Fidelis XPS™ Security Target

Version 1.0
19 June 2012

Prepared for:
Fidelis Security Systems, Inc.

4416 East West Highway, Suite 310
Bethesda, Maryland 20814

Prepared By:
Science Applications International Corporation

Common Criteria Testing Laboratory

6841 Benjamin Franklin Drive
Columbia, MD 21046

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization.

The TOE is Fidelis Extrusion Prevention System®, (Fidelis XPS) ™ provided by Fidelis Security Systems, Inc. The TOE is focused on network security where TOE appliances detect inappropriate network usage based on all aspects of the network data including the content, source, destination, application, and all aspects of the communication channel. The TOE is used to prevent intrusion of attacks and to prevent the transmission of sensitive data, either as a result of an attack or insider threat. The TOE also provides tools to view and analyze the detected activity results and to issue alerts of significant events.

The Security Target contains the following additional sections:

- TOE (Section 2) – this section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Security Problem Definition (Section 3) – this section details the expectations of the environment, including the assumptions, organizational security policies, and threats that are countered by the TOE and TOE environment.
- Security Objectives (Section 4) – this section details the security objectives of the TOE and the environment.
- IT Security Requirements (Section 5) – this section presents the Security Functional Requirements (SFRs) for the TOE, and details the assurance requirements for EAL2 augmented with ALC_FLR.3.
- TOE Summary Specification (Section 6) – this section describes the security functions represented in the TOE that satisfy the security requirements.
- Protection Profile Claims (Section 7) – this section presents the Protection Profile claims and supporting rationale.
- Rationale (Section 8) – this section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – Fidelis XPS™ Security Target

ST Version – Version 1.0

ST Date – 06/19/2012

TOE Identification –

- Fidelis XPS Scout v7.0

  OR

- One or two Fidelis CommandPost™ v7.0 management console appliances and at least one of the following sensor appliances: Fidelis XPS Direct v7.0, Fidelis XPS Internal v7.0, Fidelis XPS Web v7.0, Fidelis XPS Connect v7.0, Fidelis XPS Mail v7.0, and Fidelis XPS Edge v7.0.

Some of the appliances include multiple models as listed below:

- Fidelis CommandPost, Fidelis CommandPost Plus, and Fidelis CommandPost Virtual Machine (VM)
- Fidelis XPS Scout
- Fidelis XPS Direct 1000, Fidelis XPS Direct 2500, and Fidelis XPS Direct VM
- Fidelis XPS Internal 1000, Fidelis XPS Internal 2500, and Fidelis XPS Internal VM
- Fidelis XPS Web and Fidelis XPS Web VM

- Fidelis XPS Connect and Fidelis XPS Connect VM
- Fidelis XPS Mail and Fidelis XPS Mail VM
- Fidelis XPS Edge 25 and Fidelis XPS Edge 100

TOE Developer – Fidelis Security Systems, Inc.

Evaluation Sponsor – Fidelis Security Systems, Inc.

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments, version 1.7, July 25, 2007
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 3, July 2009.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009.
    - Part 3 Conformant
    - Assurance Level: EAL 2 augmented with ALC_FLR.3

1.3 Conventions and Terminology

This section specifies the formatting information used in the Security Target.

1.3.1 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 placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b 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 and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-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: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").

  Note that operations already performed in the claimed Protection Profile are not identified in this Security Target. Rather, only those operations performed while writing the Security Target that either complete or change the meaning of requirements is identified using the conventions identified above.

- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.2 Terminology

This section identifies TOE-specific terminology and acronyms that are unique.

ACL	Access Control List
Alert	An alert is the recorded and displayed incident of an event and are generated if the alert action for an event has been configured on. Alerts are violations of extrusion policy.
AM	Application Management—TOE policy that allows enforcement of unauthorized applications such as peer-to-peer file sharing, instant messenger, access to web-based e-mail systems, etc.
CA	Certificate Authority
Channel	A channel is the envelope(s) or wrapper(s) that enables content to flow over the network. Channels include, but may also be independent of, specific ports and protocols. A channel is one classification of a fingerprint.
CommandPost™	Unique name for the Fidelis XPS management console appliance of the TOE.
Content	Output of TOE decoder sent to TOE sensor analyzers that remove protocol layers and/or file formatting, such that only the applicable data remains.
DAP	Digital Asset Protection—TOE policy that provides the capability to detect and prevent sensitive materials being leaked through the network. Attributes of the alert after fingerprint determines if a session is in violation or not.
Decoders	Decoders work on the TCP session and interpret the payload by inspection and the output is the removal of one layer of protocol or file formatting, leaving the underlying content.
DOD	Department of Defense
ECA	External Certification Authority
Event	An extrusion/intrusion rule violation. One or more events are reported as an alert if the rule action is configured to alert.
Fidelis XPS	Fidelis Extrusion Prevention System
Fingerprint	The description of a specific kind of data based on particular characteristics. Fingerprints define either the ‘content’ within a transmission, the communication ‘channel’ of the transmission, or the sender or receiver of the transmission (e.g., ‘location’).
GUI	Graphical User Interface
ICAP	Internet Content Adaptation Protocol
Identity Profile	A fingerprint used to define personal identity information. The definition utilizes a statistical algorithm along with built-in data validation.
KEA	Key Exchange Algorithm
LDAP	Lightweight Directory Access Protocol
MTA	Mail Transfer Agent
ORC	Operational Research Consultants, Inc.

PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
Policy	TOE extrusion/intrusion policies are comprised of one or more rules, which in turn, contain one or more fingerprint definitions.
RSA	Rivest, Shamir, Adleman
Rule	A TOE rule is a logical combination of fingerprints that together are used by the TOE's event manager to generate alerts based on matches on combinations of fingerprints.
Sensor	Refers to the Fidelis XPS Direct, Fidelis XPS Internal, Fidelis XPS Connect, Fidelis XPS Web, Fidelis XPS Edge, and Fidelis XPS Mail appliances (hardware or virtual) running the Fidelis XPS software.
UT	Unauthorized Traffic—TOE policy that detects and prevents protected network users from circumventing corporate security measures by using unauthorized proxies, defeating firewall rules and/or using unauthorized encryption methods.
VM	Virtual Machine
WinSCP	Windows Secure Copy – used for secure file transfer between a local and a remote computer.

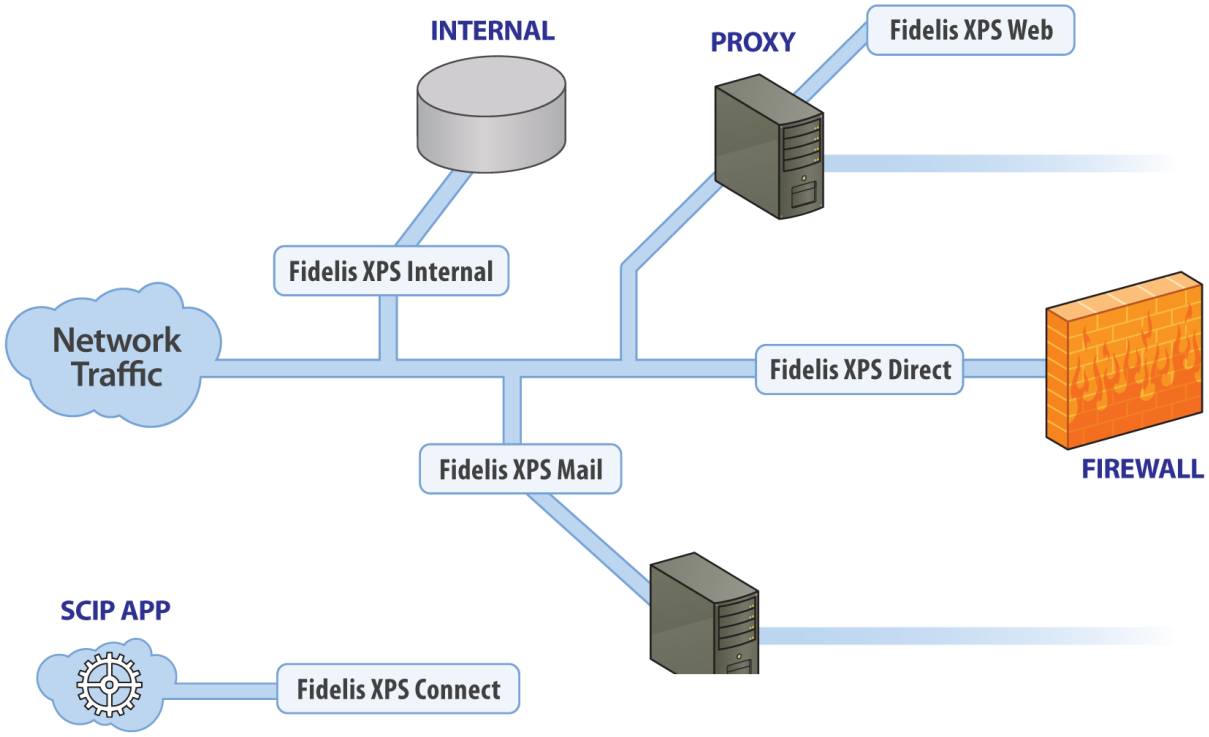
2. TOE Overview

The Target of Evaluation (TOE) is a combination of Fidelis XPS™ version 7.0 (v7.0) appliances. More specifically, the TOE consists of a Fidelis XPS v7.0 management console and one or more network sensors. The Fidelis XPS Scout appliance combines a CommandPost management console and Direct network sensor in a single laptop form-factor appliance and as such is a stand-alone instance of the TOE all by itself. Alternately, the TOE consists of a Fidelis CommandPost appliance combined with one or more of the available Fidelis XPS v7.0 network sensor appliances: Fidelis XPS Direct, Fidelis XPS Internal, Fidelis XPS Web, Fidelis XPS Connect, Fidelis XPS Mail, and Fidelis XPS Edge.

With the exception of the Fidelis XPS Scout appliance (available only in hardware), each appliance is available either as a hardware appliance or as a virtual machine (VM) appliance as identified in section 1.1. The hardware appliances are stand-alone devices ready to be plugged into the target network. The VM appliances are VMWare vSphere images ready to run (i.e., already installed and ready to start) in an environment providing VMWare vSphere with suitable connections to the target network. A Fidelis XPS system can be deployed entirely as hardware appliances, VM appliances, or a mixture, so long as there is a CommandPost and at least one sensor.

Each Fidelis XPS appliance (hardware or VM) includes a hardened CentOS 5 Linux kernel version 2.6.18-194.3.1.el5 or CentOS 4 Linux kernel version 2.6.9-89.0.23.ELsmp, MySQL 5.1.46 Enterprise Version, and custom Fidelis XPS applications.

The CommandPost is available in three models: CommandPost (supports 1-5 sensors), CommandPost Plus (supports 6 or more sensors), and CommandPost VM. Except in the case of the Fidelis XPS Scout (which is a combination of a CommandPost and a Direct sensor), a CommandPost is required when using any of the TOE sensors. Each CommandPost has the same security features, differing only in their sensor capacity and form of deployment (hardware or VM).



In the case of Fidelis XPS Sensors, several options are available to address a wide variety of network architectures (including both IPv4 and IPv6). Each appliance type id designed to monitor specific types of network traffic. The differences in the models for a given appliance type involve data rate capacities and form of deployment (hardware or VM), but each of the models for a given appliance type has the same security features.

- The Fidelis XPS Direct sensor monitors and enforces extrusion/intrusion policies across all 65,535 Internet Protocol (IP) ports on the network. This sensor is normally placed art the border of a protected network and is optimized to process lots of relatively short-lived connections.
- The Fidelis XPS Internal sensor is similar to Direct, but supports protocols typically seen only inside the network include Oracle and DB2 database access, SMB/CIFS/SAMBA file transfers, and directory queries. This sensor is normally placed within a protected network and is optimized to process a relatively small number of longer duration sessions (e.g., SMB) and is also capable of decoding the content of some protocols such as LDAP and SMB.
- The Fidelis XPS Web sensor monitors and enforces policy for traffic flowing through ICAP-enabled proxy servers
- The Fidelis XPS Mail sensor monitors and enforces policy for Simple Mail Transfer Protocol (SMTP) e-mail traffic.
- The Fidelis XPS Connect sensor facilitates business-critical content awareness to enforce policy-based decisions regarding storage, transfer, or movement of enterprise data.
- The Fidelis XPS Edge sensor combines the Direct and Web sensing capabilities into a single appliance.

Note that hereinafter, the Fidelis XPS sensor appliance identification will not include the specific type (Direct, Internal, Web, Mail, Connect, Edge), unless that has a direct impact on the specific Sensor functionality. Further, the Fidelis XPS sensor(s) may also be referred to as just sensor(s), where all references pertain to the same TOE component providing this functionality.

The Fidelis XPS sensors are used to monitor, capture, and examine network traffic sending pertinent findings and other data to the CommandPost which is used to manage its associated Fidelis XPS sensors and to further analyze the information received from those sensors. In most cases the TOE would be deployed as a single CommandPost associated with one or more sensors. However, two CommandPosts can be deployed in a redundant manner.

