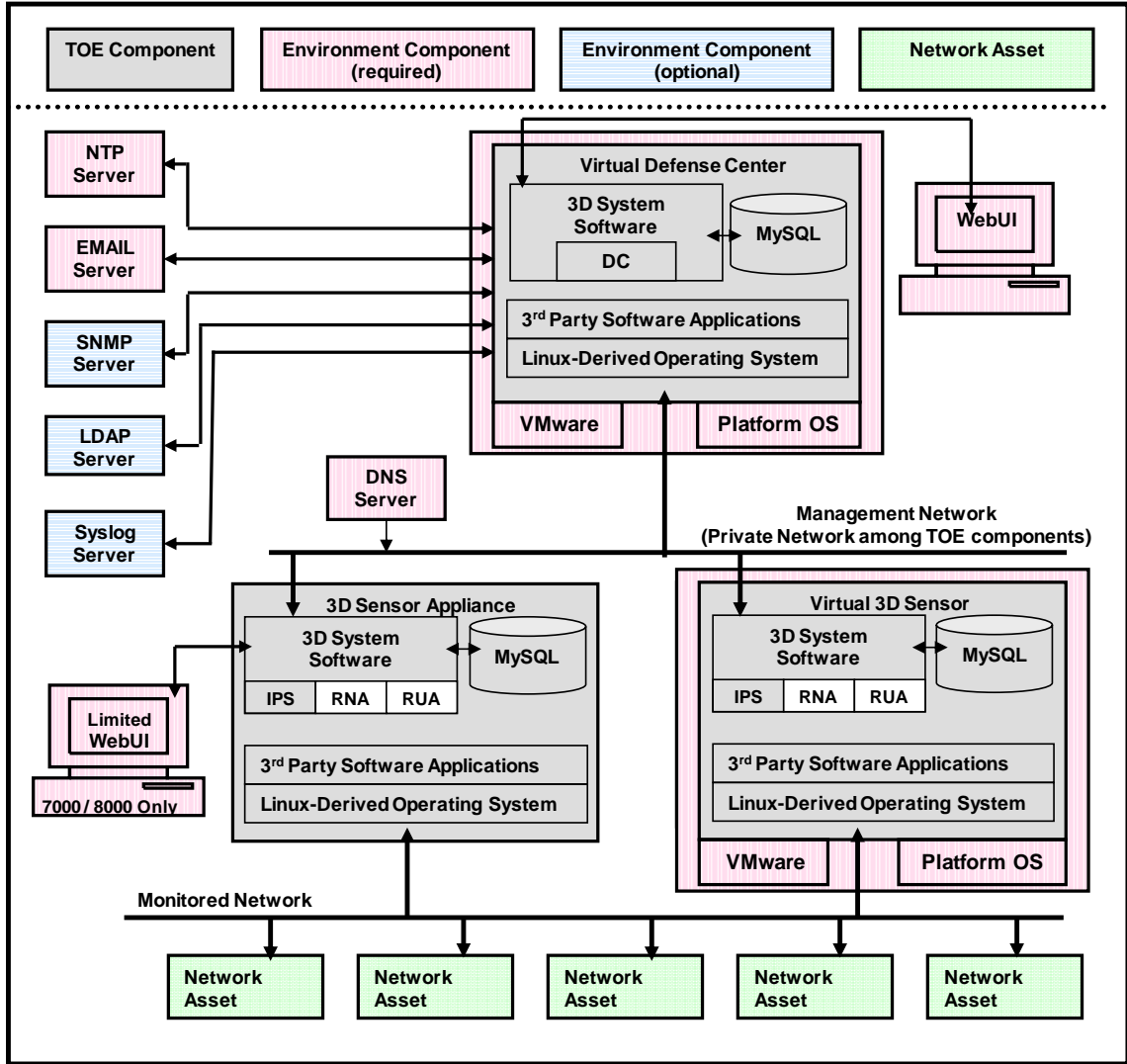
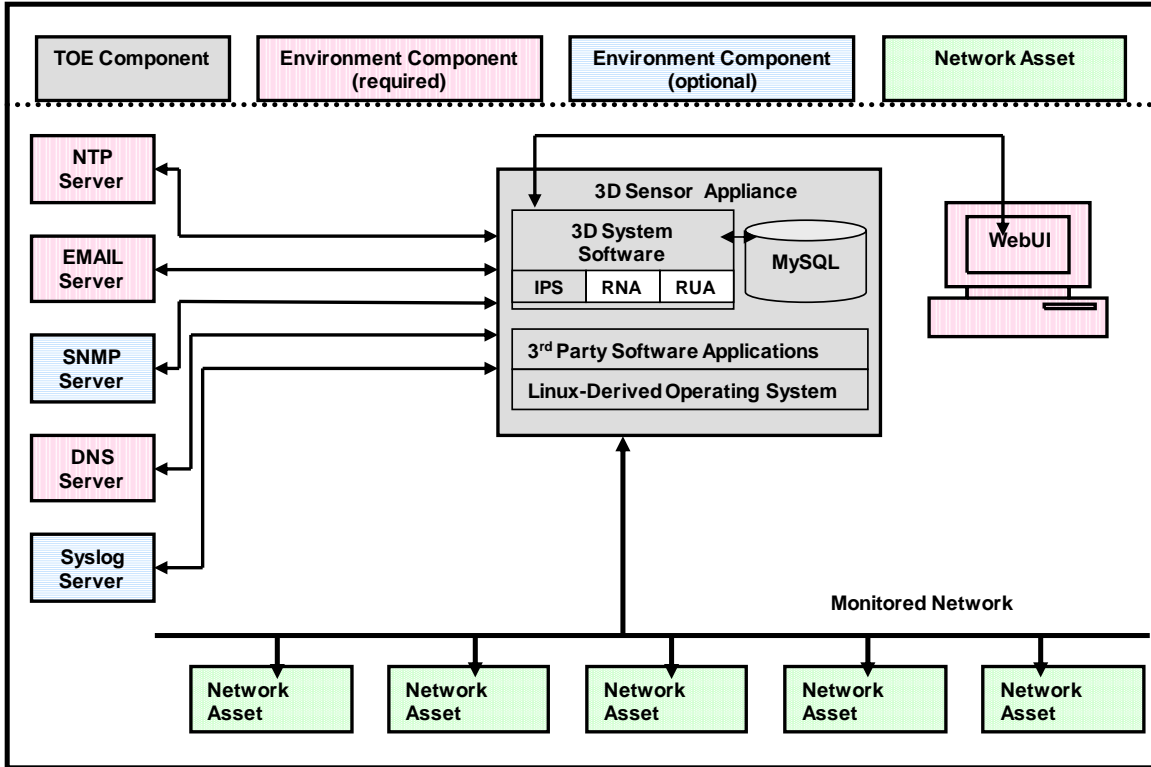


Figure 2: TOE: Boundary - Sourcefire 3D System with Virtual Defense Center



**Figure 3: TOE: Boundary - Sourcefire 3D System using a stand-alone 3D Sensor with IPS**

## 6 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the Network Security Platform and methodology for delivery of the evaluated configuration. In these tables, the following conventions are used:

Documentation that is delivered to the customer is shown with **bold** titles.

