Fidelis XPS™ Security Target

Version 1.0
29 October 2008

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

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

TABLE OF CONTENTS

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 data leakage prevention where TOE appliances detect attempts to send inappropriate information[1], based on configuration, from one network to another; raise alarms and react to extrusion attempts to prevent an attack.

The ST contains the following additional sections:

- TOE Description (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 Environment (Section 3)—this section details the expectations of the environment, the threats that are countered by the TOE and the Information Technology (IT) environment, as well as, the assumptions pertaining to TOE behavior.

- Security Objectives (Section 4)—this section details the security objectives of the TOE and the IT environment.

- IT Security Requirements (Section 5)—this section presents the Security Functional Requirements (SFRs) for the TOE and IT environment that supports the TOE; and details the Security Assurance Requirements (SARs) for Evaluated Assurance Level (EAL) 2 augmented with the Life Cycle, Systemic Flaw Remediation SAR (ALC_FLR.3).

- TOE Summary Specification (TSS) (Section 6)—this section describes the security functions represented in the TOE that satisfy the SFRs.

- Protection Profile Claims (Section 7)—this section presents any protection profile claims.

- Rationale (Section 8)—this section closes the ST with the justifications of the security objectives, requirements and TSS 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 – 29 October 2008

TOE Identification – Fidelis XPS 5.0.3 includes four hardware component options where a minimum of one (1) CommandPost appliance is required with up to three (3) sensor options[2] as:

1) Appliance:

- CommandPost (for one (1) to five (5) sensors), or

- CommandPost Plus (for six (6) or more sensors)

2) Fidelis XPS Direct Sensor(s):

- Fidelis XPS Direct 100 (for networks up to 100Mbps)

- Fidelis XPS Direct 1000 (for networks up to 1Gbps)

3) Fidelis XPS Proxy Sensor(s):

---

[1] Potentially inappropriate information refers to administrator-configured Extrusion Policies that prohibit information such as sexually-explicit, pornographic and/or offensive traffic observed on the network.

[2] The requirement is to have at least one sensor at any time; however, the upper limit is based on the CommandPost appliance.

- Fidelis XPS Proxy (for ICAP integration with proxy servers up to 100Mbps)

- Fidelis XPS Proxy Plus (for ICAP integration with proxy servers up to 1Gbps)

4) Fidelis XPS Mail Sensor

The following sensors are included in the Fidelis XPS 5.0.3 suite, however they are not included in the evaluated configuration.

- Fidelis XPS Internal (for internal network transfers)

- Fidelis XPS Web Walker (for content inspection of an enterprise's public web page)

- Fidelis XPS SCIP (for content inspection of information shared by a partner product)

- Fidelis XPS Scout (a single unit combined CommandPost and sensor used for risk assessment)

All of the claimed security functions are provided by the Fidelis XPS Direct, Fidelis XPS Proxy, and Fidelis XPS Mail sensors running software version 5.0.3.

TOE Developer – Fidelis Security Systems, Inc.

Evaluation Sponsor – Fidelis Security Systems, Inc.

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005.

    - Part 2 Extended

- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.

    - Part 3 Conformant

    - Assurance Level: EAL 2 augmented with ALC_FLR.3

    - Strength of Function Claim: SOF-Basic

1.3 Conventions, Terminology and Acronyms

1.3.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements (SFRs) – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.

    o 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 FMT_MTD.1a and FMT_MTD.1b indicate that the ST includes two iterations of the FMT_MTD.1 requirement, a and b.

    o Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).

- o 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*]).

- o 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 …").

- o Explicit: allows the specification of a new class or family of components to be created to address TOE-specific SFRs that are not readily drawn from Part 2 of the CC. This ST contains an explicit Class "Fidelis XPS Component Requirements (FEP)" that addresses the Fidelis XPS functionality of the TOE. The FEP requirements are then de-composed to similar family components from the Intrusion Detection System (IDS) PP for some consistency. Further, explicitly stated requirements have (EXP) appended to the end of each component to denote that it has been explicitly stated. Example: FEP_ANL.1 (EXP) refers to Extrusion analysis.

- • 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 and Acronyms

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

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 console appliance of the TOE.
Content	Output of TOE decoder sent to TOE sensor analyzers that removes 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.
Decoders	Attributes of the alert after fingerprint determines if a session is in violation or not. 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	A rule violation. One or more events are reported as an alert if the rule action is configured to alert.
Extrusion	An event.
Extrusion Policy	Specific policies configured within the TOE by authorized administrators to define extrusions to be monitored on the network.
Fidelis XPS	Fidelis Extrusion Prevention System
Fidelis XPS Direct	Unique name for the Fidelis XPS Direct sensor appliance of the TOE for processing data over networks connected directly to the internet. Fidelis XPS Direct sensors come in three versions: Fidelis XPS10 for networks with up to 10 Mb/s data; Fidelis XPS100 for networks up to 100Mb/s; and Fidelis XPS1000 for networks up to 1 Gb/s.

Fidelis XPS Proxy	Unique name for the Fidelis XPS Proxy sensor appliance of the TOE for processing data from a third party network proxy appliance. The Fidelis XPS Proxy sensor serves as a content inspection engine for a proxy by utilizing the Internet Content Adaptation Protocol (ICAP).
Fidelis XPS Mail	Unique name for the Fidelis XPS Mail sensor appliance of the TOE for processing e-mail. The Fidelis XPS Mail sensor can be configured as a Mail Transfer Agent (MTA) or as a content inspection engine for a third party MTA by utilizing the milter protocol.
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').
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
MTA	Mail Transfer Agent
ORC	Operational Research Consultants, Inc.
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
Policy	TOE 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 Proxy, and Fidelis XPS Mail hardware appliances 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.

2. TOE Description

The Target of Evaluation (TOE) is Fidelis XPS™, Version 5.0.3[3]. Fidelis XPS includes four hardware appliances: three Fidelis Sensor appliance options (Fidelis XPS Direct, Fidelis XPS Proxy (sometimes referred to as Fidelis XPS ICAP[4]), and Fidelis XPS Mail) and a Fidelis XPS CommandPost™ Management Console Appliance[5]. Note that the CommandPost appliance is the TOE component that allows user access and thus supports access security; however, the sensor(s) implement all extrusion functionality. There are two versions: CommandPost (supports 1-5 sensors) and CommandPost Plus (supports 6 or more sensors), depending on network deployment. The TOE appliances run on a hardened CentOS Linux kernel version 2.6.9 (2.6.9-42.10.ELsmp to be exact) with MySQL 5.0.28 Enterprise Version. A minimum of one CommandPost is required when using any of the TOE sensors, and at least one sensor is required. The following diagram pertains.

---

[3] Note that all of the TOE appliances (i.e., CommandPost, Fidelis XPS Direct, Fidelis XPS Proxy, Fidelis XPS Mail) run on Fidelis XPS, Version 5.0.3 software for the evaluated configuration.

[4] Generally this sensor will be identified as the Fidelis XPS Proxy; however, some of the documentation may indicate ICAP where it is describing the Proxy sensor.