The CommandPost is accessed via a web browser to enable authorized administrators to configure policies and review audit and analyze results. The workstation that authorized administrators use to access the CommandPost is sometimes referred to as a Client; however, the claimed security functions are provided by the CommandPost and Fidelis XPS sensor appliances. When redundant CommandPosts are deployed, administrators can access either one to configure the CommandPost or attached sensors. Note that at any given time only one of the CommandPosts can be configured to be 'active' and network results will only be available on the CommandPost which was active at the time of the event.

2.1 TOE Description

The TOE is designed to monitor network traffic for malicious content coming into the network (intrusion) and for sensitive and secure data leaving the network (extrusion). It is designed to operate continuously, observing network traffic as it is perceived on the attached networks. Traffic observed by a Fidelis XPS sensor is reassembled into sessions; protocols are identified; applications are identified; and, contents are analyzed in order to determine whether they contain anything inappropriate based on the applicable (intrusion/extrusion) policy rules. When inappropriate content is identified, the sensor takes action, as defined by the rule which was violated. Actions include alert, prevent, throttle, information flow map (i.e., update an information flow map with the occurrence), quarantine, reroute, notify sender, append message, and X-header modification. Additionally, packets can be captured in a .pcap file. A rule may invoke several actions for a single violation.

The Fidelis XPS sensor software is designed around a series of layers where the first layer receives packets from the attached networks. Unless these packets belong to a session that has already been marked for prevention by the sensor, they would be sent to the next layer for further analysis. The next layer performs session reassembly, organizing the network traffic into streams and then forwards the stream pointer to the next layer where the payload is decoded. This layer identifies protocols and applications and ultimately reveals the contents. Authorized administrators configure policies that delineate exactly what the TOE will capture, analyze and monitor. Once the content is identified, the next layer is invoked to apply a set of rules (e.g., string searches, regular expressions, etc.). These rules can combine content patterns and other attributes (e.g., protocol or application) to form either specific or generic rules. When the rules indicate a violation, the sensor performs the action identified by the rule.

The Fidelis XPS Direct and Internal sensor appliances operate directly on Ethernet packets received from the wire. Packets are reassembled into TCP or UDP sessions and analyzed. The Direct and Internal modules can take alert, prevent, throttle, packet capture and information flow map actions. Prevention is performed by dropping packets (if installed inline) and sending TCP reset packets to the source of the session. Throttling can only be performed when installed inline and is performed by randomly dropping packets and manipulating the TCP window size until the bandwidth is below the configured value.

The Fidelis XPS Web module utilizes the standard Internet Content Adaptation Protocol (ICAP) to receive information from a web proxy server. Received packets are stripped of the ICAP layer and reassembled into application sessions, ready for the protocol decoding layer of software. The Web module can take alert and prevent actions. Prevention is performed by instructing the web-proxy server to drop the session and either diverts the user's browser to a standard Error 403 (Forbidden) HTTP page or to a customized security violation page provided by the operating environment.

The Fidelis XPS Mail module processes e-mail and can act as a Mail Transfer Agent (MTA) or utilize the milter protocol to receive messages from an external MTA. In this either case, received traffic is handled by the milter protocol layer which will reassemble the email session and forward to the next layer for protocol decoding. When the Fidelis XPS Mail sensor is running as an MTA, the e-mail handler is embedded on the appliance utilizing Postfix. The Mail module can take alert, prevent, quarantine, reroute, notify sender, append message, and X-header modification actions. Prevention is performed by dropping the incoming email message. Quarantine is performed by storing the message locally on the sensor until an authorized administrator reviews the message and decides to discard or forward the message.

The Fidelis XPS Connect module is designed to analyze content received from another network device or application via Simple Content Inspection Protocol (SCIP). The Connect module receives content and performs payload decoding and responds to the originating network device with an action of alert or prevent. The originating network device performs the action.

The evaluated configuration of the TOE includes several operational modes that provide full prevention capabilities. The mode of operation is determined and configured by an authorized administrator during initial setup of the TOE on the monitored network. Supported modes of operation include:

- **Fidelis XPS Direct/Internal sensor out-of-band**: When connected via network tap the sensor implements content-based prevention without requiring an inline network device. All network traffic is passed to the Fidelis XPS Sensor through a network tap and prevention is achieved by injecting TCP reset packets that instruct the sender and recipient to reset the network connection.
- **Fidelis XPS Direct/Internal sensor inline**: when inline, a sensor sits in the network path with all network traffic flowing directly through it where prevention is achieved by dropping any packet or transfer that violates configured polices and/or sends TCP reset packets.
- **Fidelis XPS Web sensor**: when connected to a third party proxy appliance the sensor will provide content inspection. All actions are carried out by the proxy appliance based on response from the sensor. The sensor can be configured to terminate violating sessions or to redirect the user to an error page. On termination, the user will see an Error 403 (Forbidden) on their browser. On redirect, the user will see a web page informing them that their action was blocked by policy. The redirect page can be customized by an authorized administrator.
- **Fidelis XPS Mail sensor inline**: When connected inline the sensor acts as a MTA. E-mail can be blocked, quarantined, or re-directed. In addition, the system can be configured to notify the user, via e-mail and to append a message to the e-mail when forwarded. The messages for user notification and for appending can be customized by the network operator. When connected inline, all quarantined e-mail is stored on the sensor and can be managed via CommandPost.
- **Fidelis XPS Mail sensor out-of-band**: When connected out of band the sensor serves as a content inspection agent to a third party MTA. Communication between the MTA and sensor utilizes the milter protocol. All actions are the same as the corresponding sensor inline configuration, however, quarantined e-mail is held by the third party MTA in the operating environment and must be managed by its quarantine interface. CommandPost cannot be used for quarantine management in this case.
- **Fidelis XPS Connect sensor**: when connected to an applicable device or application the sensor receives data over the network using the Fidelis Simple Content Inspection Protocol (SCIP). Received content is analyzed and the action is returned using SCIP. Connect operates with a third party application which is responsible to execute the specified action..

The CommandPost interacts with authorized administrators via a web browser where the Open Secure Sockets Layer (OpenSSL) is used to implement Transport Layer Security (TLS) to secure the underlying communications. Similarly, the CommandPost uses TLS/OpenSSL to interact with its associated Sensors for the purposes of configuring the sensors and receiving information back from the sensors.

The TOE provides several system functions that are controlled by an access privilege per user where a role is a collection of these functions. The levels of access are determined for TOE features such as alerts, quarantine, policies, Fidelis XPS appliance configuration and user management. CommandPost includes several predefined roles as well as the ability to create custom roles to meet special customer access requirements.

The TOE requires a third-party DOD-approved External Certificate Authority (CA) in the operating environment to provide Public Key Infrastructure (PKI) functionality where CA certificates can be imported into the TOE in order to provide additional protection of the TOE Security Functions (TSF). The evaluated configuration of the TOE requires CA certificates to be imported into the TOE from the environment, as this additional functionality is not being provided by the TOE; however, the TOE uses the PKI interface provided for this.

2.2 TOE Architecture

The section describes the TOE physical and logical boundaries.

2.2.1 Physical Boundaries

As explained above a given Fidelis XPS configuration includes either a single Fidelis XPS Scout appliance or one or two CommandPost appliances combined with one or more Fidelis XPS sensor appliances. Each Fidelis XPS appliance is a self-contained hardware appliance device or VM image designed to interact with its environment via network connections (real or virtual).

The following sub-sections identify the specific operating environment components required for the operation of the TOE.

2.2.1.1 Certificate Authority (CA)

The TOE requires a CA in the operating environment for Public Key Infrastructure (PKI) X.509 certificate importation into the TOE. The External CA must be DOD-approved for government environments (i.e., Operational Research Consultants, Inc. (ORC), VeriSign, Inc., or IdenTrust, Inc.).

2.2.1.2 Software Requirements

In order for the CommandPost Client to connect via web-based, remote access, the following software is required on the client machine(s):

- Browser: Microsoft Internet Explorer version 7or later; Firefox versions 1 or later
- Adobe Flash Player version 10 or later
- Secure FTP client: WinSCP

The virtual (VM) appliances require a licensed copy of VMWare vSphere 4 (or later) operating with CPUs (at least 2 virtual CPUs), memory (at least 2GB), and virtual network support (at least one virtual network interface) as required for the specific appliance model.

In addition, if the optional external authentication methods are to be used the operational environment must provide an LDAP server, Active Directory, or smart card support. In the case of LDAP and Active Directory, the server must support the standard LDAP protocol. In the case of smart card support, since they are being read by client workstations, the TOE has no specific requirements other than the applicable certificates must be based on standard PKI standards.

2.2.1.3 Additional Hardware Requirements

Network Taps—required for lossless network monitoring by Fidelis XPS Direct (including Scout and Edge) and Internal sensors in an out-of-band deployment. A network tap will replicate all network traffic with no data loss or performance degradation. Network taps guarantee complete traffic replication.

SPAN Ports—connecting the Fidelis XPS Direct (including Scout and Edge) or Internal sensors to the SPAN ports on the router or switch can be done, but unlike Network Taps do not guarantee complete traffic replication and/or processing of all data due to traffic volumes. While they can be used, they are not recommended since the applicable network router or other device support SPAN ports generally treat SPAN ports with low priority and may not send all packets when under load.

Proxy appliance— required for connecting the Fidelis XPS Web (including Edge) sensor to analyze proxied traffic.

Mail Transfer Agent (MTA)—required for connecting the Fidelis XPS Mail sensor to analyze e-mail in the operating environment in an out-of-band deployment. The MTA is only required if the Fidelis XPS Mail sensor is connected out-of-band where the Fidelis XPS Mail sensor serves as a content inspection agent to a third party MTA. When the Fidelis XPS Mail sensor is connected inline, it acts as an MTA and thus an external MTA is not required.

The TOE supports e-mail, syslog, and SNMP (versions 1, 2c, and 3) alerting when an e-mail server, SNMP server, and/or other applicable third party products (e.g., ArcSight, IBM SiteProtector, Verdasys Digital Guardian) are available.

2.2.2 Logical Boundaries

This section summarizes the security functions provided by Fidelis XPS that are evident at the various network interfaces described above:

- Security Audit
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functions
- TOE access
- Intrusion Detection System

Note that some of the Fidelis appliances include an Integrated Management Module (IMM) designed to be utilized for remote monitoring. The IMM is a hardware module unrelated to the Fidelis functional software but can serve to effectively bypass some of those security functions. As a result, the IMM is out of scope of the evaluated configuration and its available connections should not be used (i.e., connected).

Similarly, each device is configured with a reserved Fidelis account that is used primarily for installation and troubleshooting when necessary. This account is not used to manage the TOE security functions once the TOE is operational and as such it is assumed the applicable password will be protected and use of that account is excluded from the scope of evaluation.

2.2.2.1 Security Audit

The TOE generates an audit record of security-relevant events that includes the date/time of event, user identity, and success or failure of the action. In addition, specific audit events are captured and those with specific details are associated with audit data as well. Auditable events can be included or excluded from the set of stored audit records based on event type. TOE audit records are stored on the CommandPost component in a MySQL data repository and audit data loss is mitigated by overwriting the oldest stored audit records if the audit trail is full. Only authorized administrators with audit read privilege are able to sort, review and interpret the results.

2.2.2.2 Identification and Authentication

Only the CommandPost provides an interactive user interface and it requires that all users are identified and authenticated before access is allowed to access any available functions or data. The CommandPost provides support for both local and remote authentication mechanisms to support user authentication. The CommandPost locally maintains user accounts that consist of the user identity (username), authentication data (password), authorizations (roles, alert management groups, and sensors).

Optionally, the TOE can be configured to make use of available LDAP, Active Directory or single-sign on smart card solutions in the operational environment to authenticate users.

Note that sensors are initially configured using directly attached keyboard and monitor, but once configured are managed and otherwise used via the CommandPost (i.e., there is no direct user interface that might require identification or authentication in normal operating situations).

2.2.2.3 Security Management

The CommandPost is accessed via its web-based Graphical User Interface (GUI) that provides the interface to manage the Fidelis XPS sensors. All users of the TOE are considered to be administrators. The CommandPost includes one default user (named admin) with full system control. Through the admin account, other users can be created with full or restricted access. The TOE Security Functions (TSF) restrict the ability to manage the functions of the system based on the user's role, the user's assigned alert management group(s), and the user's assigned sensor(s).

There are several defined functions of the system: Alert Management, Alert Details which include all information collected by the sensor, Quarantine Management, Alert Issue Tracking, Alert Reporting, Policy Authoring, User Management, Sensor Configuration, CommandPost Configuration, and Audit. The user's role defines the access level (either full control access, view-only access, or no access) per system function.

CommandPost is delivered with three primary pre-built roles: Network Administrators who are responsible for configuration of CommandPost and sensor appliances; Policy Authors who create policies and install them on sensors; and Alert Managers who manage alerts and quarantined e-mail generated by sensors. The system also includes a supervisor version of each role, which can create new users with equal or less access privileges as themselves. In addition, CommandPost pre-defined roles include System Administrator (with complete system access (e.g., full control)) and No Role (with no system access (e.g., no access)).