Documentation that was used as evidence but is not delivered is shown in a normal typeface.

The TOE is physically delivered to the End-User. The guidance is part of the TOE and is delivered in printed form and as PDFs on the installation media.

### 6.1 Product Guidance

The following documents are developed and maintained by Sourcefire and delivered to the end user of the TOE:

<b>Guidance Documentation</b>	<b>Version</b>	<b>Date</b>
<b>Sourcefire 3D System - 3D Sensor Installation Guide</b>	4.10.2	2011-12-04
<b>Sourcefire 3D System - Defense Center Installation Guide</b>	4.10.2	2011-11-01
<b>Sourcefire 3D System – Virtual Defense Center and 3D Sensor Installation Guide</b>	4.10.2	2011-09-23
<b>Sourcefire 3D System - Sourcefire 3D System User Guide</b>	4.10.2	2011-11-01
<b>Sourcefire 3D System Release Notes</b>	4.10.2.4	2012-04-09
<b>Sourcefire 3D System – Common Criteria Supplement to the Administrative Guidance Version 4.10.2.4</b>	1.1	2012-05-14

### 6.2 Evaluation Evidence

In addition to the guidance documentation listed above, the following documentation was submitted as evaluation evidence by the vendor. With the exception of the Security Target, these documents may be proprietary and not available to the general public. This list does not include small graphics files and email evidence.

<b>Design Documentation</b>	<b>Version</b>	<b>Date</b>
Sourcefire 3D System Version 4.10.2.4 Functional Specification	0.7	2012-04-09
Sourcefire 3D System Version 4.10.2 WebUI Administration Interface Details	0.7	2012-02-01
Sourcefire 3D System Version 4.10.2.4 TOE Design	0.6	2012-04-05
Sourcefire 3D System Version 4.10.2.4 Security Architecture	0.6	2012-04-05

<b>Life Cycle Documentation</b>	<b>Version</b>	<b>Date</b>
Sourcefire 3D System Configuration Management Plan	1.0.1	2012-04-11
Sourcefire Intrusion Detection System Delivery Procedures	1.0	2012-02-15
Sourcefire 3D System Version 4.10.2.4 Flaw Reporting Procedures	0.3	2012-04-19

<b>Test Documentation</b>	<b>Version</b>	<b>Date</b>
Sourcefire 3D System Version 4.10.2.4 - Test Coverage Document	0.1	2012-01-10
Test Plan for Common Criteria Evaluation (EAL2) Testing for Sourcefire 3D System 4.10.2.4	1.0.2	2012-04-11
4.10.2.4 EAL2 Test Report	--	2012-04-18
4.10.2 EAL2 Tests and Screenshots (numerous files)	--	2012-02-13
4.10.2 Test Pcaps (numerous files)	--	2012-01
EAL2 ON-SITE TESTING Sourcefire 3D System Version 4.10.2.4 (SEU 568) EAL 2 Evaluation	0.1	2012-04-18
Evaluator Testing: Test Results: DC Port Scan, Developer Tests, Independent Tests, Installation, Vulnerability Scan Reports (numerous files)	--	2012-05-04
Evaluator Testing Pcaps (numerous files)	--	2009-05-19

<b>Security Target</b>	<b>Version</b>	<b>Date</b>
Sourcefire 3D System Security Target (Sourcefire Defense Center: models DC750, DC1500, and DC3500; Sourcefire 3D Sensor licensed for IPS: models 3D500, 3D1000, 3D2000, 3D7110, 3D7120, 3D8120, 3D8130, 3D8140, and 3D8250; Sourcefire Virtual Defense Center; Sourcefire Virtual 3D Sensor licensed for IPS) Version 4.10.2.4 (SEU 568)	1.0	2012-05-14

<b>Evaluation Technical Reports</b>	<b>Version</b>	<b>Date</b>
Evaluation Technical Report for a Target of Evaluation, Volume 1: Evaluation of the ST, Sourcefire, Incorporated, Sourcefire 3D System Version 4.10.2, Security Target Version 1.0, ETR Version Volume 1.0	1.1	2012-05-21
Evaluation Technical Report for a Target of Evaluation, Volume 2: Evaluation of the TOE, Sourcefire, Incorporated, Sourcefire 3D System Version 4.10.2, Security Target Version 1.0, ETR Version Volume 2.0	2.1	2012-05-21

## 7 IT Product Testing

At EAL 2, the overall purpose of the testing activity is “independently testing a subset of the TSF, whether the TOE behaves as specified in the design documentation, and to gain confidence in the developer's test results by performing a sample of the developer's tests” (ATE\_IND.2, 14.6.2.1 [CEM])

At EAL 2, the developer’s test evidence must “show the correspondence between the tests provided as evaluation evidence and the functional specification. However, the coverage analysis need not demonstrate that all TSFI have been tested, or that all externally visible interfaces to the TOE have been tested. Such shortcomings are considered by the evaluator during the independent testing.” (ATE\_COV.1, 14.3.1.3 [CEM])

This section describes the testing efforts of the vendor and the evaluation team.

The objective of the evaluator’s independent testing sub-activity is “to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests” (ATE\_IND.2, Independent testing – sample [CC]).

### 7.1 Developer Testing

The developer testing effort that is described in detail in the Developer Test Plan involved executing the test sets in the test configurations described in Section 8: Evaluated Configuration.

#### 7.1.1 OVERALL TEST APPROACH AND RESULTS:

Sourcefire testing consisted of the following types of tests:

- **Manual Tests:**

All the developer tests except the IDS/IPS tests were performed manually. All expected results are mentioned as part of the Developer’s test procedure description and all actual results are observations to ensure that expected results match actual results.

