National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Sourcefire 3D System

(Sourcefire Defense Center: models DC500, DC1000, and DC3000; and Sourcefire 3D Sensor licensed for IPS: models 3D500, 3D1000, 3D2000, 3D2100, 3D2500, 3D3500, 3D3800, 3D4500, 3D5800, 3D6500, and 3D9800)

Version 4.8.2.1 (SEU 259)

Report Number: **CCEVS-VR-VID10334-2010**

Dated: **June 23, 2010**

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 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

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 4.8.2.1 (SEU 259) Security Target.

Table of Contents

List of Figures

1 Executive Summary

This Validation Report (VR) documents the evaluation and validation of the product Sourcefire 3D System (Sourcefire Defense Center: models DC500, DC1000, and DC3000; and Sourcefire 3D Sensor licensed for IPS: models 3D500, 3D1000, 3D2000, 3D2100, 3D2500, 3D3500, 3D3800, 3D4500, 3D5800, 3D6500, and 3D9800) Version 4.8.2.1 (SEU 259).

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 and Sourcefire 3D System Version 4.8.2.1 (SEU 259) software.

The TOE is an Intrusion Detection System that combines open-source and proprietary technology. The TOE 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 the open source Snort 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 2.8.3, 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 to management functions; trusted communication between components; display of TOE access information; and system data collection, analysis, review, availability and loss.

Note: The TOE does not meet all the technical requirements of 800-53; interested readers should refer to the validators comments in Section 10 for identified specifics.

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 in June 2010. 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 R2 [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 R2, [CEM]. This Security Target claims demonstrable compliance to *U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments*, Version 1.7, July 25, 2007. (IDS System PP).

The evaluation and validation were 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. The Security Target (ST) is contained within the document *Sourcefire 3D System Security Target (Sourcefire Defense Center: models DC500, DC1000, and DC3000; and Sourcefire 3D Sensor licensed for IPS: models 3D500, 3D1000, 3D2000, 3D2100, 3D2500, 3D3500, 3D3800, 3D4500, 3D5800, 3D6500, and 3D9800) Version 4.8.2.1 (SEU 259)*

2 Identification

Target of Evaluation: Sourcefire 3D System (Sourcefire Defense Center: models DC500, DC1000, and DC3000; and Sourcefire 3D Sensor licensed for IPS: models 3D500, 3D1000, 3D2000, 3D2100, 3D2500, 3D3500, 3D3800, 3D4500, 3D5800, 3D6500, and 3D9800) Version 4.8.2.1 (SEU 259)

Evaluated Software and Hardware:

Sourcefire 3D System Version 4.8.2.1 (SEU 259) consisting of the following components:

- *The Sourcefire 3D Sensor licensed for IPS models 3D500, 3D1000, 3D2000, 3D2100, 3D2500, 3D3500, 3D3800, 3D4500, 3D5800, 3D6500, and 3D9800*
- *The Sourcefire Defense Center models DC500, DC1000, and DC3000*

Developer: Sourcefire, Inc.

CCTL: CygnaCom Solutions
7925 Jones Branch Dr, Suite 5200
McLean, VA 22102-3321

Evaluators: Deepak Somesula

Validation Scheme: National Information Assurance Partnership CCEVS

Validators: Daniel P. Faigin, Dr. Patrick Mallett

CC Identification: Common Criteria for Information Technology Security Evaluation, Version 3.1 R2, September 2007

CEM Identification: Common Methodology for Information Technology Security Evaluation, Version 3.1 R2, September 2007

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 following security features:

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.

The audit data is protected by the access control mechanisms of the database and OS of the appliances and by the TOE management interface. Only users with the Administrator Role have access to the audit records. Users having the Administrator Role 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 though username/password authentication or optionally through the use of an external authentication server (LDAP or RADIUS) for configurations that include a Defense Center.

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 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.
- "**Restricted Event Analyst**" Role: this role provides access to the same features as the Intrusion Event Analyst role, but is restricted to only those events that match specified search criteria (specific IP Addresses or subsets of data).
- "**Restricted Event Analyst (Read Only)**" Role: this role is the same as the Restricted Event Analyst role except that users have read-only access to the intrusion events that match the specified search criteria.
- "**Policy and Response Administrator**" Role: this role can create, modify, and implement intrusion policies and intrusion rules for the IDS.

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.

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 Functions

To analyze the data collected by the 3D Sensors with IPS, the TOE uses signatures, decoders, and preprocessors. 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.

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.

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.

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). 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 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)
   - Assigned Role(s) (authorizations)
   - Use External Authentication Method
   - Force Password Reset on Login
   - Password Strength Check
   - Max Number of Failed Logins
   - Password Expiration
   - Warning Days

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 user roles:

    - Administrator
    - Maintenance
    - Intrusion Event Analyst
    - Intrusion Event Analyst (Read Only)
    - Restricted Event Analyst
    - Restricted Event Analyst (Read Only)
    - Policy and Response Administrator

15. **FPT_ITT.1: Basic internal TSF data transfer protection**

    The TOE protects data from disclosure and modification when it is transmitted between the Defense Center and the 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 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 or Intrusion Event Analyst Role 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 which 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 which 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.

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. (e.g. located within controlled access facilities, which will prevent unauthorized physical access)

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 Nessus and 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, 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 Shavlik patch management system

5. The Operational Environment needs to provide the following capabilities:
    - The Web Browser for the Defense Center and 3D Sensor with IPS Management Interfaces. Only the following are supported for Sourcefire 3D System Version 4.8.2.1:
    - Firefox Version (Minimum) 2.x
    - Microsoft Internet Explorer Version 6.0 with Service Pack 2
    - Microsoft Internet Explorer Version 7.0
    - 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 Syslog Server
    - An optional SNMP (v2 or v3) Trap Server
    - An optional LDAP or RADIUS Authentication Server

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: The following TOE components were used in testing:

- DC3000 (SFLinux)

- 3D2500 sensor (SFLinux)
- 3D5800 sensor (SBLinux)
- 3D9800 sensor (SVLinux)

Because of their identical functionality and behavior only one 3D Sensor appliance from each category of 3D Sensors was used in 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 IPS is included in the scope of this evaluation.