Alert Management Groups are provided to restrict access to alerts based on the content of the alert, as defined by the rule that was violated. Each rule is configured with an Alert Management Group. Only users that belong to this group may view the alert. Once viewed by an authenticated user with proper alert management privilege, the alert may be moved to a different group.

Users are also restricted by the sensor(s) to which they are assigned. For example, Network Administrators may only administer their assigned sensors; Policy Authors may only install policies to their assigned sensors; and Alert Managers may only view alerts generated by their assigned sensors.

Note that the CommandPost uses support from its embedded operating system to present a Secure Shell (SSH) interface along with the web-based GUI interface. Authorized CommandPost users can login using locally defined login credentials for the purpose of copying policy files and testing purposes. This interface can also be used to copy software upgrade packages to the TOE. Root login using this interface is disabled.

2.2.2.4 Protection of the TOE Security Functions

The packets passing between the CommandPost and Fidelis XPS Sensors are protected using FIPS 140-2 certified OpenSSL Version 0.9.8r utilizing the OpenSSL FIPS Object Module Software Version 1.2.3 (FIPS certificate 1051) data encryption and decryption over TLS, Version 1.0 such that all data is protected from disclosure and modification.

The sensors monitor network traffic and send the information to their registered CommandPost. Each TOE appliance provides protection from outside attacks by being self-contained devices that only provide TOE functionality. Only authorized administrators may access TOE security functions once properly identified and authenticated. Additionally, the TOE appliances provide a reliable time stamp for security audit generation as well as collected system data events.

In cases where the TOE modules are deployed as VM instances, the operational environment must supply the time stamp to the TOE. The evaluation configuration of the TOE does not support any additional software to be installed on the appliance devices.

All TOE appliances support NTP and can be configured to utilize a common NTP server in order to ensure that their clocks are synchronized.

2.2.2.5 TOE access

The TOE terminates any browser session between the web-based interface and the CommandPost after an authorized administrator configurable time-period of inactivity (the default is 15 minutes), possibly including a value of ‘never’. Once a session has been terminated the TOE requires the user to re-login to establish a new session.

2.2.2.6 Extrusion and Intrusion Detection

The TOE uses a set of rules to inspect (e.g., sense via the Fidelis XPS sensor) incoming and outgoing network traffic and collect network data based on potentially inappropriate content detected per the configured rules. The TOE contains a set of default intrusion and extrusion rules/policies and allows an authorized administrator to customize the rules and policies as necessary for their environment.

The TOE analyzes the collected data and reacts to identified policy violations. The TOE provides network data collection and restricted data review by an authorized administrator. Further, the TOE provides guarantee of system data availability and prevention of system data loss by overwriting the oldest data logged. Collected data is stored and protected within the MySQL data repository on the CommandPost.

2.3 TOE Documentation

Fidelis Security Systems offers a series of documents that describe the installation process for the TOE, as well as guidance for subsequent use and administration of the system security features.

3. Security Problem Definition

The TOE security environment describes the security aspects of the intended environment in which the TOE is to be used and the manner in which it is expected to be employed. The statement of the TOE security environment defines the following:

1. Organizational Policies that the TOE and the environment of the TOE fulfill
2. Threats that the TOE and the environment of the TOE counter
3. Assumptions made about the operational environment and the intended method of use for the TOE.

Furthermore, the TOE is intended to be used in environments where the relative assurance that its security functions are enforced is commensurate with EAL 2 augmented with ALC_FLR.3 as defined in the CC.

The security environment statements have been drawn from a validated Protection profile (U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007 – IDSSPP). However, they have been modified in some cases to reflect both extrusion and intrusion issues. Note that the TOE is both an extrusion prevention system (XPS) and an intrusion detection system (IDS) and therefore addresses a broader security problem than that found in the IDSSPP.

3.1 Organizational Policies

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

3.2 Threats

T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS **or XPS** data received from all data sources.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS **or XPS** data received from each data source.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions **or extrusions** to go undetected.
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

3.3 Assumptions

A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be accessed by authorized users.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

4. Security Objectives

The following subsections describe objectives for the TOE and its environment that correspond to with the security problems described in the previous section. Note that the identified security objectives have been derived from the IDSSPP. However, they have been modified in some cases to reflect both extrusion and intrusion issues. Note that the TOE is both an extrusion prevention system (XPS) and an intrusion detection system (IDS) and therefore addresses a broader security problem than that found in the IDSSPP.

4.1 Security Objectives for the TOE

O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.AUDIT_PROTECTION	The TOE will provide the capability to protect audit information.
O.AUDIT_SORT	The TOE will provide the capability to sort the audit information.
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDANLZ	The Analyzer must accept data from IDS **and XPS** Sensors and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
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 **and XPS**.
O.INTEGR	The TOE must ensure the integrity of all audit and System data.
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows.
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.TIME	The TOE will provide reliable timestamps to the TOE.

4.2 Security Objectives for the Environment

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.
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.
OE.INTROP	The TOE is interoperable with the IT System it monitors.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
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.

5. IT Security Requirements

The requirements for the TOE have primarily been drawn from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments (IDSSPP) with some changes and additions to update them to Common Criteria version 3.1 revision 3 and to reflect extrusion prevention and other pertinent capabilities of the TOE.

5.1 Extended Components Definition

The only extended requirements used in this Security Target are drawn from the IDSSPP and as such no additional rationale is provided herein.

5.2 TOE Security Functional Requirements

The following table describes the SFRs that are satisfied by Fidelis XPS.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1: Audit Data Generation
	FAU_SAR.1: Audit Review
	FAU_SAR.2: Restricted Audit Review
	FAU_SAR.3: Selectable Audit Review
	FAU_SEL.1: Selective Audit
	FAU_STG.2: Guarantees of Audit Data Availability
	FAU_STG.4: Prevention of Audit Data Loss
FIA: Identification and Authentication	FIA_ATD.1: User Attribute Definition
	FIA_UAU.2: User authentication before any action
	FIA_UAU.5: Multiple authentication mechanisms
	FIA_UID.2: User identification before any action
FMT: Security Management	FMT_MOF.1: Management of Security Functions Behaviour
	FMT_MTD.1: Management of TSF Data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security Roles
FPT: Protection of the TOE Security Functions	FPT_ITT.1: Basic internal TSF data transfer protection
	FPT_STM.1: Reliable time stamps
FTA: TOE access	FTA_SSL.3: TSF-initiated termination
IDS: Intrusion Detection System *Note: While the IDS PP defines a family of requirements entitled "Intrusion Detection System", those requirements are equally suitable to Extrusion Prevention Systems.*	IDS_ANL.1: Analyser analysis (EXT)
	IDS_RCT.1: Analyser react (EXT)
	IDS_RDR.1: Restricted Data Review (EXT)
	IDS_SDC.1: System Data Collection (EXT)
	IDS_STG.1: Guarantee of System Data Availability (EXT)
	IDS_STG.2: Prevention of System data loss (EXT)

Table 1 TOE Security Functional Components

5.2.1 Security Audit (FAU)

5.2.1.1 Audit Data Generation (FAU_GEN.1)

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.

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 (if applicable), 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 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 IDs, 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	
FIA_UAU. 2	All use of the authentication mechanism	User identity, location
FIA_UAU.5	**The result of each activated mechanism together with the final decision**	
FIA_UID.2	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behaviour of the functions of the TSF	
FMT_SMF.1	**Use of the management functions.**	**User identity**
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity
FTA_SSL.3	**Termination of an interactive session by the session locking mechanism**	

Table 2 Auditable Events

5.2.1.2 Audit Review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide **[users]** with the capability to read **[all audit data that the user is explicitly authorized to view]** 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.

Application Note: *Users that have a role with View Only or Full Control access to the Audit function (i.e., Audit privilege) can read all audit data.*

5.2.1.3 Restricted Audit Review (FAU_SAR.2)

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

5.2.1.4 Selectable Audit Review (FAU_SAR.3)

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

5.2.1.5 Selective Audit (FAU_SEL.1)

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes: a) event type; b) **[no additional attributes]**.

5.2.1.6 Guarantees of Audit Data Availability (FAU_STG.2)

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorised deletion.
FAU_STG.2.2 The TSF shall be able to **prevent** ~~detect~~ unauthorised modifications to the stored audit records in the audit trail.
FAU_STG.2.3 The TSF shall ensure that **[the most recent, limited by available storage space]** stored audit records will be maintained when the following conditions occur: **[*audit storage exhaustion*]**.

5.2.1.7 Prevention of Audit Data Loss (FAU_STG.4)

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

5.2.2 Identification and Authentication (FIA)

5.2.2.1 User Attribute Definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: a) User identity; b) Authentication data; c) Authorisations; and d) **[no other security attributes]**.

Application Note: *'Authorisations' consist of roles (which in turn are associated with access privileges), alert management group assignments, and sensor assignments.*

5.2.2.2 User authentication before any action (FIA_UAU.2)

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.2.3 Multiple authentication mechanisms (FIA_UAU.5)

FIA_UAU.5.1 The TSF shall provide **[local and remote authentication mechanisms]** to support user authentication.
FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**following rules:**

1. **If configured, LDAP or Active Directory authentication mechanism shall be used for users to access the TOE – the TOE then accepts or rejects the user authentication based upon the response from LDAP or Active Directory before allowing any other TSF-mediated actions on behalf of that user;**
2. **If LDAP or Active Directory is not configured as the authentication method, the TOE shall perform identification and authentication before allowing any other TSF-mediated actions on behalf of that user**].

5.2.2.4 User identification before any action (FIA_UID.2)

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.2.3 Security Management (FMT)

5.2.3.1 Management of Security Functions Behaviour (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behaviour of the functions of System data collection, analysis and reaction to authorised System administrators.

Application Note: While the IDSSPP term 'authorised System administrator' can apply to essentially any pre-defined or customer-defined administrator role, only those users with the correct combination of access privileges granted via role assignment, alert management group assignments, and sensor assignments can perform the corresponding functions.

5.2.3.2 Management of TSF Data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to query and add System and audit data, and shall restrict the ability to query and modify all other TOE data to **[System Administrators and other users explicitly granted the corresponding access based on role, alert management group assignment, and sensor assignment].**

Application Note: There are pre-defined roles that could be identified here, but given the relative complexity of the pre-defined role definitions and also the option for customers to define their own custom roles this requirement has been kept intentionally simple. Users with the System Administrator role can perform all functions and access all data, otherwise the user must have the right combination of access privileges granted via role assignment and, where applicable, alert management group and sensor assignments in order to perform functions and access data.

5.2.3.3 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **[manage audit functions; manage users and their security attributes; manage alert reports; manage functions related to System data collection, analysis and reaction; management of the authentication mechanisms and rules for authentication; management of the session timeout value]**.

5.2.3.4 Security Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles authorised administrator, authorised System administrators, and **[System Administrator, Network Admin, Network Admin Supervisor, Policy Author, Policy Author Supervisor, Alert Manager, Alert Manager Supervisor, No Role, and customer-defined roles]**.

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

Application Note: Fidelis XPS has eight pre-defined administrative roles, listed above, along with the potential for additional customer-defined roles. The IDSSPP identifies two required roles: authorized administrator and authorized System administrators. The former is designed to represent highly privileged users that might operate outside the constraints of the TOE installation, direct access to the TOE applications and databases, etc.), while the latter is designed to represent privileged users performing security management functions in the context of and under the control of the TOE (i.e., to manage and access IDS functions and data). As such, depending on the nature of the TOE these roles can overlap (such as in the case of appliances). The Fidelis XPS 'System Administrator' role corresponds with the IDSSPP roles: 'authorised administrator' and 'authorised System administrators' since it provides unrestricted access to all available functions. The Fidelis XPS 'Network Admin', 'Policy Author', and 'Alert Manager' roles corresponds with the IDSSPP role: 'authorized System administrators' since they are primarily designed to perform security management functions in the TOE. Furthermore, customer-defined roles could correspond with 'authorised administrator' and/or 'authorised System administrator' depending on how they are defined by the customer.

5.2.4 Protection of the TOE Security Functions (FPT)

5.2.4.1 Basic internal TSF data transfer protection (FPT_ITT.1)

FPT_ITT.1.1 The TSF shall protect TSF data from **[*disclosure, modification*]** when it is transmitted between separate parts of the TOE.

5.2.4.2 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.2.5 TOE access (FTA)

5.2.5.1 TSF-initiated termination (FTA_SSL.3)

FTA_SSL.3.1 The TSF shall terminate an interactive session after a**n [administrator configurable period of time of inactivity]**.