- **IDS Functionality Tests (Semi-Automated):**

Testing the IDS/IPS functionality of the product consisted of generating known attack traffic, in the form of PCAP files, using the tcpreplay tool. PCAP (packet capture) consists of an application programming interface (API) for capturing network traffic. Unix-like systems implement PCAP in the libpcap library. The traffic is collected by the TOE, and based on the policy that is applied on the TOE, alerts are generated. The expected results for each test include the alert that must be generated based on the PCAP file. The actual results included verification of the generated alert.

### **7.1.2 DEPTH AND COVERAGE**

All developer test cases test TOE security functions by stimulating an external interface. Although the developer tests are performed using the WebUI, the evaluator determined that the test cases as described in the test documentation adequately exercise the internal interfaces.

TOE testing directly tests external TSF interfaces. The behavior of the TSF is realized at its interfaces. Hostile intent will be expressed at the Network Asset Interface.

The evaluator ensured that the test sample included the tests such that:

- All Security Functions are tested
- All External interfaces are exercised
- All Security Functional Requirements are tested.
- More emphasis is laid on the Network Interface being tested.
- All relevant security relevant features mentioned in the Administration/User Guides are covered in testing.

Since the product is primarily an Intrusion Detection functionality product, it is difficult to gauge the extent of coverage for the network interfaces. Evaluators worked with Sourcefire to determine the adequate extent of coverage required at EAL 2.

### **7.1.3 RESULTS**

The evaluator checked the test procedures and the Test Evidence and found that the expected test results are consistent with the actual test results provided. For each test case examined, the evaluator checked the expected results in the test procedures with the actual results provided in the Test Evidence and found that the actual results were consistent with the expected results. The evaluator checked all of the test procedures.

Given the Evaluation Assurance level (EAL 2), the evaluator determined that Sourcefire's TOE testing is adequate. All the external TSF interfaces are tested. TOE testing exercises all security functions identified in the Functional Specification.

## ***7.2 Evaluator Independent Testing***

The evaluator performed the following activities during independent testing:

- Execution the Developer's Functional Tests (ATE\_IND.2)
- Team-Defined Functional Testing (ATE\_IND.2)
- Vulnerability/Penetration Testing (AVA\_VAN.2)

### **7.2.1 EXECUTION THE DEVELOPER'S FUNCTIONAL TESTS**

The evaluator selected to rerun 50% of the developer's tests:

- As a means of ensuring the coverage of the security features.



- As a means to gain confidence in the developer’s test results.
- A quick means of ensuring TOE is in a properly configured state.

The developer’s test cases were executed only after the TOE was installed in the evaluated configuration that is consistent with the Security Target (Section 1) and the Sourcefire Common Criteria Supplement Document. The evaluator confirmed that the test configuration was consistent with the evaluated configuration in the Security Target and the Sourcefire CC Supplement.

The test configurations used by the evaluator were the same as that used by the developer.

The test results and screenshots for the test cases were recorded during the Evaluator testing. Overall success of the testing was measured by 100% of the retests being consistent with expected results. Anomalies were documented along with suggested / required solutions.

Only one Developer Test caused a problem when run by the Evaluator:

**Sourcefire Test Case ID - 31913** – This test case could not be run as described in the document – 4.10.2 EAL2 Test Report. The evaluator detected a missing step because the test case as executed didn’t detect TCP anomalies in traffic. The missing step was added [TCP stream and check stateful inspection anomalies] to detect the IP defragmentation data.

All of the Developer’s Functional Tests rerun by the Evaluator received a ‘Pass’ verdict.

## **7.2.2 TEAM-DEFINED FUNCTIONAL TESTING**

The Evaluator selected individual test procedures from the set of Developer Functional Tests, and modified the input parameters to ensure fuller coverage of security functions and correctness of developer reported results (ensuring that the results were not canned).

Additional tests were developed for the purpose of verifying that the product operates in accordance with Vendor claims, i.e. that a bug is fixed or a capability operates as described in the product documentation.

The test results and screenshots for the test cases were recorded during the Evaluator testing. Overall success of the testing was measured by 100% of the tests being consistent with expected results. Anomalies were documented along with suggested / required solutions.

The Evaluator developed the following additional tests:

1. Test that the TOE maintains the following attribute for each user: Password Strength Check
2. Test that the following information is recorded in each audit record “data and time of event” with the event in this case being a login failure
3. Audit Log Suppression by Username
4. Test that the TOE can perform the following analysis functions on all IDS data received: SSL Configuration – Test to be performed on a 3D7120 Sensor

5. Test the TOE's capability to perform the IDS/IPS functionality by using research pcaps developed by other sources.
6. Test the automatic conversion from internal to external authentication when external authentication is enabled.

All of the Team-Defined Tests received a 'Pass' verdict.

### **7.2.3 VULNERABILITY/PENETRATION TESTING**

The Vulnerability / Penetration tests covered hypothesized vulnerabilities and potential misuse of guidance.

The search for publicly known vulnerabilities included searching for vulnerabilities that affected the IDS/IPS class of products that could potentially be applicable to the TOE.

During the Vulnerability Analysis of the TOE, the Evaluator found publicly known vulnerabilities that affected the Sourcefire product line or product. The Evaluator worked with the developer to find a rationale for the identifying the vulnerabilities.

The evaluator further investigated the areas in which the underlying OS in the TOE differed from the current STIG configuration since the OS does not strictly conform to the STIG [UNIX – Security Technical Implementation Guide – V5, R1].

The evaluator also investigated the areas in which the web server component of the TOE differed from the current STIG configuration since the web server does not strictly conform to the STIG [WEB SERVER– Security Technical Implementation Guide – V6, R1].

All identified vulnerabilities were ruled out in the evaluated configurations.

Given that the product is an IDS/IPS product offering Intrusion Detection functionality, the Evaluator found that the functional testing performed by the developer encompassed a great area of vulnerability and penetration testing. Several PCAP files with various malicious/malformed traffic, worms, viruses, etc. were tested to show that the product triggers appropriate rules, is resistant to them, and, when configured, mitigates them.

Instead of devising individual penetration tests, the evaluator felt that testing different interfaces of the product against network penetration attacks offered by the latest set of Nessus plug-ins and re-running the fuzz tests that Sourcefire uses for their SEU testing were apt. Hence, all penetration testing for this product was conducted using Nessus to test the resistance of the product to publicly available attacks, which include Denial of Service attacks.

The evaluator ran the following test on a Defense Center (DC1500), a 3D Sensor with IPS (running 32-bit SFLinux) appliance (3D2000), a 3D Sensor with IPS (running 64-bit SFLinux) appliance (3D7120), a Virtual Defense Center and a Virtual 3D Sensor with IPS.