Each 3D Sensor with IPS 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 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.

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.

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.

In a Sourcefire 3D System deployment that includes 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.

Some models of the 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 Defense Center provides the following functionality through a web-based GUI (WebUI):

- An interface which 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 Defense Center and 3D Sensor with IPS components described above. The physical boundary of the TOE is the Sourcefire 3D Sensor licensed for IPS and the Sourcefire Defense Center appliances installed with the Sourcefire 3D System Version 4.8.2.1 software, Linux-derived operating system, MySQL database, and supporting 3rd party software as commercially available from the developer. The TOE Boundary is depicted in Figure 1 and Figure 2.

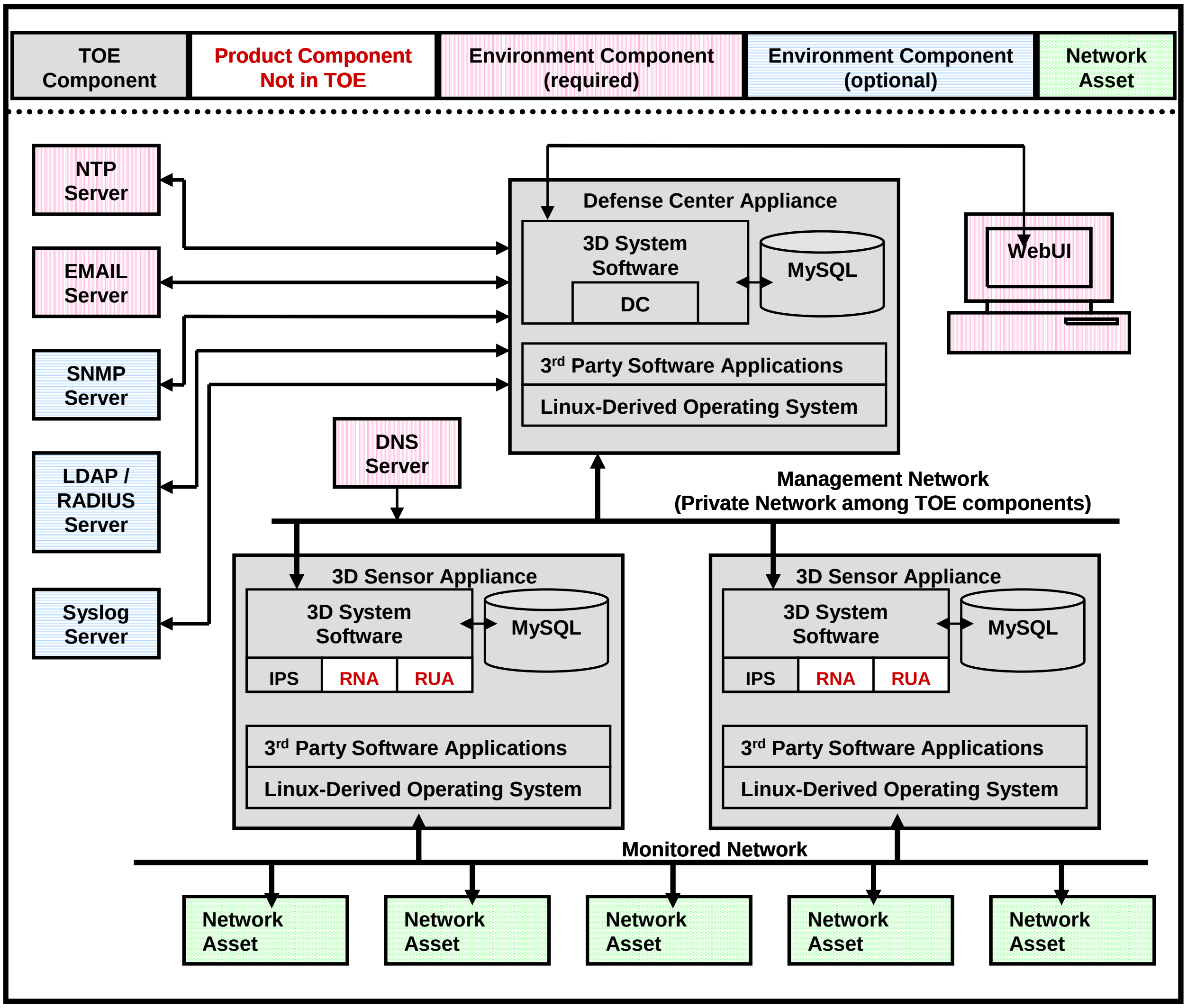

Figure 1: TOE: Boundary - Sourcefire 3D System with Defense Center

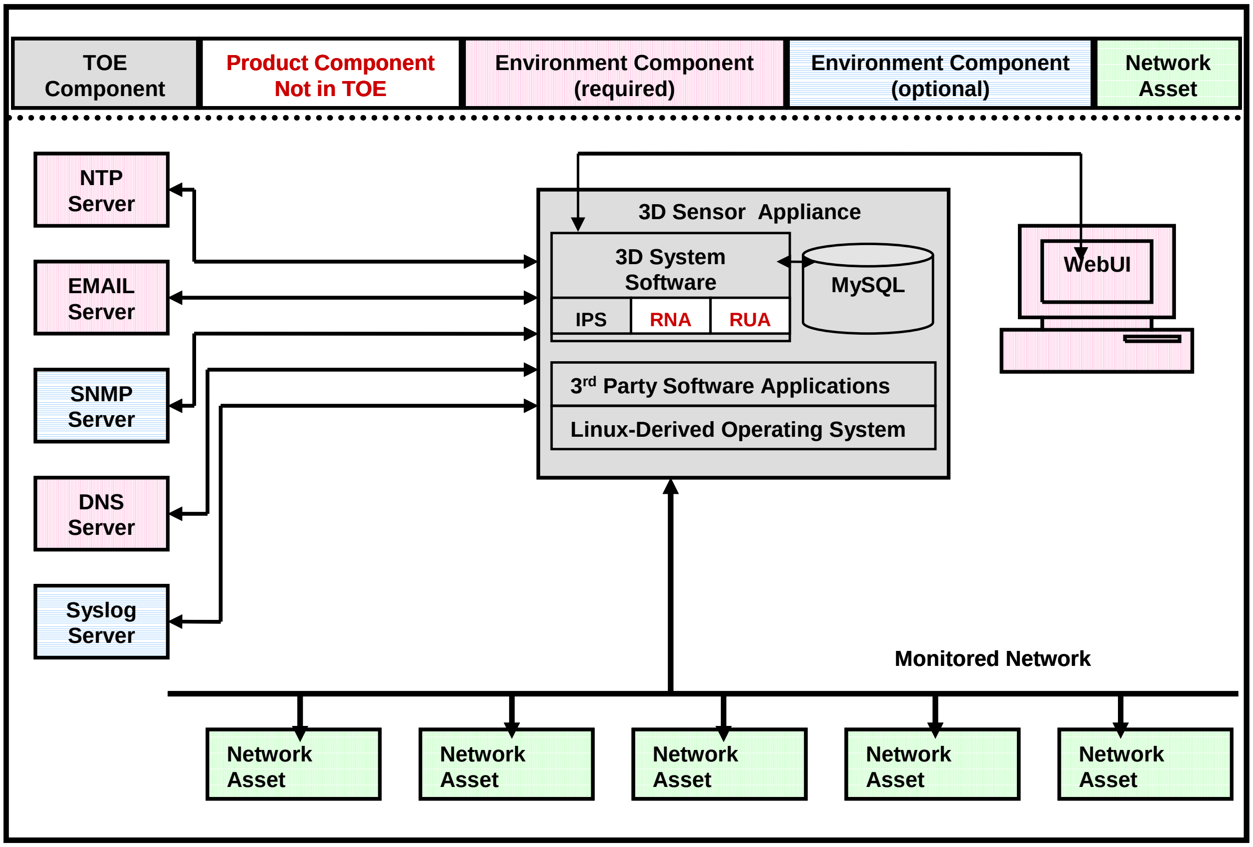

Figure 2: TOE: Boundary - Sourcefire 3D System using a stand-alone 3D Sensor with IPS

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 Guidance Documentation

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

[1] **Sourcefire 3D System - 3D Sensor Installation Guide**, Version 4.8.2, 2009-Oct-02.

[2] **Sourcefire 3D System - Defense Center Installation Guide**, Version 4.8, 2008-Jul-23.

[3] **Sourcefire 3D System - Sourcefire 3D System User Guide**, Version 4.8.2, 2009-Sep-01.

[4] **Sourcefire 3D System - CC Supplement for Version 4.8.2.1**, 2010-Jun-08**.**

6.2 Security Target (ST)

Security Target (ST)

