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 1.1

June 5, 2012

Prepared For

SOURCEfire

Sourcefire, Incorporated

9770 Patuxent Woods Drive
Columbia, MD 21046

Prepared By

CYGNACOM SOLUTIONS

7925 Jones Branch Drive♦Suite 5400 ♦McLean, VA 22102-3378♦703 848-0883♦Fax 703 848-0985

Table of Contents

Section **Page**

Figures and Tables

Figures **Page**

Tables **Page**

1 Security Target Introduction

1.1 Security Target Reference

ST Title:	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)
ST Version:	v1.1
ST Author:	CygnaCom Solutions
ST Date:	June 5, 2012
Assurance level:	EAL2 augmented with ALC_FLR.2
Keywords:	intrusion prevention, intrusion detection, IPS, IDS, intrusion prevention system, intrusion detection system, scanner, analyzer, sensor

1.1.1 References

Table 1-1 provides the references used to develop this Security Target.

Table 1-1: References

Reference Title	ID
Common Criteria for Information Technology Security Evaluation, CCMB-2009-07-002, Version 3.1, Revision 3	[CC]
Sourcefire 3D System – Defense Center Installation Guide, Version 4.10.2, 2011-Nov-01	[DC-INSTALL]
U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments, Version 1.7, July 25, 2007.	[IDS_PP]
Sourcefire 3D System Release Notes Version 4.10.2, December 7, 2011	[RELEASE-4.10.2]
Sourcefire 3D System Release Notes Version 4.10.1, May 13, 2011	[RELEASE-4.10.1]
Sourcefire 3D System Release Notes Version 4.10, May 12, 2011	[RELEASE-4.10]
Sourcefire 3D System - 3D Sensor Installation Guide, Version 4.10.2, 2011-Dec-04	[SENS-INSTALL]
Sourcefire 3D System - Sourcefire 3D System User Guide, Version 4.10.2, 2011-Oct-31	[USER]
Sourcefire 3D System - Virtual Defense Center and 3D Sensor Installation Guide, Version 4.10.2, 2011-Sep-23	[VIRTUAL-INSTALL]

1.2 TOE Reference

TOE Identification: 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)

TOE Vendor: Sourcefire, Inc.

1.3 TOE Overview

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

The Sourcefire Defense Center (Defense Center), Sourcefire 3D Sensor licensed for IPS (3D Sensor with IPS), Sourcefire Virtual Defense Center (Virtual Defense Center) and Sourcefire Virtual 3D Sensor licensed for IPS (Virtual 3D Sensor with IPS) are components of the Sourcefire 3D System Version 4.10.2.4.

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 warning banners; and system data collection, analysis, review, availability and loss.

Two previous versions of the product were evaluated and certified at EAL2:

- 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) in June 2010.
- Sourcefire 3D System (Sourcefire Defense Center: models DC500, DC1000, and DC3000; Sourcefire 3D Sensor licensed for IPS: models 3D500, 3D1000, 3D2000, 3D2100, 3D2500, 3D3500, 3D4500, 3D6500 and 3D9900; Sourcefire Virtual Defense Center, Sourcefire Virtual 3D Sensor licensed for IPS) Version 4.9.1.4 (SEU 371) in April 2011.

1.3.1 TOE Type

The TOE is an Intrusion Prevention and Detection System that combines open-source and proprietary technology. The TOE monitors 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.

1.3.2 Hardware/Firmware/Software Required by the TOE

The Sourcefire 3D System Version 4.10.2.4 (SEU 568) software is embedded in the Sourcefire Defense Center and the Sourcefire 3D Sensor licensed for IPS appliances. The appliance hardware, the underlying operating systems, and third-party applications installed on the appliances provide support for the intrusion detection functions and associated security management functions of the TOE, and are included in the TOE.

Each appliance includes a Linux-derived operating system. The hardware and operating system on which the Sourcefire 3D System application software operates provides the support necessary for the software applications to exist as processes and to access necessary disk, memory, and network connection resources.

Please see Sections 1.4.3.1 Sourcefire 3D Sensor licensed for IPS (3D Sensor with IPS) and 1.4.3.3 Sourcefire Defense Center (Defense Center) for a detailed description of the appliance-based components of the TOE.

The Sourcefire 3D System 4.10.2.4 also includes the software-only Sourcefire Virtual Defense Center and Sourcefire Virtual 3D Sensor licensed for IPS components. These components consist of only the software that implements the security functionality of the TOE. These components consist of the same Sourcefire application code, Linux-derived operating system and third-party applications as used on the appliance-based components. The platform, underlying operating system of the platform and the VMware implementation needed to run the Virtual Defense Center and Virtual 3D Sensor with IPS components are included in the Operational Environment.

Important: *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.*

Please see Sections 1.4.3.2 Sourcefire Virtual 3D Sensor licensed for IPS (Virtual 3D Sensor with IPS) and 1.4.3.4 Sourcefire Virtual Defense Center (Virtual Defense Center) for a detailed description of the virtual components of the TOE.

The evaluated configuration of the TOE requires the following Operational Environment support:

- A Web Browser for the Defense Center, Virtual Defense Center and 3D Sensor with IPS management interfaces. Sourcefire 3D System Version 4.10.2.4 was tested with the browsers as configured in the following table:

Table 1-2: Tested Web Browsers

Browser	Required Enabled Options and Settings

Browser	Required Enabled Options and Settings
Firefox 7	JavaScript Cookies Secure Sockets Layer (SSL) v3
Microsoft Internet Explorer 7.0	JavaScript Cookies Secure Sockets Layer (SSL) v3 128-bit encryption Active scripting security setting Set Check for newer versions of stored pages to Automatically
Microsoft Internet Explorer 8.0	JavaScript Cookies Secure Sockets Layer (SSL) v3 128-bit encryption Active scripting security setting Compatibility View Set Check for newer versions of stored pages to Automatically

- A private, protected network between the Defense Center (virtual and appliances) and the 3D Sensor(s) with IPS (virtual and appliances)
- The network(s) that are to be monitored
- Network Authentication Services
- A trusted DNS Server
- An NTP Server to provide reliable time
- An Email Server to send administrator alert notifications and warnings

The following Operational Environment components are needed for the Virtual Defense Center and Virtual 3D Sensor with IPS platforms:

- These platforms must be capable of hosting VMware ESX or ESXi Version 4.1.
- The ESX host for the Virtual 3D Sensor with IPS needs at least one CPU, 1GB of memory, and 20GB of disk space.
- The ESX host for the Virtual Defense Center needs at a minimum 2 CPUs, 1GB of memory, and 80GB of disk space.

The following Operational Environment components are optional for the evaluated configuration of the TOE.

- An external Syslog Server for administrator alert notifications and external storage of audit log records
- An SNMP Trap Server for administrator alert notifications
- An external authentication server (LDAP or RADIUS)

1.4 TOE Description

1.4.1 Acronyms

The following table defines product specific and CC specific acronyms used within this Security Target.

Table 1-3: Product and CC Acronyms

Acronym	Definition
CC	Common Criteria [for IT Security Evaluation]
CIDR	Classless Inter Domain Routing
CLI	Command Line Interface
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
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
SSL	Secure Sockets Layer
ST	Security Target
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Security Layer
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

1.4.2 Terminology

The following table defines product-specific and CC-specific terminology used within this Security Target.

Table 1-4: Product and CC Terminology

Terminology	Definition
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.
Access List	A list of computers can access a 3D System component 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 (Virtual) 3D Sensor with IPS performs the analyzer functions of the TOE.
Assets	Information or resources to be protected by the countermeasures of a TOE.
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.
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 (Audit Trail)	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.
Authentication	To establish the validity of a claimed user or object.
Authentication Object	An object that contains the settings for connecting to and retrieving user data from an external authentication server.
Authorized Administrator (TOE 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.
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.
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 (appliance-based and virtual) and automatically aggregates the events they generate.

Terminology	Definition
Detection Engine	The mechanism that is responsible for analyzing the traffic on the network segment where a sensor is connected.
Evaluation	Assessment of a PP, a ST or a TOE, against defined criteria.
Health Alert	An alert generated by the (Virtual) Defense Center when a specific health event occurs.
Health Event	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.
Health Module	A test of a particular performance aspect of one of the components 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.
IDS component	A sensor, scanner, or analyzer. The (Virtual) 3D Sensor with IPS is the IDS component of the TOE.
Incident	One or more intrusion events that are suspected of being involved in a possible violation of a security policy.
Information Technology (IT) System	May range from a computer system to a computer network.
Integrity	Assuring information will not be accidentally or maliciously altered or destroyed.
Interface Set	One or more sensing interfaces on a 3D Sensor (appliance-based or virtual) that can be used to monitor network segments for one or more detection engines.
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 Detection System 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 (Virtual) 3D Sensor with IPS is the analyzer component of the TOE.
Intrusion Detection System 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 (Virtual) 3D Sensor with IPS is the scanner component of the TOE.
Intrusion Detection System 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 (Virtual) 3D Sensor with IPS is the sensor component of the TOE.
Intrusion Event	A record of the network traffic that violated an intrusion policy.

Terminology	Definition
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.
Network	Two or more machines interconnected for communications.
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
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.
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).
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 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.
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).

Terminology	Definition
Signatures	Patterns of network traffic that can be used to detect attacks or exploits.
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)	An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
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 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.
Trojan Horse	An apparently useful and innocent program containing additional hidden code that allows the unauthorized collection, exploitation, falsification, or destruction of data.
TSF data	Data created by and for the TOE that might affect the operation of the TOE.
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	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Virtual 3D Sensor with IPS	A 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.
Virtual Defense Center	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.
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.

1.4.3 Product Description

Sourcefire markets an integrated Enterprise Threat Management (ETM) solution. To provide the entire ETM solution, Sourcefire 3D System integrates four core products: Sourcefire IPS, Sourcefire RNA, Sourcefire RUA, and the Sourcefire Defense Center. Sourcefire offers these products as individual components or as a system to a meet a variety of IT security needs and budgets. Each of the core products is sold separately and each product requires a separate license to run. This evaluation includes two of the four core products: Sourcefire IPS (the Sourcefire 3D Sensor licensed for IPS and the Sourcefire Virtual 3D Sensor licensed for IPS) and the Sourcefire Defense Center (the appliance-based Sourcefire Defense Center and the Sourcefire Virtual Defense Center).

The Sourcefire 3D System monitors a customer's network for traffic that could affect the availability, integrity, and confidentiality of a host and its data. By placing 3D Sensors (appliance-based or virtual) on key network segments, the packets that traverse the network can be examined for malicious activity. The TOE allows authorized administrators to monitor the network for attacks that might affect the availability, integrity, or confidentiality of hosts on the network either directly from the sensor or through a central Defense Center (either appliance-based or virtual).

The Sourcefire Intrusion Prevention System (also called IPS) is one of the components of the Sourcefire 3D System that can be run on the Sourcefire 3D Sensors and Sourcefire Virtual 3D Sensors. Each sensor licensed for IPS uses rules, decoders, and preprocessors to look for the broad range of exploits that attackers have developed. The sensors licensed for IPS allow the Sourcefire 3D System to be used as an intrusion detection system and/or an intrusion prevention system.

The Sourcefire 3D System TOE consists of the following components:

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

1.4.3.1 Sourcefire 3D Sensor licensed for IPS (3D Sensor with IPS)

The Sourcefire 3D Sensor licensed for IPS is an appliance-based component of the TOE and includes both software and hardware.

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. Snort Version: 2.9.2 is included in the CC evaluated version of the Sourcefire 3D System.

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. 3D Sensors with 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.

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 only being 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 of the 3D Sensor with IPS 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 Series 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. These sensors monitor internal traffic buffers and bypass detection engines if those buffers are full.

The 7000 Series and 8000 Series sensors have an LCD panel, which displays system information and status and also error alerts and messages. Multi-function keys on the LCD panel can be used to perform basic configuration of the sensor during installation. Input to the LCD panel is logged in the syslog but only during initial configuration of the appliance. The LCD panel is not used for management functionality during the run-time operation of the TOE and is not considered a TOE Security Functions Interface (TSFI).

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.

The 3D500, 3D1000, and 3D2000 models of the 3D Sensor with IPS included in the evaluation 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 (appliance-based or virtual) for management.

The 8000 Series of 3D Sensors with IPS (Models 3D8120, 3D8130, 3D8140 and 3D8250) and the 7000 Series of 3D Sensors with IPS (Models 3D7110 and 3D7120) 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 7000 Series and 8000 Series sensors also 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 or the sensor appliances. There are several modes with various permissions levels that can be configured on a per-user basis for use of the CLI. For security reasons, access to the CLI must be limited. This CLI is not a Security Management Interface.

The command line interface of the appliance's operating system (OS shell) is used for the initial configuration and off-line maintenance of the 3D Sensor with IPS. Use of the OS shell is also required to configure audit suppression lists (See 7.1.1.3 AU-3: Audit Selection). By default, port 443 (Secure Sockets Layer, or SSL), which is used to access the web interface (WebUI), and port 22 (Secure Shell, or SSH), which is used to access the shell, are enabled for any IP address. By default, access to the appliance is not restricted. To operate the appliance in a more secure environment, an access list must be created during the initial configuration of the system, which restricts shell access to the appliance to specific IP addresses. Ideally, only the IP address for one console will be enabled for shell access per system. Since the OS shell is needed for system maintenance, and creating and editing audit suppression lists, the administrator must be careful not to disable all access to the system.

Users who have shell access to the 3D Sensor with IPS and can access the operating system's *admin* account must also be restricted to only those administrators who need to configure and maintain the system.

Each 3D Sensor with IPS includes a MySQL (v5.1.50) database that stores audit data, configuration data (intrusion policies, system policies …), and IDS system data. The database storage options are configurable. A TOE administrator can choose to send the intrusion events to the (Virtual) Defense Center that manages the sensor, send the events to the (Virtual) Defense Center and keep a local copy in sensor's database, or if the sensor is used as a stand-alone system, all events are stored locally in the database. There is no direct access to the MySQL database through the management WebUI.

The same Sourcefire application software is installed on all models of the 3D Sensor with IPS appliances and all the sensor appliances in the evaluated configuration run the SFLinux Version 4.10 operating system. SFLinux is a Sourcefire proprietary operating system built from open-source Linux code. Only services and packages required by the TOE for secure operation are enabled in this OS. The 8000 Series and 7000 Series models of the sensor run a 64-bit version of the SFLinux v4.10 operating system. The source files are the same for all sensors; however, the files for the 8000 and 7000 Series sensors are compiled with a makefile that uses 64-bit compilers and, in some cases, 64-bit libraries. The 3D Sensors with IPS can therefore be categorized by the Linux-derived operating system installed on the appliance as follows:

Table 1-5: 3D Sensor with IPS Categories

Sourcefire 3D Sensor Category	Sourcefire 3D Sensor Appliance Model
SFLinux v4.10 (64-bit) Sourcefire Proprietary Linux-derived OS	3D8120
	3D8130
	3D8140
	3D8250
	3D7110
	3D7120
SFLinux v4.10 (32-bit) Sourcefire Proprietary Linux-derived OS	3D500
	3D1000
	3D2000

Each category of the sensors will be tested in this evaluation.

Besides the appliance hardware, Sourcefire application software, MySQL database and the operating systems mentioned above, the following supporting third-party software is included in the 3D Sensor with IPS TOE Component:

- Network connectivity provided through third-party encryption software (OpenSSL 0.9.8q)
- Protocol standards including HTTPS, SMTP, SSH, and SNMP (v2 or v3) implementations
- Perl (v5.10.1)
- Shell access through OpenSSH (v5.6p1)
- Web Server (Tomcat Apache Version 2.2.17)

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.

1.4.3.2 Sourcefire Virtual 3D Sensor licensed for IPS (Virtual 3D Sensor with IPS)

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 hypervisor.

The installation files for the Virtual 3D Sensor with IPS are delivered in VMware's Open Virtual Format (OVF). The installation files are downloaded from the Sourcefire Support Site (https://support.sourcefire.com/). The installation package contains the same Sourcefire application code, SFLinux operating system, MySQL database, and third-party applications that are installed on the appliance-based 3D Sensors with IPS. Once loaded on the hypervisor and started, initial configuration for the management interface is required via the OS shell using the Virtual 3D Sensor with IPS's *admin* account.

The Virtual 3D Sensor's sensing interface must be associated with a port on a hypervisor virtual switch that has promiscuous mode enabled.

A Virtual 3D Sensor can be managed by an appliance-based or Virtual Defense Center but IPS events cannot be collected from that sensor until the Virtual 3D Sensor IPS license is added to the managing (Virtual) Defense Center. Maximum throughput and processing capacity for the Virtual 3D Sensor with IPS (and Virtual Defense Center) are heavily influenced by a number of factors, such as:

- Amount of memory and CPU capacity of the ESX host
- Number of total virtual machines running on the ESX host
- Amount of resources assigned to each virtual machine
- Level of activity of other virtual machines sharing the platform

There are a number of performance measurement and resource allocation tools provided by VMware on the ESX host. Sourcefire recommends that these tools be used while running the Virtual 3D Sensor with IPS and monitoring traffic to determine throughput. If the throughput is not satisfactory, the resources assigned to the Virtual 3D Sensor with IPS or to other virtual machines that share the ESX host can be adjusted.

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. There are several modes with various permissions levels that can be configured on a per-user basis for use of the CLI. For security reasons, access to the CLI must be limited. This CLI is not a Security Management interface.

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.

1.4.3.3 Sourcefire Defense Center (Defense Center)

The Sourcefire Defense Center is an appliance-based component of the TOE and includes both software and hardware.

The 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.

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

- An interface which displays all the data collected by the managed sensors 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 command line interface (OS shell) of the appliance's operating system is used for the initial configuration and off-line maintenance of the Defense Center. Use of the OS shell is required to configure audit suppression lists (See Section 7.1.1.3 AU-3: Audit Selection). By default, port 443 (Secure Sockets Layer, or SSL), which is used to access the web interface (WebUI), and port 22 (Secure Shell, or SSH), which is used to access the shell, are enabled for any IP address. By default, access to the appliance is not restricted. To operate the appliance in a more secure environment for Common Criteria compliance, an access list must be created during the initial configuration of the system, which restricts shell access to the appliance to specific IP addresses. Ideally, only the IP address for one console will be enabled for shell access per system. Since the OS shell is needed for system maintenance, and creating and editing audit suppression lists, the administrator must be careful not to disable all access to the system.

Users who have shell access to the Defense Center and can access the operating system's *admin* account must also be restricted to only those administrators who need to configure and maintain the system.

The Defense Center includes the Sourcefire proprietary Linux-derived OS, SFLinux, and a MySQL (v5.1.50) database repository. The database is used to store intrusion, audit, and health events, as well as other events that are outside the TOE. Configuration information is also stored in the database. This information includes intrusion, health, and system policies. Intrusion rules are delivered as flat files that are later stored in the database. There is no direct access to the MySQL database through the management WebUI.

The Sourcefire 3D System has the capability of using an external LDAP or RADIUS server for user authentication in a configuration that uses a Defense Center. User accounts are stored in the Defense Center's MySQL database, including the initial RADIUS and LDAP information if external authentication of users is configured. When RADIUS or LDAP authentication is used, an additional file is written to disk.

The Defense Center also provides the capability to download and import Security Enhancement Updates (SEUs) that contain new intrusion rules, which are provided by the Sourcefire Vulnerability Research Team (VRT). The SEUs can be downloaded and imported by authorized administrators on command and are not necessarily automatic. However, these SEU releases may also contain new and updated decoders and preprocessors, and updates to the sensor code. Because the SEUs can contain binaries that modify the TOE software, once applied, the Sourcefire 3D System may no longer be in the evaluated configuration. Therefore, the SEU feature cannot be used in the evaluated configuration. Detailed information about the changes to rules contained in each SEU release can be obtained on the Sourcefire customer support web site for those customers who wish to make the updates manually.

The CC evaluation version of the Sourcefire 3D System includes SEU Version 568 (which in turn includes Snort Version 2.9.2).

A Master Defense Center can be used to aggregate and analyze data from up to ten Defense Centers within a Sourcefire 3D System deployment. Master Defense Centers allow the product to monitor a large-scale enterprise. A Master Defense Center will not be included in the scope of the evaluation.

The product also includes a High Availability feature that uses redundant Defense Centers to manage groups of sensors. If the primary Defense Center fails, the secondary Defense Center is used to monitor the network without interruption. The High Availability feature is not included in the evaluated configuration of the TOE.

Besides the appliance hardware, Sourcefire application software, MySQL database and the operating system mentioned above, the following supporting third-party software is included in the Defense Center TOE component:

- Network connectivity provided through third-party encryption software (OpenSSL 0.9.8q)
- Protocol standards including HTTPS, SMTP, SSH, and SNMP (v2 or v3) implementations
- Perl (v5.10.1)
- Shell access through OpenSSH (v5.6p1)
- Web Server (Tomcat Apache Version 2.2.17)

The Sourcefire software, operating system, database, and third-party products are the same for all models of the Defense Center appliances (Defense Center Models DC750, DC1500 and DC3500).