[5] Although there are two versions of the CommandPost management console appliance (CommandPost and CommandPost Plus as described in Section 1.1) they both provide the same TOE functionality.
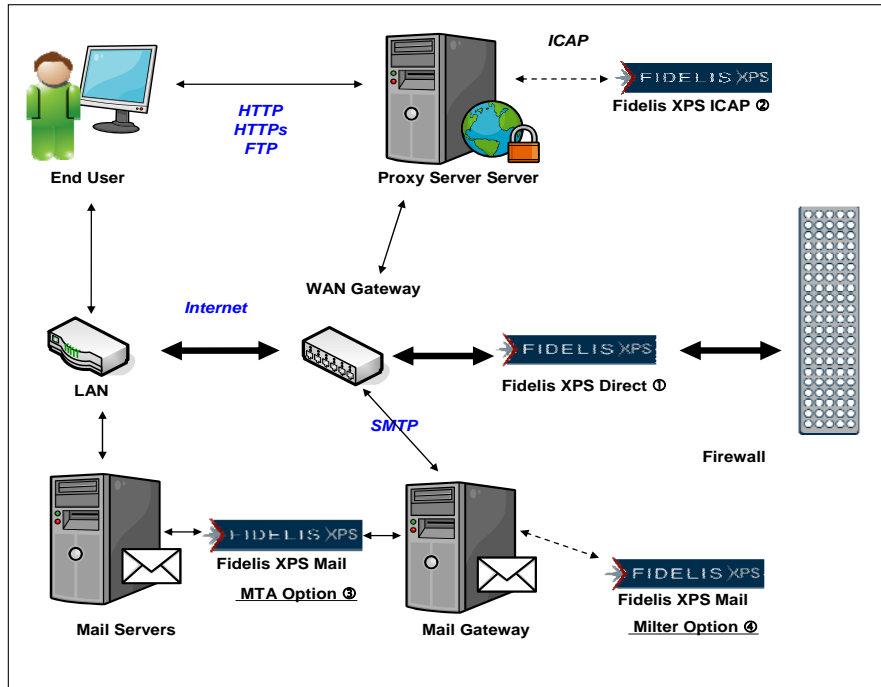
Fidelis XPS Sensor(s)—several options are available where they only differ in the hardware that is required to operate at network different bandwidth rates.

- Fidelis XPS Direct network sensor that monitors and enforces policy across all 65,535 ports on the network

  - Fidelis XPS Direct 100 – for networks up to 100Mbps

  - Fidelis XPS Direct 1000 – for networks up to 1Gbps

- Fidelis XPS Proxy sensor monitors and enforces policy for traffic flowing through ICAP-enabled proxy servers

  - Fidelis XPS Proxy – for ICAP integration with proxy servers up to 100Mbps

  - Fidelis XPS Proxy Plus – for ICAP integration with proxy servers up to 1000Mbps

- Fidelis XPS Mail sensor (single version only) monitors and enforces policy for Simple Mail Transfer Protocol (SMTP) e-mail traffic.

The sensors listed below are also included in the Fidelis XPS 5.0.3 suite, however they are not included in the evaluated configuration. All of the claimed security functions are provided by the Fidelis XPS 5.0.3 Direct, Fidelis XPS 5.0.3 Proxy, and Fidelis XPS 5.0.3 Mail sensors.

- Fidelis XPS Internal (for internal network transfers)

- Fidelis XPS Web Walker (for content inspection of an enterprise's public web page)

- Fidelis XPS SCIP (for content inspection of information shared by a partner product)

- Fidelis XPS Scout (a single unit combined CommandPost and sensor used for risk assessment)

Note that hereinafter, the Fidelis XPS Sensor appliance identification will not include the specific identifier of Direct, ICAP or Mail, unless that has a direct impact on the specific Sensor functionality. Further, the Fidelis XPS Sensor(s) may also be referred to as just the Sensor(s), where all references pertain to the same TOE component providing this functionality. Also note that for a given instance of the TOE, there would be a single CommandPost associated with one or more Fidelis XPS Sensors. The Fidelis XPS Sensor's are used to monitor and capture

network traffic and the CommandPost is used to manage the associated Fidelis XPS Sensors and to analyze the information resulting from Sensor actions, as forwarded to the CommandPost by the sensor(s).

The CommandPost is accessed via a web browser to enable authorized administrators to configure policies; review audit and analyze results. The workstation that authorized administrators use to access the CommandPost is sometimes referred to as a CommandPost Client; however, there is no functionality being provided as all security is provided by the CommandPost and Fidelis XPS sensor components.

The evaluated configuration of the TOE includes a minimum of one CommandPost (either CommandPost or CommandPost Plus) and one or more Fidelis XPS Sensors (i.e., Fidelis XPS Direct, Fidelis XPS Proxy and/or Fidelis XPS Mail). All of the component devices are part of the TOE under evaluation.

Note that the TOE requires the use of a DOD-approved External Certificate Authority (ECA) within the IT environment.

2.1 TOE Overview

The TOE is an Extrusion Prevention System® (Fidelis XPS). Unlike Intrusion Detection Systems, designed to detect potential intruders, the TOE is designed to detect attempts to send potentially inappropriate information from one network to another (e.g., network abuse). It is designed to operate continuously, observing network traffic as it is perceived on the attached networks. Traffic to a Fidelis XPS Direct sensor is reassembled into TCP packets and session; protocols are identified; applications are identified; and contents are analyzed in order to determine whether they seem to contain anything inappropriate based on the applicable rules. When inappropriate seeming content is identified, the sensor attempts to terminate the network connection by either issuing TCP resets to both ends of the TCP connection and/or dropping packets depending on configuration, and sends an alert to the CommandPost.

The Fidelis XPS sensor software is designed around a series of layers where the first layer, known as DirectWire, 'sniffs' packets from the attached networks. Unless these packets belong to a session that has already been approved by the Sensor, they would be sent to the next layer for further analysis. The next layer performs TCP Reassembly, organizing the network traffic into TCP streams and once a stream has been identified, it is forwarded to the next layer where the payload is decoded. This layer identifies protocols and applications and ultimately reveals the contents. Note that the TOE can be configured to handle unrecognized protocols and applications as the authorized administrator desires (e.g., allow or reject). Authorized administrators configure Extrusion 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 issues TCP resets to both ends of the session and sends an alert to the CommandPost logging the potential problem. At that point, the CommandPost's authorized administrator would decide whether it was an actual extrusion or something else (e.g., false positive). Note that the rules are part of the configured Extrusion Policy for TOE operation.

The Fidelis XPS Direct sensor operates as described above, utilizing all layers of the software. The Fidelis XPS Proxy sensor utilizes an ICAP protocol layer that runs in place of DirectWire. In this case, traffic received over the wire is reassembled in accordance with ICAP. The reassembled packets are sent to the next layer, as described above.

The Fidelis XPS Mail sensor processes e-mail and also utilizes the same software stack. In this case, received traffic is handled by the milter protocol layer. This layer will reassemble the TCP session and forward to the next layer for payload decoding. When the Fidelis XPS Mail sensor is running as an MTA, the e-mail handler is embedded on the appliance. This e-mail handler communicates to the sensor software using the milter protocol. When the Fidelis XPS Mail sensor is configured in out-of-band/milter mode, it relies on an external MTA in the IT environment utilizing the milter interface.