[1] Sourcefire 3D System Security Target (Sourcefire Defense Center: models DC500, DC1000, and DC3000; and Sourcefire 3D Sensor licensed for IPS: models 3D500, 3D1000, 3D2000, 3D2100, 3D2500, 3D3500, 3D3800, 3D4500, 3D5800, 3D6500, and 3D9800), Version 4.8.2.1 (SEU 259), Version 1.15, 2010-Jun-10.

6.3 Development (ADV) Evidence Documentation

[1] Sourcefire 3D System Version 4.8.2.1 Functional Specification, Version 1.1, 2010-Apr-26.

[2] Sourcefire 3D System Version 4.8.2.1 TOE Design, Version 1.1, 2010-Apr-26.

[3] Sourcefire 3D System Version 4.8.2.1 Security Architecture, Version 1.1, 2010-Apr-26.

6.4 Life-Cycle (ALC) Evidence Documentation

[1] Sourcefire 3D System Configuration Management Plan, Version 0.5, 2010-Apr-21.

[2] Sourcefire Intrusion Detection System Delivery Procedures, Version 1.1, 2010-Apr-27.

[3] Sourcefire 3D System Version 4.8.2.1 Flaw Reporting Procedures, Version 1.0, 2010-Apr-26.

6.5 Testing (ATE) and Vulnerability Analysis (AVA) Documentation

[1] Sourcefire Evaluator Test Plan and Report, Version 0.4, 2010-Jun-09.

[2] Sourcefire 3D System Version 4.8.2.1 - Test Coverage Document, Version 1.0, 2010-Apr-29.

[3] Sourcefire, Inc. - EAL2 Test Case Document v1.3 (3D 4.8.2.1 & SEU 259), 2010-Apr-26.

6.6 Evaluation Technical Report (ETR)

[1] Evaluation Technical Report For a Target of Evaluation, Volume 1: Evaluation of the ST, Sourcefire, Incorporated, Sourcefire 3D System Version 4.8.2.1, Version 1.4, 2010-Jun-16.

[2] Evaluation Technical Report For a Target of Evaluation, Volume 2: Evaluation of the TOE, Sourcefire, Incorporated, Sourcefire 3D System Version 4.8.2.1, Version 1.3, 2010-Jun-16.

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 portions of Sourcefire’s tests as the set of developer tests to execute. The evaluator re-ran the set of developer manual test procedures which are listed in the Evaluator’s Test Report.