5.2.6 **Extrusion and** Intrusion Detection System (IDS)

5.2.6.1 Analyser analysis (EXT) (IDS_ANL.1)

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all ~~IDS~~**System** data received: a) **[*signature*]**; and b) **[any combination of:**

- **Content Analysis by:**
  - **Identity profiling;**
  - **Binary profiling;**
  - **Embedded images;**
  - **Encrypted files;**
  - **Exact content (via MD5 signature);**
  - **Partial content;**
  - **File signature;**
  - **File names;**
  - **Keyword;**
  - **Keyword list;**
  - **Keyword sequence;**
  - **Protocol signature;**
  - **Regular expression;**
- **Channel Analysis;**
- **Location Analysis by:**
  - **IP Address;**
  - **LDAP/Active Directory Attributes;**
  - **Source or Destination country;**
  - **Reputational analysis]**. (EXT)

IDS_ANL.1.2 The System 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**) [alert number; Alert priority; Alert rule, policy, and the true/false result of all fingerprints in the rule; Time and date of alert; Whether a TCP session was recorded by the TOE; Sensor that identified the alert; Alert summary or rule used in detecting alert; Attributes of the alert from TOE decoders; Protocol on which alert occurred; Action taken by the sensor; Source address; Destination address; Source and Destination TCP port, if applicable; Service; IP layer information; Country where source and destination IP address are registered; PCAP file of network data, if chosen by the rule; Recorded object, as appropriate for the sensor type; and Forensic data for the alert]**. (EXT)

5.2.6.2 Analyser react (EXT) (IDS_RCT.1)

IDS_RCT.1.1 The System shall send an alarm to **[CommandPost and users or third party management systems configured to receive alarms]** and take **[one or more of the following actions per violated rule: prevent data transmission, throttle session, quarantine, add information flow map, reroute, or (only in the case of mail) append e-mail, add an X-header, or notify sending user]** when an intrusion **or extrusion** is detected. (EXT)

5.2.6.3 Restricted Data Review (EXT) (IDS_RDR.1)

IDS_RDR.1.1 The System shall provide **[users]** with the capability to read **[all System data that the user is explicitly authorized to view]** from the System data. (EXT)

IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information. (EXT)

Application Note: Users that have been granted explicit access via access privileges associated with their role, alert group membership, and sensor assignment access to System data via the associated available functions.

IDS_RDR.1.3 The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access. (EXT)

5.2.6.4 System Data Collection (EXT) (IDS_SDC.1)

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s): a) **[*network traffic*]**; and b) **[no other specifically defined events]**. (EXT)

IDS_SDC.1.2 At a minimum, the System 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 3 System Events. (EXT)

Component	Event	Details
IDS_SDC.1	Network traffic	Protocol, source address, destination address

Table 3 System Events

5.2.6.5 Guarantee of System Data Availability (EXT) (IDS_STG.1)

IDS_STG.1.1 The System shall protect the stored System data from unauthorised deletion. (EXT)

IDS_STG.1.2 The System shall protect the stored System data from modification. (EXT)

IDS_STG.1.3 The System shall ensure that **[the most recent, limited by available storage space]** System data will be maintained when the following conditions occur: **[*System data storage exhaustion*]**. (EXT)

5.2.6.6 Prevention of System data loss (EXT) (IDS_STG.2)

IDS_STG.2.1 The System shall **[*overwrite the oldest stored System data*]** and send an alarm if the storage capacity has been reached. (EXT)

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 augmented with ALC_FLR.3 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.2: Security-enforcing functional specification
	ADV_TDS.1: Basic design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: 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.3: Systematic flaw remediation
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis

Table 4 EAL 2 augmented with ALC_FLR.3 Assurance Components

5.3.1 Development (ADV)

5.3.1.1 Security architecture description (ADV_ARC.1)

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

5.3.1.2 Security-enforcing functional specification (ADV_FSP.2)

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.
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 each SFR-enforcing TSFI, 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.
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.

5.3.1.3 Basic design (ADV_TDS.1)

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.
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 behaviour 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 summarise the SFR-enforcing behaviour 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 TSFIs trace to the behaviour described in the TOE design that they invoke.
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.

5.3.2 Guidance documents (AGD)

5.3.2.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1d The developer shall provide operational user guidance.
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 fulfil 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.
AGD_OPE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Preparative procedures (AGD_PRE.1)

AGD_PRE.1.1d The developer shall provide the TOE including its preparative procedures.
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.
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.

5.3.3 Life-cycle support (ALC)

5.3.3.1 Use of a CM system (ALC_CMC.2)

ALC_CMC.2.1d 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.
ALC_CMC.2.1c The TOE shall be labelled with its unique reference.

ALC_CMC.2.2c The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.2.3c The CM system shall uniquely identify all configuration items.
ALC_CMC.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.2 Parts of the TOE CM coverage (ALC_CMS.2)

ALC_CMS.2.1d The developer shall provide a configuration list for the TOE.
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.
ALC_CMS.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.3 Delivery procedures (ALC_DEL.1)

ALC_DEL.1.1d The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.
ALC_DEL.1.2d The developer shall use the delivery procedures.
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.
ALC_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.4 Systematic flaw remediation (ALC_FLR.3)

ALC_FLR.3.1d The developer shall document and provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.3.2d 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.3.3d The developer shall provide flaw remediation guidance addressed to TOE users.
ALC_FLR.3.1c The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.3.2c 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.3.3c The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.3.4c 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.3.5c 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.3.6c The flaw remediation procedures shall include a procedure requiring timely response and the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.
ALC_FLR.3.7c 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.3.8c 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.3.9c The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.
ALC_FLR.3.10c The flaw remediation guidance shall describe a means by which TOE users may register with the developer, to be eligible to receive security flaw reports and corrections.
ALC_FLR.3.11c The flaw remediation guidance shall identify the specific points of contact for all reports and enquiries about security issues involving the TOE.

ALC_FLR.3.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Tests (ATE)

5.3.4.1 Evidence of coverage (ATE_COV.1)

ATE_COV.1.1d The developer shall provide evidence of the test coverage.
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.
ATE_COV.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.
ATE_FUN.1.2d The developer shall provide test documentation.
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.
ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.3 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.
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.
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 of tests in the test documentation to verify the developer test results.
ATE_IND.2.3e The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.3.5 Vulnerability assessment (AVA)

5.3.5.1 Vulnerability analysis (AVA_VAN.2)

AVA_VAN.2.1d The developer shall provide the TOE for testing.
AVA_VAN.2.1c The TOE shall be suitable for testing.
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. TOE Summary Specification

This chapter describes the security functions:

- Security Audit
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functions
- TOE access
- Intrusion Detection System

6.1 TOE Security Functions

6.1.1 Security Audit

The TOE provides its own audit mechanism that can generate audit records for the basic level of audit. Each audit record minimally includes date and time of event, subject/user identity where applicable, and the outcome (success or failure) of the event. The auditable events include:

- Start-up and shutdown of the audit function (which corresponds with starting and stopping the CommandPost)
- Establishing a user session on the CommandPost (i.e., logging in to access available functions) – this event also identifies the location of the user
- Use of administrator commands, which includes attempted access to available System and audit data (also identifying the requested data and access) as well as attempted configuration operations (modification of TSF data, user role assignments, etc.)

The TOE also provides the functionality to include or exclude (turn on or off) auditable events from the set of audited events based on 'event type'.

TOE audit records are stored on the CommandPost appliance in the MySQL data repository where authorized administrators (i.e., those granted View Only or Full Control access to the Audit function by role) are able to review the contents and interpret the results. The audit records can also be sorted based on date and time, subject identity, type of event, and success or failure of related event. TOE audit data is stored separately from alert data in MySQL as they occupy different tables in the database and are allocated separate space requirements since the data types are very different.

There are no interfaces provided to modify stored audit records and viewing or deleting of audit records is only permitted by the authorized administrators.

The TOE attempts to maintain free space equal to the size of the largest current table plus 200 MB for audit data (1 GB for alert data). However, once available audit data storage space is exhausted new audit records will overwrite the oldest events so that the latest events are retained in the available space and an alarm is sent (via e-mail, syslog, or SNMP) to the System Administrator and any additional audit records overwrite the oldest stored records.

For more information about audit-related functions provided by the CommandPost (Management Console), see the Security Management function description below.

The Security Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE generates audit events for the basic level of audit as well as the additional events and details identified in the requirement.
- FAU_SAR.1: The TOE provides users with the ability to review records in order to interpret the contents. Note that users assigned to a role with View Only or Full Control access to the Audit function are explicitly authorized to access all audit records.

- FAU_SAR.2: The TOE prohibits audit record access except by those users explicitly granted View Only or Full Control access to the Audit function via a role assignment.
- FAU_SAR.3: The TOE provides the ability to sort audit records on the following fields in the audit data: date and time, subject identity, type of event, and success or failure of related event.
- FAU_SEL.1: The TOE also provides the functionality to include or exclude (turn on or off) auditable events from the set of audited events based on 'event type'.
- FAU_STG.2: The CommandPost protects stored audit data from unauthorized deletion by ensuring that TOE audit data is maintained in a separate table its MySQL database. Only those areas of the database tables for which the TOE relies on are accessible based on role (privilege(s) assigned and access type).
- FAU_STG.4: The TOE prevents audit data loss by overwriting the oldest stored audit records if the audit trail is full within the allocated database tables. Also, when audit data storage is exhausted an alarm is sent (via e-mail, syslog, or SNMP) to the System Administrator and any additional audit records overwrite the oldest stored records.

6.1.2 Identification and Authentication

The TOE provides its own (local) user name and password authentication mechanism, utilizing the functions of the underlying hardened Linux OS. In order to access the TOE, a login account, including a login name and password must be created. Users are granted access to system resources based on user role assignment (a pre-defined role – System Administrator, Network Admin, Network Admin Supervisor, Policy Author, Policy Author Supervisor, Alert Manager, Alert Manager Supervisor, No Role – or a customer-defined role). Only users granted Full Control to the Users function can assign a role to other users. For more information about authorizations, see the Security Management function description below.

To log in to the TOE via the available web or secure FTP interfaces, the user provides the login name (e.g., user identity) and password to the CommandPost. That information is forwarded to the authentication mechanisms of the underlying hardened Linux OS for verification. If either the login name or the password is incorrect, the login request will fail, the session will be denied, and no CommandPost functions will be made available.

In addition to local authentication, the TOE supports alternatives for authentication.

1. Integration with an LDAP server or Active Directory. In this mode, user credentials (username and password) are supplied by the user to the CommandPost GUI login screen and then sent to the directory for authentication. The TOE enforces the authentication decision returned. If authentication is successful, the user is granted access otherwise access is denied. The role, alert group, and sensor assignments are setup by the administrator when LDAP authentication is configured and enabled. The assignment can be based on user-directory attributes (i.e., group, user).

2. For a smart card/CAC environment, the user would use their smart card or CAC with a reader on their host workstation where their certificate is accessed. When they connect to the CommandPost using HTTPS, their certificate is passed to the CommandPost for authentication against the certificates stored for the applicable user. However, the user is still required to provide credentials (username and password) at the CommandPost login screen and those credentials are verified using the local user database or LDAP/Active Directory as indicated above. Note that all the applicable certificates are generated and provided by the operational environment, though the TOE provides interfaces and guidance for their configuration.

It is not possible to disable local CommandPost authentication. By default this is the only configured authentication method. The alternative authentication methods depend on the operational environment.

As a result of a successful login, an interactive session is established that is associated with the user, role (Network Admin, Policy Author, Alert Manager, etc.), and alert group and sensor assignments. Subsequently, the session is granted access to all functionality to which the user has been explicitly granted access privileges based their role and alert group and sensor assignments.

Password requirements are configurable by an administrator with Full Control access to the CommandPost Configuration function. Utilizing the password configuration, CommandPost requirements can match the needs of the operational environment. If a user attempts to select a password that does not meet the configured requirements, the TOE will not allow in the password to be changed.

Note that the TOE sensors perform continuous monitoring of the network traffic whether an authorized user (administrator) is logged onto CommandPost or not. Except as noted below, the sensors themselves do not provide user interfaces, but rather are accessed indirectly via their associated CommandPost.

Each TOE appliance relies on its hardened CentOS Linux OS to facilitate logging directly into the TOE its own locally connected console (video, keyboard, mouse) when attached. Only users with physical access and an appropriate user account configured in the underlying Linux can log directly into an appliance. This interface is generally considered out of scope of the evaluation since it is intended to be used for installation and setup purposes and not for maintenance and operation once each TOE appliance is configured as required.

During installation and setup, a user account named 'fidelis' is created and all TOE software runs under this account. The 'fidelis' account has access to all Fidelis software and related log files, etc.. Typically, this is the only account established and used on TOE sensor appliances while the CommandPost appliance requires additional accounts to support interactive users (administrators), including those that will access the CommandPost web interface and/or secure FTP interface.

Note that file transfers to/from the CommandPost is done using secure FTP (WinSCP). Access via secure FTP is very limited where each user gets their own directory on disk and they can only access that data. In the case of external authentication, users are not provided a CommandPost login username or password and as such these users cannot do file transfers.

In the evaluated configuration, no additional (i.e., non Fidelis) software is authorized for installation onto the TOE appliances and the appliance devices are locked down such that they are configured to only support TOE functionality.