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.

1.4.3.4 Sourcefire Virtual Defense Center (Virtual Defense Center)

The Sourcefire Virtual Defense Center is a software-only version of the Sourcefire Defense Center that runs within a VMware virtual environment. The Virtual Defense Center runs on any platform that supports VMware's ESX/ESXi Version 4.1 hypervisor.

The installation files for the Virtual Defense Center are delivered in VMware's Open Virtual Format (OVF). The installation files are downloaded from the Sourcefire Support Site (https://support.sourcefire.com/). The installation package contains the same Sourcefire application code, SFLinux operating system, MySQL database, and third-party applications that are installed on the appliance-based Defense Center. Once loaded on the hypervisor and started, initial configuration for the management interface is required via the OS shell using the Virtual Defense Center's *admin* account.

Virtual Defense Center can manage both physical and virtual sensors. The Virtual Defense Center supports local event storage and can manage up to 25 sensors, physical or virtual, in any combination.

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. (A Master Defense Center is not included in the evaluated configuration.)
- A Virtual Defense Center cannot be used in a High Availability configuration with either a physical Defense Center or another Virtual Defense Center. (The High Availability feature is not included in the evaluated configuration.)

1.4.4 Data

The data managed by the TOE can be categorized as:

- Data used to configure, manage, and operate the TOE such as: user accounts and IDS rules and policies
- Audit data produced by the TOE for security significant events
- Data collected from the monitored network assets such as: Identification and authentication events, Data accesses, and Network traffic (system data)

All TOE data is considered TSF Data.

1.4.5 Users

The TOE maintains defined user roles, each with its own set of administrative privileges. When a new user account is created, it must be assigned a role. A user may be assigned more than one role. No access is allowed to the system until a user has been authenticated. Access to TSF data and functions is controlled by the TOE's interfaces only to the data and functions allowed by the authenticated user's role.

All users of the TOE have access to TSF data and management functions, and therefore they are considered administrators for the purposes of this evaluation. The terms "TOE user", "TOE administrator" and "authorized administrator" are used in this ST to refer collectively to all authorized TOE users.

The predefined 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 perform system level maintenance related actions.

- **"Policy and Response Administrator" Role**: this role can create, modify, and implement intrusion policies and intrusion rules for the IDS.

- **"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.

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,

Maintenance of the TOE also requires use of the **SFLinux *admin* user role**. The TOE administrator must have access to the Defense Center's or 3D Sensor with IPS's *admin* user account and must be able to access the Defense Center or 3D Sensor with IPS operating system's shell. It must be assumed that only authorized and limited personnel have access to the component's operating system and to its *admin* account. This is not a security role maintained by the TOE; it is maintained by the appliance OS and is equivalent to the system administrator of the OS. This role is required to set up the audit suppression mechanism. The audit suppression lists are created or modified at installation or during maintenance; this functionality is not part of the run-time operation of the TOE available through the WebUI.

1.4.6 Product Guidance

The Sourcefire 3D System documentation set includes online help and PDF files.
The following product guidance documents are provided with the TOE on the Documentation CD included with the product:

Table 1-6: User Guidance Documents

Sourcefire 3D System – Defense Center Installation Guide, Version 4.10.2, 2011-Nov-01
Sourcefire 3D System Release Notes Version 4.10.2, December 7, 2011
Sourcefire 3D System Release Notes Version 4.10.1, May 13, 2011
Sourcefire 3D System Release Notes Version 4.10, May 12, 2011
Sourcefire 3D System - 3D Sensor Installation Guide, Version 4.10.2, 2011-Dec-04
Sourcefire 3D System - Sourcefire 3D System User Guide, Version 4.10.2, 2011-Oct-31
Sourcefire 3D System - Virtual Defense Center and 3D Sensor Installation Guide, Version 4.10.2, 2011-Sep-23

The most up-to-date versions of the documentation can be accessed on the Sourcefire Support web site (https://support.sourcefire.com/).

Online help can be accessed in two ways:

- by clicking the context-sensitive help links on each page
- by selecting Operations > Help > Online

The CC evaluated version of the Sourcefire 3D System, Version 4.10.2.4 (SEU 568) also includes *Sourcefire 3D System - CC Supplement for Version 4.10.2,* [CC-SUPP]. [CC-SUPP] documents how to install, configure and maintain the Sourcefire 3D System in the CC evaluated configuration. [CC-SUPP] is packaged with the appliances in hard-copy format.

1.4.7 Physical Scope of the TOE

The TOE consists of the components described in Section 1.4.3. 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; and

- 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 third-party software.

The TOE Boundary is depicted in the following figures.

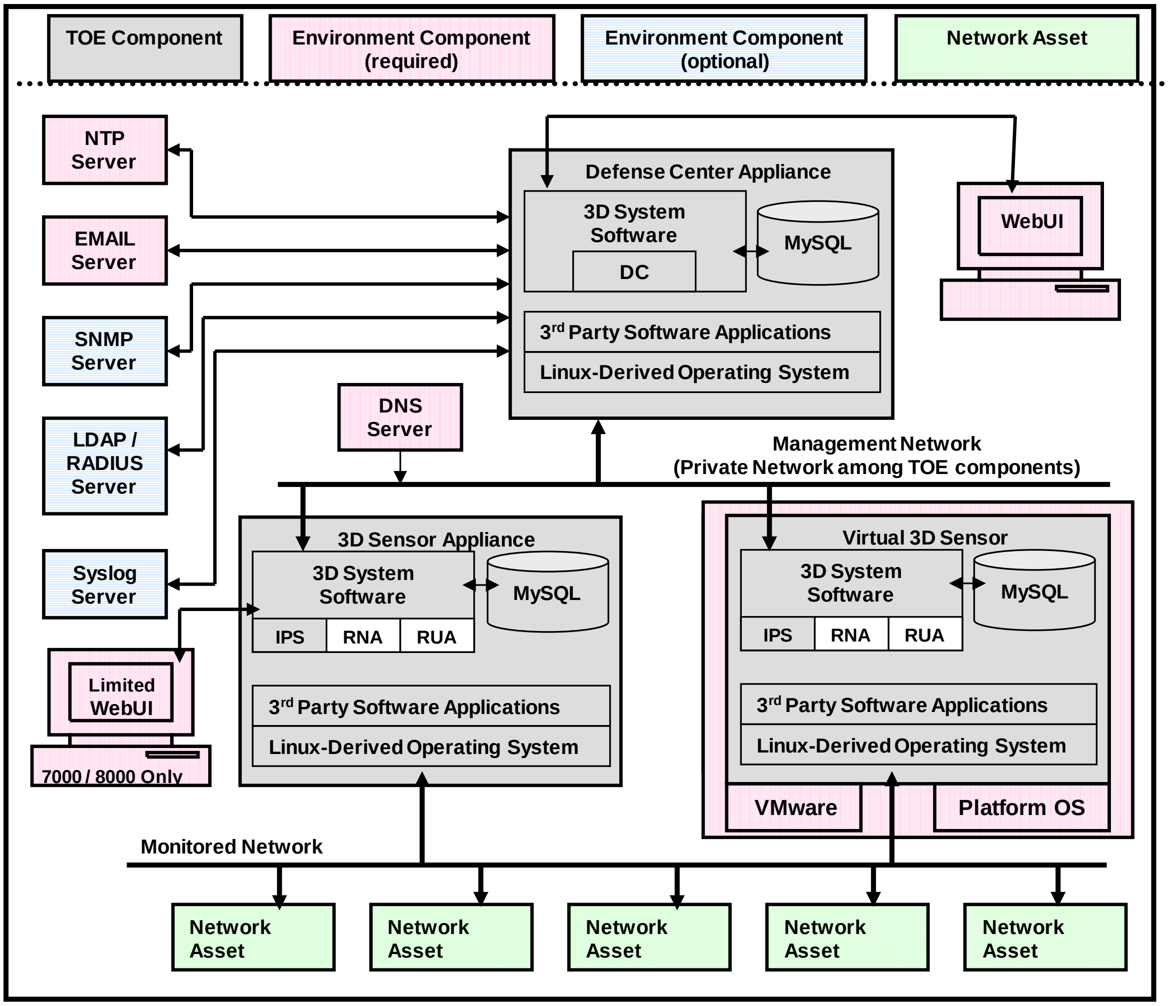

Figure 1: Sourcefire 3D System with Defense Center

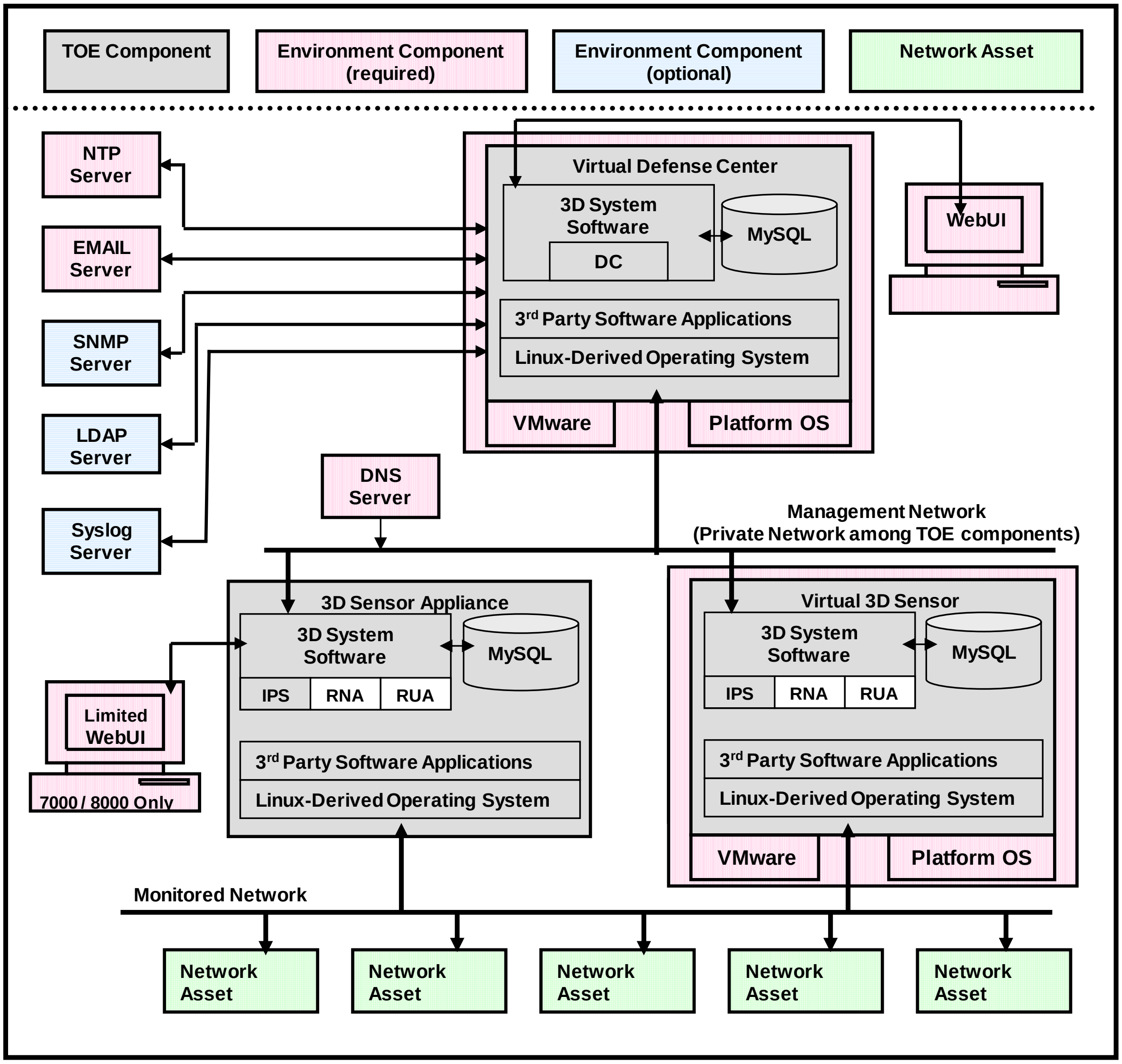

Figure 2: Sourcefire 3D System with Virtual Defense Center

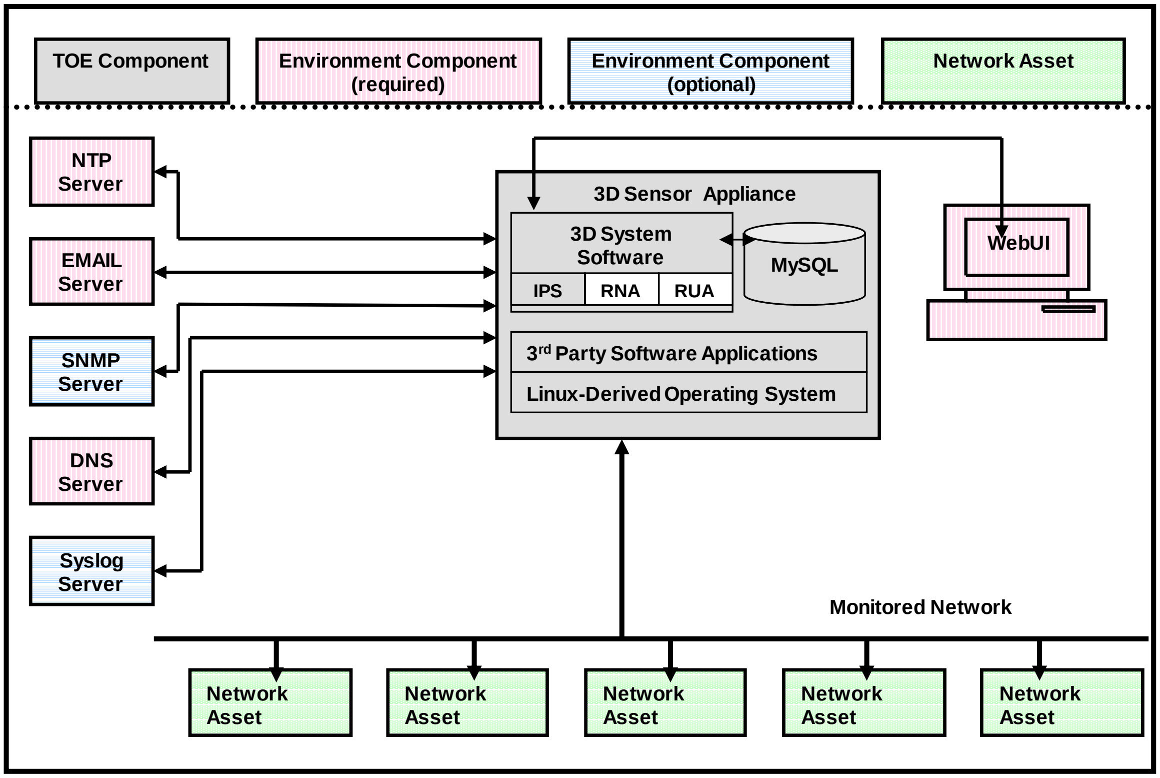

Figure 3: Sourcefire 3D System using a stand-alone 3D Sensor with IPS

The Sourcefire application software for the Defense Center and 3D Sensor with IPS components is physically installed on the Sourcefire appliances that run Linux-derived operating systems. As such, the physical interfaces for these components are based on and limited by services provided by the appliance hardware. The application software uses process, disk, and memory management services of the appliance hardware and the operating system to execute and manage itself. The application software also uses network services provided by the appliance hardware and operating system: to access network traffic, including monitoring target networks; for communication between the 3D Sensor with IPS and Defense Center; and for the web-based user interfaces (3D Sensor with IPS and Defense Center GUIs).

The Virtual Defense Center and Virtual 3D Sensor with IPS components are physically installed on platforms that support VMware. The physical interfaces for these components are based on and limited by services provided by the platform hardware. The application software depends on both the Sourcefire SFLinux OS and third-party software included in the virtual components and on the underlying VMware and platform OS for process, disk, and memory management services and network services.

The Operational Environment of the TOE includes:

- The web browsers that are used for the management interfaces of the TOE

- The network(s) used for communications between the TOE components which must be protected from unauthorized access and separate from the network that is monitored by the TOE
- The network(s) that are to be monitored
- Network Authentication Services
- A trusted DNS Server
- An NTP Server for reliable time
- An Email Server for administrator alert notifications and warnings
- The platform hardware, software and VMware to support the Virtual Defense Center and Virtual 3D Sensor with IPS
- An optional external Syslog Server for administrator alert notifications and warnings, and external storage of the audit log
- An optional SNMP Trap Server for administrator alert notifications
- An optional external authentication server (LDAP or RADIUS)

As indicated in the figures above, the TOE can consist of a single 3D Sensor with IPS or any number of 3D Sensors with IPS and Virtual 3D Sensors with IPS combined with a single Defense Center or Virtual Defense Center.

1.4.7.1 Included in the TOE:

The evaluated configuration includes the following:

- The Sourcefire 3D Sensor, Version 4.10.2.4 (SEU 568), licensed to use the Sourcefire Intrusion Prevention System (IPS)
- The Sourcefire Defense Center, Version 4.10.2.4 (SEU 568)
- The Sourcefire Virtual 3D Sensor, Version 4.10.2.4 (SEU 568), licensed to use the Sourcefire Intrusion Prevention System (IPS)
- The Sourcefire Virtual Defense Center, Version 4.10.2.4 (SEU 568)

All typical deployments as described in Chapter 1 of [SENS-INSTALL] and Chapter 2 of [VIRTUAL-INSTALL] are permitted in the evaluated configuration of the TOE.

The multi-site environment deployment as described in [SENS-INSTALL] is allowed in the evaluated configuration. To secure the data in a multi-site environment deployment, the 3D Sensors and Defense Center must be isolated from unprotected networks by transmitting the data stream from the 3D Sensors over a VPN or with some other secure tunneling protocol.

Testing includes configurations that:

- Test the 3D Sensor with IPS for each category of appliance: SFLinux v4.10 and SFLinux v4.10 (64-bit)
- Test a stand-alone 3D Sensor with IPS configuration
- Test one or more 3D Sensors with IPS and one or more Virtual 3D Sensors with IPS managed by a single Defense Center or Virtual Defense Center
- Test both inline and passive deployments of the 3D Sensors with IPS

Therefore, there are three test configurations:

1. One Defense Center managing at least one Virtual 3D Sensor with IPS and at least one 3D Sensor with IPS from each operating system category, with at least one sensor deployed inline and at least one deployed passively
2. One Virtual Defense Center managing at least one Virtual 3D Sensor with IPS and at least one 3D Sensor with IPS
3. One 3D Sensor with IPS run in a stand-alone configuration

Note: The evaluation will not include testing the secure scrub of the hard drive as documented on Pages 81 and 82 of [DC-INSTALL].This is a product feature that is used to remove sensitive data from the hard drive of the appliance. This feature is not included in the scope of the evaluation and is used in limited circumstances, such as when a defective appliance needs to be returned for service.

1.4.7.2 Excluded from the TOE:

The following product components and functionality are not included in the scope of the evaluation:

- 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)
- Stacked 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 third-party products, including:
    - Sending alerts through trouble ticket systems
    - Interfaces with patch management systems
- Integration with Checkpoint OPSEC™ Suspicious Activity Monitor (SAM), including sending OPSEC alerts and use of OPSEC responses

- Xen Hypervisor platforms for virtual components
- Defense Center database access using an external third-party client

***Important**: The customer must assume the risk of enabling excluded functionality that was not part of the evaluation and has not been tested and validated.*

The following are Operational Environment components, which are excluded from the scope of the evaluation:

- The Web Browser for the Defense Center, Virtual Defense Center and 3D Sensor with IPS Management Interfaces as specified in Table 1-2: Tested Web Browsers
- 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

***Important:** 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.*

1.4.8 Logical Scope of the TOE

The logical boundaries of the TOE are divided into two groups, one related to the administration and security of the system (Security Audit, Identification and Authentication, Security Management, and Protection of Security Functions), and the other related to the collection and analysis of the network traffic (System Data Collection, System Data Analysis and System Data Review, Availability and Loss).

The TOE provides the following security functionality:

1.4.8.1 Security Audit

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.

Audit records may optionally be recorded in the internal syslog of the TOE components or sent to an external Syslog Server depending on the configuration of the System Policy of the TOE.

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.

Note: The administrator must 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 may optionally rely on an external Syslog Server depending on the TOE configuration. Security Audit also depends on the Operational Environment to provide a secure communications path between the TOE and the external servers.

1.4.8.2 Identification and Authentication

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 by an external authentication server for configurations that include a Defense Center or Virtual 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.

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.

1.4.8.3 Security Management

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. User roles are discussed in more detail in Sections 1.4.5 and 7.1.3.2.