Fidelis XPS Internal is a network sensor that monitors and enforces Fidelis XPS policy on internal network traffic including data transfers and directory queries. Based on the same hardware as Fidelis XPS Direct 1000, Fidelis XPS Internal runs the same software as all Fidelis XPS sensors. Fidelis XPS Internal supports Oracle and DB2

databases, SMB/CIFS/SAMBA file transfers, and LDAP queries. Fidelis XPS Internal is managed by the CommandPost management console.

Fidelis XPS Web Walker is a sensor that enables organizations to scan web sites for sensitive or protected content that may violate privacy compliance or digital asset protection policies. Fidelis XPS Web Walker is based on the same hardware configuration as CommandPost and Fidelis XPS Mail, and runs the same software as all Fidelis XPS sensors. Fidelis XPS Web Walker is managed by the CommandPost management console.

The Fidelis XPS SCIP sensor is designed to analyze content received from another network device or application via Simple Content Inspection Protocol (SCIP), rather than sniffing live network traffic like the Fidelis XPS Direct and Internal sensors. Fidelis XPS SCIP is based on the same hardware as Fidelis XPS Proxy, and runs the same software as all Fidelis sensors. Fidelis XPS SCIP is managed by the CommandPost management console.

Fidelis XPS Scout combines the traffic inspection and content analysis functionality of Fidelis XPS Direct and the management capabilities of CommandPost into a single, portable appliance. The all-in-one appliance is intended for use by audit, assessment and incident response teams to quickly assess compliance with internal policies and external regulations. Fidelis XPS Scout runs the same software as all Fidelis sensors.

The Fidelis XPS Internal, Fidelis XPS Web Walker, Fidelis XPS SCIP, and Fidelis XPS Scout sensors included in the Fidelis XPS 5.0.3 suite, however they are not included in the evaluated configuration. All of the claimed security functions are provided by the Fidelis XPS 5.0.3 Direct, Fidelis XPS 5.0.3 Proxy, and Fidelis XPS 5.0.3 Mail sensors.

The sensor software for payload decoding, analysis, and rule evaluation is common to all modes. The difference occurs at the lower layers which receive packets from the appliance NIC and re-assemble them into sessions applicable for decoding.

The evaluated configuration of the TOE requires a separate sensor appliance for each mode of operation (i.e., Fidelis XPS Direct, Fidelis XPS Proxy, and/or Fidelis XPS Mail) and includes five 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 sensor out-of-band**: via network tap; 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 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 Proxy sensor**: when connected to a third party proxy appliance, the Fidelis XPS Proxy sensor will provide content inspection. All actions are carried out by the proxy appliance based on response from the Fidelis XPS Proxy 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 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**: can be connected either inline or out-of-band. While 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 Fidelis XPS Mail sensor and can be managed via CommandPost.

- **Fidelis XPS Mail sensor out-of-band[6]**: When connected out of band, the Fidelis XPS Mail sensor serves as a content inspection agent to a third party MTA. Communication between the MTA and Fidelis XPS Mail sensor utilizes the milter protocol. All Fidelis XPS Mail actions are the same as the Mail sensor inline configuration, however, quarantined e-mail is held by the third party MTA in the IT environment and must be managed by its quarantine interface. CommandPost cannot be used for quarantine management in this case.

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.

Note that the Fidelis XPS Sensor collects and conducts initial analysis of information containing events that are indicative of inappropriate activity as configured by an authorized administrator. Collected information is sent to the CommandPost for additional analysis, subsequent action and storage.

The TOE provides eight (8) 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 component configuration and users. The pre-defined roles constitute the main categories of CommandPost functionality.

The TOE supports a third-party Certificate Authority (CA) in the IT environment to provide Public Key Infrastructure (PKI) functionality where a users own CA certificate 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 indicated above a given Fidelis XPS configuration includes a CommandPost appliance and one or more Fidelis XPS sensor appliance. Each of these components is a self-contained hardware device and the following sub-sections identify the specific IT environment components required for the operation of the TOE.

2.2.1.1 Certificate Authority (CA)

The TOE requires a CA in the IT environment for Public Key Infrastructure (PKI) certificate importation into the TOE. The ECA 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 6 or 7; or Firefox 1 or 2.
- Macromedia Flash Player
- WinSCP secure FTP client

2.2.1.3 Additional Hardware Specific's

Network Taps—required for lossless network monitoring by Fidelis XPS as they replicate all network traffic with no data loss or performance degradation. Network taps guarantee complete traffic replication.

---

[6] Also known as milter mode since use of the milter protocol interface is required.

SPAN Ports—connecting the TOE appliances to the SPAN ports on the router or switch is not supported in the evaluated configuration due to traffic volumes as they do not guarantee complete traffic replication and/or processing of all data.

Proxy appliance—connecting the TOE Proxy appliance to analyze proxied traffic.

Mail Transfer Agent (MTA)—connecting the TOE Mail appliance to analyze e-mail, if desired in the IT environment. The MTA is only required if the Fidelis XPS Mail sensor is connected in the out-of-band mode 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.

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
- Cryptographic support
- User data protection
- Fidelis XPS Component Requirements (EXP)
- Identification and authentication
- Security management
- Protection of the TSF
- Session Locking

2.2.2.1 Security audit

The TOE generates an audit record of security-relevant events that includes the data/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. TOE audit records are stored on the CommandPost appliance in a MySQL data repository and prevents audit data loss by overwriting the oldest stored audit records if the audit trail is full. Only an authorized administrators with audit read privilege are able to review and interpret the results.

Refer to Sections 5.1.1 and 6.1.1 specific security audit information.

2.2.2.2 Cryptographic support

The TOE hashes passwords using the MySQL's embedded SHA1() function to hash and store user passwords and the TOE implements the RFC 1321-based free implementation of the RSA MD5 checksum library to hash exact file detection for Exact Content analyzer fingerprints.

Refer to Sections 5.1.2 and 6.1.2 for specific cryptographic support information.

2.2.2.3 User data protection

The TOE enforces an access control mechanism to control users' access to Fidelis XPS objects and administrative interfaces.

Refer to Sections 5.1.3 and 6.1.3 for specific user data protection information.

2.2.2.4 Fidelis XPS Component Requirements (EXP)

The TOE uses a set of rules to inspect (e.g., sense via the Fidelis XPS Sensor) the network traffic and collect Fidelis XPS data based on potentially inappropriate content detected per the configured rules. The TOE contains a set of default rules/policies and allows an authorized administrator to customize the rules and policies used. The TOE analyzes the collected data and reacts to data leakage events. The TOE provides extrusion 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 within the MySQL data repository on the CommandPost.

Refer to Sections 5.1.4 and 6.1.4 for specific functional Fidelis XPS component requirements information.

2.2.2.5 Identification and authentication

The CommandPost requires that all administrative users are identified and authenticated before access is allowed to perform security-relevant management functions. The CommandPost maintains the administrator accounts that consist of the user identity (username), authentication data (password), authorizations (role with privileges and access) and assignments (alert management group and sensor). The TOE verifies password length and allowed character (e.g., authorized) compliance and rejects those that do not comply.