The evaluator selected this approach in order to:

- Ensure the coverage of the principle security features of the TOE

- Gain confidence in the developer's test results
- Ensure TOE is in a properly configured state

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

- All Security Functions were tested
- All External interfaces were exercised
- All Security Functional Requirements were tested.

Since the product is an Intrusion Detection System testing emphasis was on the IDS functionality along with the Security Management (SM) and Identification and Authentication (I&A) functionality. The sample of the developer tests selected to be re-run exercised the security functions at an appropriate level of rigor commensurate with EAL 2. The evaluator augmented the IDS_* SFR tests to test the signature based detection and protocol behavior detection functionality.

Testing emphasis was also laid on the Network Interface (where the IDS functionality is implemented) being tested. The evaluator ensured that the test sample contained a good representative sample of the protocols and policy violations referenced in the Functional Specification and User Guidance Documents.

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.

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 Inspection – Test to be performed on a 3D Sensor 3800 (SBLinux V4.8)
5. Test the TOE’s capability to configure a port with capture role and verify that this port can be used to capture packets
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.

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 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 (DC3000) and on 3D Sensor with IPS (running SFLinux) appliance (3D2500), 3D Sensor with IPS (running SBLinux) appliance (3D5800) and 3D Sensor with IPS (running SVLinux) appliance (3D9800)

- Set up the Nessus Laptop such that a ping from the laptop can reach the Management Ports of the appliance. 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.

All identified vulnerabilities were ruled out in the evaluated configurations.

8 Evaluated Configuration

The TOE was tested the following test bed components:

- DC3000 (SFLinux)
- 3D2500 sensor (SFLinux)
- 3D5800 sensor (SBLinux)
- 3D9800 sensor (SVLinux)

The Operational Environment includes the following test bed components:

- Host 1
- Host 2
- LDAP Server
- RADIUS Server
- Syslog Server
- SNMP Server
- Email Server
- NTP Server
- DNS Server
- WebUI station

Note: The following TOE components were used in testing:

- DC3000 (SFLinux)
- 3D2500 sensor (SFLinux)
- 3D5800 sensor (SBLinux)
- 3D9800 sensor (SVLinux)

Because of their identical functionality and behavior only one 3D Sensor appliance from each category of 3D Sensors was used in 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.

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 three sensor types (SFLinux, SBLinux and SVLinux) deployed in inline mode managed by a Defense Center. This is configuration 1.

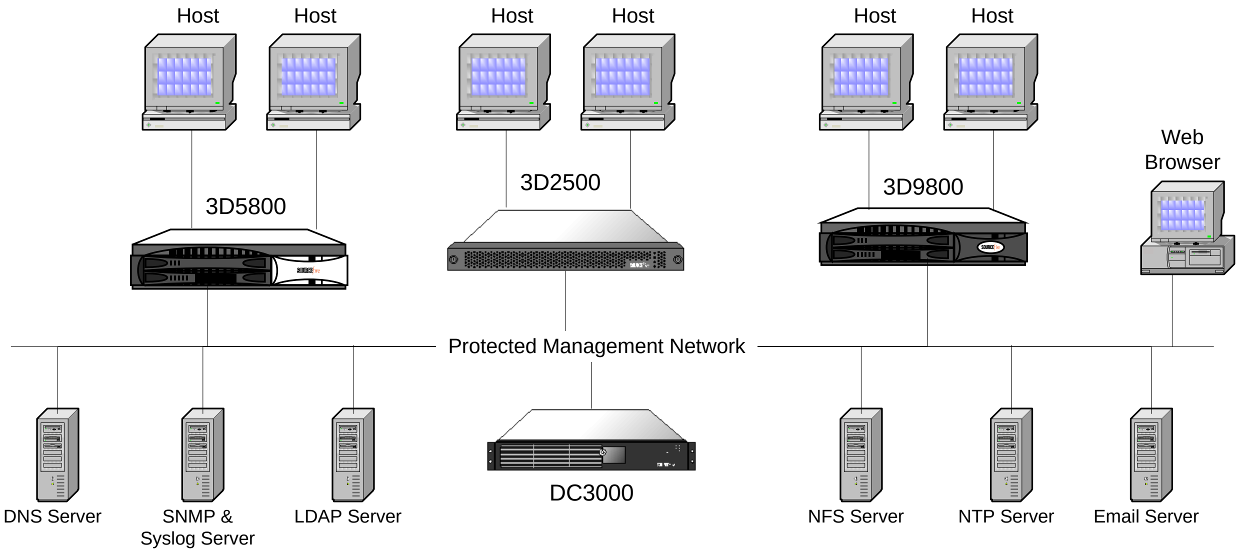

Figure 3 : A DC3000 Defense Center managing three sensors deployed in inline mode (Configuration 1)

The next figure shows a Sourcefire Intrusion Sensor deployed in inline mode managed by a Defense Center. This is configuration 2a.