The TOE also provides a command line interface (CLI) and shell access to the underlying operating system of the TOE components the use of these must be restricted. Both of these are used for off-line installation, configuration and maintenance of the TOE. The OS shell interface is only used for Security Management functionality when creating or modifying Audit Suppression Lists. The CLI is not a Security Management interface.

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

1.4.8.4 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 by transmission of data between the TOE Components over a secure, SSL-encrypted TCP tunnel.

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.

1.4.8.5 TOE Access Functions

The TOE enhances the functionality of user session establishment by being able to display a warning banner regarding unauthorized use of the TOE when a user attempts to login.

1.4.8.6 System Data Collection

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.

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 secure communications path between the TOE and the external time server.

1.4.8.7 System Data Analysis

To analyze the data collected by the 3D Sensors with IPS and Virtual 3D Sensors with IPS, the TOE uses statistical analysis, signatures, decoders, and preprocessors. Statistical analysis uses rate-base attack prevention features to detect and block denial-of-service (DoS) and distributed denial of service (DDoS) attacks. 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 statistical analysis, signatures, decoders, and preprocessors in rules that can be designed and exercised by the TOE.

The TOE administrators can manage the data analysis capabilities of the TOE 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.

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

1.4.8.8 System Data Review, Availability and Loss

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. Note that a Custom User Role must also have the "Analysis & Reporting -> Searches -> Intrusion Events" Permission to search for and retrieve intrusion event data.

Note: The administrator must 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.

1.4.8.9 Excluded Functionality

The following product functionality is not included in the scope of the evaluation:

- Functionality provided by the Real-Time Network Awareness (RNA) feature which includes:
  - Vulnerability Assessment (VA) (NMAP integration)
  - Network Behavior Analysis (NBA)
  - NetFlow Functionality
  - Adaptive IPS
  - Compliance Policies
- Functionality provided by the Real-Time User Awareness (RUA) feature which includes:
  - NAC and Network Usage Control (NUC)
- Intrusion Agents - Requires an existing installation of Snort
- Functionality provided by custom programming via the Estreamer Application Programming Interface (API)
- Security Enhancement Updates (SEU)
- Functionality provided by a Master Defense Center
- The High Availability feature provided by redundant Defense Centers

- Integration with and remediation of traffic to firewalls, including:
    - Integration with Cisco PIX and Checkpoint firewalls
- Integration with and remediation of traffic to external third-party products, including:
    - Interfaces with patch management systems
    - Sending alerts through trouble ticket systems
- IPS for Crossbeam Systems Security Switches (software-only sensors)

1.4.9 Differences between Versions 4.9 and Versions 4.10.2

Sourcefire 3D System
(Sourcefire Defense Center: models DC500, DC1000, and DC3000;
Sourcefire 3D Sensor licensed for IPS: models 3D500, 3D1000, 3D2000, 3D2100, 3D2500, 3D3500, 3D4500, 3D6500 and 3D9900;
Sourcefire Virtual Defense Center,
Sourcefire Virtual 3D Sensor licensed for IPS)
Version 4.9.1.4 (SEU 371)
was Common Criteria certified by NIAP at EAL 2 augmented with ALC_FLR.2;
Validation Report Number: CCEVS-VR-VID10406-2011; Date Issued; 6 April 2011.

The following is a summary of the major differences between the Sourcefire 3D System versions 4.9 and 4.10.2:

- **New Appliance Models**
  Three new Defense Center models were introduced with Version 4.10: the DC750, DC1500, and DC3500.

  New 3D Sensor models were introduced with Version 4.10: the 3D8120, 3D8130, 3D8140 and 3D8250 (called the 8000 Series sensors), and the 3D7110 and 3D7120 (called the 7000 Series sensors). These sensors cannot be run stand-alone, however they do provide a Limited WebUI management interface.

- **New Preprocessors and Decoders**
  New and enhanced preprocessors and decoders have been added to the product for the analysis of the network traffic.

- **VMware support**
  Version 4.10.2.4 supports VMware ESX 4.1 or ESXi 4.1.

- **Browser support**
  Version 4.10.2.4 was tested with Firefox version 7 and Internet Explorer versions 7 and 8.

- **Custom User Role Management**
  A new custom user role management feature allows administrators to create and assign new user roles with customized permissions, in addition to the predefined Sourcefire roles.

- **Custom User Role Escalation**
  Custom user roles can be given the permission, with a password, to gain the privileges of another user role temporarily. This allows administrators to substitute one user for another during an absence, or to track more closely the use of advanced user privileges.

- **Policy Comparison**
  It is possible to compare intrusion, health, PEP, and system policies and view the differences in the WebUI. Comparison reports can be generated for all of these policy types.

- **Change Reconciliation**
  The Change Reconciliation feature allows administrators to track changes to the system, both with daily change reconciliation reports and in the audit log. When a user makes a change to any part of the Sourcefire 3D System, information relating to the change (time, nature of changes, username, and IP address) is saved to the audit log, where it can be viewed.

- **Original Client IP**
  The original client IP address that was extracted from the X-Forwarded-For (XFF) or True-Client-IP HTTP headers can be viewed for intrusion events with the WebUI. To display a value for this field, the HTTP Inspect preprocessor *Extract Original Client IP Address* option must be enabled.

- **New Inline Result**
  For intrusion events, the Inline Result field has a new value: *would have dropped*. This value indicates that IPS would have dropped the packet in an inline deployment if the *Drop when Inline* intrusion policy option was enabled. The Inline Results are displayed when viewing intrusion events on the WebUI.

- **Reviewed Intrusion Events by User**
  The audit log will include the username of the user who reviewed each reviewed intrusion event.

- **Database Access (Not included in the Scope of the Evaluation)**
  A new optional database access feature allows users to query intrusion, network discovery, user identity, vulnerability, and some system-level database tables on a Defense Center, using an external third-party client that supports JDBC SSL connections. This feature is not included in the scope of the evaluation.

- **PEP Policy Changes**
  In Version 4.10, IPv4 and IPv6 packet filters are now called fast path rules. Traffic can be filtered by any protocol using either PEP rules or fast path rules. In addition, initiator and responder settings can be customized in IPv6 PEP rules.

- **SNMP Polling Support (Not included in the Scope of the Evaluation)**
  The system policy can be used to enable Simple Network Management Protocol

(SNMP) polling of an appliance, and thereby allow a network management system to obtain access to the appliance's standard management information base (MIB). Integration with an external network management system is not included in the evaluation.

- **SNMP Version Support**
  The TOE's security functions no longer support SNMP v1.

- **Root User Account**
  The *root* user account has been depreciated. Access to the operating system for installation, configuration and maintenance is via the *admin* user account. The *admin* account is also used for creating audit suppression lists. Version 4.10.1 also has a new feature to access the operating system named "expert mode". When a user goes into "expert mode" on the command line, the user can run any Linux command appropriate to the shell. When "expert mode" is enabled, a user with the "Configuration" command line interface access attribute can use the *sudo* command of the operating system shell to perform tasks that require *root* privileges. The "expert mode" setting can be disabled for a (virtual) appliance. As with the *admin* account, access to "expert mode" must also be restricted to only those administrators who need to configure and maintain the system, if this feature has not been disabled.

- **Command Line Interface**
  On 8000 Series, 7000 Series and Virtual 3D Sensors with IPS, a command line interface with a controlled set of commands and options is available. There are several CLI modes with various permissions levels that can be configured on a per-user basis. The CLI is used for off-line installation, configuration and maintenance of these sensors. This CLI is not a Security Management interface.

- **Password Hashing**
  Protection of the user account passwords stored in the TOE database is done by a salted SHA512 hash rather than by a MD5 one-way hash as in previous version of the product.

- **Security Improvements**
  Several security-related improvements were added to the Sourcefire 3D System:
  - Administrators or users with the Custom User Role with the "Operations -> System Settings" Permission can use the system settings to configure appliances to use an authenticated web proxy when downloading updates and rules.
  - Administrators or users with the "Custom User Role with the Operations -> System Settings" Permission can use the system settings to replace the default SSL (Secure Sockets Layer) certificate used to initiate encrypted communications between the web browser and a stand-alone sensor appliance. This allows use of a custom certificate signed by a globally known certificate authority (CA).

  - The connection between the TOE appliances and the mail relay host (SMTP server) in the environment can be configured in the system policy to support encryption either through SSLv3 or TLS
  - The MySQL database was upgraded to Version 5.1.50, which addresses multiple query-based DoS attacks.

- **Resolved Issues**
  Issues reported for version 4.9 have been resolved in version 4.10.2, using Sourcefire's documented Flaw Remediation Procedures. The resolved issues are listed in *Sourcefire 3D System Release Notes Version 4.10*, May 12, 2011 [RELEASE-4.10], *Sourcefire 3D System Release Notes Version 4.10.1*, May 13, 2011 [RELEASE-4.10.1] and *Sourcefire 3D System Release Notes Version 4.10.1*, December 7, 2011 [RELEASE-4.10.2].

2 Conformance Claims

2.1 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2 augmented with ALC_FLR.2 from the Common Criteria Version 3.1 R3. This Security Target conforms to the Common Criteria Version 3.1 R3.

2.2 Protection Profile Claim

This ST complies with U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments, Version 1.7, July 25, 2007 (IDS System PP). This protection profile has a NIAP sunset date of 2011-11-30; at the time of evaluation, no approved profile was available.

2.3 Package Claim

This ST claims conformance to the assurance requirements package: Evaluation Assurance Level (EAL) 2 augmented with ALC_FLR.2.

3 Security Problem Definition

The IDS System PP provides the following policies, threats and assumptions about the TOE.

3.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated. This section identifies the threats applicable to the IDS System PP as specified in the Protection Profile, verbatim.

Table 3-1: TOE Threats

TOE Threats		
1	T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
2	T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
3	T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
4	T.NOHALT	An unauthorized user may attempt to compromise the continuity of the system's collection and analysis functions by halting execution of the TOE.
5	T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
6	T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
7	T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
8	T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.

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

Table 3-2: IT System Threats

IT System Threats		
9	T.SCNCFG	Improper security configuration settings may exist in the IT System the TOE monitors.
10	T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the protected IT System data or undermines the IT System security functions.
11	T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors.

IT System Threats		
12	T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
13	T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
14	T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
15	T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
16	T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors.
17	T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

3.2 Organizational Security Policies (OSPs)

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section identifies the organizational security policies applicable to the IDS System PP as specified in the Protection Profile, verbatim.

Table 3-3: Organizational Security Policies

Organizational Security Policies		
1	P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
2	P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.
3	P.MANAGE	The TOE shall only be managed by authorized users.
4	P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
5	P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
6	P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
7	P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

3.3 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE applicable to the IDS System PP as specified in the Protection Profile, verbatim.

Table 3-4: TOE Usage Assumptions

TOE Intended Usage Assumptions		
1	A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
2	A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
3	A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.

Table 3-5: TOE Physical Assumptions

TOE Physical Assumptions		
4	A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
5	A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
6	A.VMXMIT	All packets coming in to the physical ports of the VMware hosts are transmitted unchanged to the virtual ports in the VMware environment.

Table 3-6: TOE Personnel Assumptions

TOE Personnel Assumptions		
7	A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
8	A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
9	A.NOTRST	The TOE can only be accessed by authorized users.

4 Security Objectives

This section defines the security objectives of the TOE and its supporting environment. These security objectives, categorized as IT security objectives for either the TOE or its environment are taken from the IDS System PP as specified in the Protection Profile, verbatim, with the following exceptions:

- OE.AUDIT PROTECTION and OE.AUDIT_SORT have been made TOE objectives: O.AUDIT_PROTECTION and O.AUDIT_SORT, since these security objectives are met by the functionality of the TOE itself.
- OE.ALARMS has been added to cover the functionality of an Email Server in the environment to send an alarm when a possible intrusion occurs.
- OE.XAUTH has been added to cover the functionality of an external authentication service that can be invoked by the TOE to support user authentication.
- OE.PROTECTCOMM has been added to state that the Operational Environment must provide secure communications between the TOE and the servers in the environment that support the security functionality of the TOE.

4.1.1 Security Objectives for the TOE

The following are the TOE security objectives:

Table 4-1: TOE Security Objectives

TOE Security Objectives		
1	O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
2	O.IDSCAN	The scanner must collect and store 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.
3	O.IDSENS	The sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
4	O.IDANLZ	The analyzer must accept data from IDS sensors or IDS scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
5	O.RESPON	The TOE must respond appropriately to analytical conclusions.
6	O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
7	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
8	O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
9	O.OFLOWS	The TOE must appropriately handle potential audit and system data storage overflows.

TOE Security Objectives		
10	O.AUDITS	The TOE must record audit records for data accesses and use of the system functions.
11	O.INTEGR	The TOE must ensure the integrity of all audit and system data.
12	O.EXPORT	When any IDS component makes its data available to another IDS component, the TOE will ensure the confidentiality of the system data.
13	O.AUDIT_PROTECTION	The TOE must provide the capability to protect audit information.
14	O.AUDIT_SORT	The TOE must provide the capability to sort the audit information.

4.1.2 Security Objectives for the Operational Environment

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

Table 4-2: Security Objectives for the Operational Environment

Security Objectives for the Operational Environment		
16	OE.INSTAL	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.
17	OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
18	OE.CREDEN	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.
19	OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.
20	OE.INTROP	The TOE is interoperable with the IT System it monitors.
21	OE.TIME	The Operational Environment will provide reliable timestamps to the TOE.
22	OE.ALARMS	The Operational Environment will provide mechanisms to notify responsible personnel of a possible problem.
23	OE.PROTECTCOMM	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.
24	OE.XAUTH *	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.
25	OE.VMXMIT	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: OE.XAUTH is only applicable when the TOE is configured to use an external LDAP or RADIUS authentication service.*

4.2 Security Objectives Rationale

This section provides the rationale for the selection of the IT security objectives, assumptions, policies and threats. In particular, it shows that the security objectives are suitable to cover all aspects of the TOE security environment.

4.2.1 Rationale for the IT Security Objectives

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the IDS System PP. Table 4-3: Security Objectives and Security Environment Mapping demonstrates the mapping between the assumptions, threats, and policies to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

Table 4-3: Security Objectives and Security Environment Mapping

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.AUDIT_SORT	O.AUDIT_PROTECTION	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.ALARMS	OE.TIME	OE.PROTECTCOMM	OE.XAUTH	OE.VMXMIT
A.ACCESS																			X					
A.DYNMIC																		X	X					
A.ASCOPE																			X					
A.PROTCT																X								
A.LOCATE																X								
A.VMXMIT																								X
A.MANAGE																		X						
A.NOEVIL															X	X	X							
A.NOTRST																X	X							
T.COMINT	X						X	X			X											X	X	
T.COMDIS	X						X	X				X										X	X	
T.LOSSOF	X						X	X			X											X	X	
T.NOHALT		X	X	X			X	X														X	X	
T.PRIVIL	X						X	X														X	X	
T.IMPCON						X	X	X							X							X	X	
T.INFLUX									X											X		X		
T.FACCNT										X														
T.SCNCFG		X																						
T.SCNMLC		X																						
T.SCNVUL		X																						
T.FALACT					X															X		X		
T.FALREC				X																				
T.FALASC				X																				
T.MISUSE			X																					
T.INADVE			X																					
T.MISACT			X																					
P.DETECT		X	X							X											X	X		
P.ANALYZ				X																				
P.MANAGE	X					X	X	X							X		X	X				X	X	
P.ACCESS	X						X	X						X						X		X	X	
P.ACCACT								X		X			X								X	X	X	
P.INTGTY											X													
P.PROTCT									X							X								

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

The OE.INTROP objective ensures the TOE has the needed access.

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

The OE.INTROP objective ensures the TOE has the proper access to the IT System. The OE.PERSON objective ensures that the TOE will be managed appropriately.

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

The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.

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

The OE.PHYCAL objective provides for the physical protection of the TOE hardware and software.

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

The OE.PHYCAL objective provides for the physical protection of the TOE.

A.VMXMIT: All packets coming in to the physical ports of the VMware hosts are transmitted unchanged to the virtual ports in the VMware environment.

The OE.VMXMIT objectives provides for secure transmission of data between the physical ports and virtual ports on the VMware host machine.

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

The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

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

The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

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

The OE.PHYCAL objective provides for physical protection of the TOE against unauthorized access. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

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

The O.IDAUTH and OE.XAUTH objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and

OE.XAUTH objectives by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified. The O.PROTCT objective addresses this threat by providing TOE self-protection. OE.PROTECTCOMM provides for secure communications between the TOE and the external authentication server.

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

The O.IDAUTH and OE.XAUTH objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.XAUTH objectives by only permitting authorized users to access TOE data. The O.EXPORT objective ensures that confidentiality of TOE data will be maintained. The O.PROTCT objective addresses this threat by providing TOE self-protection. OE.PROTECTCOMM provides for secure communications between the TOE and the external authentication server.

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

The O.IDAUTH and OE.XAUTH objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.XAUTH objectives by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection. OE.PROTECTCOMM provides for secure communications between the TOE and the external authentication server.

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

The O.IDAUTH and OE.XAUTH objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.XAUTH objectives by only permitting authorized users to access TOE data. The O.IDSCAN, O.IDSENS, and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze system data, which includes attempts to halt the TOE. OE.PROTECTCOMM provides for secure communications between the TOE and the external authentication server.

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

The O.IDAUTH and OE.XAUTH objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.XAUTH objectives by only permitting authorized users to access TOE data. The O.PROTCT objective addresses this threat by providing TOE self-protection. OE.PROTECTCOMM provides for secure communications between the TOE and the external authentication server.

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

The OE.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH and OE.XAUTH objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.XAUTH objectives by only permitting authorized users to access TOE data. OE.PROTECTCOMM provides for secure communications between the TOE and the external authentication server.

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

The O.OFLOWS objective counters this threat by requiring that the TOE must handle data storage overflows. OE.ALARMS provides Operational Environment support to send warnings when the audit and/or collected system data is about to be overwritten. OE.PROTECTCOMM provides for secure communications between the TOE and the external server that provides the warnings.

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

The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.

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

The O.IDSCAN objective counters this threat by requiring a TOE, which contains a scanner, collect and store static configuration information that might be indicative of a configuration setting change. The ST will state whether this threat must be addressed by a scanner.

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

The O.IDSCAN objective counters this threat by requiring a TOE, which contains a scanner, collect and store static configuration information that might be indicative of malicious code. The ST will state whether this threat must be addressed by a scanner.

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

The O.IDSCAN objective counters this threat by requiring a TOE, which contains a scanner, collect and store static configuration information that might be indicative of a vulnerability. The ST will state whether this threat must be addressed by a scanner.

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

The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity. The OE.ALARMS objective provides Operational Environment support mechanisms for alarms to notify responsible personnel of possible intrusions. OE.PROTECTCOMM provides for secure communications between the TOE and the external servers that provide the alarm mechanisms.

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

The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.

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

The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.

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

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE that contains a sensor, collect audit and sensor data.

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

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE that contains a sensor, collect audit and sensor data.

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

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE that contains a sensor, collect audit and sensor data.

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

The O.AUDITS, O.IDSENS, and O.IDSCAN objectives address this policy by requiring collection of audit, sensor, and scanner data. OE.TIME supports the data collection by providing reliable timestamps for the collected audit, sensor, and scanner data. OE.PROTECTCOMM provides for secure communications between the TOE and the external time server.

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

The O.IDANLZ objective requires analytical processes are applied to data collected from sensors and scanners.

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

The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrators follow all provided documentation and maintain the security policy. The O.IDAUTH and OE.XAUTH objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.XAUTH objectives by only permitting authorized users to access TOE data. The OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection.

OE.PROTECTCOMM provides for secure communications between the TOE and the external authentication server.

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

The O.IDAUTH and OE.XAUTH objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.XAUTH objectives by only permitting authorized users to access TOE data. The O.PROTCT objective addresses this policy by providing TOE self-protection. O.AUDIT_PROTECTION provides for the protection of the audit data from unauthorized deletion and modification. OE.ALARMS provides Operational Environment support to send warnings when the audit and/or collected system data is about to be overwritten. OE.PROTECTCOMM provides for secure communications between the TOE and the external server that provides the warnings and between the TOE and the external authentication server.

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

The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH and OE.XAUTH objectives support this policy by ensuring each user is uniquely identified and authenticated. OE.TIME supports the generation of audit data by providing reliable timestamps. OE.PROTECTCOMM provides for secure communications between the TOE and the external time server and between the TOE and the external authentication server. O.AUDIT_SORT supports the interpretation of the audit records by sorting the data.

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

The O.INTEGR objective ensures the protection of data from modification.

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

The O.OFLOWS objective implements this policy by requiring the TOE handle disruptions. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.