- Set up the Nessus Laptop such that a ping from the laptop can reach the Management Ports of the component. Make sure that there are no routers between the TOE and the Nessus Laptop.

- Run a Nessus Scan with all plugins turned on against one of the Management Ports.

The test results and screenshots for the test cases were recorded during the evaluator testing. Overall success of this testing was measured by 100% of the tests being consistent with expected results.

## 8 Evaluated Configuration

The TOE was tested the following test bed components:

- DC1500 (32-bit SFLinux)
- 3D2000 sensor (32-bit SFLinux)
- 3D7120 sensor (64-bit SFLinux)
- 3D8140 sensor (64-bit SFLinux)
- Virtual Defense Center
- Virtual 3D Sensor with IPS

**Note:** Because of their identical functionality and behavior, not every 3D Sensor appliance from each category of 3D Sensors was used in evaluator testing.

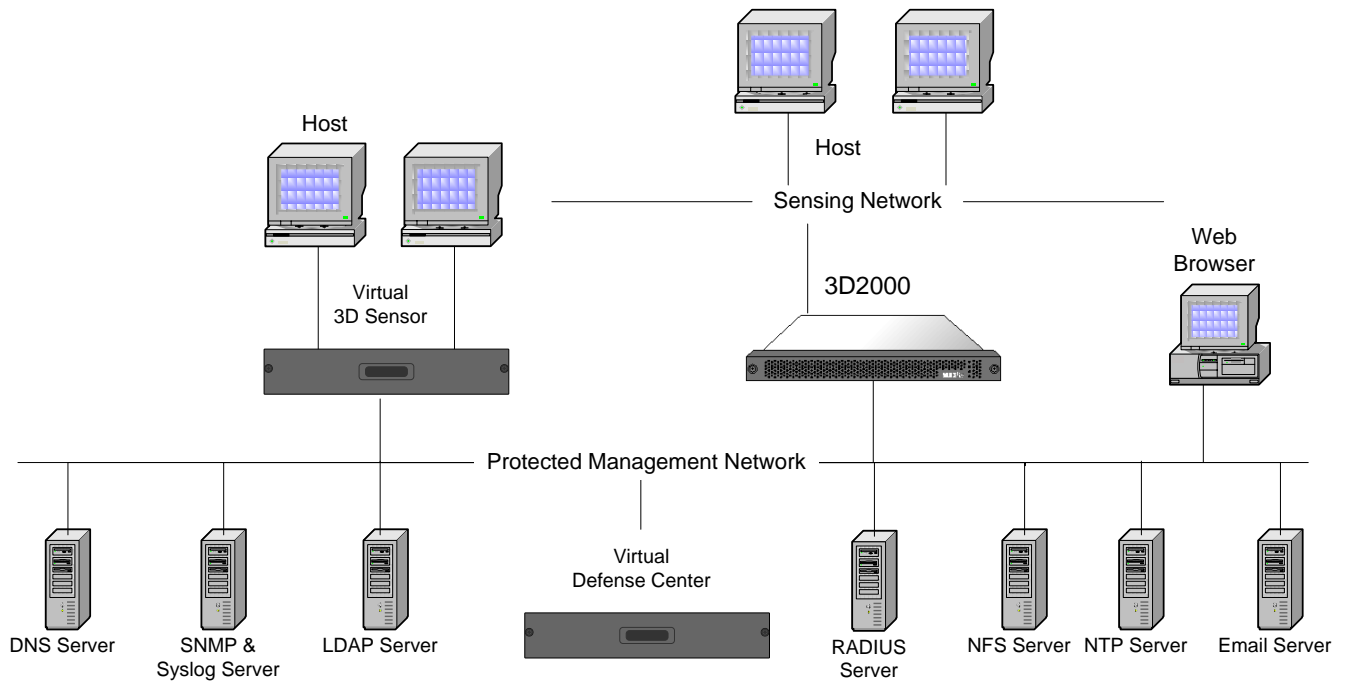
The Operational Environment includes the following test bed components:

- Hosts – 10.5.32.108 & 10.5.32.121
- Virtual Hosts – 10.4.10.163 & 10.4.10.170
- LDAP Server – 10.5.45.19 (sleepers.sfeng.sourcefire.com)
- Syslog Server – 10.5.1.18 (romulus.sfeng.sourcefire.com)
- 1 SNMP Server – 10.5.1.18 (romulus.sfeng.sourcefire.com)
- Email Server – smtps.sourcefire.com
- NTP Server – 10.4.3.20 (frodo.sfeng.sourcefire.com)
- NFS Server – 10.5.1.18 (romulus.sfeng.sourcefire.com)
- DNS Server – 10.1.1.92

**Note:** The sensors were located in the same physical location as the Defense Center in the testing scenarios. This is equivalent to deployment scenarios where the sensors are in multiple physical locations because the same SSL-encrypted communications channel is used between the sensors and Defense Center, except that it is transmitted over a VPN in the multi-site scenario.