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1: The TOE maintains user identity (username), authentication data (password), authorizations (role with access privileges) and assignments (alert management group and sensor).
- FIA_UAU.2: The TOE offers no functions until the user is successfully authenticated.
- FIA_UAU.5: The TSF provides support for local and remote authentication mechanisms to support user authentication. The TSF authenticates any user's claimed identity according to the following rules: if configured, LDAP or Active Directory authentication mechanisms are used for authorized administrators to access the TOE. The TOE then accepts or rejects the authentication decision based on the response from LDAP or Active Directory, before allowing any other TSF-mediated actions on behalf of that authorized administrator. If LDAP or Active Directory is not configured or available, the TOE performs identification and authentication before allowing any other TSF-mediated actions on behalf of that authorized administrator.
- FIA_UID.2: The TOE offers no functions until the user is successfully identified.

6.1.3 Security Management

All TOE security management functionality is handled via the CommandPost appliance. Each defined CommandPost user is assigned one role that determines the parts of the system the user may access (i.e., access privileges). Access privileges are associated with specific functions (e.g., Users) and serve to grant 'Full Control' (read/write), 'View Only' (read), or 'No Access' to the corresponding function.

Alert management groups can be created and used to divide (or isolate) the work of violation review since each rule is associated with an alert management group. When a rule is violated, an alert may only be managed by users assigned to its associated alert management group. Once viewed, an alert manager may move the alert to a different alert management group, as needed, after which it would be accessible by users assigned to the resulting alert management group.

Furthermore, work can be divided (or isolated) based on sensor. Users can be assigned specific sensors that they can manage and/or access.

The following table identifies the available functions, applicable access privileges, and applicability of alert management group and sensor assignments.

FUNCTION	ROLE MUST PROVIDE	ALERT MANAGEMENT GROUP ASSIGNED	SENSOR ASSIGNMENT
Alerts – Alert management	Full Control or View Only access to alerts	Users must be assigned to the same group as the alert	Users must be assigned to the sensor that generated the alert to access the alert.
Details – Alert Details which include all information collected by the sensor	Full Control or View Only access to Alerts; Full access to Details.	Users must be assigned to the same group as the alert	Users must be assigned to the sensor that generated the alert to access the alert details.
Quarantine - Quarantine Management	Full Control or View Only access to quarantine	Users must be assigned to the same group as the quarantined e-mail.	Users must be assigned to the sensor that generated the quarantined e-mail.
Tickets – Alert Issue Tracking Information	Full Control or View Only access to both Tickets and Alerts	Users must be assigned to the same group as the alert to access the alert ticket.	Users must be assigned to the sensor that generated the alert to access the alert ticket.
Reports – Alert Reporting	Full Control or View Only access to Alerts; Full Control to Reports	Reports will include only those alerts assigned groups to which the user is assigned.	Reports will include only those alerts generated by a sensor to which the user is assigned.
Policies – Policy Authoring	Full Control or View Only access to policies	No impact	Users can only assign policies to sensors to which they are assigned.
Users – User Management	Full Control or View Only access to users	A new user may be added to any group to which the user manager belongs.	A new user may be added to any sensor to which the user manager belongs.
Sensor Configuration	Full Control or View Only access to Sensor Configuration	No impact	Users can only configure sensor components on sensors on which they are assigned.
CommandPost Configuration	Full Control or View Only access to CommandPost Configuration	No impact	No impact
Audit – Audit management	Full Control	No impact	No impact

Table 5 Security Management Function Overview

The TOE contains eight built-in, pre-defined roles that cannot be edited or deleted. The System Administrator role has full control over the system and can performs all TOE security management functions.

Users are granted a role based on the actions they will be performing within the TOE (sensor management, policy management, alert management, etc.).

Default Authorized Administrator role summaries:

- System Administrator—complete access to all TOE functionality and components, including all those functions identified below plus the ability to manage the security audit function and access TOE audit records.
- Network Admin—manage CommandPost and sensors; full access to CommandPost configuration, sensor configuration and report functions; read-only access to alerts, quarantined e-mail, alert tickets, policies, and users functions; no access to audit. Note that sensor configuration only applies to sensors to which the user is explicitly assigned. Alert read access is only available to those associated with sensors and alert management groups to which the user is explicitly assigned.
- Network Admin Supervisor—manage CommandPost and sensors as above Network Admin with full access to the users function. May create new roles that do not exceed their current (Network Admin) role and apply that role to users.
- Policy Author—create policies; authorized administrators with the Policy Author role use the policies screen to create policies and assign them to sensors for policy enforcement, thus creating Extrusion Policies [see below]. The Policy Author also has full access to reports; read-only access to alerts, quarantined e-mail, and alert tickets; no access to CommandPost configuration, sensor configuration, users, or audit functions. Note that policy assignment is only permitted to sensors to which the user is explicitly assigned. Alert read access is only available to those associated with sensors and alert management groups to which the user is explicitly assigned.
- Policy Author Supervisor—create policies as above Policy Author with full access to the users function. May create new Policy Authors with this role.
- Alert Manager—manages alerts and quarantined e-mail; has full access to Alerts, quarantined e-mail, alert tickets, and reports; has read-only access to policies; has no access to CommandPost configuration, sensor configuration, users, and audit functions. Alert and quarantine access is only available to those associated with sensors and alert management groups to which the user is explicitly assigned.
- Alert Manager Supervisor—manages alerts and quarantined e-mail as above Alert Manager with full access to the users function. May create new Alert Managers with this role.
- No Role—no role assignment.

The following table more directly identifies the functions and access privileges associated with each of the eight pre-defined roles.

ROLE	FUNCTION	ACCESS TYPE
System Administrator	Alerts	Full Control
	Details	Full Control
	Quarantine	Full Control
	Tickets	Full Control
	Reports	Full Control
	Policies	Full Control
	Users	Full Control
	Sensor Config	Full Control
	CommandPost Config	Full Control
	Audit	Full Control
Network Admin	Alerts	View Only
	Details	Full Control
	Quarantine	View Only
	Tickets	View Only
	Reports	Full Control
	Policies	View Only
	Users	View Only
	Sensor Config	Full Control

ROLE	FUNCTION	ACCESS TYPE
	CommandPost Config	Full Control
	Audit	No Access
Network Admin Supervisor	Alerts	View Only
	Quarantine	View Only
	Details	Full Control
	Tickets	View Only
	Reports	Full Control
	Policies	View Only
	Users	Full Control
	Sensor Config	Full Control
	CommandPost Config	Full Control
	Audit	No Access
Policy Author	Alerts	View Only
	Details	Full Control
	Quarantine	View Only
	Tickets	View Only
	Reports	Full Control
	Policies	Full Control
	Users	No Access
	Sensor Config	No Access
	CommandPost Config	No Access
	Audit	No Access
Policy Author Supervisor	Alerts	View Only
	Details	Full Control
	Quarantine	View Only
	Tickets	View Only
	Reports	Full Control
	Policies	Full Control
	Users	Full Control
	Sensor Config	No Access
	CommandPost Config	No Access
	Audit	No Access
Alert Manager	Alerts	Full Control
	Details	Full Control
	Quarantine	Full Control
	Tickets	Full Control
	Reports	Full Control
	Policies	View Only
	Users	No Access
	Sensor Config	No Access
	CommandPost Config	No Access
	Audit	No Access
Alert Manager Supervisor	Alerts	Full Control
	Details	Full Control
	Quarantine	Full Control
	Tickets	Full Control
	Reports	Full Control
	Policies	View Only
	Users	Full Control
	Sensor Config	No Access

ROLE	FUNCTION	ACCESS TYPE
	CommandPost Config	No Access
	Audit	No Access
No Role	No Access	No Access

Table 6 Default Access Control Policy by Role

In addition to the eight pre-defined roles with default privileges and access levels, a user with Full Control to the Users privilege can create additional (customer-defined) roles using any combination of the privileges (i.e., alerts, details, quarantine, tickets, reports, policies, users, CommandPost config, sensor config, audit) with the appropriate access level (i.e., full control, view only, none) for the desired effect or based on assigned administrative responsibilities, as one privilege has no bearing on others.

Users log in to the CommandPost to manage TOE security functions via a web-based interface from client workstations and the communications channel is encrypted with TLS.

The access privileges of CommandPost users are assigned and managed by an authorized administrator using the CommandPost Users screen. New users are added to the TOE by user name, password, and other attributes (e.g., role, alert group assignments, sensor assignments, name, e-mail address). If external authentication via LDAP or Active Directory is to be used then a user profile is created that includes a mapping between user parameters (extracted from the external user directory) and authorization settings. Current user accounts may be modified to reflect updated personal information (name, e-mail) or to modify authorizations assigned. Alternately, users who no longer require access to manage the TOE or its data may be deleted. Only users with the Full Control access to the Users function may modify, delete and create user definitions.

Users with access to the 'fidelis' account (i.e., the user who knows the applicable password, such as the one that installed the product) can execute a limited number of commandline functions which are useful to research problem situations. This interface should only be accessed in problem situations or when directed to do so by Fidelis Customer Support. The guidance document advises users not to use this interface in the evaluated configuration.

The Security Management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1: Only those users granted Full Control access to the functions related to system data collection, analysis and reaction (i.e., authorized System Administrators) can change the associated behaviors within the scope of their assigned alert management groups and sensor assignments.
- FMT_MTD.1: As summarized above, only those users granted View Only or Full Control access to a given function can read or read/write (respectively) the associated data within the scope of their assigned alert management groups and sensor assignments where applicable.
- FMT_SMF.1: The TOE offers a wide range of security management functions including managing audit functions (Audit function); users and their security attributes (Users function); alert reports (Alert, Details, Tickets, and Reports functions); functions related to system data collection, analysis and reaction (Quarantine, Policies, Sensor configuration, and CommandPost configuration functions)); as well as management of the TOE configuration in general including, but not limited to, management the authentication mechanisms, rules for authentication, and the session timeout value (CommandPost Config functions).
- FMT_SMR.1: The TOE supports pre-defined roles (i.e., System Administrator, Network Admin, Network Admin Supervisor, Policy Author, Policy Author Supervisor, Alert Manager, Alert Manager and No Role) as well as customer-defined roles that can be built using access privileges (full control, view only, or no access) to ten function areas (i.e., Alerts, Details, Quarantine, Tickets, Reports, Policies, Users, Sensor Configuration, CommandPost Configuration, and Audit) to perform security management functions on the TOE as assigned. These roles correspond to the IDSSPP-defined authorized administrator and authorized System administrator roles as follows:
  - The 'System Administrator' role corresponds with the IDSSPP roles: 'authorised administrator' and 'authorised System administrators'.

- The 'Network Admin', 'Policy Author', and 'Alert Manager' roles correspond with the IDSSPP role: 'authorized System administrators'.
- Customer-defined roles *could* correspond with 'authorised administrator' and/or 'authorised System administrator' depending on how they are defined by the customer.

6.1.4 Protection of the TOE Security Functions

The TOE restricts access to its interfaces by requiring authorized administrators to log into the CommandPost appliance. Commands sent from the CommandPost appliance to the Fidelis XPS sensor appliances are encrypted and decrypted by use of the included FIPS 140-2 certified OpenSSL Version 0.9.8r utilizing the OpenSSL FIPS Object Module Software Version 1.2.3 (FIPS certificate 1051) data encryption and decryption over TLS, Version 1.0 encrypted communications channel and the sensors are configured to accept packets only from a specific network address (e.g., CommandPost).

Communication between TOE appiances can also be secured by use of Public Key Infrastructure (PKI) certificate cryptography where it can use public key cryptography for endpoint authentication, Ephemeral Diffie-Hellman (DHE) for symmetric key exchange, symmetric cryptography to encrypt messages for confidentiality, and Message Authentication Code (MAC) to maintain messages integrity.

This table shows the algorithms and their strength in the adopted cipher suite "DHE-RSA-AES256-SHA".

PURPOSE	ALGORITHM	STRENGTH (KEY LENGTH, BITS)
Authentication	RSA	2048
Key exchange	DHE	1024
Encryption	AES	256
MAC hash function	SHA-1	160

Table 7 TOE Cipher Suite Details

The RSA encryption public key algorithm uses 2048-bit public key, and 65537 (0x10001) as the exponent.

Each TOE appliance is equipped with the following PKI functionality by use of a third-party Certificate Authority (CA) [External Certification Authority (ECA) where the TOE provides the interface] where the information can be stored on hard disk with the highest access restriction:

- Its own PKI private key and public key certificate;
- CA certificate; and
- Certificate Revocation List (CRL), as issued by a CA.

To avoid the Man-In-The-Middle attack, the public key cryptography based authentication includes two parts:

- Verify the certificate was signed by a CA, and
- Verify the endpoint's entity name is the same as the certificate's unique name.

Note that the evaluated configuration does not include a CA for TOE functionality to operate as stated within this ST. This information is only provided to clarify an optional capability using a CA server in the operating environment.

TOE sensors must be registered to the CommandPost and no communication is possible until successful registration takes place. This registration process limits the access to the inter-component communication channels, and associates a certificate's unique name with the TOE component, thus providing the necessary support for the second step in the authentication procedure above.

The CommandPost can be accessed from anywhere on the network by using a web browser that supports TLS/SSL to navigate to the IP address of the console device and logging in with valid username and password.