4.2.2 Rationale for the Security Objectives for the Environment

The purpose for the environmental objectives is to provide protection for the TOE that cannot be addressed through IT measures. The defined objectives provide for physical protection of the TOE, proper management of the TOE, interoperability requirements on the TOE and for external components that support the TOE objectives. Together with the IT security objectives, these environmental objectives provide a complete description of the responsibilities of TOE in meeting security needs.

5 Extended Components Definition

All of the components defined below have been taken from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007 (IDS System PP), verbatim, except for FIA_UAU_EXT.1, which has been modeled on FIA_UAU.1 from Part 2 of the CC Version 3.1 R3. The extended components are denoted by adding "_EXT" in the component name.

Table 5-1: Extended Components

Item	SFR ID	SFR Title
1	FIA_UAU_EXT.1	Timing of authentication
2	IDS_SDC_EXT.1	System Data Collection
3	IDS_ANL_EXT.1	Analyser analysis
4	IDS_RCT_EXT.1	Analyser react
5	IDS_RDR_EXT.1	Restricted Data Review
6	IDS_STG_EXT.1	Guarantee of System Data Availability
7	IDS_STG_EXT.2	Prevention of System data loss

5.1 FIA_UAU_EXT.1 Timing of authentication

5.1.1 Class FIA: Identification and authentication

See Section 12 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.1.2 Family: User authentication (FIA_UAU)

5.1.3 Family Behaviour

This family defines the types of user authentication mechanisms supported by the TSF. This family also defines the required attributes on which the user authentication mechanisms must be based.

5.1.4 Management

The following actions could be considered for the management functions in FMT:

- Management of the authentication data by an administrator
- Management of the authentication data by the user associated with this data

5.1.5 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Unsuccessful use of the authentication mechanism
- Basic: All use of the authentication mechanism

5.1.6 Definition

FIA_UAU_EXT.1 Timing of authentication

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU_EXT.1.1 The TSF shall allow ***[assignment: list of TSF mediated actions]*** on behalf of the user to be performed before the user is authenticated.

FIA_UAU_EXT.1.2 The TSF shall require each user to be successfully authenticated either by the TSF or by an authentication service in the Operational Environment invoked by the TSF before allowing any other TSF-mediated actions on behalf of that user.

5.1.7 Rationale

FIA_UAU_EXT.1 is modeled closely on the standard component FIA_UAU.1: Timing of authentication. FIA_UAU_EXT.1 needed to be defined as an extended component because the functionality of the standard component was extended by adding the text *"either by the TSF or by an authentication service in the Operational Environment invoked by the TSF".*

5.2 IDS_SDC_EXT.1 System Data Collection

5.2.1 Class IDS: Intrusion Detection System

5.2.2 Family: System Data Collection (IDS_SDC)

5.2.3 Family Behavior

This family defines the requirements for the TSF to be able to collect information from targeted IT System resources.

5.2.4 Management

The following actions could be considered for the management functions in FMT:

- the management (addition, removal, or modification) of specific IDS information that will be obtained from targeted IT System resource(s);
- the management (addition, removal, or modification) of specific targeted IT System resources.

5.2.5 Audit

There are no auditable events foreseen.

5.2.6 Definition

IDS_SDC_EXT.1 System Data Collection

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

IDS_SDC_EXT.1.1 The TSF shall be able to collect the following information from the targeted IT System resource(s): ***[selection: Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction, detected malicious code, access control configuration, service configuration, authentication configuration, accountability policy configuration, detected known vulnerabilities];*** and ***[assignment: other specifically defined events].***

IDS_SDC_EXT.1.2 At a minimum, the TSF shall collect and record the following information

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) The additional information specified in the Details column of Table 5-2: System Events.

Table 5-2: System Events

Component	Event	Details
IDS_SDC.1	Start-up and shutdown	none
IDS_SDC.1	Identification and authentication events	User identity, location, source address, destination address
IDS_SDC.1	Data accesses	Object IDS, requested access, source address, destination address
IDS_SDC.1	Service Requests	Specific service, source address, destination address
IDS_SDC.1	Network traffic	Protocol, source address, destination address
IDS_SDC.1	Security configuration changes	Source address, destination address
IDS_SDC.1	Data introduction	Object IDS, location of object, source address, destination address

Component	Event	Details
IDS_SDC.1	Start-up and shutdown of audit functions	none
IDS_SDC.1	Detected malicious code	Location, identification of code
IDS_SDC.1	Access control configuration	Location, access settings
IDS_SDC.1	Service configuration	Service identification (name or port), interface, protocols
IDS_SDC.1	Authentication configuration	Account names for cracked, passwords, account policy, parameters
IDS_SDC.1	Accountability policy configuration	Accountability policy configuration parameters
IDS_SDC.1	Detected known vulnerabilities	Identification of the known, vulnerability

5.2.7 Rationale

IDS_SDC_EXT.1 is taken from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007. IDS_SDC_EXT.1 had to be defined because the Common Criteria v3.1 Part 2 does not provide a Security Functional Requirement for Intrusion Detection functionality, specifically System data collection.

5.3 IDS_ANL_EXT.1 Analyser analysis

5.3.1 Class IDS: Intrusion Detection System

5.3.2 Family: Analyser analysis (IDS_ANL)

5.3.3 Family Behavior

This family defines the requirements for the TSF to be able to analyze the IDS data that has been gathered from targeted IT System resources.

5.3.4 Management

The following actions could be considered for the management functions in FMT:

- the management (addition, removal, or modification) of specific IDS information that will be obtained from targeted IT System resource(s).

5.3.5 Audit

There are no auditable events foreseen.

5.3.6 Definition

IDS_ANL_EXT.1 Analyser analysis

Hierarchical to: No other components

Dependencies: IDS_SDC_EXT.1

IDS_ANL_EXT.1.1 The TSF shall perform the following analysis function(s) on all IDS data received:

a) ***[selection: statistical, signature, integrity]; and***
b) ***[assignment: other analytical functions].***

IDS_ANL_EXT.1.2 The TSF shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and
b) ***[assignment: other security relevant information]***

5.3.7 Rationale

IDS_ANL_EXT.1 is taken from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007. IDS_ANL_EXT.1 had to be defined because the Common Criteria v3.1 Part 2 does not provide a Security Functional Requirement for Intrusion Detection functionality, specifically the analysis function.

5.4 IDS_RCT_EXT.1 Analyser react

5.4.1 Class IDS: Intrusion Detection System

5.4.2 Family: Analyser react (IDS_RCT)

5.4.3 Family Behavior

This family defines the requirements for the TSF to be able to send an alarm and react when an intrusion is detected.

5.4.4 Management

The following actions could be considered for the management functions in FMT:

- the management (addition, removal, or modification) of actions

5.4.5 Audit

There are no auditable events foreseen.

5.4.6 Definition

IDS_RCT_EXT.1 Analyser react

Hierarchical to: No other components

Dependencies: IDS_SDC_EXT.1

IDS_RCT_EXT.1.1 The TSF shall send an alarm to ***[assignment: alarm destination]*** and take ***[assignment: appropriate actions]*** when an intrusion is detected.

5.4.7 Rationale

IDS_RCT_EXT.1 is taken from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007. IDS_RCT_EXT.1 had to be defined because the Common Criteria v3.1 Part 2 does not provide a Security Functional Requirement for Intrusion Detection functionality, specifically the alarm and reaction function.

5.5 IDS_RDR_EXT.1 Restricted Data Review

5.5.1 Class IDS: Intrusion Detection System

5.5.2 Family: Security data review (IDS_RDR)

5.5.3 Family Behavior

This family defines the requirements for data tools that should be available to authorized users to assist in the review of system data.

5.5.4 Management

There are no management activities foreseen.

5.5.5 Audit

There are no auditable events foreseen.

5.5.6 Definition

IDS_RDR_EXT.1 Restricted Data Review

Hierarchical to: No other components

Dependencies: IDS_SDC_EXT.1

IDS_RDR_EXT.1.1 The TSF shall provide ***[assignment: authorised users]*** with the capability to read ***[assignment: list of system data]*** from the system data.

IDS_RDR_EXT.1.2 The TSF shall provide the system data in a manner suitable for the user to interpret the information.

IDS_RDR_EXT.1.3 The TSF shall prohibit all users read access to the system data, except those users that have been granted explicit read-access.

5.5.7 Rationale

IDS_RDR_EXT.1 is taken from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007. IDS_RDR_EXT.1 had to be defined because the Common Criteria v3.1 Part 2 does not provide a Security Functional Requirement for Intrusion Detection functionality, specifically the restricted data review function.

5.6 IDS_STG_EXT.1 Guarantee of System Data Availability

5.6.1 Class IDS: Intrusion Detection System

5.6.2 Family: System data storage (IDS_STG)

5.6.3 Family Behavior

This family defines the requirements for the TSF to be able to secure system data.

5.6.4 Management

There are no management activities foreseen.

5.6.5 Audit

There are no auditable events foreseen.

5.6.6 Definition

IDS_STG_EXT.1 Guarantee of System Data Availability

Hierarchical to: No other components

Dependencies: IDS_SDC_EXT.1

IDS_STG_EXT.1.1 The TSF shall protect the stored system data from unauthorized deletion.

IDS_STG_EXT.1.2 The TSF shall protect the stored system data from modification.

IDS_STG_EXT.1.3 The TSF shall ensure that ***[assignment: metric for saving system data]*** system data will be maintained when the following condition occurs: ***[selection: system data storage exhaustion, failure, attack].***

5.6.7 Rationale

IDS_STG_EXT.1 is taken from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007. IDS_STG_EXT.1 had to be defined because the Common Criteria v3.1 Part 2 does not provide a Security Functional Requirement for Intrusion Detection functionality, specifically the guarantee of System data availability.

5.7 IDS_STG_EXT.2 Prevention of System data loss

5.7.1 Class IDS: Intrusion Detection System

5.7.2 Family: System data storage (IDS_STG)

5.7.3 Family Behavior

This family defines the requirements for the TSF to be able to secure system data.

5.7.4 Management

The following actions could be considered for the management functions in FMT:

- the maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure

5.7.5 Audit

There are no auditable events foreseen.

5.7.6 Definition

IDS_STG_EXT.2 Prevention of System data loss (EXT)

Hierarchical to: No other components

Dependencies: IDS_SDC_EXT.1

IDS_STG_EXT.2.1 The TSF shall ***[selection: 'ignore system data', 'prevent system data, except those taken by the authorised user with special rights', 'overwrite the oldest stored system data ']*** and send an alarm if the storage capacity has been reached.

5.7.7 Rationale

IDS_STG_EXT.2 is taken from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007. IDS_STG_EXT.2 had to be defined because the Common Criteria v3.1 Part 2 does not provide a Security Functional Requirement for Intrusion Detection functionality, specifically the prevention of system data loss

6 Security Requirements

6.1 Security Functional Requirements

Conventions
The following conventions have been applied in this document:

- **Security Functional Requirements –** Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - **Iteration**: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FDP_ACC.1(a) and FDP_ACC.1(b) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
  - **Assignment**: allows the specification of an identified parameter. Assignments are indicated using bold italics and are surrounded by brackets (e.g., ***[assignment]).***
  - **Selection**: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., ***[selection]***).
  - **Refinement**: are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in <u>***italicized bold and underlined text***</u>.

Note: Operations already performed in the corresponding Protection Profile are not identified in this Security Target.

- **Application notes** provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*

- **Explicitly stated Security Functional Requirements** (i.e., those not found in Part 2 of the CC) are identified "_EXT" in the component name.

The TOE security functional requirements are listed in Table 6-1. All SFRs are based on requirements defined in Part 2 of the Common Criteria or the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007.

Table 6-1: TOE Security Functional Components

No.	Component	Component Name
1	FAU_GEN.1	Audit data generation
2	FAU_SAR.1	Audit review
3	FAU_SAR.2	Restricted audit review
4	FAU_SAR.3	Selectable audit review

No.	Component	Component Name
5	FAU_SEL.1	Selective audit
6	FAU_STG.2	Guarantees of data availability
7	FAU_STG.4	Prevention of audit data loss
8	FIA_ATD.1	User attribute definition
9	FIA_UAU_EXT.1	Timing of authentication
10	FIA_UID.1	Timing of identification
11	FMT_MOF.1	Management of security functions behavior
12	FMT_MTD.1	Management of TSF data
13	FMT_SMF.1	Specification of Management Functions
14	FMT_SMR.1	Security roles
15	FPT_ITT.1	Basic internal TSF data transfer protection
16	FTA_TAB.1	Default TOE access banners
17	IDS_SDC_EXT.1	System Data Collection
18	IDS_ANL_EXT.1	Analyzer analysis
19	IDS_RCT_EXT.1	Analyzer react
20	IDS_RDR_EXT.1	Restricted Data Review
21	IDS_STG_EXT.1	Guarantee of System Data Availability
22	IDS_STG_EXT.2	Prevention of System data loss

6.1.1 Class FAU: Security Audit

6.1.1.1 FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate 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

Application Note: The IDS_SDC and IDS_ANL requirements address the recording of results from IDS scanning, sensing, and analyzing tasks (i.e., system data).

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, the additional information specified in the Details column of Table 6-2: Auditable Events.

Table 6-2: Auditable Events

Component	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to System	
FAU_GEN.1	Access to the TOE and System data	Object ID, Requested access
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FAU_STG.2	None	
FAU_STG.4	Actions taken due to the audit storage failure	
FIA_ATD.1	None	
FIA_UAU_EXT.1	All use of the authentication mechanism	User identity, location
FIA_UID.1	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMF.1	Use of the management functions	User identity
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity
FPT_ITT.1	None	
FTA_TAB.1	None	
IDS_SDC_EXT.1	None	
IDS_ANL_EXT.1	None	
IDS_RCT_EXT.1	None	
IDS_RDR_EXT.1	None	
IDS_STG_EXT.1	None	
IDS_STG_EXT.1	None	

6.1.1.2 FAU_SAR.1 Audit Review

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide ***[users with the Administrator Role, Custom User Role with “Analysis & Reporting -> Searches -> Audit Log” Permission, Custom User Role with “Operations -> Monitoring -> Audit” Permission]*** with the capability to read ***[all audit information]*** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.3 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users who have been granted explicit read-access.

6.1.1.4 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform sorting of audit data based on date and time, subject identity, type of event, and success or failure of related event.

Application Note: Type of event is contained in the Subsystem field of the audit records. Success or Failure of the event is part of the Message field.

6.1.1.5 FAU_SEL.1 Selective audit

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FMT_MTD.1 Management of TSF data

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) event type
b) ***[IP address, message, subsystem, and username]***

6.1.1.6 FAU_STG.2 Guarantees of audit data availability

Hierarchical to: FAU_STG.1

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to detect unauthorized modifications to the audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that ***[the most recent, limited by available audit storage, at least one]*** audit records will be maintained when the following conditions occur: ***[audit storage exhaustion].***

6.1.1.7 FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall ***[overwrite the oldest stored audit records]*** and send an alarm if the audit trail storage is full.

6.1.2 Class FIA: Identification and Authentication

6.1.2.1 FIA_ATD.1 User attribute definition

Hierarchical to: No other components

Dependencies: No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) User identity; (user name)
b) Authentication data; (password)
c) Authorizations (user roles); and
d) ***[***

1) Restrict Deletion Rights

2) Use External Authentication Method

3) Force Password Reset on Login

4) Password Strength Check

5) Max Number of Failed Logins

6) Password Expiration

7) Days Until Expiration Warning

8) Command-Line Interface Access

].

6.1.2.2 FIA_UAU_EXT.1 Timing of authentication

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU_EXT.1.1 The TSF shall allow ***[entry of identification and authentication data]*** on behalf of the user to be performed before the user is authenticated.

FIA_UAU_EXT.1.2 The TSF shall require each user to be successfully authenticated either by the TSF or by an authentication service in the Operational Environment invoked by the TSF before allowing any other TSF-mediated actions on behalf of that user

Application Note: Use of an external authentication server is allowed only for TOE configurations that include a Defense Center or Virtual Defense Center.

6.1.2.3 FIA_UID.1 Timing of identification

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UID.1.1 The TSF shall allow ***[entry of identification and authentication data]*** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.3 Class FMT: Security Management

6.1.3.1 FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MOF.1.1 The TSF shall restrict the ability to ***[modify the behavior]*** of the functions ***[See column 1 of Table 6-3]*** to ***[See column 2 of Table 6-3].***

Table 6-3: Management of Security Functions Behavior

Function	User Role
System Data Collection (Create and Edit IPS Rules)	Administrator Role
	Policy & Response Administrator Role
	Custom User Role with “Policy & Response -> IPS -> Intrusion Policy” Permission
Analysis and Reaction (Create and Edit Detection Engines)	Administrator Role
	Custom User Role with “Operations -> Configuration -> Detection Engines” Permission
Audit Data Generation (Create and Modify Audit Suppression Lists)	SFLinux “*admin”* User Role *

* This is not a security role maintained by the TOE; it is maintained by the TOE component’s OS and is equivalent to the system administrator of the OS.

6.1.3.2 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to ***[operations as specified in Table 6-4]*** the ***[TSF data as specified in Table 6-4]*** to ***[user security roles and access permissions as specified in Table 6-4].***

Table 6-4: Management of TSF data

Custom User Role Access Permission	Predefined User Role *	Platform **	Operations	TSF Data
Analysis & Reporting -> Event Summary -> Intrusion Event Statistics	ADMIN IPS IPS-RO	DC SENS	View	Intrusion Event Statistics
Analysis & Reporting -> Event Summary -> Event Graphs	ADMIN IPS IPS-RO	DC SENS	Generate	Intrusion Event Graph
Analysis & Reporting -> IPS -> Intrusion Events	ADMIN IPS IPS-RO	DC SENS	View, mark as reviewed	Intrusion Events
			View, edit	Intrusion Event Rule Actions
			Set	Intrusion Event Rule Threshold Options
			Set	Intrusion Event Rule Suppression Options
Analysis & Reporting -> IPS -> Reviewed Events	ADMIN IPS IPS-RO	DC SENS	View, mark as un-reviewed	Reviewed Intrusion Events

Custom User Role Access Permission	Predefined User Role *	Platform **	Operations	TSF Data
Analysis & Reporting -> IPS -> Clipboard	ADMIN IPS IPS-RO	DC SENS	Generate	Intrusion Event Report
Analysis & Reporting -> IPS -> Incidents	ADMIN IPS IPS-RO	DC SENS	Create, edit	Incident
			Generate	Incident Report
			Create	Incident Type
Analysis & Reporting -> Report Profiles	ADMIN IPS IPS-RO	DC SENS	Generate, view, download, run remote	Report
	ADMIN IPS	DC SENS	Delete	Report
Analysis & Reporting -> Reporting	ADMIN IPS IPS-RO	DC SENS	Create, edit	Report Profile
	ADMIN IPS	DC SENS	Delete	Report Profile
Analysis & Reporting -> Searches -> Audit Log	ADMIN	DC SENS	Search	Audit Records
Analysis & Reporting -> Searches -> Intrusion Events	ADMIN IPS IPS-RO	DC SENS	Search	Intrusion Events
Analysis & Reporting -> Searches -> Health Events	ADMIN IPS	DC SENS	Search	Health Events
Analysis & Reporting -> Custom Workflow	ADMIN IPS IPS-RO	DC SENS	Create, edit, export	Custom Workflow
	ADMIN IPS	DC SENS	Delete	Custom Workflow
Policy & Response -> IPS -> Intrusion Policy	ADMIN P&R	DC SENS	View, create, edit, delete, commit, apply, import, export	Intrusion Policy
			Generate	Intrusion Policy Report
			Compare	Intrusion Policies
			Create, edit, delete	Intrusion Policy Variables
			View, sort, filter, create, edit, set alert for, set state	Intrusion Policy Rule
			Set, edit	Intrusion Policy Rule Filter
			View, create, edit, delete	Intrusion Policy Thresholds
			View, create, edit, delete	Intrusion Event Suppression
			Add, edit, delete,	Alerts

Custom User Role Access Permission	Predefined User Role *	Platform **	Operations	TSF Data
			Configure	Intrusion Policy Layers
			Configure	Preprocessors & Decoders
			Configure	Rate Based Attack Prevention
			Configure	Sensitive Data Attack Prevention
			Configure	Event Queues
			Configure	Performance Statistics Parameters
Policy & Response -> IPS -> Rule Editor	ADMIN P&R	DC SENS	Create, edit, search, delete, import	Intrusion Policy Rule
Policy & Response -> PEP -> Policy Management	ADMIN P&R	DC	Create, edit, apply, export, compare, delete	PEP Policy
			Create, edit	Fast Path Rules
			Create, edit	PEP Rules
Operations -> Configuration -> Detection Engines	ADMIN	DC SENS	Create, edit, delete	Detection Engine
		DC	Create, edit, delete	Detection Engine Group
		DC SENS	Create, edit, delete, reset	Detection Engine Variables
		DC SENS	List	Interface Sets
		DC	View	PEP Policy
		DC SENS	Generate	Intrusion Report for Detection Engine
Operations -> Configuration -> Interface Sets	ADMIN	DC SENS	Create, edit, delete, list	Interface Set
		DC	Create, edit, delete	Interface Set Group
Operations -> Configuration -> Login Authentication	ADMIN	DC	Create, edit, delete	Authentication Objects
Operations -> Sensors	ADMIN	DC	Add to, delete from, Defense Center	Sensor
			Reset communications with, disable communications with Defense Center	Sensor
			Stop, restart	Sensor
			Set time	Sensor
			Create, edit, delete	Sensor Group
			Edit, view	Sensor System Settings