Refer to Sections 5.1.5 and 6.1.5 for specific identification and authentication information.

2.2.2.6 Security management

The CommandPost is accessed via its web-based Graphical User Interface (GUI) that provides the interface to manage the Fidelis XPS Sensor(s). All users of the TOE are considered authorized 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 Function (TSF) restricts 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 eight (8) defined functions of the system: Alert Management, Quarantine Management, Alert Issue Tracking, Alert Reporting, Policy Authoring, User Management, System Configuration, and Audit Trail. 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 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-built roles includes 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. Alerts are generated by rule violations. 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 Alert Manager role, 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 (hereinafter referred to as Network Admin) 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.

Refer to Sections 5.1.6 and 6.1.6 for specific security management information.

2.2.2.7 Protection of the TSF

The packets passing between the CommandPost and Fidelis XPS Sensors are protected using FIPS 140-2 certified OpenSSL, Version 1.1.2 (FIPS certificate 918) 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 sends the information to the 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 to provide non-bypassability and domain separation. Additionally, the CommandPost hardware provides a reliable time stamp for security audit generation as well as collected system data events. The evaluation configuration of the TOE does not support any additional software to be installed on the appliance devices.

Refer to Sections 5.1.7 and 6.1.7 for specific protection of the TSF information.

2.2.2.8 Session Locking

The TOE terminates any browser session between the web-based interface and the CommandPost after 15 minutes of inactivity and requires the authorized administrator to re-login to establish a new session. This functionality is hard-coded within the TOE.

Refer to Sections 5.1.8 and 6.1.8 for additional TOE access information.

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.

Refer to Section 6.2 for information about these and other evidence assurance documents associated with the Fidelis XPS.

3. Security Environment

This section contains assumptions, threats and objectives regarding the security environment and the intended usage of the TOE. Note that the majority of the identified security environment has been derived from the Intrusion Detection System (IDS) System PP (IDSSPP), although they have been modified to reflect the Fidelis XPS functionality of the TOE. Note that the TOE is not an IDS and therefore is not claiming conformance with the IDSSPP.

3.1 Threats

T.CHANNELS	An authorized administrator may attempt to use an unapproved channel or non-standard ports to circumvent the security functionality of the TOE.
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	Attempts to access TOE data or security functions by unauthorized users may go undetected.
T.FAIL	An authorized administrator may not configure the TOE to react to identified/recognized or suspected vulnerabilities and/or inappropriate activity based on extrusion data thus circumventing the purpose of the TOE to protect the network.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential extrusions to go undetected.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.RESPOND	Inappropriate network traffic may go undetected and not be subject to analysis.
T.STORAGE	Potential audit and system data may not be recorded due to storage loss or overflow.
T.TIME	A reliable time stamp may not be available for audit purposes.

3.2 Assumptions

A.ACCESS	The TOE has access to all network data for collection and analysis.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.
A.LOCATE	The TOE appliances will be located within controlled access facilities, which will prevent unauthorized physical access.

A.MANAGE   There will be one or more competent and appropriately trained 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.

4. Security Objectives

The following subsections describe objectives for the TOE and its environment that are consistent with the environment described in the previous section. Note that the majority of the identified security objectives have been derived from the IDSSPP, although they have been modified to reflect the Fidelis XPS functionality of the TOE vice IDS as the TOE does not claim conformance to any PP. The IDSSPP security objectives were used as a baseline to reflect the similarity between IDS and Fidelis XPS, although these have been revised to reflect the TOE (e.g., Fidelis XPS).

4.1 Security Objectives for the TOE

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

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

O.CRYPTO   The TOE must provide cryptographic encryption and decryption for communications between components.

O.EADMIN   The TOE must include a set of functions that allow effective management of its functions and data by properly trained administrators who are not evil and follow administrator guidance.

O.EPANLZ   The TOE console must accept data from sensors and then apply analytical processes and information to derive conclusions about extrusions (past, present, or future).

O.FIDELISXPSENS   The sensor must collect all data that is indicative of inappropriate activity that results from misuse, access, or malicious activity of the monitored network and forwards collected data to CommandPost for further analysis, action and storage.

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

O.INTEGR   The TOE must ensure the integrity of all collected, analyzed and stored audit and system data.

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

O.RESPON   The TOE must respond appropriately to analytical conclusions where the TOE is the source.

O.TIME   The TOE must have a reliable time stamp for audit purposes.

4.2 Security Objectives for the IT 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.CRYPTO   The IT environment must provide the TOE with a secure and effective capability to protect sensitive, security-relevant data transferred across a network between itself and other network entities.

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 systems 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

This section includes the statements of security requirements that are included in the Fidelis XPS for which operations have been completed. This section describes the Security Functional Requirements (SFRs) for the TOE and the IT environment, as well as the Security Assurance Requirements (SARs) for the TOE at EAL2 augmented with ALC_FLR.3.

5.1 TOE Security Functional Requirements

The following table describes the SFRs that are being satisfied by Fidelis XPS. All SFRs are drawn from Part 2 of the CC and are supplemented with explicitly stated requirements in the created FEP class.

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_STG.1: Protected audit trail storage
	FAU_STG.4: Prevention of audit data loss
FCS: Cryptographic support	FCS_COP.1a: Cryptographic operation
	FCS_COP.1b: Cryptographic operation
FDP: User data protection	FDP_ACC.1: Subset access control
	FDP_ACF.1: Security attribute based access control
FEP: Fidelis XPS Component Requirements (EXP)	FEP_ANL.1 (EXP): Extrusion analysis
	FEP_RCT.1 (EXP): Extrusion react
	FEP_RDR.1 (EXP): Restricted Data Review
	FEP_SDC.1 (EXP): Extrusion Data Collection
	FEP_STG.1 (EXP): Guarantee of System Data Availability
	FEP_STG.2 (EXP): Prevention of System Data Loss
FIA: Identification and authentication	FIA_ATD.1: User attribute definition
	FIA_UAU.1: Timing of authentication
	FIA_UID.1: Timing of identification
FMT: Security management	FMT_MOF.1: Management of security functions behavior
	FMT_MSA.1: Management of security attributes
	FMT_MSA.3: Static attribute initialization
	FMT_MTD.1a: Management of TSF data
	FMT_MTD.1b: Management of TSF data
	FMT_MTD.1c: Management of TSF data
	FMT_MTD.1d: Management of TSF data
	FMT_MTD.1e: Management of TSF data
	FMT_SMF.1: Specification of management functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_ITT.1: Basic internal TSF data transfer protection
	FPT_RVM.1: Non-bypassability of the TSP
	FPT_SEP.1: TSF domain separation
	FPT_STM.1: Reliable time stamps
FTA: Session Locking	FTA_SSL.1: TSF-initiated session locking

Table 1 TOE Security Functional Components

5.1.1   Security audit (FAU)

5.1.1.1   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 [*not specified*] level of audit; and c) [**events listed in Table 2**].

FAU_GEN.1.2   The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **the additional information specified in the Details column of the following table**].