Note that when SSL is enabled on the TOE, the CommandPost will use TLS (iniaited by the LDAP/Active Directory server) to protect communication with associated LDAP/Active Directory servers as well. While the use of

TLS/SSL is generally required in the evaluated configuration, if the configured LDAP/Active Directory does not support TLS, the TOE can be configured to communicate without using TLS, but that configuration is beyond the scope of the evaluation as it would require the operational environment to otherwise provide the necessary communication protections.

Each appliance provides reliable time stamps for collected data and TOE auditing purposes. In the case of hardware appliances, a hardware clock is included which provides time information for the embedded software components. In the case of the VM appliances, the embedded OS is dependent upon its VMWare vSphere host for timing signals it can use to reliably formulate time stamps.

All TOE appliances support NTP and can be configured to utilize a common NTP server in order to ensure that their clocks are synchronized.

The Protection of the TOE Security Functions function is designed to satisfy the following security functional requirements:

- FPT_ITT.1: The TSF protects all sensitive data from disclosure and modification when transmitted between separate parts of the TOE via SSL/TLS encryption/decryption.
- FPT_STM.1: The TOE appliance provides a reliable time stamp for its own use. When the TOE is deployed as a VM instance rather than an appliance, the operational environment must supply timing information suitable for the TOE to generate reliable time stamps.

6.1.5 TOE Access

A user can access the CommandPost from multiple web-based client workstations simultaneously by logging in successfully; however, session(s) will timeout after a period of inactivity (15 minutes is the default) and are terminated when that occurs. Once a session is terminated the user must successfully log in once again to re-establish a new session with the CommandPost appliance.

The TOE access function is designed to satisfy the following security functional requirements:

- FTA_SSL.3: The TOE provides administrator configurable session termination after a period of time of inactivity. The default is 15 minutes.

6.1.6 Extrusion and Intrusion Detection

At a high level, the TOE sensors collect network traffic from the network to which they are attached. The specific network attachment (e.g., direct, SPAN port, proxy) is dependent upon the specific TOE sensor, each of which has been designed for specific purposes as described earlier in this ST. Once collected the network traffic is analyzed, and potentially stored (e.g., for forensic purposes), in an attempt to identify any rule violations that might indicate a potential intrusion or extrusion. Any rule violations result in configured actions that serve to notify appropriate users and also may attempt to stop or otherwise mitigate the perceived problem.

The TOE uses fingerprints to identify protected or prohibited data that can be combined together into rules using logical operations. Fingerprints are used to match some characteristic in network transmission. The logic imposed within the rule will determine whether a match of this fingerprint is acceptable or not. Different rules can use the same fingerprints and different rules can be configured to different sensors. A policy is a set of rules that guide business practices within an enterprise. Some examples include determining acceptable use of network resources, preventing transmission of sensitive information, detecting deeply embedded malicious code, and ensuring compliance with privacy laws. Policies are comprised of one or more rules. Rules, in turn, contain one or more fingerprints that refer to either the content within a transmission, the communication channel of the transmission, the sender, or the receiver of the transmission (e.g., location). The following illustrates basic elements that a rule can contain:

- Generate ACTION if content is detected over channel coming from/to location.
- ACTION is the result that occurs if a rule is violated. Actions can be configured as either alert, prevent, alert and prevent, throttle, alert and throttle, alert and quarantine, reroute, and alert and reroute. In the case of mail, X-header modification, append message, and user notification can also be specified. In addition, Packet Capture can be added to any rule. When applied to Direct or Internal sensors, the action will store

entire packets. Content, channel, and location are fingerprint definitions as described in the following sections.

The TOE contains pre-built policies, rules and fingerprints that can be used immediately or used as examples for custom policy creation. At a high level, the policy creation process is as follows:

Create fingerprints based on the following:

- The sender or receiver, which can be described as a single IP address, or more commonly, as a group of addresses representing a corporate location. The sender or receiver can also be determined by LDAP or Active Directory attributes, by country of origin, or by reputational data to mark a location as a phishing site, a malware distributor, a botnet command and control, or other such classification.
- Communication channels that include the network protocol and attributes of the transmission.
- The content within a transmission.

Create rules using one or more fingerprints.

Create a policy that includes one or more rules.

Assign the policy to one or more sensors.

When a rule is violated, a TOE sensor detects the violation and performs an action in response. A rule is a logical expression that must be evaluated based on comparison between the message stream and the fingerprints used in the logical expression. The result of this evaluation is a logical value that indicates that the message stream is either legitimate (false) or in violation (true) of the policy (or portion of the policy) that the rule implements.

TOE Sensors are manually updated with current, configured Policies by user granted the Policy Manager privilege (i.e., Full Control access to the Policies function).

Note that fingerprints are logically combined into rules. Policy violations are based on the rules and not the fingerprints.

Fingerprints share a common header and contain the following types that are either content-based, channel-based, or location-based and each results in a true/false logical conclusion when compared to collected network traffic:

- Identity Profiling—Identity profiling is used to describe personal identity information. The TOE has twelve built-in identity items that include name, postal address, e-mail address, national ID (i.e social security number), credit card number, vehicle identification number (VIN), SWIFT and American banking association (ABA) codes, international bank account numbers (IBAN) FDA-approved drug names, dates, phone numbers, and magnetic stripe data. Authorized administrators with the Policy Manager privilege may add custom identity items by describing them with a regular expression. Custom and built-in identity items may be combined into one or more profiles to describe the information that is desired and limits can be set regarding the number of identity sets and the distribution of the items within those sets.

- Binary Profile –is used to detect the content of a file before it is decoded. Utilizing this fingerprint the sensor can detect a regular expression of content within non-visible text within a document, for example embedded executable code or JavaScript. The fingerprint may also be used to match an MD5 of the file, prior to decoding. This fingerprint is most often used to detect malicious content within files.

- Embedded Images—users granted the Policy Manager permission will register an image with TOE. Upon detection of this image in a file transfer, the fingerprint will evaluate to true. The act of registration involves copying the image to the TOE, performing the image registration via GUI button click and saving the results. The results are then stored in a fingerprint.

- Encrypted Files—the TOE cannot decrypt files on the fly, but can detect that a file has been encrypted and this fingerprint will evaluate to true if an encrypted file is detected on the network.

- Exact Content (via MD5 Signature)—user will register a file with the TOE and the fingerprint will match when this exact file is found in network traffic. All fingerprints result in a true/false logical value when compared to network traffic.

- Partial Content—user will register a file with the TOE and the fingerprint will match when a portion of this file is found in network traffic. When the fingerprint is created, the user can specify the size and number of file portions that must be found to result in a match when compared to network traffic.

- File Signature—this fingerprint is used to describe binary file formats. TOE will analyze the content of many textual file types but cannot analyze the content of binary files such as CAD drawings. File signature uses a UNIX MAGIC description of the file type. The fingerprint is looking at the contents to extract and compare the MAGIC descriptor to the fingerprint. It does not look at the name of the file.

- Protocol Signature—this fingerprint is used to describe protocols that are not decoded by Fidelis. It includes the ability to match all unknown protocols and the ability to match a protocol based on a regular expression.

- File Names—this fingerprint uses regular expressions to describe the name of a file and if a matching file name is detected, the fingerprint will evaluate to true. It uses regular expressions to describe the file name, therefore wildcards are not needed. To match the string 'xyz' within a file name, the regular expression is 'xyz'. To match a filename that is exactly xyz, an authorized administrator granted the Policy Manager privilege would configure an expression such as '\bxyz\b'.

- Keywords—content is described in terms of keywords. Once these words are found in network traffic, the fingerprint will evaluate to true. Note that a keyword may include any valid character, including spaces; however, the fingerprint requires an exact match. The fingerprint can be configured to be case sensitive or case insensitive.

- Keyword List—similar to Keywords in function but the analyzer utilizes a different search algorithm. The keyword list analyzer is optimized for very long lists of words, on the order of 100,000 whereas Keywords is optimized for short lists.

- Keyword Sequence—a list of keywords that must appear in the proper order within network traffic.

- Regular Expression—this fingerprint is much like the keyword fingerprint, except that regular expressions are used to describe the data.

- Channel—integrity analysis based on detection of user behavior including all attributes of network communication, the protocol, the day of the week, time of day, TCP port number, etc. Channel may also refer to any attribute of the communication such as the FTP login ID, the SMTP to/from/subject, the URL, etc.

- IP Address—refers to the IP address of the sender or receiver of a network communication. Like channel, this fingerprint has nothing to do with content.

- Country—Fidelis XPS sensors include GeoIP data to associate an IP address with the country of registration. The country fingerprint will match when the geographical data matches the IP address of the sensor or receiver of a network communication.

- Directory—User information can be gathered from LDAP or Active Directory, pending CommandPost configuration with a directory server supplied by the operational environment. The Directory fingerprint is based on user attributes and matching is performed when the sender or receiver of network communications matches the user data from the directory.

- Reputation—Fidelis XPS sensors include feeds from external sources, either sold by Fidelis or Fidelis partners, or supplied by the operating environment. Feeds associate IP addresses with certain intelligence, for example lists of phishing sites, malware distributors, or local hosts for which the authorized administrator wishes to white list or black list. The fingerprint returns true when an IP address in the reputational feed matches the sender or recipient IP address of network communication.

TOE Analyzers

The TOE contains several analyzers to analyze network traffic. The analyzer portion of the TOE is the software that compares network traffic to information stored in a fingerprint. Specific analyzer functionality is described herein.

The Regular Expression analyzer uses the Perl Compatible Regular Expression (PCRE)[1] open source library to identify data that matches a particular pattern. The TOE analyzer takes a list of regular expressions and compares them to data extracted from the network traffic. A score is assigned to each regular expression from the list that can be either a positive or negative number. A regular expression can match more than once, up to an optional limit. Each match adds or subtracts the assigned score to the total score. If the result exceeds an assigned threshold, an alert is generated. The analyzer identifies data that has a similar pattern. Each regular expression line contains three columns, in order: weight, limit and regular expression.

The Channel analyzer allows a sensor to generate alerts based on matches on the values of attributes of sessions based on a triggering rule. Rules are specified in the configuration file and can use the following session envelope information:

- Source port number
- Destination port number
- Length of session in bytes
- Start time of session
- Day of session
- Duration of session
- Session protocol type
- Session attributes
- Session decode path
- Format type
- Format size

The File Name Regular Expression analyzer identifies certain files in order to document them or to prevent the file's transfer and is applicable in situation when file names are transferred over the network as a part of client-server conversation. The file names are defined by an authorized administrator within a fingerprint. This analyzer can flag or prevent the transfer of certain types of protected or prohibited files.

The Exact Content analyzer provides a way to positively match a particular file by utilizing an MD5 checksum for exact file detection.

The Partial Content analyzer provides recognition of a registered document, either in its entirety or parts of it. The registration process requires a user to copy the file to the CommandPost and generate a fingerprint. After the fingerprint is generated and saved, all documents can be removed from CommandPost.

The Encrypted file analyzer checks many common types of files (such as encrypted Microsoft word, Excel, Zipped files, and PDF) for encryption. The TOE does not decrypt the data, the TOE examines the header information to determine the algorithm that was used to encrypt the file. The TOE does not perform analysis of the data (i.e. crypto-analysis).

The Binary Profile analyzer is applied prior to the file decoding process, whereas all other content analyzers match against the fully decoded file content. The analyzer utilizes both PCRE and MD5 as identified by the fingerprint. PCRE matches apply to the content of the file and can include binary expressions. MD5 matches against the entire, non-decoded file.

The File Signature analyzer evaluates files transferred based on the type of file regardless of file name or extension.

The Protocol Signature analyzer evaluates protocols that are not recognized by the protocol decoder software on the sensor.

The Identity Profile analyzer evaluates data based on the statistical attributes of the data.

[1] PCRE, also known as Perl Compatible Regular Policy, written and copyrighted by Philip Hazel. Documentation available at www.pcre.org.

The Keyword and Keyword List analyzers evaluate data for keywords.

The Keyword Sequence analyzer evaluates data for keywords appearing in order.

The Embedded Image File analyzer looks for embedded image files.

The IP Address, Country, and Reputation analyzers evaluate the source and destination IP addresses.

The Directory analyzer utilizes user attributes extracted from an LDAP or Active directory server in the operating environment. The fingerprint matches the email address or IP address found in network data to the user attributes in the fingerprint. To utilize the IP address on the network, the operating environment must also provide domain server login records to correlate IP address to user name.

Alerts

The TOE CommandPost compiles alerts from all connected sensors and this aggregated data can be viewed from the CommandPost. The TOE's Radar screen utilizes the Adaptive Alert Classifier sub-component to group specific alerts that are related. The CommandPost considers the signature, packet source, packet destination, time, duration and other configurable parameters to group alerts. Alerts are inspected from multiple sensors together to uncover patterns not apparent from watching normal alert logs by a system administrator or an authorized administrator granted the Alert Manager privilege. The TOE is capable of collecting the following events: 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; and detected known vulnerabilities.