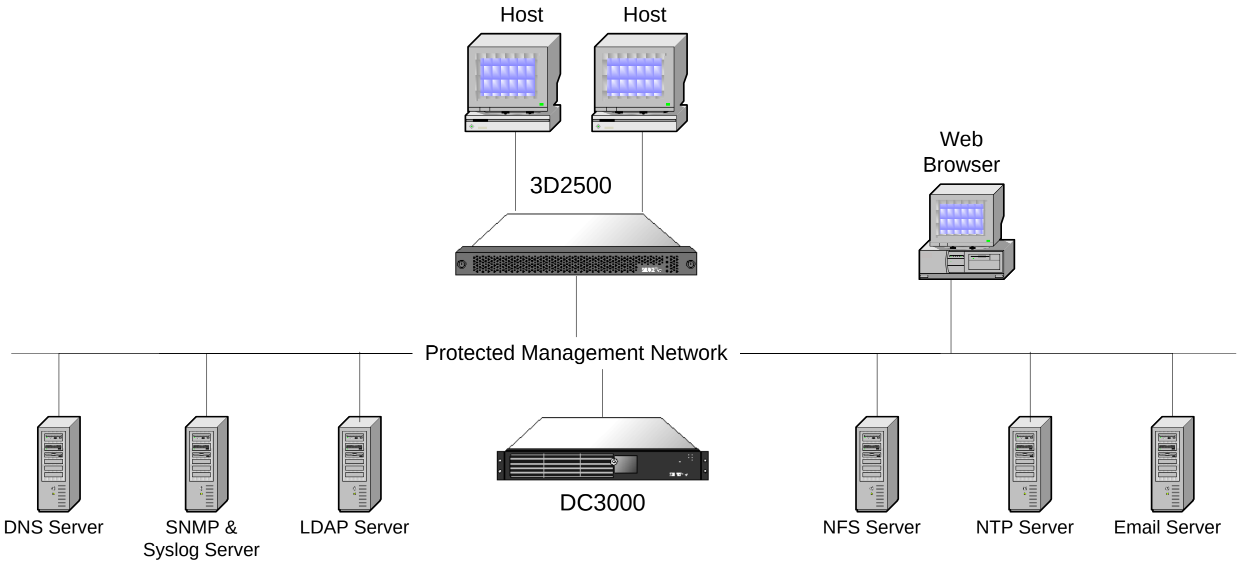

Figure 4: A DC3000 Defense Center managing a 3D2500 Intrusion Sensor deployed in inline mode (Configuration 2a)

The next figure shows a Sourcefire Intrusion Sensor deployed in passive mode managed by a Defense Center. This is configuration 2b.

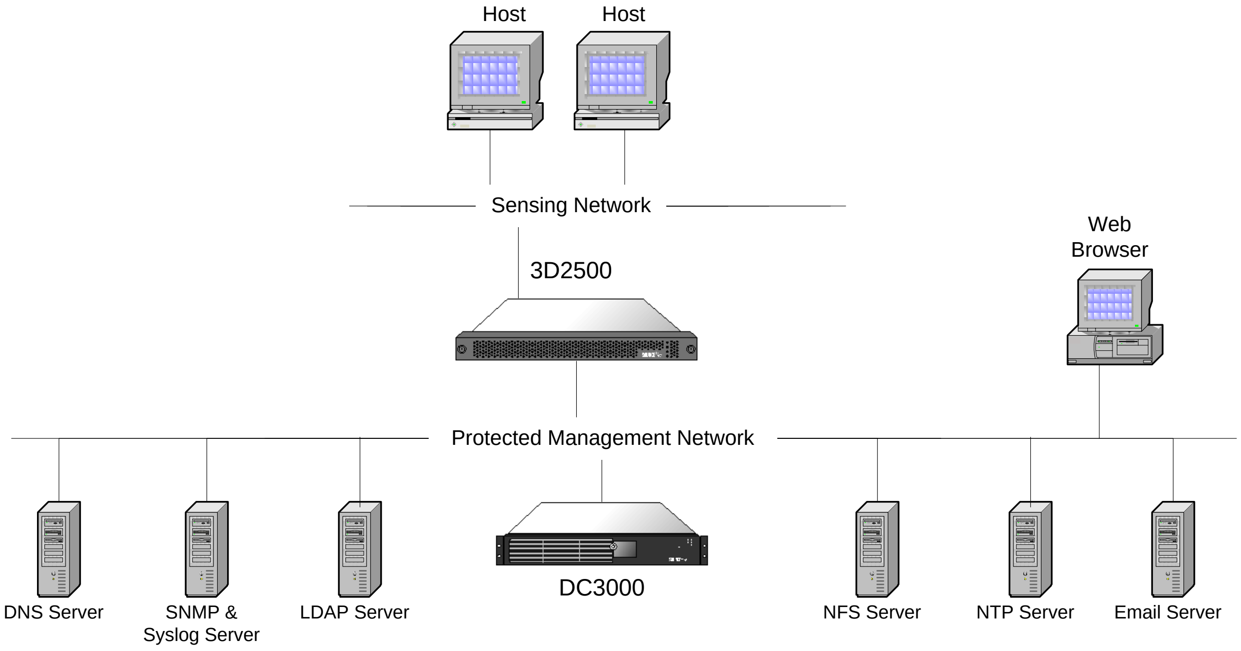

Figure 5: A DC3000 Defense Center managing a 3D2500 Intrusion Sensor deployed in passive mode