Custom User Role Access Permission	Predefined User Role *	Platform **	Operations	TSF Data
Operations -> User Management	ADMIN	DC SENS	View, add, edit, delete	User Accounts
			Configure, export, import	User Roles
			Modify	User Privileges
			Modify	User Passwords
			Configure	User Role Escalation
			Configure	CLI Access
Operations -> System Settings	ADMIN	DC SENS	View, modify	Appliance information
			Manage, verify	Appliance licenses
			View, request, upload	HTTPS Server Certificates
			Configure	Network Settings
			Configure	Network Interface Settings
			Shutdown, restart	System
			Configure	Remote Management Settings
			Configure	Backup and Report Storage
			Manually set	Time Settings
			Enable	Change Reconciliation
Operations -> System Policy	ADMIN	DC SENS	Create, edit, apply, delete, export	System Policy
			Configure	Appliance Access List
			Configure	Audit Log Settings
			Configure	CLI Access Settings
			Configure	Database Event Limits
			Configure	DNS Cache Properties
			Configure	Email Settings
			Create, edit, delete	Intrusion Policy Preferences
			Create, edit, delete	Login Banner
			Configure	Time Settings
		DC	Compare	System Policies
			Configure	Authentication Profile
Operations -> Monitoring -> Statistics	ADMIN MAINT	DC SENS	View	Host Statistics
			View	System Status
			View	Disk Space Usage
			View	System Process Status
Operations -> Monitoring -> Performance -> IPS	ADMIN MAINT	DC SENS	View	IPS Performance Statistics
			Generate	IPS Performance Statistics Graphs

Custom User Role Access Permission	Predefined User Role *	Platform **	Operations	TSF Data
Operations -> Monitoring -> Audit	ADMIN	DC SENS	View, sort, search	Audit Records
Operations -> Monitoring -> Task Status	ADMIN MAINT P&R	DC SENS	View, manage	Task Queue
Operations -> Monitoring -> Syslog	ADMIN MAINT	DC SENS	View, filter	Syslog
Operations -> Monitoring -> Health	ADMIN MAINT IPS IPS-RO	DC	Create, edit, apply, unapply, compare, import, export	Health Policy
			Configure	Health Monitor Alerts
			View	Health Status (Health Events, Troubleshooting Files, Alert Graphs)
			Run	Health Modules
	ADMIN MAINT IPS	DC	Delete	Health Policy
			Blacklist	Health Policy, Health Policy Module, Appliances
			Run	Health Modules
Operations -> Tools -> Scheduling	ADMIN MAINT	DC SENS	Add, edit, delete, view	Re-occurring Task
Operations -> Tools -> Backup/Restore	ADMIN MAINT	DC SENS	Create, download, upload, restore from	Backup File
			Create, edit delete	Backup Profile
Operations -> Tools -> Import/Export	ADMIN	DC SENS	Import, export	Custom User Role
			Import, export	Health Policy
			Import, export	Intrusion Policy
			Import, export	PEP Policy
			Import, export	System Policy
N/A	ADMIN	7000/8000	Search, view	Audit Log
			View	Detection Engines
			View	Interface Sets
			Create, edit, delete	Sensor User Accounts
			View, modify	Appliance Information
			View, request, upload	HTTPS Server Certificates
			Configure	Network Settings
			Configure	Network Interface Settings
			Configure	Remote Management Settings
			Configure	Change Reconciliation

Custom User Role Access Permission	Predefined User Role *	Platform **	Operations	TSF Data
			View	Host Statistics
			View, manage	Task Queue
			View, search	Syslog
			Create, download, restore from	Backup File
			Create, edit, delete	Backup Profile
			View, generate graphs	IPS Performance Statistics
			Control	Appliance Processes
All	All	All	Change	Own Password
			Escalate	Own Role (if so configured)
N/A	SFLinux *admin* ***	DC SENS	Create, modify	Audit Suppression Lists

*	ADMIN – Administrator Role
MAINT – Maintenance Role
P&R- Policy & Response Administrator Role
IPS – Intrusion Event Analyst Role
IPS-RO – Intrusion Event Analyst (Read Only) Role

**	DC – (Virtual and Appliance-Based) Defense Center WebUI
SENS – Stand-alone Sensor WebUI
7000/8000 – 7000 Series and 8000 Series Sensor Limited WebUI

***	This is not a security role maintained by the TOE; it is maintained by the (virtual) appliance OS and is equivalent to the system administrator of the OS.

6.1.3.3 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components

Dependencies:	No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: ***[***

1) ***View Intrusion Event Statistics***
2) ***Generate and view Intrusion Event Graphs***
3) ***View Intrusion Events***
4) ***Mark Intrusion Events as Reviewed***
5) ***View and Edit Intrusion Event Rule Actions***
6) ***Set Intrusion Event Rule Threshold Options***
7) ***Set Intrusion Event Rule Suppression Options***

8) View Reviewed Intrusion Events

9) Mark Reviewed Intrusion Events as Un-reviewed

10) Generate Intrusion Event Reports

11) Generate Incident Reports

12) Create and edit Incidents

13) Create Incident Types

14) Generate, view, download, delete and run remote Reports

15) Create, edit, and delete Report Profiles

16) View and Search Audit Records,

17) View and Search Intrusion Events,

18) View and Search Health Events

19) Create, edit, export, delete custom workflow

20) View, create, edit, delete, commit, apply, import, export, and compare Intrusion Policies

21) Generate Intrusion Policy Report

22) Create, edit, and delete Intrusion Policy Variables

23) View, sort, filter, create, edit, set alert for, and set state of Intrusion Policy Rules

24) Set and edit Intrusion Policy Rule Filter

25) View, create, edit, and delete Intrusion Policy Thresholds

26) View, create edit and delete Intrusion Event Suppression

27) Add, edit, and delete Alerts

28) Configure Intrusion Policy Layers

29) Configure Preprocessors & Decoders

30) Configure Rate Based Attack Prevention

31) Configure Sensitive Data Attack Prevention

32) Configure Event Queues

33) Configure Performance Statistics Parameters

34) Create, edit, search, delete and import Intrusion Policy Rules

35) View, create, edit, apply, , export, compare, and delete PEP Policies

36) Create and edit Fast Path Rules

37) Create and edit PEP Rules

38) View create, edit, and delete Detection Engines

39) View, create, edit, and delete Detection Engine Groups

40) Create, edit, delete, and reset Detection Engine Variables

41) Create, edit, view and delete Interface Sets

42) Create, edit and delete Interface Set Groups

43) Create, edit, and delete Authentication Objects

44) Add Sensor to Defense Center, Delete Sensor from Defense Center

45) Reset Sensor communications with Defense Center, disable Sensor communications with Defense Center,

46) Stop and Restart Sensors

47) Set time on Sensors

48) Create, edit, and delete Sensor Groups

49) Edit and view Sensor System Settings

50) View, add, edit, and delete User Accounts

51) Configure, export, and import User Roles

52) Modify User Privileges

53) Modify User Passwords

54) Configure User Role Escalation

55) Configure CLI Access

56) View and modify Appliance Information

57) Manage and verify Appliance Licenses

58) View, request, and upload HTTPS Server Certificates

59) Configure Network Settings

60) Configure Network Interface Settings

61) Shutdown and restart the Sourcefire 3D System

62) Configure Remote Management Settings

63) Configure backup and report storage

64) Manually set Time Settings

65) Enable Change Reconciliation

66) Create, edit, apply, delete, import, and compare System Policies

67) Configure Appliance Access Lists

68) Configure CLI Access Settings

69) Configure Audit Log Settings

70) Configure Database Event Limits

71) Configure DNS Cache Properties

72) Configure Email Settings

73) Create, edit, and delete Intrusion Policy Preferences

74) Create, edit, and delete Login Banners

75) Configure Time Settings

76) Configure Authentication Profiles

77) ***View Host Statistics, System Status, Disk Space Usage and System Process Status***

78) ***View IPS Performance Statistics***

79) ***Generate IPS Performance Statistics Graphs***

80) ***View, sort, and search Audit Records***

81) ***View and manage Task Queues***

82) ***View and Filter Syslog***

83) ***Create, edit, apply, unapply, delete, and compare Health Policies***

84) ***Configure Health Monitor Alerts***

85) ***View Health Status (Health Events, Troubleshooting files, Alert Graphs)***

86) ***Run Health Modules***

87) ***Blacklist Health Policy, Health Policy Module, Appliances***

88) ***Add, edit, delete, and view Re-occurring Tasks***

89) ***Create, download, upload and restore from Backup Files***

90) ***Create, edit and delete Backup Profile***

91) ***Import and export Custom User Role***

92) ***Import and export Health Policy***

93) ***Import and export Intrusion Policy***

94) ***Import and export PEP Policy***

95) ***Import and export System Policy***

96) ***Change User's own Password***

97) ***Escalate User's own Role***

98) ***Create and Modify Audit Suppression Lists***

].

Application Note: FMT_SMF.1 is not included in the IDS System PP; however, it needed to be included to satisfy the dependencies of the SFRs FMT_MOF.1 and FMT_MTD.1.

6.1.3.4 FMT_SMR.1 Security Roles

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles ***[***

1) ***Administrator***
2) ***Maintenance***
3) ***Policy & Response Administrator***

4) ***Intrusion Event Analyst***
5) ***Intrusion Event Analyst (Read Only)***
6) ***Custom User Role(s)***

].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.4 Class FPT: Protection of the TSF

6.1.4.1 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components

Dependencies: No dependencies

FPT_ITT.1.1 **Refinement:** The TSF shall protect TSF data from ***[disclosure, modification]*** when it is transmitted between ***<u>the Defense Center or Virtual Defense Center and the 3D Sensor(s) with IPS or Virtual 3D Sensor(s) with IPS by using a secure, SSL-encrypted TCP tunnel that uses OpenSSL Version 0.9.8g and Cipher AES256-SHA (strength:256 bits).</u>***

Application Note: FPT_ITT.1 replaces the IDS System PP SFRs: FIA_AFL.1, FPT_ITA.1, FPT_ITC.1, and FPT_ITI.2, through the precedence of PD-0097.

6.1.5 Class FTA: TOE Access

6.1.5.1 FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

6.1.6 Class IDS: IDS Component Requirements

6.1.6.1 IDS_SDC_EXT.1 System Data Collection

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

IDS_SDC_EXT.1.1 The TSF shall be able to collect the following information from the targeted IT System resource(s):

a) ***[network traffic]; and***

b) ***[no other events]***

IDS_SDC_EXT.1.2 At a minimum, the TSF shall collect and record the following information

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) The additional information specified in the Details column of Table 6-5: System Events.

Table 6-5: System Events

Component	Event	Details
IDS_SDC_EXT.1	Network traffic	Protocol
		Source address
		Destination address

6.1.6.2 IDS_ANL_EXT.1 Analyser analysis

Hierarchical to: No other components

Dependencies: IDS_SDC_EXT.1 System Data Collection

IDS_ANL_EXT.1.1 The TSF shall perform the following analysis function(s) on all IDS data received:

a) ***[statistical, signature]; and***

b) ***[***

1) DCE/RPC Configuration

2) DNS Configuration

3) FTP & Telnet Configuration

4) HTTP Inspection

5) Sun RPC Configuration

6) SMTP Configuration

7) SSH Configuration

8) SSL Configuration

9) Checksum Verification

10) Inline Normalization

11) ***IP Defragmentation***

12) ***Packet Decoding***

13) ***TCP Stream Configuration***

14) ***UDP Stream Configuration***

15) ***Back Orifice Detection***

16) ***Portscan Detection***

17) ***Rate-Based Attack Prevention***

18) ***Sensitive Data***

19) ***Session Initiation Protocol (SIP)***

20) ***POP3 Data***

21) ***IMAP Data***

22) ***SCADA (Distributed Network Protocol v3.0 (DNP3) and the Modbus protocol)***

23) ***GPPRS Tunneling Protocol (GTP)***

].

IDS_ANL_EXT.1.2 The TSF shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and
b) ***[The packets analyzed to determine the result]***

6.1.6.3 IDS_RCT_EXT.1 Analyser react (EXT)

Hierarchical to: No other components

Dependencies: IDS_SDC_EXT.1 System Data Collection

IDS_RCT_EXT.1.1 The TSF shall send an alarm to ***[***

- ***A defined email administrative address, and/or***
- ***Syslog facilities, and/or***
- ***An SNMP Trap Server***

] and take ***[***

- ***no actions for passive deployment of 3D Sensors with IPS***
- ***no actions if the automatic application bypass feature is on and the configured bypass threshold time has been exceeded***

- ***no actions if the PEP feature has been configured to drop or fastpath network traffic***
- ***actions to Drop, Replace packets containing suspicious network traffic according to configured rules for inline deployment of 3D Sensors with IPS***

] when an intrusion is detected.

6.1.6.4 IDS_RDR_EXT.1 Restricted Data Review (EXT)

Hierarchical to: No other components

Dependencies: IDS_SDC_EXT.1 System Data Collection

IDS_RDR_EXT.1.1 The TSF shall provide ***[users with the Administrator Role, Intrusion Event Analyst Role, Custom User Roles with "Analysis & Reporting -> IPS -> Intrusion Events" Permission]*** with the capability to read ***[all captured IDS data]*** from the system data.

IDS_RDR_EXT.1.2 The TSF shall provide the system data in a manner suitable for the user to interpret the information.

IDS_RDR_EXT.1.3 The TSF shall prohibit all users read access to the system data, except those users that have been granted explicit read-access.

6.1.6.5 IDS_STG_EXT.1 Guarantee of System Data Availability

Hierarchical to: No other components

Dependencies: No dependencies

IDS_STG_EXT.1.1 The TSF shall protect the stored system data from unauthorized deletion.

IDS_STG_EXT.1.2 The TSF shall protect the stored system data from modification.

IDS_STG_EXT.1.3 The TSF shall ensure that ***[the most recent, limited by available system data storage, at least one]*** system data will be maintained when the following condition occurs: ***[system data storage exhaustion]***.

6.1.6.6 IDS_STG_EXT.2 Prevention of System data loss

Hierarchical to: No other components

Dependencies: IDS_SDC_EXT.1 System Data Collection

IDS_STG_EXT.2.1 The TSF shall ***[overwrite the oldest stored system data]*** and send an alarm if the storage capacity has been reached.

6.2 Security Assurance Requirements for the TOE

This Section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. None of the assurance components is refined. Table 6-6 summarizes the components.

Table 6-6: EAL2+ Assurance Components

Assurance Class	Assurance Components	
Development	ADV_ARC.1	Architectural Design with Domain Separation and non-bypassability
	ADV_FSP.2	Security enforcing Functional Specification
	ADV_TDS.1	Basic Design
Guidance documents	AGD_OPE.1	Operational User guidance
	AGD_PRE.1	Preparative User guidance
Life cycle support	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
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.2	Vulnerability Analysis

6.2.1 Class ADV: Development

6.2.1.1 ADV_ARC.1 Security architecture description

Dependencies: ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1 4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements:

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.1.2 ADV_FSP.2 Security-enforcing functional specification

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content elements:

ADV_FSP.2.1C The functional specification shall completely represent the TSF.

ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For SFR-enforcing TSFIs, the functional specification shall describe direct error messages resulting from processing associated with the SFR enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

6.2.1.3 ADV_TDS.1 Basic design

Dependencies: ADV_FSP.2 Security-enforcing functional specification

Developer action elements:

ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C The design shall describe the behavior of each SFR-supporting or SFR-non interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C The design shall summarize the SFR-enforcing behavior of the SFR enforcing subsystems.

ADV_TDS.1.5C The design shall provide a description of the interactions among SFR enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C The mapping shall demonstrate that all behavior described in the TOE design is mapped to the TSFIs that invoke it.

Evaluator action elements:

ADV_TDS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.1.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

6.2.2 Class AGD: Guidance documents

6.2.2.1 AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

AGD_OPE.11D The developer shall provide operational user guidance.

Content and presentation elements:

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.2.2 AGD_PRE.1 Preparative procedures

Dependencies: No dependencies

Developer action elements:

AGD_PRE.11D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

6.2.3 Class ALC: Life-cycle support

6.2.3.1 ALC_CMC.2 Use of a CM system

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMC.21D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.2.2D The developer shall provide the CM documentation.

ALC_CMC.2.3D The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.2.1C The TOE shall be labeled with its unique reference.

ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.23C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ALC_CMC.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.3.2 ALC_CMS.2 Parts of the TOE CM coverage

Dependencies: No dependencies

Developer action elements:

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

ALC_CMS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.3.3 ALC_DEL.1 Delivery procedures

Dependencies: No dependencies

Developer action elements:

ALC_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements:

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.3.4 ALC_FLR.2 Flaw reporting procedures

Dependencies: No dependencies

Developer action elements:

ALC_FLR.2.1D The developer shall document flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users.

Content and presentation elements:

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE users' reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

ALC_FLR.2.7C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.2.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

Evaluator action elements:

ALC_FLR.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.4 Class ATE: Tests

6.2.4.1 ATE_COV.1 Evidence of coverage

Dependencies: ADV_FSP.2 Security-enforcing functional specification
ATE_FUN.1 Functional testing

Developer action elements:
ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation elements:
ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

Evaluator action elements:
ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.4.2 ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:
ATE_FUN.1.1D The developer shall test the TSF and document the results.
ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:
ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.
ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements:
ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.4.3 ATE_IND.2 Independent testing - sample

Dependencies: ADV_FSP.2 Security-enforcing functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures
ATE_COV.1 Evidence of coverage
ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

6.2.5 Class AVA: Vulnerability assessment

6.2.5.1 AVA_VAN.2 Vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description
ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.2.1C The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6.3 Security Requirements Rationale

6.3.1 Dependencies Satisfied

Table 6-7 shows the dependencies between the functional requirements including the extended components defined in Section 5. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference.

Table 6-7: TOE Dependencies Satisfied

Item	SFR ID	SFR Title	Dependencies	Item Reference
1	FAU_GEN.1	Audit data generation	FPT_STM.1	Environment *
2	FAU_SAR.1	Audit review	FAU_GEN.1	1
3	FAU_SAR.2	Restricted audit review	FAU_SAR.1	2
4	FAU_SAR.3	Selectable audit review	FAU_SAR.1	2
5	FAU_SEL.1	Selective audit	FAU_GEN.1	1
			FMT_MTD.1	12
6	FAU_STG.2	Guarantees of data availability	FAU_GEN.1	1
7	FAU_STG.4	Prevention of audit data loss	FAU_STG.1	6 (H)
8	FIA_UAU_EXT.1	Timing of authentication	FIA_UID.1	10
9	FIA_ATD.1	User attribute definition	None	None
10	FIA_UID.1	Timing of identification	None	None
11	FMT_MOF.1	Management of security functions behavior	FMT_SMR.1	14
			FMT_SMF.1	13
12	FMT_MTD.1	Management of TSF data	FMT_SMF.1	13
13	FMT_SMF.1	Specification of Management Functions	None	None
14	FMT_SMR.1	Security roles	FIA_UID.1	10
15	FPT_ITT.1	Basic internal TSF data transfer protection	None	None
16	FTA_TAB.1	Default TOE access banners	None	None
17	IDS_SDC_EXT.1	System Data Collection (EXT)	FPT_STM.1	Environment *
18	IDS_ANL_EXT.1	Analyzer analysis (EXT)	IDS_SDC_EXT.1	17
19	IDS_RCT_EXT.1	Analyzer react (EXT)	IDS_SDC_EXT.1	17
20	IDS_RDR_EXT.1	Restricted Data Review (EXT)	IDS_SDC_EXT.1	17
21	IDS_STG_EXT.1	Guarantee of System Data Availability (EXT)	IDS_SDC_EXT.1	17
22	IDS_STG_EXT.2	Prevention of System data loss (EXT)	IDS_SDC_EXT.1	17

* Reliable time is satisfied by the external time server in the Operational Environment (OE.TIME)

6.3.2 Functional Requirements

Table 6-8 traces each SFR back to the security objectives for the TOE.