Alert data differs depending on the protocol, on which the alert occurred, but in general includes:

- Unique alert number;
- Alert priority;
- Alert rule, policy, and the true/false result of all fingerprints in the rule (i.e., outcome of the event);
- Time and date of alert;
- Whether a TCP session was recorded by the TOE;
- Sensor that identified the alert;
- Alert summary or rule used in detecting alert (i.e., type of result or event);
- Attributes of the alert from TOE decoders[2];
- Protocol on which alert occurred;
- Action taken by the sensor;
- Source address (i.e., identity of data source);
- Destination address;
- Source and Destination TCP port, if applicable;
- Service;
- IP layer information;
- Country where source and destination IP address are registered;
- PCAP file of network data, if chosen by the rule;
- Recorded object (TCP session, email message, file, as appropriate for the sensor type);
- Forensic data for the alert, representing the data used to determine the rule violation; and
- Option to view either hexadecimal or text data for forensic data.

Alerts are sent by Fidelis sensors to their associated CommandPost where they are stored in an embedded MySQL database. Access (e.g., for access, deletion, modification) is protected by limiting access to the associated management functions using access privileges and alert group membership and sensor assignments, and by providing no other unrestricted functions to access that data.

[2] Decoders versus fingerprints—fingerprints are what determines if a session is a violation or not. When there is a violation, the decoders extract many attributes from the session and this is what is displayed herein.

Alert retention can be configured to remove alerts on a nightly or weekly basis. Alert retention can be controlled by an adminsitrator to remove some alerts sooner than others. Criteria for retention can be based upon the sensor that generated the alert, severity, rule, policy, label, alert action, alert ticket status, and alert ticket resolution. Further, the retention process can be configured to archive alerts prior to deletion. An administrator can purge alerts through the CommandPost GUI.

A hardcoded space management process performs space checks upon the insertion of new alerts. The CommandPost MySQL database attempts to maintain free space equal to the size of the largest current table plus 1 GB and has been tested to store a maximum of 10 million alerts. However, once available System data storage is exhausted an alarm is sent to the System Administrator and any additional alerts overwrite the oldest stored System alert records. When this situation occurs, System Monitor alarms are also sent to the configured e-mail, syslog, or SNMP recipients.

CommandPost continuously measures its own alert insertion rate. When the rate of alert insertion is too high, it will supply back pressure to the sensor, which will begin to compress alerts in an effort to reduce the rate of new alerts. Data can be stored on the sensor for short periods to handle overload and attack scenarios. If CommandPost fails, each sensor will detect the state and send alerts to a backup (redundant) CommandPost, if one has been configured for the system.

Alerts can be exported (i.e., sent) to administrators or third party management systems by configuring an Export. Exports can be created by an authorized administrator with alert and CommandPost administration privileges. Exports allow CommandPost data to be sent to an external system provided by the operational environment. Exports can be performed for standard protocols (email, Syslog, SNMP), custom third party interfaces (ArcSight, IBM SiteProtector, Verdasys Digital Guardian) or the Fidelis alert archive format.

When the Export is configured, the location of the information is selected. The location can be a server (syslog or SNMP), e-mail address (for email), or a third party device (ArcSight, IBM SiteProtector, Verdasys Digital Guardian).

Alerts can be filtered by many alert attributes; such as:

- All alerts (that meet current search criteria, as listed in the table display header)
- Breakdown by alert type
- Breakdown by protocol
- Breakdown by sensor
- Breakdown by rule summary
- Breakdown by source or destination IP address

Information Flow Map

The TOE sensors collect metadata from all network sessions whether they result in a policy violation or not. The metadata is transmitted to CommandPost once per minute and is the source of the Information Flow Map available on CommandPost.

Information Flow Map is a visualization of all network traffic, including transport layer data (TCP, UDP, ICMP), application protocols, file formats, content, rules, alerts, and locations. Transport layer, protocols, file formats, and locations are available without any configuration.

Content refers to fingerprint matches, whether they result is a policy violation or not. Content requires the creation of fingerprints, applied to rules and polices, and assigned to a sensor. Rules refers to those rules running on the sensor with an action of Information Flow Map. Utilizing this action, a user can watch specific activity on the network to test a rule or to witness certain behavior. Alerts refers to rules with an action of alert.

Collected metadata is stored in the CommandPost embedded MySQL database.

Extrusion and Intrusion Detection Data Access

All data collected and stored by the TOE is accessible only by users that have been granted explicit access (via roles granting applicable access privileges, alert group membership, and sensor assignment) to the functions that provide access to access or otherwise manage that data. This includes the ability to examine and generate reports based on information related to potential extrusions or intrusions.

The Intrusion Detection System function is designed to satisfy the following security functional requirements:

- IDS_ANL.1: The TOE performs analysis on network packet data collected via its sensors such that TCP packets are reconstructed, sessions are identified, sessions are analyzed in terms of protocol, application and data content and a set of rules applied to identify inappropriate network traffic. As explained above, the TOE implements numerous fingerprints that can be used in several analytical processes in order to obtain results about potential extrusion and intrusions as required.
- IDS_RCT.1: The TOE can send alarms to the CommandPost alarm database and also to users and third party management systems configured to receive alarms (known as exports). The TOE can also take various actions as configured per violated rule including, but not limited to: prevent data transmission (e.g., sending TCP resets), throttle session, quarantine, or reroute. In the case of e-mail, an e-mail can be appended, an X-header can be added, or the sender can be notified. Information is also added to an information flow map whether there is a violation or not.
- IDS_RDR.1: The TOE provides users that have been granted explicit access via access privileges associated with their role, alert group membership, and sensor assignment access to System data via the associated available functions. These functions render the data readable to the user and cannot be used to query data for which the user is not granted explicit access.
- IDS_SDC.1: The TOE is able to collect network traffic, including protocol and source/destination data, via its various sensor connections to the network. Note that collected information is time stamped, but other than protocol and source/destination addresses, the required type, subject identifier, and outcome are not relevant attributes. However, the TOE does record when the associated traffic is found to represent an intrusion or extrusion based on its configured rules.
- IDS_STG.1: The TOE protects the stored data from unauthorized deletion and modification using access privileges, alert group membership, and sensor assignments. It also prevents System data loss by overwriting the oldest stored System data if the available space is exhausted within the allocated database tables.. When system data storage is exhausted an alarm is sent to the System Administrator and any additional System data overwrites the oldest stored System data.
- IDS_STG.2: The CommandPost data repository overwrites the oldest stored System data if the configured storage capacity has been reached and sends an alarm to the System Administrator.

7. Protection Profile Claims

The TOE conforms to the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007 (IDSSPP).

The security problem definition has been copied from the IDSSPP with the following exceptions:

- T.SCNCFG, T.SCNMLC, and T.SCNVUL have been removed since the TOE does not including any scanning capabilities; it operates exclusively via sensing. The IDSSPP indicates that "A System is one or more Sensors and/or Scanners, and one or more Analyzers" so *both* sensing and scanning are not required for a conforming solution.
- P.ACCACT, P.ANALYZ, P.DETECT, T.FALASC, T.FALREC, and T.IMPCON have been revised (see bolded text in each case) to expand their respective scopes to include extrusion as well as intrusion.

The security objectives have been copied from the IDSSPP with the following exceptions:

- O.EXPORT has been removed since the TOE does not communicate with IDS System components outside of itself. Note that the forwarding of alarms is not considered export in this regard.
- O.IDSCAN was removed since the TOE does not including any scanning capabilities and to coincide with the removal of T.SCNCFG, T.SCNMLC, and T.SCNVUL.
- O.IDANLZ and O.IDSENS have been revised (see bolded text in each case) to expand their respective scopes to include extrusion as well as intrusion.
- The IDSSPP IT environment objects OE.AUDIT_PROTECTION, OE.AUDIT_SORT, and OE.TIME have been changed to TOE objectives O.AUDIT_PROTECTION, O.AUDIT_SORT, and O.TIME, respectively. The IDSSPP is somewhat ambiguous about whether those are IT environment objectives vs. TOE objectives since one identified the TOE explicitly and all three map to TOE SFRs.

The security requirements have been copied from the IDSSPP, and all incomplete operations performed and identified, with the following exceptions:

- All of the requirements in the IDSSPP were compared against the CC version 3.1 revision 3 requirements and adjusted accordingly. These minor changes are not marked in this ST and do not serve to change the meaning of any requirement. Note that only operations performed in this ST based on the CC version 3.1 revision 3 adjusted requirements are identified in this document in accordance with the conventions defined earlier in the document.
- Along with O.EXPORT, FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1 have been removed per PD-0097 since the TOE does not communicate with IDS System components outside of itself. However, FPT_ITT.1 has been added since the TOE does protect communication between its distributed appliances.
- FIA_AFL.1 has been omitted per PD-0097 since the TOE does not provide a capability for external IT products to login to it, therefore this requirement is not applicable.
- FAU_STG.2 has been refined to indicate that the TOE prevents modification of audit records which is stronger than detecting modifications after they occur.
- FIA_UAU.5 has been added to address the TOE feature to configure alternate authentication services (LDAP, Active Directory). This does not impair the ability of the TOE to ensure users are identified and authenticated prior to providing access to its security-related functions.
- FTA_SSL.3 has been added to address the TOE feature to terminate inactive sessions after a configured time limit. This serves only to make the product more secure and does not have any bearing on any other requirement.
- FMT_SMF.1 has been added to identify the minimum set of required security management functions available in the TOE.

- The IDSSPP requirements ALC_FLR.2 has been increased to ALC_FLR.3 to reflect the TOE feature to be subject to automatic distribution of security updates.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Requirement Dependencies;
- TOE Summary Specification.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the security objectives.

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

Table 8 Security Problem Definition to Objective Correspondence

8.1.1.1 P.ACCACT

Users of the TOE shall be accountable for their actions within the IDS and XPS.

This Organizational Policy is satisfied by ensuring that:

- O.AUDIT_SORT: The O.AUDIT_SORT helps ensure accountability by providing tools to sort audit data.
- O.AUDITS: The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions.
- O.IDAUTH: The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated.
- O.TIME: The O.TIME objective ensures records can have time data to assist in ensuring user accountability.

8.1.1.2 P.ACCESS

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

This Organizational Policy is satisfied by ensuring that:

- O.ACCESS: The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
- O.AUDIT_PROTECTION: The O.AUDIT_PROTECTION ensures audit data is protected so it can be limited to access by authorized users.
- O.IDAUTH: The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses.
- O.PROTCT: The O.PROTCT objective addresses this policy by providing TOE self-protection.

8.1.1.3 P.ANALYZ

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

This Organizational Policy is satisfied by ensuring that:

- O.IDANLZ: The O.IDANLZ objective requires analytical processes be applied to data collected from Sensors and Scanners.

8.1.1.4 P.DETECT

Static configuration information that might be indicative of the potential for a future intrusion or extrusion or the occurrence of a past intrusion or extrusion 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.

This Organizational Policy is satisfied by ensuring that:

- O.AUDITS: The O.AUDITS objective addresses this policy by requiring collection of audit data.
- O.IDSENS: The O.IDSEN objective addresses this policy by requiring collection of Sensor data.
- O.TIME: The O.TIME objective ensures that the TOE can obtain or generate reliable time information for its audit and system data records.

8.1.1.5 P.INTGTY

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

This Organizational Policy is satisfied by ensuring that:

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

8.1.1.6 P.MANAGE

The TOE shall only be managed by authorized users.

This Organizational Policy is satisfied by ensuring that:

- O.ACCESS: The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.

- O.EADMIN: The O.EADMIN objective ensures there is a set of functions for administrators to use.
- O.IDAUTH: The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses.
- O.PROTCT: The O.PROTCT objective addresses this policy by providing TOE self-protection.
- OE.CREDEN: The OE.CREDEN objective requires administrators to protect all authentication data.
- OE.INSTAL: The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy.
- OE.PERSON: The OE.PERSON objective ensures competent administrators will manage the TOE.

8.1.1.7 P.PROTCT

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

This Organizational Policy is satisfied by ensuring that:

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

8.1.1.8 T.COMDIS

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

This Threat is satisfied by ensuring that:

- O.ACCESS: The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data.
- O.IDAUTH: The O.IDAUTH objective provides for authentication of users prior to any TOE data access.
- O.PROTCT: The O.PROTCT objective addresses this threat by providing TOE self-protection.

8.1.1.9 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.

This Threat is satisfied by ensuring that:

- O.ACCESS: The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data.
- O.IDAUTH: The O.IDAUTH objective provides for authentication of users prior to any TOE data access.
- O.INTEGR: The O.INTEGR objective ensures no TOE data will be modified.
- O.PROTCT: The O.PROTCT objective addresses this threat by providing TOE self-protection.

8.1.1.10 T.FACCNT

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

This Threat is satisfied by ensuring that:

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

8.1.1.11 T.FALACT

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

This Threat is satisfied by ensuring that:

- O.RESPON: The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.

8.1.1.12 T.FALASC

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

This Threat is satisfied by ensuring that:

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

8.1.1.13 T.FALREC

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

This Threat is satisfied by ensuring that:

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

8.1.1.14 T.IMPCON

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

This Threat is satisfied by ensuring that:

- O.ACCESS: The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
- O.EADMIN: The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product.
- O.IDAUTH: The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses.
- OE.INSTAL: The OE.INSTAL objective states the authorized administrators will configure the TOE properly.