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

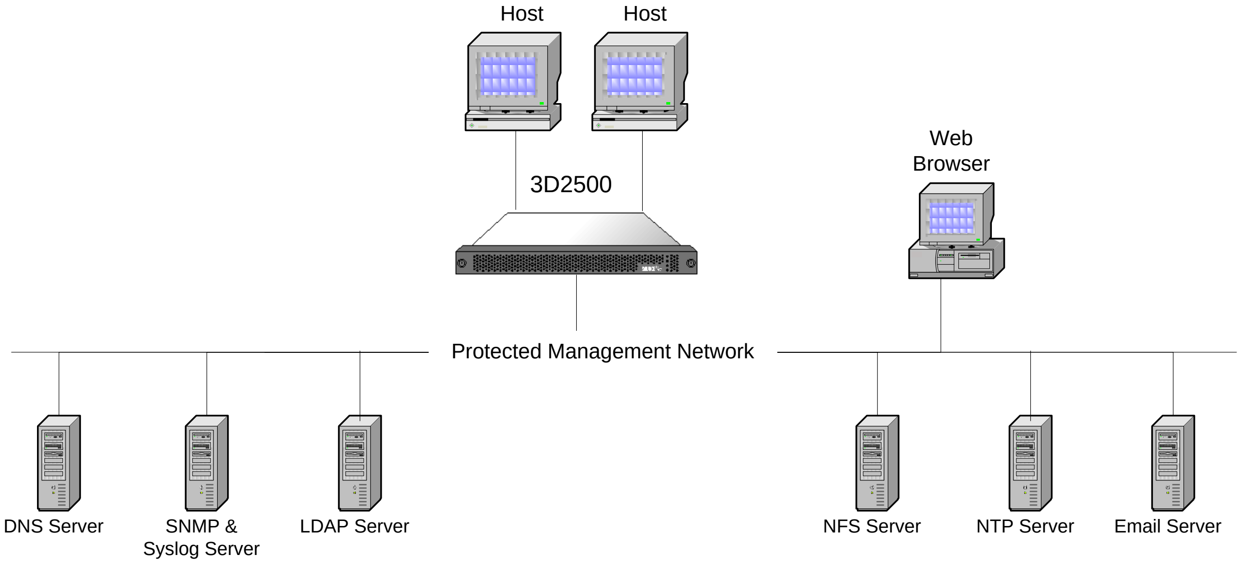

Figure 6: A standalone 3D2500 Intrusion Sensor deployed in inline mode (Configuration 3a)

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

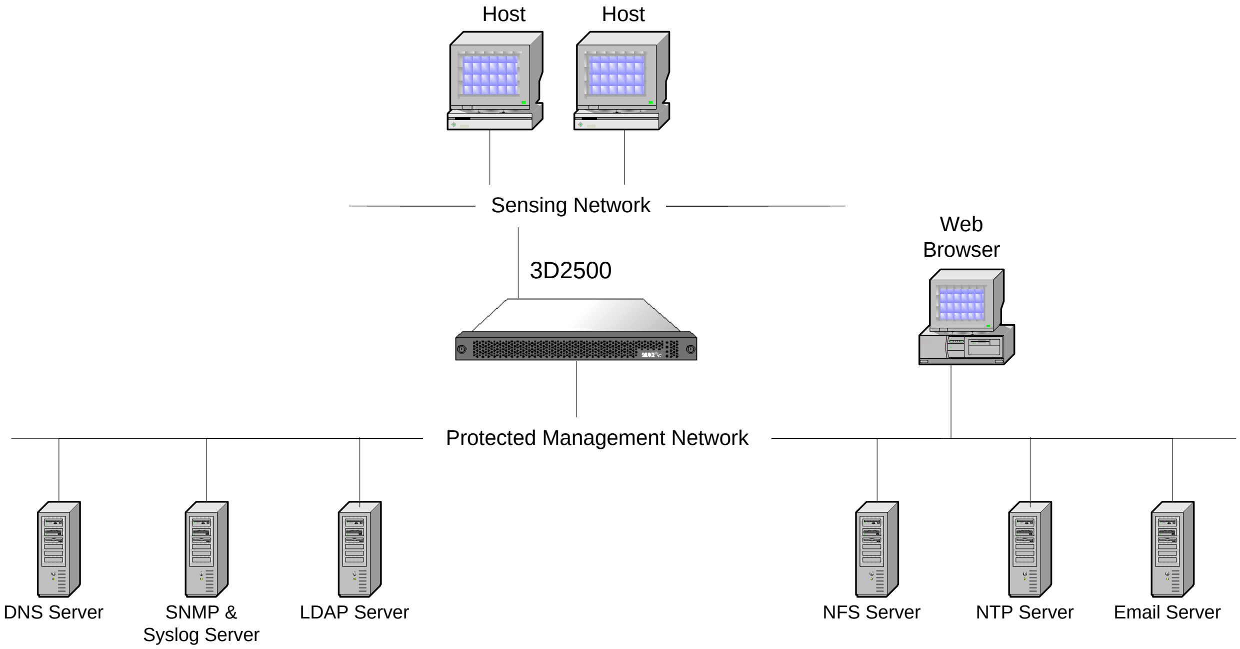

Figure 7: A standalone 3D2500 Intrusion Sensor deployed in passive mode (Configuration 3b)

The next figure shows a SVLinux Intrusion Sensor deployed in inline mode managed by a Defense Center. This is configuration 4.

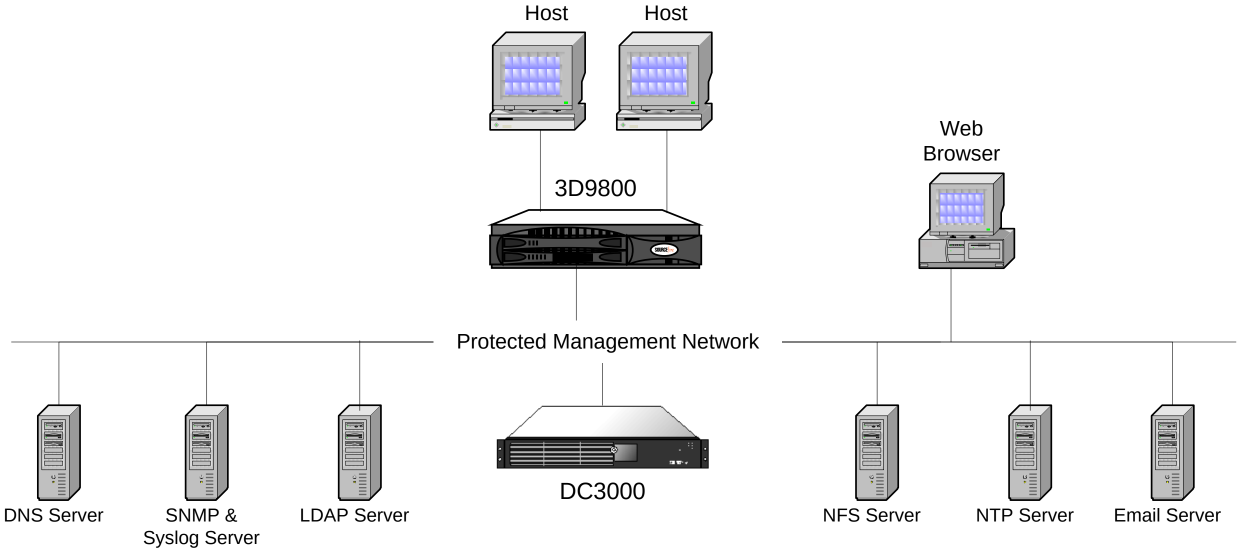

Figure 8: A DC3000 Defense Center managing a SVLinux Intrusion Sensor deployed in inline mode (Configuration 4)

The next figure shows a SBLinux Intrusion Sensor deployed in inline mode managed by a Defense Center. This is configuration 5.