Table 6-8: Requirements vs. Objectives Mapping

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.AUDIT_PROTECTION	O.AUDIT_SORT
FAU_GEN.1										X				
FAU_SAR.1						X								
FAU_SAR.2							X	X						
FAU_SAR.3						X								X
FAU_SEL.1						X				X				
FAU_STG.2	X						X	X	X		X		X	
FAU_STG.4									X	X			X	
FIA_ATD.1								X						
FIA_UAU_EXT.1							X	X						
FIA_UID.1							X	X						
FMT_MOF.1	X						X	X						
FMT_MTD.1	X						X	X			X			
FMT_SMF.1	X						X	X			X			
FMT_SMR.1								X						
FPT_ITT.1											X	X		
FTA_TAB.1							X							
IDS_SDC_EXT.1		X	X											
IDS_ANL_EXT.1				X										
IDS_RCT_EXT.1					X									
IDS_RDR_EXT.1						X	X	X						
IDS_STG_EXT.1	X						X	X	X		X			
IDS_STG_EXT.2									X					
ADV_ARC.1	X					X		X		X	X			

The following discussion provides detailed evidence of coverage for each security objective:

O.PROTCT: The TOE must protect itself from unauthorized modifications and access to its functions and data.

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE is required to protect the system data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG_EXT.1]. The TOE is required to provide the ability to restrict modifying the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the TOE may query audit data, and only authorized administrators of the TOE may query and modify all other TSF data [FMT_SMF.1, FMT_MTD.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

O.IDSCAN: The scanner must collect and store 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.

> A TOE containing a scanner is required to collect and store static configuration information from an IT System. The type of configuration information collected must be defined in the ST [IDS_SDC_EXT.1].

O.IDSENS: The sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.

> A TOE containing a sensor is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity by the assets of an IT System. These events must be defined in the ST [IDS_SDC_EXT.1].

O.IDANLZ: The analyzer must accept data from IDS sensors or IDS scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

> The analyzer is required to perform intrusion analysis and generate conclusions [IDS_ANL_EXT.1].

O.RESPON: The TOE must respond appropriately to analytical conclusions.

> The TOE is required to respond accordingly in the event an intrusion is detected [IDS_RCT_EXT.1].

O.EADMIN: The TOE must include a set of functions that allow effective management of its functions and data.

> The TOE must provide the ability to review and manage the audit trail of the system [FAU_SAR.1, FAU_SAR.3, FAU_SEL.1]. The TOE must provide the ability for authorized administrators to view all system data collected and produced [IDS_RDR_EXT.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

O.ACCESS: The TOE must allow authorized users to access only appropriate TOE functions and data.

> The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The TOE is required to restrict the review of system data to those granted with explicit read-access [IDS_RDR_EXT.1]. The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE is required to protect the system data from any modification and unauthorized deletion [IDS_STG_EXT.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU_EXT.1]. The TOE is required to provide the ability to restrict modifying the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the TOE may query audit data, and only authorized administrators of the TOE may query and modify all other TSF data [FMT_SMF.1, FMT_MTD.1]. The TOE is required to present a warning banner when a user attempts to login to the TOE [FTA_TAB.1].

O.IDAUTH: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

> The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The TOE is required to restrict the review of system data to those granted with explicit read-access [IDS_RDR_EXT.1]. The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.2]. The TOE is required to protect the system data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG_EXT.1]. Security attributes of subjects used to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU_EXT.1]. The TOE is required to provide the ability to restrict modifying the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the TOE may query audit data, and only authorized administrators of the TOE may query and modify all other TSF data [FMT_SMF.1, FMT_MTD.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

O.OFLOWS: The TOE must appropriately handle potential audit and system data storage overflows.

> The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE must prevent the loss of audit data in the event its audit trail is full [FAU_STG.4]. The TOE is required to protect the system data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG_EXT.1]. The TOE must prevent the loss of audit data in the event its audit trail is full [IDS_STG_EXT.2].

O.AUDITS: The TOE must record audit records for data accesses and use of the system functions.

> Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must provide the capability to select which security-relevant events to audit [FAU.SEL.1]. The TOE must prevent the loss of collected data in the event that its audit trail is full [FAU_STG.4]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

O.INTEGR: The TOE must ensure the integrity of all audit and system data.

> The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE is required to protect the system data from any modification and unauthorized deletion [IDS_STG_EXT.1]. Only authorized administrators of the TOE may query audit data, and only authorized administrators of the TOE may query and modify all other TSF data [FMT_SMF.1, FMT_MTD.1]. The TOE must protect the

collected data from modification and ensure its integrity when the data is transmitted to another part of the TOE [FPT_ITT.1]. The TOE must ensure that all functions to protect the data are not bypassed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

O.EXPORT: When any IDS component makes its data available to another IDS component, the TOE will ensure the confidentiality of the system data.

The TOE must protect all data from modification and ensure its integrity when the data is transmitted to another TOE component [FPT_ITT.1].

O.AUDIT_PROTECTION: The TOE must provide the capability to protect audit information.

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE must also prevent the loss of audit data in the event that its audit trail is full [FAU_STG.4].

O.AUDIT _SORT: The TOE must provide the capability to sort the audit information.

The TOE is required to perform sorting of audit data based on date and time, subject identity, type of event, and success or failure of related event [FAU_SAR.3].

6.3.3 Assurance Rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the TOE may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the TOE will have incurred a search for obvious flaws to support its introduction to the non-hostile environment.

7 TOE Summary Specification

7.1 IT Security Functions

Section 7 describes the specific Security Functions of the TOE that meet the criteria of the security features that are described in Section 1.4.8 Logical Scope of the TOE. The following sub-sections describe how the TOE meets each SFR listed in Section 6.

Table 7-1: Security Functional Requirements Mapped to Security Functions

Security Functions	Sub-Functions	SFRs
Security Audit	AU-1 Audit Generation	FAU_GEN.1
	AU-2 Audit Review	FAU_SAR.1
		FAU_SAR.2
		FAU_SAR.3
	AU-3 Audit Selection	FAU_SEL.1
	AU-4 Audit Record Protection	FAU_STG.2
		FAU_STG.4
User I&A	IA-1 User Security Attributes	FIA_ATD.1
	IA-2 User Identification & Authentication	FIA_UAU_EXT.1
		FIA_UID.2
Security Management	SM-1 Management Functions	FMT_MOF.1
		FMT_MTD.1
		FMT_SMF.1
	SM-2 Management Security Roles	FMT_SMR.1
Protection of Security	PT-1 Internal Data Transfer Protection	FTP_ITT.1
TOE Access Functions	TA-1 TOE Login Information	FTA_TAB.1
Intrusion Detection System	ID-1 System Data Collection	IDS_SDC_EXT.1
	ID-2 System Data Analysis	IDS_ANL_EXT.1
	ID-3 Analyzer Alarms	IDS_RCT_EXT.1
	ID-4 System Data Review	IDS_RDR_EXT.1
	ID-5 System Data Protection	IDS_STG_EXT.1
		IDS_STG_EXT.2

7.1.1 Security Audit Functions

7.1.1.1 AU-1: Audit Generation

(FAU_GEN.1)

Auditing is the recording of events within the system. The TOE records two classes of events: security events and IDS events. IDS events are dealt with separately under the System Data security functions. Security events relate to the proper functioning and use of the system, and allow a TOE administrator to track the management functions performed.

The following events are audited by the TOE:

a) Startup and shutdown of the audit function
b) Access to the system
c) Access to the TOE and system data
d) Viewing of the audit records
e) Unsuccessful attempts to view the audit records
f) All modification to the audit configuration that occurs during collection
g) Actions taken due to an audit storage failure
h) All identification and authentication attempts, including the user and location where authentication was attempted
i) All modification to the behavior of the TSF
j) All modifications to TSF data values
k) Creation, deletion, and modification of user accounts

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 does not record information to the audit log itself, but depends on its controlling Defense Center for audit functionality. Changes to the configuration of any sensor that happens as a result of the management functions of its managing Defense Center are audited by that Defense Center.

The audit log stores a maximum of 100,000 entries in the MySQL database of each component. Each component generates an audit event for each user interaction with the web interface. The following fields are recorded for each audit event in the audit log table:

- **Time**: The time and date that the appliance generated the audit record.
- **User**: The user name of the user that triggered the audit event.
- **Subsystem**: The menu path the user followed to generate the audit record. For example, “Operations > Monitoring > Audit” is the menu path to view the audit log.
- **Message**: The action the user performed. For example, “Page View” signifies that the user simply viewed the page indicated in the Subsystem, while “Save” means that the user clicked the Save button on the page.
- **Source IP**: The IP address of the host used by the user.

Administrators or users with the Custom User Role with the “Operations -> System Policy -> Modify System Policy” Permission can also configure a setting in the System Policy that forces users to enter comments for the audit log each time they edit an intrusion policy.

If so configured in the System Policy, audit log records will be sent to the internal syslog of the TOE component or sent to an external Syslog Server as they are generated.

In addition to the audit log described above, the TOE records audit information in the system log (syslog) of each component. The system log displays each message generated by the TOE for system events such as the startup and shutdown of the TOE. System log information for each component can be viewed on the System Log page of the WebUI. The following items are listed in order:

- The **date** the message was generated
- The **time** the message was generated
- The **host** that generated the message
- The **message** itself

AU-1: Audit Generation relies on the Operational Environment to supply reliable timestamps for the audit records. (OE.TIME) AU-1 may rely on an external Syslog Server if external logging is configured in the System Policy. AU-1 also relies on the Operational Environment to provide secure communications between the TOE and the external Time Server and optionally between the TOE and an external Syslog Server. (OE.PROTECTCOMM)

7.1.1.2 AU-2: Audit Review

(FAU_SAR.1, FAU_SAR.2, FAU_SAR.3)

The management interfaces of the TOE allow only users who have the Administrator Role or users with a Custom User Role and either “Analysis & Reporting -> Searches -> Audit Log” Permission, or “Operations -> Monitoring -> Audit” Permission to view security audit data for the system.

While viewing the security audit records, the audit review interface, available from the Defense Center, Virtual Defense Center and 3D Sensor with IPS GUIs, provides the ability to sort the data for display based upon the following properties:

- Date and Time
- User
- Type of event (subsystem field)
- Success or Failure of the event (contained in the message field)

In addition to sorting, searches of the audit records are available to users having the Administrator Role or a Custom User Role with an appropriate permission as well.

The audit log can also be used to view detailed reports of changes to the system. These reports compare the current configuration of the system to its most recent configuration before a particular change. A compare icon appears next to audit log events that reflect changes to the system. The administrator can click the compare icon to access the Compare Configurations page and view a detailed report of a change. The Compare Configurations page displays the differences between the system configuration before changes and the running configuration in a side-by-side format. The audit event type, time of last modification, and name of the user who made the change are displayed in the title bar above each configuration. This feature is available to users having the Administrator Role or a Custom User Role with an appropriate permission via the Defense Center, Virtual Defense Center and 3D Sensor with IPS GUIs.

7.1.1.3 AU-3: Audit Selection

(FAU_SEL.1)

Suppression lists can be created for audit events based on IP address, message, subsystem, and username. Any one of these four field types can be suppressed, preventing the audit event from being generated.

To set up the suppression mechanism, a TOE administrator must have access to the (Virtual) Defense Center's or 3D Sensor with IPS's *admin* user account and must be able to access the Defense Center or 3D Sensor with IPS operating system's shell. It must be assumed that only authorized and limited personnel have access to the component's operating system and to its *admin* account. The audit suppression lists are created or modified at installation or during maintenance; this functionality is not part of the run-time operation of the TOE available through the WebUI.

To suppress audit records one or more files must be created in the */etc/sf* directory in the following form:

AuditBlock.type

where ***type*** is: ***IP address***, ***message***, ***subsystem***, or ***username***.

The contents for each audit block type must be in a specific format as described below:

- ***IP address*** - Create a file named AuditBlock.address and include, one per line, each IP address that will be suppressed from the audit log.

- ***message*** - Create a file named AuditBlock.message and include, one per line, the message substrings that will be suppressed. Substrings are matched so that if the file includes “backup”, all messages that include the word “backup” are suppressed.

- ***subsystem*** - Create a file named AuditBlock.subsystem and include, one per line, each subsystem that will be suppressed. Substrings are matched so that if the word “Health” is included in the file, both the “Health” and the “Health Events” subsystems are suppressed. The subsystem names and the definition of the events audited by each are listed below:

- ***Admin*** - administrative features such as system and access configuration, time synchronization, backup and restore, sensor management, user account management, and scheduling.
- ***Alerting*** - the alerting functions such as email, SNMP, and syslog alerting
- ***Audit Log*** – audit event views
- ***Audit Log Search*** – audit event searches
- ***Configuration*** – email alerting
- ***Coop*** - the continuity of operations feature.
- ***Date*** - the date and time range for event views.
- ***Default Subsystem*** - options that do not have assigned subsystems
- ***Detection & Prevention Policy*** – menu options for intrusion policies
- ***Error*** - system-level errors
- ***EULA*** – reviewing the end user license agreement
- ***Events*** – intrusion event views
- ***Events Clipboard*** - the intrusion event clipboard
- ***Events Reviewed*** - reviewed intrusion events
- ***Events Search*** - any event search
- ***Header*** - the initial presentation of the user interface after a user logs in.
- ***Health*** - health monitoring
- ***Health Events*** - health monitoring event views
- ***Help*** - the online help
- ***High Availability*** - the high availability feature
- ***IDS Impact Flag*** - impact flag configuration
- ***IDS Policy*** - intrusion policies
- ***IDSPolicy > policy_name > Appliance > det_engine_name*** - applying intrusion policies
- ***IDSRule sid:sig_id rev:rev_num*** - intrusion rules by SID.
- ***Incidents*** - intrusion incidents
- ***Insert Policy Apply Job*** - applying policies
- ***Install*** - installing updates
- ***Intrusion Events*** - intrusion events
- ***Login*** – web interface login and logout functions
- ***Menu*** - any menu option
- ***Object export > obj_type > obj_name*** - importing objects of a specific type and name
- ***Preferences*** - user preferences such as the time zone for a user account and individual event preferences
- ***Policy*** - any policy, including intrusion and OPSEC policies
- ***Register*** - registering sensors on a Defense Center
- ***RemoteStorageDevice*** - configuring remote storage devices
- ***Reports*** - the report listing and report designer features
- ***Rules*** - intrusion rules including the rule editor and the rule importation process.
- ***Status*** - the syslog, as well as host and performance statistics
- ***System*** - various system-wide settings
- ***System Policy > policy_name Appliance > appliance_name*** - applying system policies
- ***Task Queue*** - the task queue
- ***Users*** - creating and modifying user accounts

Note: subsystems pertaining to features not included in the scope of the evaluation (e.g. SEU) have not been included in this list

- ***Username -*** Create a file named AuditBlock.user and include, one per line, each user account that will be suppressed.

7.1.1.4 AU-4: Audit Record Protection

(FAU_STG.2, FAU_STG.4)

The audit records are protected by the access control functionality of the MySQL database and the Linux-derived operating system of the 3D Sensors with IPS, Defense Center and Virtual Defense Center. The only way to access the audit records is through the Defense Center, Virtual Defense Center, or 3D Sensor with IPS GUIs. The TOE provides protection for the security audit records primarily by preventing access to the system without successful authentication. Subsequently, the TOE requires that a user must have the Administrator Role or a Custom User Role with the appropriate permissions before it grants access to the audit records via the audit record management functions. Further, since the audit function starts automatically with the TOE, and cannot be disabled, all selected (see FAU_SEL.1) actions are recorded, including possible modification to the records.

As indicated below, 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.

When the TOE begins to run out of storage space for the audit records, (85% of the component's disk capacity is allotted for record storage) or the database limit of 100,000 records has been reached, the oldest audit events are pruned until the database is back within limits. This can also occur if the event database, security databases, or the log files grow and exceed the 85% limit for disk capacity. If the audit process runs out of disk space or the database limit is exceeded, then the oldest current log files will be automatically overwritten to prevent new actions from occurring without being tracked.

The TOE can be configured so that a warning is sent to a designated TOE administrator via email to inform them when the audit records are automatically overwritten.

Note: The administrator must perform periodic backups of the audit data (via the WebUI backup function) to prevent loss of data.

AU-4: Audit Record Protection relies on an Email Server in the environment to send warnings to the designated TOE administrator when the audit data is overwritten. (OE.ALARMS) AU-4 also relies on the Operational Environment to provide secure communications between the TOE and the external Email Server. (OE.PROTECTCOMM)

7.1.2 User I&A Functions

7.1.2.1 IA-1: User Security Attributes

(FIA_ATD.1)

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

- **User Name (User Identity)**

- **Sourcefire User Role(s) (Authorizations)** – One or more of the following:
    - **Administrator**
    - **Maintenance**
    - **Policy & Response Administrator**
    - **Intrusion Event Analyst**
    - **Intrusion Event Analyst (Read Only)**
    - **Custom User Role(s)**

  Note: The Sourcefire 3D product also supports the following roles which are not included in the TOE: RNA Event Analyst, RNA Event Analyst (Read Only) and External Database User

- **Restrict Deletion Rights** – Used only for users with event analyst roles so that he/she is can only delete objects that he/she created. Can be one or more of the following:
    - User Cannot Delete Bookmarks Created by Other Users
    - User Cannot Delete Searches Created by Other Users
    - User Cannot Delete Reports Created by Other Users
    - User Cannot Delete Report Profiles Created by Other Users
    - User Cannot Delete Custom Workflows Created by Other Users
    - User Cannot Delete Custom Tables Created by Other Users

- **Use External Authentication Method** – If selected, the user's credentials are to be externally authenticated. If selected and the external authentication server is unavailable, the user cannot log into the Defense Center or Virtual Defense Center GUI. If this option is enabled, the password management options are not used and are not visible on the WebUI**.**

- **Password (Authentication Data)** – Can be up to 32 alphanumeric characters.

- **Force Password Reset on Login –** If selected, the TOE forces the user to change his password the first time he logs in.

- **Password Strength Check –** If selected, the TOE enforces strong passwords. A strong 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.

- **Max Number of Failed Logins** – A value that determines the maximum number of times each user can try to login after a failed login attempt before her account is locked. The default setting is five tries; if set to zero, the TOE allows an unlimited number of failed logins. This attribute cannot be changed after the user account is created.

- **Password Expiration –** The number of days after which the user's password will expire. The default setting is 0, which indicates that the password never expires. This attribute cannot be changed after the user account is created.

- **Days Until Expiration Warning** - The number of warning days users have to change their password before their password actually expires. The default setting is 0 days.

  Note: The number of warning days must be less than the number of days before the password expires

- **Command-Line Interface Access –** Applies only to 8000 Series, 7000 Series and Virtual 3D Sensors with IPS. Sets access to the command line interface (CLI) of the sensor, which is used for installation, configuration and maintenance. Can have one of the following values:
  - None - disables access to the CLI (the user cannot log into the CLI)
  - Basic - allows the user to log into the CLI and to access a specific subset of commands
  - Configuration - allows the user to access any CLI option

  Note: The access level defaults to "None" on user creation via the management interfaces. Shell access granted to externally authenticated users defaults to the Configuration level of command line access.

A user account can have multiple roles assigned, which allows a broader and more focused set of privileges. The user account information is stored in a TSF database that is modifiable only by an authorized user with the Administrator Role. The user account passwords stored in the database are protected by a salted SHA512 hash. After adding user accounts to the system, a user's assigned roles or password may be modified at any time.

The user accounts that allow access to the 7000 and 8000 Series sensors' Limited WebUI are kept separate from the managing Defense Center user accounts. They can only be modified through the Limited WebUI on the sensor itself.

Note: The password management attributes do not apply to users who authenticate to an external authentication server. Those settings are managed on the external server.

7.1.2.2 IA-2: User Identification & Authentication

(FIA_UAU_EXT.1, FIA_UID.1)

Each individual must be successfully identified and authenticated with a username and password by the TSF before access is allowed to the TOE.

User identification and authentication by the TSF uses the security attributes of the user account described in Section 7.1.2.1 above. When identification and authentication data is entered, the TOE attempts to identify the applicable user account from the provided identity and if a match is found, the password provided is compared against that stored with the user account information in the internal Sourcefire 3D System database. If a user account cannot be associated with the provided identity or the provided password does not match that stored with the user account information, identification and authentication will fail. No actions are allowed, other than entry of identification and authentication data, until successful identification and authentication.

Creation of a TSF authenticated TOE user through the WebUI does not give that user an account on any of the Sourcefire 3D System appliances' LINUX-based operating systems (use of the OS shell). Conversely creating a OS user account on an appliance does not create a user account in the TSF; i.e. when a shell access user logs into an appliance, a TOE user account is not created and that user does not have access to the management functions of the WebUI.

By default, the Sourcefire 3D System uses internal authentication to check user credentials when a user logs in.

Alternately, the TOE can be configured to use an external authentication service for user identification and authentication. Both LDAP and RADIUS servers are supported. However, the use of an external authentication server requires a TOE configuration that includes a Defense Center or Virtual Defense Center; a stand-alone 3D Sensor with IPS configuration cannot use external authentication. User login for the Limited WebUI of the 7000 and 8000 Series sensors cannot use an external authentication server either. The Virtual Defense Center does not support RADIUS authentication.