8.1.1.15 T.INADVE

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

This Threat is satisfied by ensuring that:

- O.AUDITS: The O.AUDITS objective addresses this threat by requiring a TOE collect audit data.
- O.IDSENS: The O.IDSENS objective addresses this threat by requiring a TOE, that contains a Sensor, collect Sensor data.

8.1.1.16 T.INFLUX

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

This Threat is satisfied by ensuring that:

- O.OFLOWS: The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.

8.1.1.17 T.LOSSOF

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

This Threat is satisfied by ensuring that:

- O.ACCESS: The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data.
- O.IDAUTH: The O.IDAUTH objective provides for authentication of users prior to any TOE data access.

- O.INTEGR: The O.INTEGR objective ensures no TOE data will be deleted.
- O.PROTCT: The O.PROTCT objective addresses this threat by providing TOE self-protection.

8.1.1.18 T.MISACT

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

This Threat is satisfied by ensuring that:

- O.AUDITS: The O.AUDITS objective addresses this threat by requiring a TOE collect audit data.
- O.IDSENS: The O.IDSENS objective addresses this threat by requiring a TOE, that contains a Sensor, collect Sensor data.

8.1.1.19 T.MISUSE

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

This Threat is satisfied by ensuring that:

- O.AUDITS: The O.AUDITS objective addresses this threat by requiring a TOE collect audit data.
- O.IDSENS: The O.IDSENS objective addresses this threat by requiring a TOE, that contains a Sensor, collect Sensor data.

8.1.1.20 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.

This Threat is satisfied by ensuring that:

- O.ACCESS: The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
- O.IDANLZ: The O.IDANLZ objective addresses this threat by requiring the TOE to analyze System data, which includes attempts to halt the TOE.
- O.IDAUTH: The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses.
- O.IDSENS: The O.IDSENS objective addresses this threat by requiring the TOE to collect System data, which includes attempts to halt the TOE.

8.1.1.21 T.PRIVIL

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

This Threat is satisfied by ensuring that:

- O.ACCESS: The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
- O.IDAUTH: The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses.
- O.PROTCT: The O.PROTCT objective addresses this threat by providing TOE self-protection.

8.1.1.22 A.ACCESS

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

This Assumption is satisfied by ensuring that:

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

8.1.1.23 A.ASCOPE

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

This Assumption is satisfied by ensuring that:

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

8.1.1.24 A.DYNMIC

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

This Assumption is satisfied by ensuring that:

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

8.1.1.25 A.LOCATE

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

This Assumption is satisfied by ensuring that:

- OE.PHYCAL: The OE.PHYCAL provides for the physical protection of the TOE.

8.1.1.26 A.MANAGE

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

This Assumption is satisfied by ensuring that:

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

8.1.1.27 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.

This Assumption is satisfied by ensuring that:

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

8.1.1.28 A.NOTRST

The TOE can only be accessed by authorized users.

This Assumption is satisfied by ensuring that:

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

8.1.1.29 A.PROTCT

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

This Assumption is satisfied by ensuring that:

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

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that **Table 9** indicates the requirements that effectively satisfy the individual objectives. .

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.ACCESS	O.AUDIT_PROTECTION	O.AUDIT_SORT	O.AUDITS	O.EADMIN	O.IDANLZ	O.IDAUTH	O.IDSENS	O.INTEGR	O.OFLOWS	O.PROTCT	O.RESPON	O.TIME
FAU_GEN.1				X									
FAU_SAR.1					X								
FAU_SAR.2	X						X						
FAU_SAR.3			X										
FAU_SEL.1					X								
FAU_STG.2	X	X					X		X	X	X		
FAU_STG.4				X						X			
FIA_ATD.1							X						
FIA_UAU.2	X						X						
FIA_UAU.5							X						
FIA_UID.2	X						X						
FMT_MOF.1	X						X				X		
FMT_MTD.1	X						X		X		X		
FMT_SMF.1					X								
FMT_SMR.1							X						
FPT_ITT.1									X				
FPT_STM.1				X									X
FTA_SSL.3							X						
IDS_ANL.1						X							
IDS_RCT.1												X	
IDS_RDR.1	X				X		X						
IDS_SDC.1								X					
IDS_STG.1	X						X		X	X	X		
IDS_STG.2										X			
ADV_ARC.1				X	X		X		X		X		

Table 9 Objective to Requirement Correspondence

8.2.1.1 O.ACCESS

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

This TOE Security Objective is satisfied by ensuring that:

- FAU_SAR.2: The TOE is required to restrict the review of audit data to those granted with explicit read-access.
- FAU_STG.2: 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.
- FIA_UAU.2: Users authorized to access the TOE are defined using an identification and authentication process.
- FIA_UID.2: Users authorized to access the TOE are defined using an identification and authentication process.
- FMT_MOF.1: The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE.
- FMT_MTD.1: Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data.
- IDS_RDR.1: The System is required to restrict the review of System data to those granted with explicit read-access.
- IDS_STG.1: The System is required to protect the System data from any modification and unauthorized deletion.

8.2.1.2 O.AUDIT_PROTECTION

The TOE will provide the capability to protect audit information.

This TOE Security Objective is satisfied by ensuring that:

- FAU_STG.2: 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.

8.2.1.3 O.AUDIT_SORT

The TOE will provide the capability to sort the audit information.

This TOE Security Objective is satisfied by ensuring that:

- FAU_SAR.3: The TOE must provide the ability to review and manage the audit trail of the System to include sorting the audit data.

8.2.1.4 O.AUDITS

The TOE must record audit records for data accesses and use of the System functions.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: Security-relevant events must be defined and auditable for the TOE.
- FAU_STG.4: The TOE must prevent the loss of collected data in the event the audit trail is full.
- FPT_STM.1: Time stamps associated with an audit record must be reliable.

8.2.1.5 O.EADMIN

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

This TOE Security Objective is satisfied by ensuring that:

- FAU_SAR.1: The TOE must provide the ability to review and manage the audit trail of the System.
- FAU_SEL.1: The TOE must provide the ability to review and manage the audit trail of the System.

- FMT_SMF.1: The TOE is required to provide security management functions.
- IDS_RDR.1: The System must provide the ability for authorized administrators to view all System data collected and produced.

8.2.1.6 O.IDANLZ

The Analyzer must accept data from IDS and XPS Sensors and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

This TOE Security Objective is satisfied by ensuring that:

- IDS_ANL.1: The Analyzer is required to perform intrusion analysis and generate conclusions.

8.2.1.7 O.IDAUTH

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

This TOE Security Objective is satisfied by ensuring that:

- FAU_SAR.2: The TOE is required to restrict the review of audit data to those granted with explicit read-access.
- FAU_STG.2: The TOE is required to protect the stored audit records from unauthorized deletion.
- FIA_ATD.1: Security attributes of subjects use to enforce the authentication policy of the TOE must be defined.
- FIA_UAU.2: Users authorized to access the TOE are defined using an identification and authentication process.
- FIA_UAU.5: The TOE provides a built in authentication mechanism and is also able to support external authentication mechanisms. These mechanisms are used by the TOE to authenticate the claimed identities of administrative users.
- FIA_UID.2: Users authorized to access the TOE are defined using an identification and authentication process.
- FMT_MOF.1: The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE.
- FMT_MTD.1: Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data.
- FMT_SMR.1: The TOE must be able to recognize the different administrative and user roles that exist for the TOE.
- FTA_SSL.3: The TOE terminates an authorized administrators interactive session after a defined period of inactivity and requires new login with identity and authentication prior to accessing TOE functions and data.
- IDS_RDR.1: The System is required to restrict the review of System data to those granted with explicit read-access.
- IDS_STG.1: The System 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.

8.2.1.8 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 and XPS.

This TOE Security Objective is satisfied by ensuring that:

- IDS_SDC.1: A System containing a Sensor is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System. These events must be defined in the ST.

8.2.1.9 O.INTEGR

The TOE must ensure the integrity of all audit and System data.

This TOE Security Objective is satisfied by ensuring that:

- FAU_STG.2: 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.
- FMT_MTD.1: Only authorized administrators of the System may query or add audit and System data.
- FPT_ITT.1: The TOE must protect all data from modification and ensure its integrity when the data is transmitted between components of the TOE.
- IDS_STG.1: The System is required to protect the System data from any modification and unauthorized deletion.

8.2.1.10 O.OFLOWS

The TOE must appropriately handle potential audit and System data storage overflows.

This TOE Security Objective is satisfied by ensuring that:

- FAU_STG.2: 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.4: The TOE must prevent the loss of audit data in the event the audit trail is full.
- IDS_STG.1: The System 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.2: The System must prevent the loss of audit data in the event the its audit trail is full.

8.2.1.11 O.PROTCT

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

This TOE Security Objective is satisfied by ensuring that:

- FAU_STG.2: 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.
- FMT_MOF.1: The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE.
- FMT_MTD.1: Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data.
- IDS_STG.1: The System 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.

8.2.1.12 O.RESPON

The TOE must respond appropriately to analytical conclusions.

This TOE Security Objective is satisfied by ensuring that:

- IDS_RCT.1: The TOE is required to respond accordingly in the event an intrusion is detected.

8.2.1.13 O.TIME

The TOE will provide reliable timestamps to the TOE.

This TOE Security Objective is satisfied by ensuring that:

- FPT_STM.1: The TOE will provide reliable time stamp to the TOE. Time stamps associated with an audit record must be reliable.

8.3 Security Assurance Requirements Rationale

The rationale for the assurance requirements can be found in the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments, version 1.7, July 25, 2007. The only change was to further augment ALC_FLR from ALC_FLR.2 to ALC_FLR.3 to reflect the capability for automatically update the TOE based on remediated flaws.

8.4 Requirement Dependency Rationale

The following table demonstrates that all dependencies among the claimed security requirements are satisfied, and therefore the requirements work together to accomplish the overall objectives defined for the TOE.

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_SEL.1	FAU_GEN.1 and FMT_MTD.1	FAU_GEN.1 and FMT_MTD.1
FAU_STG.2	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.2
FIA_ATD.1	none	none
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.5	none	none
FIA_UID.2	none	none
FMT_MOF.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_ITT.1	none	none
FPT_STM.1	none	none
FTA_SSL.3	none	none
IDS_ANL.1	none	none
IDS_RCT.1	none	none
IDS_RDR.1	none	none
IDS_SDC.1	none	none
IDS_STG.1	none	none
IDS_STG.2	none	none
ADV_ARC.1	ADV_FSP.1 and ADV_TDS.1	ADV_FSP.2 and ADV_TDS.1
ADV_FSP.2	ADV_TDS.1	ADV_TDS.1
ADV_TDS.1	ADV_FSP.2	ADV_FSP.2
AGD_OPE.1	ADV_FSP.1	ADV_FSP.2
AGD_PRE.1	none	none
ALC_CMC.2	ALC_CMS.1	ALC_CMS.2
ALC_CMS.2	none	none
ALC_DEL.1	none	none
ALC_FLR.3	none	none
ATE_COV.1	ADV_FSP.2 and ATE_FUN.1	ADV_FSP.2 and ATE_FUN.1
ATE_FUN.1	ATE_COV.1	ATE_COV.1
ATE_IND.2	ADV_FSP.2 and AGD_OPE.1 and AGD_PRE.1 and ATE_COV.1 and ATE_FUN.1	ADV_FSP.2 and AGD_OPE.1 and AGD_PRE.1 and ATE_COV.1 and ATE_FUN.1
AVA_VAN.2	ADV_ARC.1 and ADV_FSP.2 and ADV_TDS.1 and AGD_OPE.1 and	ADV_ARC.1 and ADV_FSP.2 and ADV_TDS.1 and AGD_OPE.1 and

ST Requirement	CC Dependencies	ST Dependencies
	AGD_PRE.1	AGD_PRE.1

Table 10 Security Requirement Dependencies

Note that the 'ST Requirement' column identifies the requirements found in this ST; the 'CC Dependencies' column identifies dependencies per requirement as defined in the CC; and, the 'ST Dependencies' column identifies the requirements in this ST that satisfy the CC dependencies.

8.5 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 11 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Security Audit	Identification and Authentication	Security Management	Protection of the TOE Security Functions	TOE access	Extrusion and Intrusion Detection
FAU_GEN.1	X					
FAU_SAR.1	X					
FAU_SAR.2	X					
FAU_SAR.3	X					
FAU_SEL.1	X					
FAU_STG.2	X					
FAU_STG.4	X					
FIA_ATD.1		X				
FIA_UAU.2		X				
FIA_UAU.5		X				
FIA_UID.2		X				
FMT_MOF.1			X			
FMT_MTD.1			X			
FMT_SMF.1			X			
FMT_SMR.1			X			
FPT_ITT.1				X		
FPT_STM.1				X		
FTA_SSL.3					X	
IDS_ANL.1						X
IDS_RCT.1						X

IDS_RDR.1						X
IDS_SDC.1						X
IDS_STG.1						X
IDS_STG.2						X

Table 11 Security Functions vs. Requirements Mapping