COMPONENT	EVENT	DETAILS
FAU_SAR.1	Audit review	User identity
FAU_SAR.2	Audit access	User identity
FIA_UAU.1	All use of the authentication mechanism	User identity
FIA_UID.1	All use of the user identification mechanism	User identity
FMT_MOF.1	All modifications of the functions related to system data collection, analysis and reaction	User identity
FMT_MSA.1	Modifications to the Access Control Policy role/group assignment(s)	User identity
FMT_MSA.3	All modifications to the Access Control Policies restrictive default values for security attributes	
FMT_MTD.1a,b,d	All modifications to the values of TSF data	User identity
FMT_SMF.1	All use of the management functions	User identity
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

Table 2 Auditable Events

5.1.1.2   Audit review (FAU_SAR.1)

FAU_SAR.1.1   The TSF shall provide [**System Administrators, Authorized Administrators granted the Audit privilege, by role**] with the capability to read [**all audit data**] 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.

5.1.1.3   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.

5.1.1.4   Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1   The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2   The TSF shall be able to [*prevent*] unauthorized modifications to the stored audit records in the audit trail.

5.1.1.5   Prevention of audit data loss (FAU_STG.4)

FAU_STG.4.1   The TSF shall provide [*overwrite the oldest stored audit records*] and [**no additional actions**] if the audit trail is full.

5.1.2 Cryptographic support (FCS_COP)

5.1.2.1 Cryptographic operation (FCS_COP.1a)

FCS_COP.1a.1 The TSF shall perform [**password hashing**] in accordance with a specified cryptographic algorithm [**SHA-1**] and cryptographic key sizes **[N/A]** that meet the following: [**FIPS 180-2**]**.**

5.1.2.2 Cryptographic operation (FCS_COP.1b)

FCS_COP.1b.1 The TSF shall perform [**Exact Content analyzer fingerprint hashing**] in accordance with a specified cryptographic algorithm [**MD5**] and cryptographic key sizes **[N/A]** that meet the following: [**RFC 1321**]**.**

5.1.3 User data protection (FDP)

5.1.3.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1 The TSF shall enforce the [**Access Control Policy**] on [
subjects: users;
objects: alerts, quarantine, tickets, reports, policies, users, config, audit, no access;
operations: full control (read, write), view only (read), no access].

5.1.3.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the [**Access Control Policy**] to objects based on the following: [**subject user security attributes: user identity, sensor/group assignment (object privilege assignment are based on role via sensor group membership);
object security attributes: ACL**].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
- **The full control operation is granted if the ACL associated to the TOE functionality access level and the object grants the user name/sensor privilege;**
- **The view only operation is granted if the user name via the user's sensor group has the appropriate object viewing privilege access level;**
- **Every user access first verifies user privilege; and/or**
- **Other requested operations are granted if the ACL associated to the object grants the user name/sensor group access permission.**].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [
- **The System Administrator is granted all access to all objects;**
- **No user can create new users with privileges greater than those held by the user creating the new user; and**
- **No user can add users to a role with privileges greater than those held by the user adding the user to a role.**]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [
- **The No Role user(s) are explicitly denied access to all objects as this user has the No Access administrative object privilege**].

Application Note: Within the TOE, users are assigned to a role, granted access to sensors and access to alert groups. Note that the role is only applicable to the assigned sensors/group within the TOE.

5.1.4 Fidelis XPS Component Requirements (FEP) (EXP)

5.1.4.1 Extrusion analysis (FEP_ANL.1 (EXP)) [7]

FEP_ANL.1.1 (EXP)   The TSF shall perform the following extrusion analysis function(s) on all data received:
  a)   Identity profiling;
  b)   Embedded images;
  c)   Encrypted files;
  d)   Exact content (via MD5 signature);
  e)   Partial content;
  f)   File signature;
  g)   File names;
  h)   Keyword;
  i)   Keyword sequence;
  j)   Regular expression;
  k)   Channel; and
  l)   Location.

FEP_ANL.1.2 (EXP)   The TSF shall apply a set of rules based on any combination of protocol, application, application data content patterns where analysis data is logged as defined by either a System Administrator or an authorized administrator with the policies privilege to identify potentially inappropriate network traffic.

FEP_ANL.1.3 (EXP)   The TSF shall record within each analytical result at least the following information:
  a.   Unique alert number;
  b.   Alert priority;
  c.   Alert rule;
  d.   Time and date of alert;
  e.   Whether a TCP session was recorded by the TOE; if applicable
  f.   Sensor that identified the alert;
  g.   Alert summary or rule used in detecting alert;
  h.   Attributes of the alert from TOE decoders[8];
  i.   Protocol on which alert occurred;
  j.   Source address;
  k.   Destination address;
  l.   Source and Destination TCP port, if applicable;
  m.   IP layer information;
  n.   Forensic data for the alert, representing the data used to determine the rule violation; and
  o.   Option to view either hexadecimal or text data for forensic data.

Application Note: Each sensor performs all analysis on the traffic supplied to it, where the only difference is in the reaction possibilities reflected in FEP_RCT.1.3-5.

5.1.4.2 Extrusion react (FEP_RCT.1 (EXP))

FEP_RCT.1.1 (EXP)   The TSF Direct sensor out-of-band shall issue an alert to the CommandPost and/or prevent the session by sending TCP resets to the session endpoints when potentially inappropriate network traffic is detected.

FEP_RCT.1.2 (EXP)   The TSF Direct sensor in-line shall issue an alert to the CommandPost, send TCP resets to the session endpoints, drop the packets and/or throttle the session by dropping packets at a configured rate when potentially inappropriate network traffic is detected.

---

[7] Application refers to the software that creates the content such as Microsoft Word whereas application data refers to the content of the file such that FEP_ANL.1.2 states that a rule can combine the protocol (e.g., HTTP) with the application (Word) with the content of the file.

[8] 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.

FEP_RCT.1.3 (EXP)   The TSF Mail sensor in MTA mode shall issue an alert to the CommandPost, quarantine email, redirect email, and/or prevent email by dropping it when potentially inappropriate network traffic is detected.

FEP_RCT.1.4 (EXP)   The TSF Mail sensor in milter mode shall issue an alert to the CommandPost and respond to the external MTA using the milter protocol with the appropriate action of forward, quarantine, or prevent the email when potentially inappropriate network traffic is detected.

FEP_RCT.1.5 (EXP)   The TSF ICAP sensor shall issue an alert to the CommandPost and respond to the external proxy using the ICAP protocol to allow, deny, or redirect to a pre-configured custom URL when potentially inappropriate network traffic is detected.

Application Note: Each sensor performs all analysis on the traffic supplied to it, where the only difference is in the reaction possibilities reflected in the aforementioned elements. For example, if only one sensor is configured, then the other types of traffic are not being collected and no alerts would be generated.

5.1.4.3 Restricted Data Review (FEP_RDR.1 (EXP))

FEP_RDR.1.1 (EXP)   The TSF shall provide an authorized administrator with the capability to read all collected data.

FEP_RDR.1.2 (EXP)   The TSF shall provide collected data in a manner suitable for the user to interpret the information.

FEP_RDR.1.3 (EXP)   The TSF shall prohibit all users read access to the collected data, except those users that have been granted explicit read-access.