Note: Only one type of external authentication can be configured for an appliance.

A locally authenticated user (one who is authenticated by the TSF) is automatically converted to an externally authenticated user if:

- External authentication is enabled (the **Use External Authentication Method** attribute is set for that user account),
- The same username exists for the user on the external server, and
- The user logs in using the password stored for that user on the external server.

Important*: Once a locally authenticated user is converted to an externally authenticated user, that user account cannot changed back to use local authentication*.

For LDAP authentication, an LDAP authentication object must be created to provide user authentication services. The Administrator uses the Defense Center or Virtual Defense Center Web GUI to:

- define settings for the connection to the LDAP server
- select the directory context
- define search criteria used to retrieve user data from the server

- optionally configure shell access authentication

The LDAP directory server can be optionally used to authenticate accounts for shell access on a local appliance (3D Sensor or Defense Center). Note that an Administrator can only configure shell access for the first authentication object in the system policy. Shell users are not configured as local users (TOE users) on the appliance, even after they log in. Addition and deletion of shell access users occurs only on the LDAP server, and the filter set there determines which set of users on the LDAP server can log into the OS of the appliance.

Similarly, for RADIUS authentication, a RADIUS authentication object must be created. The Administrator uses the Defense Center Web GUI to:

- define settings for the connection to the RADIUS server
- grant user roles to specific and default users
- define custom attributes if the RADIUS server returns custom attributes
- optionally configure shell access authentication.

As with LDAP authentication, the RADIUS server can be used to authenticate accounts for shell access on a local appliance (3D Sensor or Defense Center). The Administrator specifies user names for users who are granted shell access. Only the first authentication object in the system policy can be configured for shell access. With the exception of the *admin* account, the shell access list set on the RADIUS authentication object entirely controls shell access on the appliance. Shell users are configured as local users on the appliance when the system policy is applied.

Note: Both LDAP and RADIUS servers require TCP/IP access from the TOE to the authentication server.

IA-2: User Identification & Authentication relies on the Operational Environment to provide an external authentication service if either LDAP or RADIUS authentication is configured. (OE.XAUTH) IA-2 also relies on the Operational Environment to provide secure communications between the TOE and the authentication server. (OE.PROTECTCOMM)

7.1.3 Security Management Functions

7.1.3.1 SM-1: Management Functions

(FMT_MOF.1, FMT_MTD.1, FMT_SMF.1)

The TOE requires user authentication before any actions (other than entry of identification and authentication data) can be performed through the TOE interfaces (the WebUI of the Defense Center, Virtual Defense Center and the 3D Sensor with IPS and the Limited WebUI of the 7000 and 8000 Series sensors). Access to TSF data and management functions are restricted by a user’s assigned role(s) and the access permissions for custom user roles as specified in FMT_MTD.1 (see Section 6.1.3.2 FMT_MTD.1 Management of TSF data).

Use of the Defense Center, Virtual Defense Center, 3D Sensor with IPS WebUI and the Limited WebUI for the 7000 and 8000 Series sensors requires a management console with a properly configured web browser as specified in Table 1-2: Tested Web Browsers.

A stand-alone 3D Sensor with IPS configuration has the same user account types as a configuration that uses a Defense Center or Virtual Defense Center. The stand-alone sensor GUI has the same functionality as the Defense Center and Virtual Defense Center GUI with the following exceptions:

- A sensor cannot manage other sensors, so the 'Sensors' menu option is hidden on the sensor GUI; therefore management functions such as creating a sensor group, or pushing a policy to a sensor only applies to the Defense Center and Virtual Defense Center GUI.
- Health monitoring is a Defense Center and Virtual Defense Center feature, so that option is not available on the sensor GUI.
- External authentication of users is only applicable to a Defense Center or Virtual Defense Center configuration.

The Limited WebUI of the 7000 and 8000 Series sensors is available to authorized user accounts maintained on the sensor. The only user role is "Administrator" for these sensors; there are no custom user roles.

The management functions available for each type of hardware-based or virtual appliance are indicated in Table 6-4: Management of TSF data.

SM-1: Management Functions depends on the Operational Environment for an administrative console with a properly configured Web Browser to support the TOE's management interfaces.

7.1.3.2 SM-2: Management Security Roles

(FMT_SMR.1)

All users of the TOE have access to TSF data and management functions, and therefore they are considered administrators for the purposes of this evaluation. The terms "TOE user", "TOE administrator" and "authorized administrator" are used in this ST to refer collectively to all authorized TOE users.

Each Sourcefire 3D System user has an associated user access role or roles. The Sourcefire 3D System includes predefined user roles designed for a variety of administrators and analysts. Administrators can also create custom user roles with specialized access privileges. The menus and other options in the web interface that users can access depend on their roles. Predefined user roles have a set of predetermined access privileges, while custom user roles have granular access privileges that can be configured.

Predefined User Roles
The TOE supports the following predefined user roles:

- **Administrators** can set up the appliance's network configuration, manage user accounts, and configure system policies and system settings. The Administrator Role provides access to analysis and reporting features, rule and policy configuration, system management, and all maintenance features. Administrator users see the main toolbar as well as all the menu options. Users with the Administrator role also have Intrusion Event Analyst, Policy & Response Administrator, and Maintenance access rights.

  Note: For all 8000 Series and 7000 Series sensors, the only TOE user role is "Administrator". This role is granted when a new user account is created and cannot be changed.

  Note: Use of the Administrator role must be limited for security reasons.

- **Policy & Response Administrators** can manage intrusion rules, policies, and responses. The Policy & Response Administrators Role provides access to rules and policy configuration. Policy & Response Administrators have access to the main toolbar and rule and policy-related options on the Policy & Response and Operations menus.

- **Maintenance** Administrators can access monitoring functions (including health monitoring, host statistics, performance data, and system logs) and maintenance functions (including task scheduling and backing up the system). The Maintenance Role provides access to monitoring and maintenance features. Maintenance users see the main toolbar and maintenance-related options on the Operations menu. Maintenance administrators do not have access to the functions in the Policy & Response menu and can only access the dashboard from the Analysis & Reporting menu.

- **Intrusion Event Analysts** can view, analyze, review, and delete intrusion events. They can also create incidents, generate reports, and view (but not delete or modify) health events. The Intrusion Event Analyst Role provides access to IPS analysis features, including intrusion event views, incidents, and reports. Intrusion Event Analysts see the main toolbar and IPS analysis-related options on the Analysis & Reporting and Operations menus.

- **Intrusion Event Analysts (Read Only)** have all the same rights as Intrusion Event Analysts, except that they cannot delete events. The Intrusion Event Analyst (Read Only) Role provides read-only access to IPS analysis features, including intrusion event views, incidents, and reports. Intrusion Event Analysts see the main toolbar and IPS analysis-related options on the Analysis & Reporting and Operations menus.

Note: Along with assigning an event analyst role to a user, Administrators can restrict that user's deletion rights only allow deletion of report profiles, searches, bookmarks, custom tables, and custom workflows created by that user.

Note: The Sourcefire 3D product also supports the following pre-defined roles which are not included in the TOE: RNA Event Analyst, RNA Event Analyst (Read Only) and External Database User

Predefined user roles cannot be edited; however, their access privilege sets can be used as the basis for custom user roles. Predefined user roles cannot be deleted either, but they can be deactivated. Deactivating a role removes that role and all associated permissions from any user who is assigned that role.

Custom User Roles

In addition to the predefined user roles, custom user roles can be created with specialized access privileges. Custom user roles can have any set of menu based and system permissions, and may be completely original or based on a predefined user role. Like predefined user roles, custom roles can serve as the default role for externally authenticated users. Unlike predefined roles, custom roles can be modified and deleted. Custom user roles can also be copied and then modified to create other custom user roles.

The permissions assigned to custom user roles are hierarchical, and are based on the Sourcefire 3D System WebUI menu layout. Permissions are expandable if they have sub-pages or if they have more fine-grained permissions available beyond simple page access. In that case, the parent permission grants page view access and the children granular access to related features of that page. Permissions that contain the word “Manage” grant the ability to edit and delete information that other users create. Restricted searches can be applied to a custom user role. These constrain the data a user may see in the event viewer. Administrators can configure a restricted search by first creating a private saved search and selecting it from the “Restricted Search” drop-down menu under the appropriate menu based permission.

Role Escalation

Custom user roles can be given the permission, with a password, to gain temporarily the privileges of another, targeted user role in addition to those of the base role. This allows administrators to substitute one user for another during an absence easily, or to track the use of advanced user privileges more closely.

For example, a user whose base role has very limited privileges can escalate to the Administrator role to perform administrative actions. This feature can be configured so that users can use their own passwords, or so that they use the password of another specified user. The second option allows one escalation password for all applicable users.

Any user role, predefined or custom, can be assigned to act as the system-wide escalation target role. This is the role to which any other role may escalate, if it has the ability.

Note: Only one user role at a time can be the escalation target role. Each escalation lasts for the duration of a login session and is recorded in the audit log.

Externally Authenticated User Roles

The Sourcefire 3D System allocates user privileges based on the user’s role. In the system policy on the Defense Center, a default access role is set for all users who are externally authenticated. After an externally authenticated user logs in for the first time, administrators can add or remove access rights for that user on the User Management page. If these rights are not modified, the user has only the rights granted by default. Because internally authenticated users are created manually, the access rights are set on creation.

Externally authenticated users have minimum access rights based on the settings in LDAP or RADIUS authentication objects and in the system policy. Any role can be the default access role for externally authenticated users.

If management of access rights was configured through LDAP groups, the access rights for users are based on their membership in LDAP groups. They receive the default access rights for the group that they belong to that has the highest level of access. If they do not belong to any groups and group access has been configured, they receive the default user access rights configured in the authentication object for the LDAP server. Configured group access, settings override the default access setting in the system policy.

Similarly, a user is assigned to specific user role lists in a RADIUS authentication object; the user receives all assigned roles, unless one or more of those roles are mutually incompatible. If a user is on the lists for two mutually incompatible roles, the user receives the role that has the highest level of access. If the user does not belong to any lists and you have configured a default access role in the authentication object, the user receives that role.

SFLinux “admin” Role
Maintenance of the TOE also requires the operating system’s (SFLinux) *admin* user account (“*admin*” role). The TOE administrator must have access to the Defense Center’s or 3D Sensor with IPS’s *admin* user account and must be able to access the Defense Center or 3D Sensor with IPS operating system’s shell. It must be assumed that only authorized and limited personnel have access to the component’s operating system and to its *admin* account. This is not a security role maintained by the TOE; it is maintained by the appliance OS and is equivalent to the system administrator of the OS. This role is required to set up the audit suppression mechanism. The audit suppression lists are created or modified at installation or during maintenance; this functionality is not part of the run-time operation of the TOE available through the WebUI.

7000 and 8000 Series Sensors
The 7000 and 8000 Series sensors must be managed by a Defense Center, but also have a Limited WebUI for management of the sensor. The only user role allowed for the Limited WebUI is “Administrator”; there are no custom user roles. User accounts are maintained on the sensor through the Limited WebUI and are separate from those on the managing Defense Center. These sensors come with a predefined “admin” account.

7.1.4 Protection of Security Functions

7.1.4.1 PT-1: Internal Data Transfer Protection

(FPT_ITT.1)

The TSF ensures that data transmitted between separate parts of the TOE are protected from disclosure or modification. This protection is ensured by transmission of data between the Defense Center and the 3D Sensor(s) with IPS over a secure, SSL-encrypted TCP tunnel. 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.

There are four types of communications that can occur between TOE components:

- event transmission
- status updates
- remote copy
- remote execution

All communications between TOE components use the Management Network: a private protected network used only by the Defense Center (or Virtual Defense Center) and the 3D Sensors with IPS and Virtual 3D Sensors with IPS it manages. All communications go through a single channel in the SFLinux operating system used by the TOE components, which uses the following encryption strength:

> Cipher used = AES256-SHA (strength: 256 bits), which is (DHE-RSA-AES256-SHA)

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.

Note: This function is not applicable for the stand-alone sensor configuration of the TOE.

7.1.5 TOE Access Functions

7.1.5.1 TA-1 TOE Login Information

(FTA_TAB.1)

The TOE has the functionality to present warning information to a user when attempting to login.

Users with the Administrator role or with a Custom User Role with the “Operations -> System Policy -> Modify System Policy” Permission can create a custom login banner to display an advisory warning message regarding unauthorized use of the TOE. The banner appears when users log into a Defense Center or 3D Sensor with IPS on the login page of the WebUI.

Banners can contain any printable characters except the less-than symbol (‘<’) and the greater than symbol (‘>’). Custom login banners are part of the system policy. The login banner can be specified either by creating a new system policy or by editing an existing policy. In either case, the new or modified login banner will not be displayed until the System Policy is applied.

There is no limit to the number of characters that can be entered in the login banner field through the WebUI, but the banner is truncated to a 64K character limit for display.

7.1.6 Intrusion Detection System Functions

7.1.6.1 ID-1: System Data Collection

(IDS_SDC_EXT.1)

The TOE has the ability to set rules to govern the collection of data regarding potential intrusions. Each 3D Sensor with IPS and Virtual 3D Sensor with IPS uses rules, decoders, and preprocessors to look for the broad range of exploits that attackers have developed. While the TOE contains default intrusion rules to detect currently known attacks and exploits, new rules can be created to detect attacks most likely to occur in a given environment. This allows the TOE administrators control over the types of traffic that will be monitored. The sensors run decoders and preprocessors against detected network traffic to normalize traffic and detect malicious packets.

The following features can affect the collection of network traffic:

- All evaluated sensors (virtual and appliance-based) support the **automatic application bypass** feature. This feature allows the administrators to balance packet-processing delays with the network's tolerance for packet latency. Automatic application bypass can be applied on an interface set basis. The feature functions with both passive and inline interface sets; however, it is most valuable in inline deployments. Automatic application bypass limits the time allowed to process packets through an IPS detection engine and allows packets to bypass the detection engine if the time is exceeded. The automatic application bypass option is off by default. If the option is on, the administrator can configure the bypass threshold. The default setting is 750 milliseconds (ms). The valid range is from 250 ms to 60,000 ms.

- **PEP** is an optional feature available only for the 7000 Series and 8000 Series models of the sensor appliances. PEP allows users to drop immediately or fastpath (send through the sensor without analysis) network traffic thereby bypassing the data collection rules for specified targets. Users can create PEP or fast path rules to block, analyze, or send traffic directly through these sensors with no further inspection.
  - **Fast path rules** divert traffic that does not need to be analyzed to bypass the sensor. Fast path rules either send traffic to the fast path (out of the interface) or allow it to continue into the 3D Sensor for further analysis. They use the 8000 Series hardware capabilities. Their advantage is the speed at which they determine the correct path for the traffic. Because the fast path rules function at the hardware level, they only determine limited information about the packet. These rules, therefore, are restricted. For example, individual ports can be specified in a fast path rule, but a range of ports cannot.
  - **PEP rules** are more complex than fast path rules. Additional rule actions can be configured in PEP rules. The disposition or action taken because of a PEP rule offers more options than the one-of-two paths determination a fast path rule makes. PEP rules can be configured to:
    - fast path all traffic
    - drop all traffic
    - drop all traffic with reset

  - analyze all traffic
  - analyze or fast path traffic based on the detection type of the traffic

The TOE collects network traffic information from the targeted IT System resources including:

- Date and time
- Type of event
- Subject identity (e.g., source address or addresses)
- Outcome of the event (e.g., packet met an intrusion rule and was dropped)
- The additional information specified in the Details column of Table 6-5: System Events:
  - Protocol
  - Source address
  - Destination address

ID-1: System Data Collection relies on the Operational Environment to provide reliable timestamps for the collected data records. (OE.TIME) ID-1 also relies on the Operational Environment to provide secure communications between the TOE and the external Time Server. (OE.PROTECTCOMM)

7.1.6.2 ID-2: System Data Analysis

(IDS_ANL_EXT.1)

A detection engine is the mechanism on a 3D Sensor that is responsible for analyzing the traffic on the network segment where the sensor is connected. The TOE uses the IPS type of detection engine. 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

Administrators or users with a Custom User Role with the Operations > Configuration > Detection Engines can create, edit and delete detection engines through the WebUI management functions.

To analyze the network data collected, the TOE uses decoders and preprocessors, policies, signatures, and statistical analysis.

DECODERS and PREPROCESSORS

As the detection engine captures packets, it sends them to the packet decoder. The packet decoder converts the packet headers and payloads into a format that can be easily used by the preprocessors and the rules engine. Each layer of the TCP/IP stack is decoded in turn, beginning with the data link layer and continuing through the network and transport layers. After the packets are decoded through the first three TCP/IP layers, they are sent to preprocessors, which normalize traffic at the application layer and detect protocol anomalies. After the packets have passed through the preprocessors, they are sent to the rules engine. The rules engine inspects the packet headers and payloads to determine whether they trigger any of the shared object rules or standard text rules.

The following decoders and preprocessors are available for the detection of stateful or malformed intrusions:

Application Layer Protocol Decoders:

- **DCE/RPC Configuration** - Examines DCE/RPC traffic for fragmented request packets, and reassembles them so the rules engine can inspect the complete packets.

- **DNS Configuration** - Inspects DNS name server responses for the following specific exploits:
    - Overflow attempts on RData text fields
    - Obsolete DNS resource record types
    - Experimental DNS resource record types

- **FTP & Telnet Configuration** - Decodes Telnet traffic and the FTP command channel for analysis against signatures (similar to HTTP Normalization).

- **HTTP Inspection** - Detects HTTP traffic to non-standard ports and on HTTP traffic using proxy servers. Responsible for:
    - Decoding and normalizing HTTP requests sent to and HTTP responses received from web servers on the network
    - Separating messages sent to web servers into URI, non-cookie header, cookie header, method, and message body components to improve performance of HTTP-related intrusion rules
    - Separating messages received from web servers into status code, status message, non-set-cookie header, cookie header, and response body components to improve performance of HTTP-related intrusion rules
    - Detecting possible URI-encoding attacks
    - Making the normalized data available for additional rule processing
    - Generating an event when HTTP traffic is received by ports not specified as web server ports in an intrusion policy.
    - Extracts URI and hostname data from HTTP traffic to allow inspection of that data.
    - Handles normalization of the HTTP response body so that IPS can detect JavaScript-based attacks; detects and normalizes JavaScript data in HTTP responses.

- **Sun RPC Configuration** - Decodes RPC traffic for analysis against signatures (similar to HTTP Normalization).

- **Session Initiation Protocol (SIP)** - Decodes and analyzes SIP 2.0 traffic. Extracts the SIP header and message body, including SDP data when present, and passes the extracted data to the rules engine for further inspection.

- **GPPRS Tunneling Protocol (GTP)** - Detects attacks in traffic between GPRS support nodes (GSNs); detects anomalies in version 0, 1, and 2 GTP traffic and forwards command channel signaling messages for these versions to the rules engine for inspection. This preprocessor specifically detects intrusion attempts in both the GTP control plane (GTP-C) and data transfer (GTP-U) protocols.

- **Internet Message Application Protocol (IMAP) -** inspects server-to-client IMAP4 traffic and, when associated preprocessor rules are enabled, generates events on anomalous traffic. The preprocessor can also extract and decode email attachments in client-to-server IMAP4 traffic and send the decoded attachments to the rules engine.

- **Post Office Protocol (POP3) -** Inspects server-to-client POP3 traffic and, when associated preprocessor rules are enabled, generates events on anomalous traffic. The preprocessor can also extract and decode email attachments in client-to-server POP3 traffic and send the decoded attachments to the rules engine.

- **SMTP Configuration** - Decodes SMTP traffic for analysis against signatures (similar to HTTP Normalization). Extracts data about message sender and recipient and attachment filenames from SMTP traffic to allow inspect of that data.

- **SSH Configuration** - Detects and alerts on the Challenge-Response Buffer Overflow exploit, the CRC-32 exploit, the SecureCRT SSH Client Buffer Overflow exploit, protocol mismatches, and incorrect SSH message direction. The preprocessor also alerts on any version string other than version 1 or 2.

- **SSL Configuration –** Analyzes the contents of the handshake and key exchange messages exchanged at the beginning of an SSL session to determine when the session becomes encrypted; makes the SSL version and state information available for additional rule processing.

- **SCADA Preprocessors** - Handles attacks related to the Distributed Network Protocol v3.0 (DNP3) and the Modbus Protocol; these preprocessors detect anomalies in Modbus and DNP3 SCADA traffic and forward data to the rules engine for inspection.

Transport/Network Layer Preprocessors:

- **Checksum Verification** - Verifies the size of packets being sent to the network, detecting malformed packets that may be used in various attacks**.**

- **Inline Normalization** - Normalizes traffic to minimize the chances of attackers evading detection in inline deployments. Prepares packets for use by other preprocessors and the rules engine in inline deployments. Helps ensure that the packets IPS processes are the same as the packets received by the hosts on the network.