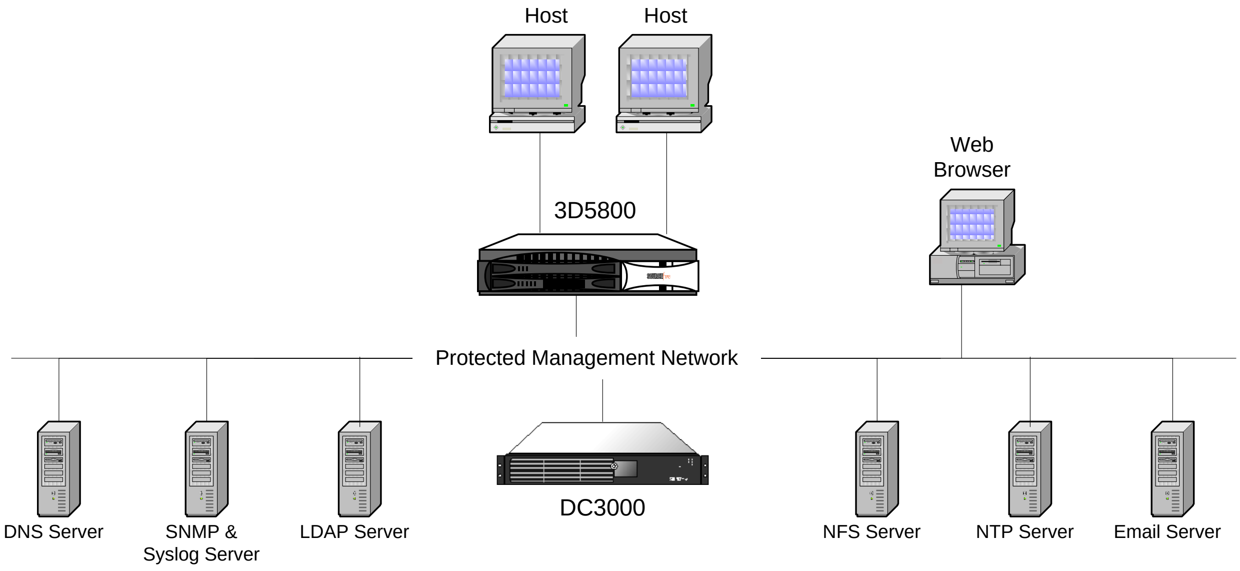

Figure 9: A DC3000 Defense Center managing a SBLinux Intrusion Sensor deployed in inline mode (Configuration 5)

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 R2 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 and Recommendations

1. 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.
2. 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, which notes that PDF is now the most common Malware vector).
3. 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).
4. 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.
5. 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
6. 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

The security target is *Sourcefire 3D System Security Target (Sourcefire Defense Center: models DC500, DC1000, and DC3000; and Sourcefire 3D Sensor licensed for IPS: models 3D500, 3D1000, 3D2000, 3D2100, 3D2500, 3D3500, 3D3800, 3D4500, 3D5800, 3D6500, and 3D9800) Version 4.8.2.1 (SEU 259)*, Version 1.15, June 10, 2010. The ST is compliant with the Specification of Security Targets requirements found within Annex B of Part 1of 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.

CC	Common Criteria [for IT Security Evaluation]
CIDR	Classless Inter Domain Routing
CM	Configuration Management
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication
GB	Gigabyte
HTTP	HyperText Transmission Protocol
HTTPS	HyperText Transmission Protocol, Secure
ICMP	Internet Control Message Protocol
ID	Identifier
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
NIST	National Institute of Standards and Technology
PCAP	Packet Capture
PP	Protection Profile
RPC	Remote Procedure Call
SEU	Security Enhancement Updates
SF	Security Function
SFIDS	Sourcefire Intrusion Detection System
SFP	Security Function Policy
SFR	Security Functional Requirements
SNMP	Simple Network Management Protocol
ST	Security Target
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface

TSP	TOE Security Policy
UDP	User Datagram Protocol
UI	User Interface
URI	Uniform Resource Identifier

12.2 Terminology

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

Access List A list of computers can access the appliance on specific ports.

Analyzer Data Data collected by the analyzer functions.

Analyzer Functions 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 3D Sensor with IPS performs the analyzer functions of the TOE.

Assets Information or resources to be protected by the countermeasures of a TOE.

Assignment The specification of an identified parameter in a component.

Assurance Grounds for confidence that an entity meets its security objectives

Attack 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.

Attack Potential 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.

Audit 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.

Audit Log 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.

Audit Trail See **Audit Log**

Augmentation The addition of one or more assurance component(s) to a package

Authentication To establish the validity of a claimed user or object.

Authentication Data Information used to verify the claimed identity of a user

Authentication Object An object that contains the settings for connecting to and retrieving user data from an external authentication server.

Authorised User A user who may, in accordance with the SFR, perform an operation.

Authorized Administrator The authorized users that manage the TOE or a subset of its TSF data and management functions.

Availability Assuring information and communications services will be ready for use when expected.

Class A grouping of families that share a common focus.