5.1.4.4 Extrusion Data Collection (FEP_SDC.1 (EXP))

FEP_SDC.1.1 (EXP)   The TSF shall be able to collect network TCP sessions (i.e., extrusions) from IT Systems that violate System Administrator defined policies.

FEP_SDC.1.2 (EXP)   The TSF shall store TCP packet session payload, up to the limit specified by the System Administrator.

5.1.4.5 Guarantee of System Data Availability (FEP_STG.1 (EXP))

FEP_STG.1.1 (EXP)   The TSF shall protect stored data from unauthorized deletion and modification.

5.1.4.6 Prevention of System data loss (FEP_STG.2 (EXP))

FEP_STG.2.1 (EXP)   The TSF shall overwrite the oldest stored data if the storage capacity has been reached.

5.1.5   Identification and authentication (FIA)

5.1.5.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1   The TSF shall maintain the following list of security attributes belonging to individual users: [**User identity, Authentication data, Authorizations and Assignment(s)**].

5.1.5.2 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1   The TSF shall allow [**network traffic collection and analysis**] on behalf of the user to be performed before the user is authenticated.

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

5.1.5.3 Timing of identification (FIA_UID.1)

FIA_UID.1.1   The TSF shall allow [**network traffic collection and analysis**] on behalf of the user to be performed before the user is identified.

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

Application Note: TOE appliances continue to monitor the network for inappropriate content events when no authorized administrator is logged on based on stored configuration; however, all administrators are required to log on to the CommandPost to perform any actions.

5.1.6   Security management (FMT)

5.1.6.1   Management of security functions behaviour (FMT_MOF.1)

FMT_MOF.1.1   The TSF shall restrict the ability to [*modify the behavior of*] the functions [**related to system data collection, analysis and reaction**] to [**System Administrator, Authorized Administrators granted the Policies privilege, by role**].

5.1.6.2   Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1   The TSF shall enforce the [**Access Control Policy**] to restrict the ability to [**assign users to roles/groups**] the security attributes [**privileges and access levels**] to [**System Administrator, Authorized Administrators granted the Users privileges, by role**].

5.1.6.3   Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1   The TSF shall enforce the [**Access Control Policy**] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2   The TSF shall allow the [**System Administrator**] to specify alternative initial values to override the default values when an object or information is created.

5.1.6.4   Management of TSF data (FMT_MTD.1a)

FMT_MTD.1a.1 The TSF shall restrict the ability to [*query, modify, delete,* [**create**]] the [**user definitions**] to [**System Administrator, Authorized Administrators granted the Users privileges, by role.**].

5.1.6.5   Management of TSF data (FMT_MTD.1b)

FMT_MTD.1b.1 The TSF shall restrict the ability to [*query*] the [**audit data records**] to [**System Administrator, Authorized Administrators granted the Audit privileges, by role**].

5.1.6.6   Management of TSF data (FMT_MTD.1c)

FMT_MTD.1c.1 The TSF shall restrict the ability to [*query* **and create**] the [**alert reports**] to [**System Administrator, Authorized Administrators granted the Reports privilege, by role**].

5.1.6.7   Management of TSF data (FMT_MTD.1d)

FMT_MTD.1d.1 The TSF shall restrict the ability to [*query, modify, delete,* [**create**]] the [**extrusion prevention policies**] to [**System Administrator, Authorized Administrators granted the Policies privilege, by role**].

5.1.6.8   Management of TSF data (FMT_MTD.1e)

FMT_MTD.1e.1 The TSF shall restrict the ability to [*query, modify,* [**assign**]] the [**alerts**] to [**System Administrator, Authorized Administrators granted the Ticketing privilege, by role**].

5.1.6.9   Management of TSF data (FMT_MTD.1f)

FMT_MTD.1f.1 The TSF shall restrict the ability to [*query, delete* the [**alerts**] to [**System Administrator, Authorized Administrators granted the Alerts privilege, by role**].

5.1.6.10 Specification of management functions (FMT_SMF.1)

FMT_SMF.1.1   The TSF shall be capable of performing the following security management functions: [**manage audit functions; manage user security attributes; manage alert reports; manage functions related to system data collection, analysis and reaction**].

5.1.6.11 Security roles (FMT_SMR.1)

FMT_SMR.1.1   The TSF shall maintain the roles [**System Administrator, Network Admin, Network Admin Supervisor, Policy Author, Policy Author Supervisor, Alert Manager, Alert Manager Supervisor, No Role**].

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

> **Application Note:** All users of the TOE are considered authorized administrators.

5.1.7 Protection of the TSF (FPT)

5.1.7.1 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.

> **Application Note:** The TOE uses the OpenSSL FIPS Object Module, Version 1.1.2, Certificate 918 over TLS, Version 1.

5.1.7.2 Non-bypassability of the TSP (FPT_RVM.1)

FPT_RVM.1.1   The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.7.3 TSF domain separation (FPT_SEP.1)

FPT_SEP.1.1   The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1.2   The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.7.4 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1   The TSF shall be able to provide reliable time stamps for its own use.

5.1.8 Session Locking (FTA)

5.1.8.1 TSF-initiated session locking (FTA_SSL.1)

FTA_SSL.1.1   The TSF shall lock an interactive session after [**15 minutes**] by:
a) clearing or overwriting display devices, making the current contents unreadable;
b) disabling any activity of the user's data access/display devices other than unlocking the session.
FTA_SSL.1.2   The TSF shall require the following events to occur prior to unlocking the session: [**require the user to re-establish browser session (login) between the client workstation (e.g., CommandPost client) and the CommandPost**].

5.2 IT Environment Security Functional Requirements

This section includes the SFRs that pertain to the IT environment.

REQUIREMENT CLASS	REQUIREMENT COMPONENT
FCS: Cryptographic Support	FCS_COP.1c: Cryptographic operation
	FCS_CKM.4: Cryptographic key destruction
FDP: User data protection	FDP_ITC.2: Import of user data with security attributes
FMT: Security management	FMT_MSA.2: Secure security attributes
FPT: Protection of the TSF	FPT_TDC.1: Inter-TSF basic TSF data consistency
FTP: Trusted path/channel	FTP_ITC.1: Inter-TSF trusted channel

5.2.1 Cryptographic Support (FCS)

5.2.1.1 Cryptographic operation (FCS_COP.1.c)

FCS_COP.1c.1   The **IT environment** shall perform [**PKI Certificate for key exchange encrypted authentication**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**see application note below**] that meet the following: [**DOD X.509, PKCS-1**].

Application Note: The TOE uses a DOD-approved External Certification Authority (ECA) for encrypted authentication. The key must be at least 160-bit private key (x) and at least 1024 bit prime modulus (p) and the minimum subscriber public key sizes shall be 1024 bits for Key Exchange Algorithm (KEA) and Rivest, Shamir, Adleman (RSA).

5.2.1.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1   The **IT environment** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**zeroization**] that meets the following: [**DOD X.509, PKCS-1**].

5.2.2 User data protection (FDP)

5.2.2.1 Import of user data with security attributes (FDP_ITC.2)

FDP_ITC.2.1   The **IT environment** shall enforce the [**Access Control Policy**] when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.2.2   The **IT environment** shall use the security attributes associated with the imported user data.