- **IP Defragmentation** - Enables the TOE to rebuild packets that have been fragmented by the network prior to inspection against other decoders, preprocessors, and signatures.

- **Packet Decoding** - Performs the initial decoding so that it can be processed by the other decoders, preprocessors, and intrusion rules. The primary packet decoder for traffic from the NIC.

- **TCP Stream Configuration** - Provides stateful inspection of packets for TCP traffic, allowing detection of intrusion attempts that span multiple packets. The Stream reassembly allows detection of sessions between clients and servers, and then the analysis of this traffic for specific patterns.

- **UDP Stream Configuration** - Provides stateful inspection of packets for UDP traffic, allowing detection of intrusion attempts that span multiple packets. The Stream reassembly allows detection of sessions between clients and servers, and then the analysis of this traffic for specific patterns.

Specific Threat Detection Preprocessors:

- **Back Orifice Detection** - Searches for packets that can show the presence of Back Orifice, or attempts to install Back Orifice onto computers on the network.

- **Portscan Detection**- Determines which ports are open on the host and, either directly or by inference, which services are running on these ports; designed to help determine which portscans might be malicious by detecting patterns of activity and generating events accordingly.

- **Rate-Based Attack Prevention –** Enables detection of rate-based attacks as described in the Statistical Analysis description above.

- **Sensitive Data** - Detects and Generate events on sensitive data in ASCII text (Social Security numbers, credit card numbers, driver's license numbers …) which can be used to detect accidental data leaks.

Sourcefire 3D System Version 4.10.2.4 includes preprocessor rules. Just as users can enable, disable, and set to drop any Snort-based intrusion rule, they can also use those same concepts to control preprocessor behavior.

POLICIES

Sourcefire provides default intrusion policies for both passive and inline deployments. However, users may find that the rules and preprocessor options configured in those policies do not address the security needs of their network. In these cases, administrators can tune the policy 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. Intrusion policies provide the following ways to tune preprocessors:

- Deactivate preprocessors that do not apply to the traffic on the subnet that is monitored.
- Specify ports, where appropriate, to focus the activity of the preprocessor.

- Determine whether the preprocessor will generate an event when it acts on a packet.
- Configure preprocessors to generate events when they encounter certain features in packets, for example, state problems or certain combinations of TCP flags.

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. Further, a hierarchy exists among policy layers. Sourcefire-defined policies form the foundation, and can be superseded by user-defined policy layers. Users can define their own policy layers by company, by department, by network, or even by user. Settings in higher policy layers take precedence over settings in lower policy layers.

For example, an intrusion rule can be set to generate an event in the Company-Wide layer, but then disabled in the Site-Specific layer. In this case, the rule is disabled in the overall intrusion policy as the higher configuration layer takes precedence. Administrators or users with a Custom User Role with Policy & Response > IPS > Intrusion Policy > Modify Intrusion Policy can add, rename, rearrange, and share policy layers and can view whether a rule or preprocessor setting is configured in a layer or in a layer above or below it in the stack.

In Sourcefire 3D System Version 4.10.2.4, a policy can be associated with a detection engine or set of detection engines as it is created. Administrators or users with a Custom User Role with Policy & Response > IPS > Intrusion Policy > Modify Intrusion Policy can also customize intrusion policies to inspect traffic for one or more VLANs or subnets. This capability affords greater flexibility by enabling organizations to inspect traffic differently for distinct network segments. It also allows the ability to leverage multiple policies on a single detection engine, and prevents the mixing of intrusion events from multiple network segments.

Note: A policy can be filtered by network or VLAN, but not by both.

When an intrusion policy is created, variable definitions can be included as part of the policy. Variables represent values that are commonly used within intrusion rules. The Sourcefire 3D System provides predefined variables for use within rules. When intrusion policy is applied to a detection engine, those variables are used in conjunction with the detection engine to monitor network traffic and generate events.

Besides the predefined variables, a variable with the reserved name USER_CONF can be used to configure features not otherwise available via the standard WebUI menu items (Non-Standard Features). USER_CONF can be used as an intrusion policy variable or as an IPS detection engine variable. IPS recognizes only one definition of USER_CONF for each detection engine, and that definition takes effect when an intrusion policy is applied to the detection engine.

Users must therefore be careful not to use the reserved variable USER_CONF to configure an IPS feature unless they are instructed to do so in the feature description or by Sourcefire Support. Conflicting or duplicate configurations will halt IPS. Deleting USER_CONF from any intrusion policy or detection engine deletes it from all intrusion policies and detection engines.

SIGNATURES

Signatures are patterns of traffic that can be used to detect 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. Rules are used to embody signatures, decoders and preprocessors in the TOE. The TOE is packaged with default signatures for known exploits, and the TOE administrators can add new signatures at any time.

New signatures are available from the Sourcefire support organization and from public Snort forums. The evaluated configuration of the TOE does not allow importing SEUs that contain updated signatures and rules, since an SEU may also contain new binaries, including new versions of Snort, which will alter the TOE. However, the signature data on the Sourcefire and public Snort sites can be used by the TOE administrators to manually update and create rules and policies.

Note: Sourcefire cannot guarantee the correctness of signatures available on public Snort forums and websites.

The WebUI provides a graphical rule editor, which allows the creation and modification of signatures through the use of standard GUI controls (check boxes, drop down lists …). Custom rules may be created by the Administrator role, the Policy and Response Administrator role, or a Custom User Role with the “Policy & Response -> IPS -> Rule Editor” Permission. Use of the WebUI to create custom rules is described in detail in Chapter 20: Understanding and Writing Intrusion Rules, of the Sourcefire 3D System User Guide.

The Administrator or Policy and Response Administrator, or a Custom User Role with the “Policy & Response -> IPS -> Rule Editor” Permission may also import a text rule file that has been created with a text editor on a local machine. Importation of a local rule file is available through the ‘Policy & Response > IPS > Rules’ menu of the WebUI.

Signatures are used for stateless detections, those intrusion attempts that can be detected with individual packets. Signatures cannot be used to detect intrusions that require multiple packets, such as a Denial of Service attack. To detect these types of events, the IDS uses various decoders and preprocessors for stateful inspections, which allow these multi-packet intrusions to be detected. Decoders and preprocessors can also provide detection of malformed packets.

All signatures entered into the TOE by any means, must conform to this format:

> <type field> <protocol field> <source IP> <source port> <operator> <destination IP> <destination port> (option1; option2; …; optionN)

Header – defines the network addresses involved for the traffic to be considered for evaluation by the signature options:

- <type field> - Identifies the action the system should take when a packet triggers the rule.

    - Alert - Sends an alert then logs the details about the packet that triggered the event
    - Drop – Drops the packet that triggered the event
    - Pass - Ignores the packet that triggered the event
- <protocol field> - Specifies the protocol of the packets against which the rule executes.
    - TCP - Executes against traffic using the Transmission Control Protocol
    - UDP - Executes against traffic using the User Datagram Protocol
    - ICMP - Executes against traffic using the Internet Control Message Protocol
    - IP - Executes against traffic using the Internet Protocol
- <source IP> - Specifies the source IP address or range of addresses.
    - Any - Executes against packets from any source IP.
    - Numeric IP address - Executes against packets with the specified source IP.
    - CIDR blocks - Executes against packets whose source IP address falls within the specified CIDR block.
- <source port> – Specifies the source port.
    - Any - Executes against traffic with any source port
    - Numeric - Executes against traffic with the specified source port
    - Numeric: numeric - Executes against traffic with the specified range of source ports
    - ! numeric - Executes against traffic with any source port except the port specified after the exclamation point (!)
- <operator> - Specifies the direction of the traffic to which the rule applies
    - Evaluates all traffic from the source IP to the destination IP
    - Evaluates traffic between the source IP to the destination IP
- <destination IP> - Specifies the destination IP address or range of addresses
    - Any - Executes against packets with any destination IP. For example, in the following rule, the any in bold specifies any destination IP address: alert tcp any any -> any any (rest of rule)
    - Numeric IP address - Executes against packets with the specified destination IP. For example, in the following rule, the numbers in bold specify a specific destination IP address: alert tcp any any -> 192.168.17.1 any (rest of rule)
    - CIDR blocks - Executes against packets whose destination IP address falls within the specified CIDR block. For example, in the following rule, the bracketed numbers specify a range of destination IP address: alert tcp any any -> [10.1.0.0/16,192.168.1.2/24] any (rest of rule)
- <destination port> - Specifies the destination port
    - Any - Executes against traffic with any destination port
    - Numeric - Executes against traffic with the specified destination port
    - Numeric: numeric - Executes against traffic with the specified range of destination ports
    - ! numeric - Executes against traffic with any destination port except the port specified after the exclamation point (!)

Options – defines the attributes of a packet that must be inspected to determine whether the packet is a match for a specific signature. Options are defined as a keyword and a value, and are listed as keyword:value within the options field of the signature. The Section

‘Understanding Keywords and Arguments in Rules’ in Chapter 20 of the Sourcefire 3D System User Guide lists the keywords and how to use them when writing or modifying a rule.

STATISTICAL ANALYSIS

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 (for example, SYN floods). 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.

(Virtual) 3D Sensors with IPS deployed in passive mode can detect certain kinds of rate-based attacks, while (Virtual) 3D Sensors with IPS deployed in inline mode can block such attacks.

Intrusion policies can be configured to include a rate-based filter which detects when too many matches for a rule occur in a given time period. This filter identifies excessive rule matches in traffic going to a particular destination IP address(es) or coming from a particular source IP address(es). Intrusion policies can also be configured to respond to excessive matches for a particular rule across all traffic detected by the detection engine.

A rate-based filter can be configured for any intrusion or preprocessor rule in an intrusion policy. The rate-based filter contains three components:

- The rule matching rate, which is configured as a count of rule matches within a specific number of seconds
- A new action to be taken when the rate is exceeded, with three available actions:
    - do not alert
    - alert
    - alert and drop
- The duration of the action, which is configured as a timeout value

Note that once started, the new action occurs until the timeout is reached, even if the rate falls below the configured rate during that period. When the timeout is reached, if the rate has fallen below the threshold, the action for the rule reverts to that initially configured for the rule.

Rate-based attack prevention can be configured in an inline deployment to block attacks, either temporarily or permanently. Without rate-based configuration, enabled rules generate events, but IPS does not drop packets for those rules. However, if the attack traffic matches rules that have rate-based criteria configured, the rate action can cause packet dropping to occur for the period of time that the rate action is active, even if those rules are not initially set to drop.

ID-2: 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.

7.1.6.3 ID-3: Analyzer Alarms

(IDS_RCT_EXT.1)

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.

<u>Email Alerting</u>

Email alerts are notifications of intrusion events by email. Email alerts include the following information:

- total number of alerts in the database
- last email time (the time that the system generated the last email report)
- current time (the time that the system generated the current email report)
- total number of new alerts
- number of events that matched specified email filters (if events are configured for specific rules)
- timestamp, protocol, event message, and session information (source and destination IPs and ports with traffic direction) for each event (if Summary Output is off)
  If multiple intrusion events originate from the same source IP, a note appears beneath the event that displays the number of additional events.
- number of events per destination port
- number of events per source IP

For each rule or rule group, the TOE administrators can enable or disable email alerting on intrusion events. Email alerting can be configured for any detection engine on the appliance rather than per detection engine. The email alert settings are used regardless of the policy in place for each detection engine on the sensor.

<u>Syslog Alerting</u>

The TOE can send syslog alerts, which are intrusion event notifications, to the syslog of a TOE component. The syslog allows authorized administrators to categorize information in the syslog by priority and facility. The priority reflects the severity of the alert and the facility indicates the subsystem that generated the alert. Facilities and priorities are not displayed in the actual message that appears in syslog, but are instead used to tell the system that receives the syslog message how to categorize it. Syslog messages are stored in flat files on the component’s operating system. Syslog alerts contain the following information:

- date and time of alert generation
- event message
- event data
- generator ID of the triggering event
- Snort ID of the triggering event
- revision

In an intrusion policy, the authorized administrators can turn on syslog alerting and specify the syslog priority and facility associated with intrusion event notifications in the syslog. When the policy is applied to a detection engine, the detection engine then sends syslog alerts for the intrusion events it detects to the syslog facility on the component or to a logging host (external Syslog Server) specified in the policy. The host receiving the alerts uses the facility and priority information that has been set when configuring syslog alerting to categorize the alerts.

SNMP Alerting

An SNMP trap is a network management notification. The authorized administrators can configure the sensor to send intrusion event notifications as SNMP traps, also known as SNMP alerts. Each SNMP alert includes:

- the name of the server generating the trap
- the IP address of the sensor that detected it
- the name of the detection engine that detected it
- the event data

Intrusion event response SNMP traps use the Message Digest 5 (MD5) authentication protocol and the Data Encryption Standard (DES) encryption algorithm. In addition to enabling and disabling SNMP alerting, a variety of parameters can be set depending on the version of SNMP used.

Note: Sourcefire 3D System Version 4.10.2.4 *supports SNMP v2, and v3.*

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 of 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

ID-3: Analyzer Alarms relies on an Email Server in the environment to send Email Alarms to a designated TOE administrator. Analyzer Alarms may also use an external Syslog Server and/or SNMP Trap Server to send alarms. (OE.ALARMS) ID-3 also relies on the Operational Environment to provide secure communications between the TOE and the external servers. (OE.PROTECTCOMM)

7.1.6.4 ID-4: System Data Review

(IDS_RDR_EXT.1)

Only successfully authenticated, users can access the TOE, and then only users with the Administrator Role, the Intrusion Event Analyst Role, or a Custom User Role with “Analysis &

Reporting -> IPS -> Intrusion Events" Permission can view the IDS events collected and analyzed. The data gathered is interpreted into a readable format for the authorized administrators and can then be viewed through the web-based management interfaces.

The Defense Center and Virtual Defense Center WebUI allows the authorized administrators to view and interpret the aggregation of the collected and analyzed data from multiple 3D Sensors with IPS.

7.1.6.5 ID-5: System Data Protection

(IDS_STG_EXT.1, IDS_STG_EXT.2)

The TOE protects the gathered system (event) data logs from unauthorized modification or deletion by presenting only the web-based interface to all users. No users are allowed to edit the logs; they are marked for read-only access, preventing user modification. Only users with the Administrator, Restricted Event Analyst, or Intrusion Event Analyst Roles, or a Custom User Role with the "Analysis & Reporting -> IPS -> Intrusion Events -> Modify Intrusion Events" Permission can delete the logs.

Event data log records are stored by the Defense Center, Virtual Defense Center and 3D Sensor with IPS in their corresponding MySQL database. The Virtual 3D Sensor with IPS does not store event data; rather the data is passed for storage to the sensor's managing Defense Center (or Virtual Defense Center).

To prevent loss of new/current event data, there are three mechanisms to limit event data loss: event database limit, audit record limit (refer to FAU_STG.4 "Prevention of Audit Data Loss" for more detail), and disk capacity. A user with the Administrator Role or with a Custom User Role with the "Operations -> System Policy -> Modify System Policy" Permission can set a size limit for the number of events stored in the TOE component's database. The TSF overwrites the oldest events when it reaches the defined database limit or disk size limit for the event records. This limits the number of events that can be stored in the database and allows for new event insertions. The database limits for intrusion events are 2 million for the 3D Sensors with IPS, and from 2.5 million to 100 million for the Defense Center depending on the model of the appliance. The limit is 10 million intrusion events on the Virtual Defense Center. When the disk space of the component reaches 85% of its capacity, the TSF will delete as few log files as possible to keep the space below 85% capacity. These mechanisms maintain the system disk space in order to handle the case when a flood of data comes in before overwriting can occur and always ensures that more than one event can always be added in the log.

The TOE can be configured so that users assigned to the Administrator Role will receive an email warning when the event data is automatically overwritten.

Note: The administrator must perform periodic backups of the event data (via the WebUI backup function) to prevent loss of data.

ID-5: System Data Protection relies on an Email Server in the environment to send warnings to the designated TOE administrator when the system data is overwritten. (OE.ALARMS) ID-5 also relies on the Operational Environment to provide secure communications between the TOE and the external Email Server. (OE.PROTECTCOMM)

7.2 TOE Protection against Interference and Logical Tampering

The TOE consists of both hardware (the 3D Sensor with IPS and Defense Center appliances) and software (the Sourcefire 3D System applications, the MySQL database, the Linux-derived operating system and the supporting third-party applications which are installed on the appliances and which comprise the Virtual 3D Sensor with IPS and Virtual Defense Center components).

The TOE offers only well-defined services at its network interfaces that are specifically designed to provide only the services that are necessary to enforce the TSP and not to offer additional services that might be used to interfere with the operation of the TOE.

The TOE protects the security functions it provides through a variety of mechanisms. One of the primary protections is that TOE users must authenticate before any administrative operations can be performed on the system, including creating new rules or viewing the IDS data. Access to the TOE is also protected by the access control functions of the MySQL database and the Linux-derived operating system that are part of the TOE components.

The IDS collection portion of the TOE is protected on the monitored network by “hiding” the fact it is there. This is done primarily by using a non-TCP/IP network stack on the TOE, which prevents it from being accessed as a network device on the network. In addition, the rule set is protected doubly as the system is configured to not accept any management requests or input from the monitored network.

TSF data stored in each component’s database is protected by the security mechanisms of the MySQL database. Data files and configuration files are protected by the security mechanisms of the Linux-derived operating system of each TOE component. Communications between the (Virtual) 3D Sensors with IPS and the (Virtual) Defense Center are on a protected network separate from the monitored network. All data transmitted between TOE components is protected from disclosure and modification by encryption mechanisms (OpenSSL) included in the TOE. The interfaces between TOE components can be configured to use either IPv6 or IPv4 protocol.

The TOE protects the ability to continue recording data by periodically clearing the stored logs, starting with the oldest records first. This assures there is always adequate disk space to record current and new data that has been found to match the current rule set.

The TOE also implements health policies that allow administrators to monitor the health and performance (CPU, disk, memory, temperature) of all TOE components both (Virtual) 3D Sensors with IPS and (Virtual) Defense Centers.

The 3D Sensor with IPS and Defense Center rely on the appliance hardware that is part of these components for protection. Besides the security features of the TOE itself, the Virtual 3D Sensor with IPS and Virtual Defense Center TOE components rely on the hardware of their host platform and the security features of the platform OS and VMware ESX implementation, which are part of the Operational Environment, for protection.

7.3 TOE Protection against Bypass of Security Functions

The TSF requires that all users successfully authenticate before any TSF functions (other than entering identification and authentication data) can be performed. Only the Defense Center (appliance-base and virtual) and the 3D Sensors with IPS offer web-based administrative interfaces; the Virtual 3D Sensor with IPS does not. Once a user is identified and authenticated, they are associated with a role that determines which function interfaces the TOE will offer to the user. Each user interface is defined to offer specific capabilities, all controlled by the TSF. The TSS does not offer general programming capabilities that might offer the opportunity to attempt to bypass the TSP.

Additionally, the TSF does not accept any commands from or offer any functions to the networks that are monitored by the TOE. This ensures that network entities cannot cause the TOE not to apply its TSPs to applicable network traffic.

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.

IPSs are deployed as part of an overall strategy for network defense. The customer must choose a 3D Sensor model that matches or exceeds the traffic bandwidth of the network segment it monitors. In addition, depending on the criticality of the hosts on the network segment, the sensor should be deployed with an optional fail-open network card. The fail-open card ensures that traffic continues to pass through the interfaces even if the appliance itself fails or loses power (although a few packets may be lost when the appliance is rebooted). Note that paired fail-open interfaces on the sensor’s network interface cards must be used for an inline with fail-open interface set. Virtual 3D sensors do not support inline with fail-open. In the case of wanting to block traffic if the appliance fails, then inline mode can be used rather than inline with fail-open interface sets.

The Sourcefire 3D System administrator should read [SENS-INSTALL] and/or [VIRTUAL-INSTALL] and choose the optimal sensor deployment configuration (outside the firewall, in the DMZ, or on the internal network) and sensor connection to the network (using a hub, using a span port, or using a network tap) for their network architecture and security needs.

The administrator should also understand the information in the administrative guidance in order to properly configure and manage the detection engines and interface sets of the sensors. In some circumstances, editing an interface set or detection engine can cause the detection engines on the sensor to restart, which can cause a short pause in processing. For most 3D Sensors with inline interface sets, a software bridge is automatically set up to transport packets when the sensor restarts. Although some packets are transmitted without inspection during this time, no packets are lost.

Note: For any TOE configuration, there cannot be a 100% certainty that all network packets will be analyzed by the IPS functionality of the TOE. The customer must make an informed choice of equipment and configuration that best suits their particular network configuration, traffic volume and security needs.