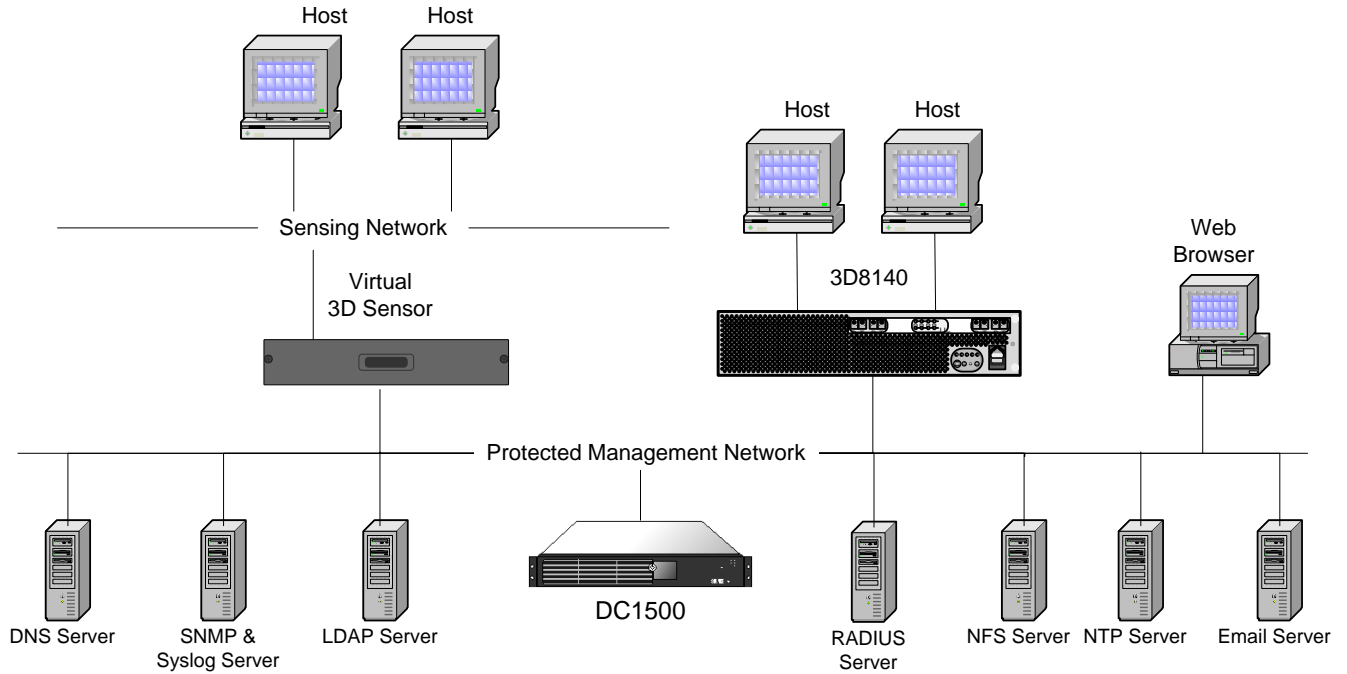
The following figures illustrate the main components required for running all test cases. They describe all the different test configurations described in the ST.

The first figure shows the two sensor types (3D2000\_32 deployed in passive mode and Virtual 3D Sensor deployed in inline mode) managed by a Virtual Defense Center. This is configuration 1.



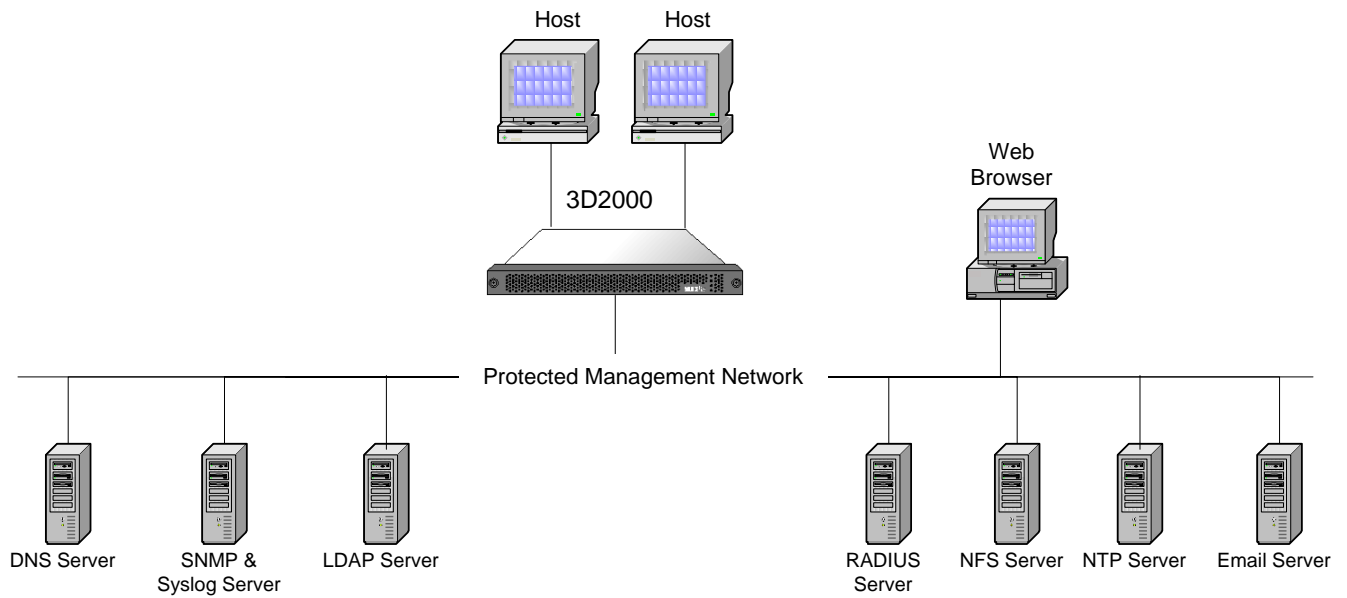
**Figure 4: A Virtual Defense Center managing a 3D2000\_32 Sensor deployed in passive mode and a Virtual 3D Sensor deployed in inline mode**

The next figure shows the two sensor types (3D8140\_64 deployed in inline mode and Virtual Sensor deployed in passive mode) managed by a Virtual Defense Center. This is configuration 2.



**Figure 5: A DC1500 Defense Center managing a 3D8140\_64 Sensor deployed in inline mode and a Virtual Sensor deployed in passive mode**

The next figure shows a standalone Sourcefire Intrusion Sensor deployed in inline mode. This is configuration 3.



**Figure 6: A standalone 3D2000 Intrusion Sensor deployed in inline mode**

## 9 Results of Evaluation

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 version 3.1 R3 of the CC and the CEM.

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 issues requiring resolution or clarification within the evaluation evidence. 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.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL.

Below lists the assurance requirements the TOE was required meet to be evaluated and pass at Evaluation Assurance Level 2 augmented with ALC\_FLR.2. The following components are taken from CC part 3. The components in the following section have no dependencies unless otherwise noted.

- ADV\_ARC.1 Security architecture description
- ADV\_FSP.2 Security-enforcing functional specification
- ADV\_TDS.1 Basic design
- AGD\_OPE.1 Operational user guidance
- AGD\_PRE.1 Preparative procedures
- ALC\_CMC.2 Use of a CM system
- ALC\_CMS.2 Parts of the TOE CM coverage
- ALC\_DEL.1 Delivery procedures
- ALC\_FLR.2 Flaw reporting procedures
- 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
- ATE\_COV.1 Evidence of coverage
- ATE\_FUN.1 Functional testing
- ATE\_IND.2 Independent testing – sample

- AVA\_VAN.2 Vulnerability analysis

The evaluators concluded that the overall evaluation result for the target of evaluation is Pass. The evaluation team reached Pass verdicts for all applicable evaluator action elements and consequently all applicable assurance components.