FDP_ITC.2.3   The **IT environment** shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4   The **IT environment** shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5   The **IT environment** shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [**ECA certificates imported into the TOE will be RSA, 1024 bits that meet DOD X.509 and PKCS.1**].

5.2.3 Security management (FMT)

5.2.3.1 Secure security attributes (FMT_MSA.2)

FMT_MSA.2.1   The **IT environment** shall ensure that only secure values are accepted for security attributes.

5.2.4 Protection of the TSF (FPT)

5.2.4.1 Inter-TSF basic TSF data consistency (FPT_TDC.1)

FPT_TDC.1.1   The **IT environment** shall provide the capability to consistently interpret [**CA certificates**] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2   The **IT environment** shall use [**DOD X.509 PKI interpretation rules**] when interpreting the TSF data from another trusted IT product.

5.2.5 Trusted path/channels (FTP)

5.2.5.1 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1   The **IT environment** shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2   The **IT environment** shall permit [*the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3   The **IT environment** shall initiate communication via the trusted channel for [**ECA exchange**].

5.3 TOE Security Assurance Requirements

The SARs for the TOE are the EAL 2 augmented with ALC_FLR.3 components as specified in Part 3 of the CC. No operations are applied to the assurance components.

REQUIREMENT CLASS	REQUIREMENT COMPONENT
ACM: Configuration management	ACM_CAP.2: Configuration items
ADO: Delivery and operation	ADO_DEL.1: Delivery procedures
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.1: Descriptive high-level design
	ADV_RCR.1: Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ALC: Life cycle support	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_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

Table 3 EAL 2 Augmented with ALC_FLR.3 Assurance Components

5.3.1 Configuration management (ACM)

5.3.1.1 Configuration items (ACM_CAP.2)

ACM_CAP.2.1d The developer shall provide a reference for the TOE.
ACM_CAP.2.2d The developer shall use a CM system.
ACM_CAP.2.3d The developer shall provide CM documentation.
ACM_CAP.2.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.2.2c The TOE shall be labelled with its reference.
ACM_CAP.2.3c The CM documentation shall include a configuration list.
ACM_CAP.2.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.2.6c The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.
ACM_CAP.2.7c The CM system shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and operation (ADO)

5.3.2.1 Delivery procedures (ADO_DEL.1)

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2d The developer shall use the delivery procedures.
ADO_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
ADO_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.
ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.
ADO_IGS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.
ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.1.2c The functional specification shall be internally consistent.
ADV_FSP.1.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.
ADV_FSP.1.4c The functional specification shall completely represent the TSF.
ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Descriptive high-level design (ADV_HLD.1)

ADV_HLD.1.1d The developer shall provide the high-level design of the TSF.
ADV_HLD.1.1c The presentation of the high-level design shall be informal.
ADV_HLD.1.2c The high-level design shall be internally consistent.
ADV_HLD.1.3c The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.1.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.1.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.1.6c The high-level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.1.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
ADV_HLD.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_HLD.1.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.
ADV_RCR.1.1c For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.
ADV_RCR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.
AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.
AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.
AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.
AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.
AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.
AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.
AGD_ADM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.
AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3c The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4c The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

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

5.3.5 Life cycle support (ALC)

5.3.5.1 Systematic flaw remediation (ALC_FLR.3)

ALC_FLR.3.1d The developer shall 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 documentation 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 procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

ALC_FLR.3.7c The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.3.8c 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.3.9c The flaw remediation procedures shall include a procedure requiring timely responses for the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.

ALC_FLR.3.10c 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.

5.3.6 Tests (ATE)

5.3.6.1 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 identified in the test documentation and the TSF as described 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.

5.3.6.2 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, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

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

5.3.6.3 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 test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability assessment (AVA)

5.3.7.1 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

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

AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.3.7.2 Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.

AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.

AVA_VLA.1.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

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

AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 Security audit

The TOE provides its own audit mechanism that can generate audit records for the not specified level of audit. Each audit record includes date and time of event, subject identity, and the outcome (success or failure) of the event. The auditable events include:

- Start-up and shutdown of the audit function
- Audit review
- Audit access
- All use of the authentication mechanism
- All use of the user identification mechanism
- All modifications of the functions related to system data collection, analysis and reaction
- All modifications to the values of TSF data
- Modifications to the Access Control Policy role/group assignment(s)
- All modifications to the Access Control Policies restrictive default values for security attributes
- All use of the management functions
- Modifications to the group of users that are part of a role

TOE audit records are stored on the CommandPost appliance in the MySQL data repository where System Administrators and authorized administrators are able to review the contents and interpret the results (i.e., associate auditable events with the date, time, subject identity of the user that caused the event, as well as whether the event was successful or unsuccessful). TOE audit data is stored separately from extrusion data in MySQL as they occupy different tables in the database and are allocated separate space requirements since the data types are very different.

The TOE prevents audit data loss by overwriting the oldest stored audit records if the audit trail is full within the allocated database tables. Note that only an authorized administrator with audit privilege can access the audit data records from the GUI, such that users that are not granted this authorization do not have access.

The TOE hardware provides a reliable time stamp for audit purposes. Note that the FEP_SDC and FEP_ANL requirements address the recording of results from network data scanning, sensing and analyzing tasks (e.g., auditing of system data).

For more information about functions provided by the CommandPost (e.g., Administrator Console), see the security management function description below.

Refer to Sections 6.1.4, Fidelis XPS Component Requirements for additional MySQL space restrictions.

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

- FAU_GEN.1: The TOE generates audit events for the not specified level of audit. Note that the FEP_SDC and FEP_ANL requirements address the recording of results from network system data; and FEP_RDR addresses restricted data review.

- FAU_SAR.1: The TOE provides authorized administrators granted the System Administrator role with the ability to review all audit records in order to interpret the contents. No other role is granted the audit privilege and cannot access audit records, unless a custom role is created that includes the audit permission. Within the TOE, administrative users granted the Audit access control have access to audit records.

- FAU_SAR.2: The TOE prohibits all users audit record access except those explicitly designated with audit privilege. By default, only the System Administrator role has access to the audit trail via the CommandPost.

- FAU_STG.1: The CommandPost protects stored audit data from unauthorized deletion by ensuring that TOE audit data is maintained in a separate table within the MySQL database of the underlying hardened Linux OS. 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 when the audit trail is full.

6.1.2 Cryptographic support (FCS)

The TOE hashes user passwords with the use of MySQL's embedded "SHA1()" function to hash and store the user password. During user validation, the TOE uses this function to hash the incoming password and then compares the resulting string to that stored in the TOE configuration data.

The TOE provides a way to positively match a particular file by utilizing an MD5 checksum for exact file detection where the RFC 1321-based free implementation RSA MD5 library available from www.sourceforge.net/projects/libmd5-rfc is used. The MD5 hash of the transferred file is compared to the hash in the fingerprint. If the transferred file has been modified, it will not match the hash stored in the fingerprint.

Refer to Sections 6.1.4, Fidelis XPS Component Requirements, 6.1.5, Identification and authentication; and 6.1.6, Security management for additional cryptographic hashing functionality specifics.