Component The smallest selectable set of elements on which requirements may be based.

Compromise An intrusion into an IT System where unauthorized disclosure, modification or destruction of sensitive information may have occurred.

Confidentiality Assuring information will be kept secret, with access limited to appropriate persons.

Connectivity 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.

Defense Center The Sourcefire 3D System Defense Center appliance and the software installed upon it. A central management point that allows the management of the 3D Sensors and automatically aggregates the events they generate.

Dependency 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.

Detection Engine The mechanism that is responsible for analyzing the traffic on the network segment where a sensor is connected.

Element An indivisible security requirement.

Evaluation Assessment of a PP, an ST, or a TOE against defined criteria.

Evaluation Assurance Level (EAL) A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.

Evaluation Authority

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.

Evaluation Scheme

The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.

Extension

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.

External Entity

Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.

Family

A grouping of components that share security objectives but may differ in emphasis or rigor.

Formal

Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Health Alert

An alert generated by the Defense Center when a specific health event occurs.

Health Event

An event that is generated when one of the appliances 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.

Health Module

A test of a particular performance aspect of one of the appliances in a deployment.

Health Policy

The criteria used when checking the health of an appliance in a deployment. Health policies use health modules to indicate whether Sourcefire 3D System hardware and software are working correctly.

Identity

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.

IDS Analyzer (analyzer)

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 3D Sensor with IPS is the analyzer component of the TOE.

IDS Component

A sensor, scanner, or analyzer. The 3D Sensor with IPS is the IDS component of the TOE.

IDS Scanner (scanner)

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 3D Sensor with IPS is the scanner component of the TOE.

IDS Sensor (sensor) The component of an IDS that collects real-time events that may be indicative of vulnerabilities in or misuse of IT resources. The 3D Sensor with IPS is the sensor component of the TOE.

Incident One or more intrusion events that are suspected of being involved in a possible violation of a security policy.

Informal Expressed in natural language.

Integrity Assuring information will not be accidentally or maliciously altered or destroyed.

Interface Set One or more sensing interfaces on a 3D Sensor that can be used to monitor network segments for one or more detection engines.

Internal Communication Channel A communication channel between separated parts of TOE.

Internal TOE Transfer Communicating data between separated parts of the TOE.

Inter-TSF Transfers Communicating data between the TOE and the security functions of other trusted IT products.

Intrusion Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.

Intrusion Detection The process of passively analyzing network traffic for potential intrusions and storing attack data for security analysis.

Intrusion Detection System (IDS) 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.

Intrusion Event A record of the network traffic that violated an intrusion policy.

Intrusion Policy 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.

Intrusion Protection The concept of intrusion detection with the added ability to block or alter malicious traffic as it travels across a network.

Intrusion Rule 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.

IT Product A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.

IT System May range from a computer system to a computer network.

Iteration The use of the same component to express two or more distinct requirements.

Network Two or more machines interconnected for communications.

Object A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Organizational Security Policies 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.

Package A named set of either functional or assurance requirements (e.g. EAL 3).

Packet A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.

Packet Sniffer A device or program that monitors the data traveling between computers on a network.

Preprocessor 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.

Protection Profile (PP) An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Prove 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.

Refinement The addition of details to a component.

Reviewed Event 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.

Role A predefined set of rules establishing the allowed interactions between a user and the TOE.

Root (root user, root account) The superuser, a user on Unix-like systems, usually with full administrative privileges.

Scanner Data Data collected by the scanner functions.

Scanner Functions 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).

Secret Information that must be known only to authorized users and/or the TSF in order to enforce a specific SFP.

Secure State A state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs.

Security A condition that results from the establishment and maintenance of protective measures that ensures a state of inviolability from hostile acts or influences.

Security Attribute 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.

Security Function Policy (SFP) A set of rules describing specific security behavior enforced by the TSF and expressible as a set of SFRs.

Security Objective A statement of intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions.

Security Policy The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Target (ST) A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Selection The specification of one or more items from a list in a component.

Semiformal Expressed in a restricted syntax language with defined semantics.

Sensor (3D Sensor with IPS) 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.

Sensor Data Data collected by the Sensor functions.

Sensor Functions 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).

Signatures Patterns of network traffic that can be used to detect attacks or exploits.

Subject An active entity in the TOE that performs operations on objects.

System Policy 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.

Target of Evaluation (TOE) A set of software, firmware and/or hardware possibly accompanied by guidance.

Threat 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.

TOE Administrator See **Authorized Administrator**

TOE Resource Anything useable or consumable in the TOE.

TOE Security Functions (TSF) A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP) A set of rules that regulate how assets are managed, protected, and distributed within a TOE.

Transfers outside TSF TSF mediated communication of data to entities not under control of the TSF.

Trojan Horse An apparently useful and innocent program containing additional hidden code that allows the unauthorized collection, exploitation, falsification, or destruction of data.

Trusted Channel A means by which a TSF and a remote trusted IT product can communicate with necessary confidence.

Trusted Path A means by which a user and a TSF can communicate with necessary confidence.

TSF Data Data created by and for the TOE, which might affect the operation of the TOE.

TSF Interface (TSFI) 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.

TSF Scope of Control (TSC) The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

User See **External Entity**

User Data Data created by and for the user that does not affect the operation of the TSF.

Virus A program that can "infect" other programs by modifying them to include a, possibly evolved, copy of itself.

Vulnerability 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 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).

CCEVS Documents

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, September 2006 Version 3.1 Revision 1, CCMB-2006-09-001.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, September 2007 Version 3.1 Revision 2, CCMB-2007-09-002.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, September 2007, Version 3.1 Revision 2, CCMB-2007-09-003.

[4] Common Methodology for Information Technology Security Evaluation - Evaluation methodology, September 2007, Version 3.1 Revision 2, CCMB-2007-09-004.