- The TOE is CC Part 2 Extended
- The TOE is CC Part 3 Conformant.
- The validators reviewed the findings of the evaluation team, and have concurred that the evidence and documentation of the work performed support the assigned rating.



## 10 Validators Comments/Recommendations

The following are comments from the Validation Panel.

1. Note that TOE does not have the capability to configure the password complexity mechanisms to meet requirements of NIST SP 800-53 Revision 3 control IA-5(2), as completed by CNSSI 1253 (March 2012).
2. Note that password frustration parameters (e.g., maximum number of failed logins, password expiration time) cannot be modified once an account is created.
3. Note that the support LDAP configurations in the evaluated configuration are dated.
4. The appliances include a Linux-derived OS, which is not configured in a STIG-compliant manner. DISA performs the evaluation of the OS against the STIG. The only information Sourcefire receives from DISA are their recommendations which Sourcefire incorporates in their subsequent releases. Since the TOE doesn't claim STIG conformance, Sourcefire does not have the information on how the underlying OS of the TOE differs from the current STIG confirmation. The web server in the TOE is not evaluated against the STIG either by DISA or Sourcefire.
5. The product generates reports in PDF. Customers are cautioned to use the latest version of Acrobat and to keep it patched due to all the reported vulnerabilities (see [http://www.schneier.com/blog/archives/2010/03/pdf\\_the\\_most\\_co.html](http://www.schneier.com/blog/archives/2010/03/pdf_the_most_co.html), which notes that PDF is now the most common Malware vector).
6. When the available audit storage is exhausted, the TOE overwrites the oldest stored audit records and sends an alarm that the audit trail storage is full. The audit trail is backed up by mirroring it to a syslog server. There should be periodic backups of that syslog record in accordance with the customer's applicable IA control (e.g., ECTB in DOD 8500.2 or AU-9 in NIST 800-53r3).
7. There is a lack of tamper-evident packaging for the TOE. If tamper-evident packaging is a concern of the customer, this should be conveyed to the vendor at the time the order is placed.
8. The evaluation did not assess whether the Sourcefire supplied rule sets that are bundled with the TOE for suitability to task—only that the tests included in the rule sets work correctly
9. The cryptographic functions used by the TOE are not FIPS certified. Correctness of the encryption mechanisms used by the TOE is by Vendor Assertion.

## **11 Security Target**

*Sourcefire 3D System Security Target (Sourcefire Defense Center: models DC750, DC1500, and DC3500; Sourcefire 3D Sensor licensed for IPS: models 3D500, 3D1000, 3D2000, 3D7110, 3D7120, 3D8120, 3D8130, 3D8140, and 3D8250; Sourcefire Virtual Defense Center; Sourcefire Virtual 3D Sensor licensed for IPS) Version 4.10.2.4 (SEU 568), Version 1.0, May 14, 2012 is compliant with the Specification of Security Targets requirements found within Annex B of Part 1 of the CC.*

## 12 Glossary

### 12.1 Acronyms

The following are product specific and CC specific acronyms. Not all of these acronyms are used in this document.

<b>API</b>	Application Programming Interface
<b>CC</b>	Common Criteria [for IT Security Evaluation]
<b>CCEVS</b>	Common Criteria Evaluation and Validation Scheme
<b>CCTL</b>	Common Criteria Testing Laboratory
<b>CEM</b>	Common Evaluation Methodology
<b>CIDR</b>	Classless Inter Domain Routing
<b>CISSP</b>	Certified Information Systems Security Professional
<b>CLI</b>	Command Line Interface
<b>CM</b>	Configuration Management
<b>CVE</b>	Common Vulnerability Enumeration
<b>DC</b>	Defense Center
<b>DISA</b>	Defense Information Systems Agency
<b>DNS</b>	Domain Name Service
<b>DOD</b>	Department of Defense
<b>DoS</b>	denial-of-service
<b>DDoS</b>	distributed denial of service
<b>EAL</b>	Evaluation Assurance Level
<b>ETR</b>	Evaluation Technical Report
<b>FIPS</b>	Federal Information Processing Standards Publication
<b>GB</b>	Gigabyte
<b>GUI</b>	Graphical User Interface
<b>HTTP</b>	HyperText Transmission Protocol
<b>HTTPS</b>	HyperText Transmission Protocol, Secure
<b>ICMP</b>	Internet Control Message Protocol
<b>ID</b>	Identifier
<b>IDS</b>	Intrusion Detection System
<b>IP</b>	Internet Protocol

<b>IPS</b>	Intrusion Prevention System
<b>IT</b>	Information Technology
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>Mbps</b>	megabits per second
<b>MDC</b>	Master Defense Center
<b>MITM</b>	man-in-the-middle
<b>NBA</b>	Network Behavior Analysis
<b>NFS</b>	Network File System
<b>NIST</b>	National Institute of Standards and Technology
<b>Nmap</b>	Network Mapper
<b>NTP</b>	Network Time Protocol
<b>NUC</b>	Network Usage Control
<b>OS</b>	Operating System
<b>PCAP</b>	Packet Capture
<b>PDF</b>	Portable Document Format (PDF), a file format created by Adobe Systems in 1993 for document exchange.
<b>PEP</b>	Policy Enforcement Point
<b>PP</b>	Protection Profile
<b>RADIUS</b>	Remote Authentication Dial In User Service
<b>RNA</b>	Real-Time Network Awareness
<b>RPC</b>	Remote Procedure Call
<b>RUA</b>	Real-Time User Awareness
<b>SEU</b>	Security Enhancement Updates
<b>SF</b>	Security Function
<b>SFIDS</b>	Sourcefire Intrusion Detection System
<b>SFP</b>	Security Function Policy
<b>SFR</b>	Security Functional Requirements
<b>SNMP</b>	Simple Network Management Protocol
<b>SSL</b>	Secure Sockets Layer
<b>ST</b>	Security Target
<b>STIG</b>	Security Technical Implementation Guide
<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol
<b>TLS</b>	Transport Security Layer

<b>TOE</b>	Target of Evaluation
<b>TSC</b>	TSF Scope of Control
<b>TSF</b>	TOE Security Functions
<b>TSFI</b>	TOE Security Functions Interface
<b>TSP</b>	TOE Security Policy
<b>UDP</b>	User Datagram Protocol
<b>UI</b>	User Interface
<b>URI</b>	Uniform Resource Identifier
<b>VA</b>	Vulnerability Assessment
<b>VM</b>	Virtual Machine
<b>VPN</b>	Virtual Private Network
<b>VR</b>	Validation Report
<b>VRT</b>	Vulnerability Research Team
<b>WebUI</b>	Web User Interface

## ***12.2 Terminology***

This section defines the product-specific and CC-specific terms. Not all of these terms are used in this document.

<b>3D Sensor with IPS</b>	An appliance-based sensor that, as part of the Sourcefire 3D System, can run the IPS component. The 3D Sensor with IPS includes the appliance hardware and the Sourcefire application software, Linux derived operating system, and supporting 3rd party software installed on the appliance.
<b>Access List</b>	A list of computers can access a 3D System component on specific ports.
<b>Analyzer Data</b>	Data collected by the analyzer functions.
<b>Analyzer Functions</b>	The active part of the analyzer responsible for performing intrusion analysis of information that may be representative of vulnerabilities in and misuse of IT resources, as well as reporting of conclusions. The (Virtual) 3D Sensor with IPS performs the analyzer functions of the TOE.
<b>Assets</b>	Information or resources to be protected by the countermeasures of a TOE.
<b>Assignment</b>	The specification of an identified parameter in a component.

<b>Assurance</b>	Grounds for confidence that an entity meets its security objectives.
<b>Attack</b>	An attempt to bypass security controls on an IT System. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the IT System and the effectiveness of existing countermeasures.
<b>Attack Potential</b>	The perceived potential for success of an attack, should an attack be launched, expressed in terms of a threat agent's expertise, resources and motivation.
<b>Audit</b>	The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend indicated changes in controls, policy, or procedures.
<b>Audit Log</b>	In an IT System, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.
<b>Audit Trail</b>	See <b>Audit Log</b>
<b>Augmentation</b>	The addition of one or more assurance component(s) to a package.
<b>Authentication</b>	To establish the validity of a claimed user or object.
<b>Authentication Data</b>	Information used to verify the claimed identity of a user.
<b>Authentication Object</b>	An object that contains the settings for connecting to and retrieving user data from an external authentication server.
<b>Authorised User</b>	A user who may, in accordance with the SFR, perform an operation.
<b>Authorized Administrator</b>	The authorized users that manage the TOE or a subset of its TSF data and management functions.
<b>Availability</b>	Assuring information and communications services will be ready for use when expected.
<b>Class</b>	A grouping of families that share a common focus.
<b>Component</b>	The smallest selectable set of elements on which requirements may be based.

<b>Compromise</b>	An intrusion into an IT System where unauthorized disclosure, modification or destruction of sensitive information may have occurred.
<b>Confidentiality</b>	Assuring information will be kept secret, with access limited to appropriate persons.
<b>Connectivity</b>	The property of the TOE that allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.
<b>Defense Center</b>	The Sourcefire 3D System Defense Center appliance and the software installed upon it. A central management point that allows the management of the (appliance-based and virtual) 3D Sensors and automatically aggregates the events they generate.
<b>Dependency</b>	A relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package.
<b>Detection Engine</b>	The mechanism that is responsible for analyzing the traffic on the network segment where a sensor is connected.
<b>Element</b>	An indivisible security requirement.
<b>Evaluation</b>	Assessment of a PP, an ST, or a TOE against defined criteria.
<b>Evaluation Assurance Level (EAL)</b>	A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.
<b>Evaluation Authority</b>	A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted community.
<b>Evaluation Scheme</b>	The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.
<b>Extension</b>	The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.

<b>External Entity</b>	Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.
<b>Family</b>	A grouping of components that share security objectives but may differ in emphasis or rigor.
<b>Formal</b>	Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.
<b>Health Alert</b>	An alert generated by the (Virtual) Defense Center when a specific health event occurs.
<b>Health Event</b>	An event that is generated when one of the components in a deployment meets (or fails to meet) performance criteria specified in a health module. Health events indicate which module triggered the event and when the event was triggered.
<b>Health Module</b>	A test of a particular performance aspect of one of the components in a deployment.
<b>Health Policy</b>	The criteria used when checking the health of a component in a deployment. Health policies use health modules to indicate whether Sourcefire 3D System hardware and software are working correctly.
<b>Identity</b>	A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
<b>IDS Analyzer (analyzer)</b>	The component of an IDS that accepts data from sensors, scanners and other IT System resources, and then applies analytical processes and information to derive conclusions about intrusions (past, present, or future). The (Virtual) 3D Sensor with IPS is the analyzer component of the TOE.
<b>IDS Component</b>	A sensor, scanner, or analyzer. The (Virtual) 3D Sensor with IPS is the IDS component of the TOE.
<b>IDS Scanner (scanner)</b>	The component of an IDS that collects 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. The (Virtual) 3D Sensor with IPS is the scanner component of the TOE.
<b>IDS Sensor (sensor)</b>	The component of an IDS that collects real-time events that may be indicative of vulnerabilities in or



	misuse of IT resources. The (Virtual) 3D Sensor with IPS is the sensor component of the TOE.
<b>Incident</b>	One or more intrusion events that are suspected of being involved in a possible violation of a security policy.
<b>Informal</b>	Expressed in natural language.
<b>Integrity</b>	Assuring information will not be accidentally or maliciously altered or destroyed.
<b>Interface Set</b>	One or more sensing interfaces on a 3D Sensor that can be used to monitor network segments for one or more detection engines.
<b>Internal Communication Channel</b>	A communication channel between separated parts of TOE.
<b>Internal TOE Transfer</b>	Communicating data between separated parts of the TOE.
<b>Inter-TSF Transfers</b>	Communicating data between the TOE and the security functions of other trusted IT products.
<b>Intrusion</b>	Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.
<b>Intrusion Detection</b>	The process of passively analyzing network traffic for potential intrusions and storing attack data for security analysis.
<b>Intrusion Detection System (IDS)</b>	A combination of sensors, scanners, and analyzers that monitor an IT System for activity that may inappropriately affect the IT System's assets and react appropriately.
<b>Intrusion Event</b>	A record of the network traffic that violated an intrusion policy.
<b>Intrusion Policy</b>	Intrusion policies include a variety of components that are configured to inspect network traffic for intrusions and policy violations. These components include preprocessors; intrusion rules that inspect the protocol header values, payload content, and certain packet size characteristics; and tools that control how often events are logged and displayed.
<b>Intrusion Protection</b>	The concept of intrusion detection with the added ability to block or alter malicious traffic as it travels across a network.

<b>Intrusion Rule</b>	A set of keywords and arguments that, when applied to captured network traffic, identify potential intrusions, policy violations, and security breaches. IPS compares packets against the conditions specified in each rule and, if the packet data matches all the conditions specified in the rule, the rule triggers and generates an intrusion event.
<b>IT Product</b>	A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.
<b>IT System</b>	May range from a computer system to a computer network.
<b>Iteration</b>	The use of the same component to express two or more distinct requirements.
<b>Network</b>	Two or more machines interconnected for communications.
<b>Object</b>	A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.
<b>Organizational Security Policies</b>	A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment.
<b>Package</b>	A named set of either functional or assurance requirements (e.g. EAL 3).
<b>Packet</b>	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
<b>Packet Sniffer</b>	A device or program that monitors the data traveling between computers on a network.
<b>Preprocessor</b>	A feature of IPS that normalizes traffic and helps identify network layer and transport layer protocol anomalies by identifying inappropriate header options, defragmenting IP datagrams, providing TCP stateful inspection and stream reassembly, and validating checksums.
<b>Protection Profile (PP)</b>	An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs
<b>Prove</b>	This term refers to a formal analysis in its mathematical sense. It is completely rigorous in all

ways. Typically, “prove” is used when there is a desire to show correspondence between two TSF representations at a high level of rigor.

<b>Refinement</b>	The addition of details to a component.
<b>Reviewed Event</b>	An intrusion event that has been examined by an administrator who has determined that the event does not represent a threat to network security and who has marked the event as reviewed.
<b>Role</b>	A predefined set of rules establishing the allowed interactions between a user and the TOE.
<b>Root (root user, root account)</b>	The superuser, a user on Unix-like systems, usually with full administrative privileges.
<b>Scanner Data</b>	Data collected by the scanner functions.
<b>Scanner Functions</b>	The active part of the scanner responsible for collecting configuration information that may be representative of vulnerabilities in and misuse of IT resources (i.e., scanner data).
<b>Secret</b>	Information that must be known only to authorized users and/or the TSF in order to enforce a specific SFP.
<b>Secure State</b>	A state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs.
<b>Security</b>	A condition that results from the establishment and maintenance of protective measures that ensures a state of inviolability from hostile acts or influences.
<b>Security Attribute</b>	A property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs.
<b>Security Function Policy (SFP)</b>	A set of rules describing specific security behavior enforced by the TSF and expressible as a set of SFRs.
<b>Security Objective</b>	A statement of intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions.
<b>Security Policy</b>	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

<b>Security Target (ST)</b>	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
<b>Selection</b>	The specification of one or more items from a list in a component.
<b>Semiformal</b>	Expressed in a restricted syntax language with defined semantics.
<b>Sensor Data</b>	Data collected by the sensor functions.
<b>Sensor Functions</b>	The active part of the sensor responsible for collecting information that may be representative of vulnerabilities in and misuse of IT resources (i.e., sensor data).
<b>Signatures</b>	Patterns of network traffic that can be used to detect attacks or exploits.
<b>Subject</b>	An active entity in the TOE that performs operations on objects.
<b>System Policy</b>	Settings that are likely to be similar for multiple appliances in a deployment, such as access configuration, authentication profiles, database limits, DNS cache settings, the mail relay host, a notification address for database prune messages, and time synchronization settings.
<b>Target of Evaluation (TOE)</b>	A set of software, firmware and/or hardware possibly accompanied by guidance.
<b>Threat</b>	The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security.
<b>TOE Administrator</b>	See <b>Authorized Administrator</b>
<b>TOE Resource</b>	Anything useable or consumable in the TOE.
<b>TOE Security Functions (TSF)</b>	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
<b>TOE Security Policy (TSP)</b>	A set of rules that regulate how assets are managed, protected, and distributed within a TOE.
<b>Transfers outside TSF</b>	TSF mediated communication of data to entities not under control of the TSF.
<b>Trojan Horse</b>	An apparently useful and innocent program containing additional hidden code that allows the

	<p>unauthorized collection, exploitation, falsification, or destruction of data.</p>
<b>Trusted Channel</b>	<p>A means by which a TSF and a remote trusted IT product can communicate with necessary confidence.</p>
<b>Trusted Path</b>	<p>A means by which a user and a TSF can communicate with necessary confidence.</p>
<b>TSF Data</b>	<p>Data created by and for the TOE, which might affect the operation of the TOE.</p>
<b>TSF Interface (TSFI)</b>	<p>A means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF.</p>
<b>TSF Scope of Control (TSC)</b>	<p>The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.</p>
<b>User</b>	<p>See <b>External Entity</b></p>
<b>User Data</b>	<p>Data created by and for the user that does not affect the operation of the TSF.</p>
<b>Virtual 3D Sensor with IPS</b>	<p>An software-only sensor that, as part of the Sourcefire 3D System, can run the IPS component. The Virtual 3D Sensor with IPS includes the same Sourcefire application software, Linux derived operating system, and supporting 3rd party software as the appliance-based 3D Sensor with IPS but is installed on a VMware ESX host platform.</p>
<b>Virtual Defense Center</b>	<p>The software-only component of the Sourcefire 3D System that allows the management of the 3D Sensors (appliance-based and virtual) and automatically aggregates the events they generate. The Virtual Defense Center consists of the same the Sourcefire application software, Linux derived operating system, and supporting 3rd party software as the appliance-based Defense Center, but is installed on a VMware ESX host platform.</p>
<b>Virus</b>	<p>A program that can "infect" other programs by modifying them to include a, possibly evolved, copy of itself.</p>
<b>Vulnerability</b>	<p>Hardware, firmware, or software flow that leaves an IT System open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by</p>

a threat to gain unauthorized access to information or disrupt critical processing.

### **Workflow**

A series of Web pages available on the TOE's WebUI that the administrators can use to view and evaluate events by moving from a broad view of event data to a more focused view that contains only the events of interest.

## 13 Bibliography

### URLs

- [1] Common Criteria Evaluation and Validation Scheme (CCEVS): (<http://www.niap-ccevs.org/cc-scheme>).
- [2] CygnaCom Solutions CCTL (<http://www.cygnacom.com/labs/common-criteria/index.htm>).

### CCEVS Documents

- [1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, July 2009 Version 3.1 Revision 3 Final, CCMB-2009-07-001.
- [2] Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, July 2009 Version 3.1 Revision 3 Final, CCMB-2009-07-002.
- [3] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, July 2009, Version 3.1 Revision 3 Final, CCMB-2009-07-003.
- [4] Common Methodology for Information Technology Security Evaluation - Evaluation methodology, July 2009, Version 3.1 Revision 3 Final, CCMB-2009-07-004.