The Cryptographic support function is designed to satisfy the following security functional requirements:

- FCS_COP.1a: The CommandPost provides SHA-1 password hashing; the Vendor affirms the SHA-1 implementation meets FIPS 180-2.

- FCS_COP.1b: The Exact Content analyzer performs MD5 fingerprint hashing, and the Vendor affirms the MD5 hashing implementation conforms to RFC 1321.

6.1.3 User data protection (FDP)

All users for the TOE are considered authorized administrators; and Fidelis XPS implements security functionality protection for CommandPost access based on user identity, role, sensor assignment and sensor group assignment.

For each type of administrative objects (associated with/by privileges), Fidelis XPS enforces an access control policy based upon the access levels assigned to the privileges that are assigned to a role/group. TOE administrative objects subject to the access control policy include the combination of the nine (9) privileges available as alerts, quarantine, tickets, reports, policies, users, config, audit and/or no access assigned to each role. The TOE enforces this association in order to control who may access what security functionally needed to be performed.

Since the TOE requires users to be assigned to a role and group/sensor assignments vary, the following table provides complete TOE functionality for access determinations:

FUNCTION	ROLE MUST PROVIDE	ALERT MANAGEMENT GROUP ASSIGNED	SENSOR ASSIGNMENT
Alerts	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.
Quarantine	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	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.

FUNCTION	ROLE MUST PROVIDE	ALERT MANAGEMENT GROUP ASSIGNED	SENSOR ASSIGNMENT
Reports	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	Full Control or View Only access to policies	No impact	Users can only assign policies to sensors to which they are assigned.
Users	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.
Config	Full Control	No impact	Users can only configure sensor components on sensors on which they are assigned.
Audit	Full Control	No impact	No impact

Table 4 Functionality Overview

A role(s) access (user) to each TOE feature is also determined by the access levels associated to the privilege as:

ACCESS LEVEL	DESCRIPTION
Full Control (aka Full— read, write)	Provides read and modify access to the feature and is depicted by a full green circle on the CommandPost roles screen.
View Only (aka View— read)	Provides read-only access to the feature and is depicted by a half-green circle.
No Access (aka None)	Provides no access to the feature and is depicted by an empty circle.

Table 5 Access Levels

When a user is created, they are assigned privileges based on role which are stored with user credentials in the database. Privileges are enforced by:

- Users are not provided access to portions of the TOE where they lack privilege. Links to these pages, where appropriate, will not be available.

- Every user access first verifies user privileges. If a non-privileged user attempts to access or execute, they will be denied.

- A user with the User Manager privilege is not permitted to create new users with more privileges than themselves (i.e., if the creator has "User Manager" and "Network Admin" privileges, then they cannot create a new user with the "Policy Manager" privilege, nor can they grant "Policy Manager" to an existing user.

When users log on, their access is determined by user identity and role privileges granted and they are not authorized to access any security management functionality for which an explicit privilege has not been granted by a System Administrator or authorized administrator granted the user privilege. Note that all administrators have the ability to change their own passwords and that is the only exception.

The TOE's access control policy has eight (8) pre-defined roles as depicted in the following table that are subject to the access control policy:

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

ROLE	FUNCTION	ACCESS TYPE
Alert Manager Supervisor	Alerts	Full Control
	Quarantine	Full Control
	Tickets	Full Control
	Reports	Full Control
	Policies	View Only
	Users	Full Control
	Config	No Access
	Audit	No Access
No Role	No Access	No Access

Table 6 – Default Access Control Policy by Role

The 'No Role' role is provided to specifically place previously assigned authorized administrators into when they either temporarily or no longer require TOE access.

Refer to Section 6.1.6, Security management, for additional information.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_ACC.1: The CommandPost enforces an access control policy for access to TOE security functionality objects where the TOE permits specific operations based on authorized access to privilege(s) assigned to the role. The ACL object defines the privileges allowed the user based on user identity with role/group assignment.

- FDP_ACF.1: The TOE CommandPost enforces an access control policy based on the ACL associated to a role upon assignment. The access control policy permits operations on the object depending on the ACL that defines the privileges and access allowed the user and/or role group.

6.1.4 Fidelis XPS Component Requirements (FEP_EXP)

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, 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. 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.

  - Communication channels that include the network protocol and attributes of the transmission.

- The <u>content</u> 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 Extrusion Policies by authorized administrators granted the Policy Manager privilege.

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 12 types that are either content-based, channel-based or location-based:

- <u>Identity Profiling</u>—Identity profiling is used to describe personal identity information. The TOE has ten built-in identity items that include name, postal address, e-mail address, social security number, credit card number, vehicle identification number, American banking association routing numbers, FDA-approved drug names, and phone numbers. 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.

- <u>Embedded Images</u>—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.

- <u>Encrypted Files</u>—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.

- <u>Exact Content (via MD5 Signature)</u>—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.

- <u>Partial Content</u>—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.

- <u>File Signature</u>—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.

- <u>File Names</u>—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'.

- <u>Keywords</u>—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 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—refers to 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.

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

The TOE contains an extrusion monitor sub-component of the TOE that detects potential transfers of restricted digital assets. Within the extrusion monitor, there are a variety of analyzers to process data and check for positive matches. Digital assets are defined in a fingerprint and the type of fingerprint determines the analyzer.

The CommandPost contains a MySQL database that has been tested to store a maximum of 2.5 million alerts. Regardless, the TOE overwrites the oldest stored system data if the storage capacity limit is reached, as configured.

The CommandPost GUI only provides the options available to each logged on user based on privilege(s) assigned. If a user does not have a particular access privilege (i.e., Policy Manager, User Manager, Network Admin and/or Alert Manager), then that functionality option is not available to them on the console.

TOE Analyzers

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

The Regular Expression analyzer uses the Perl Compatible Regular Expression (PCRE)[9] 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

---

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

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

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

The Keyword analyzer evaluates data for keywords.

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

The Embedded Image File analyzer looks for embedded image files.

The Location analyzer evaluates the source and destination IP addresses.

Alerts

The TOE CommandPost compiles alerts from all connected sensors and this aggregated data can be viewed from the CommandPost. The TOE's Adaptive Alert Classifier sub-component groups 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.

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

- Unique alert number;
- Alert priority;
- Alert 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[10];
- Protocol on which alert occurred;
- Source address;
- Destination address;
- Source and Destination TCP port, if applicable;
- IP layer information;
- 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.

---

[10] 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.

Alerts are stored in the CommandPost embedded MySQL database and can be filtered by many alert attributes as the following sample reflects:

- 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

For additional information on the TOE functionality with regard to access authorizations, policies and rules, see Sections 6.1.3, User data protection and 6.1.6, Security management.

The Fidelis XPS Component Requirements (FEP) function is designed to satisfy the following security functional requirements:

- FEP_ANL.1 (EXP): The TOE performs analysis on received data 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.

- FEP_RCT.1 (EXP): The TOE issues an alert and sends TCP resets to the session endpoints or optionally drops the packet when potential inappropriate network traffic is detected. The action is controlled per rule such that different policy violations may incur different actions.

- FEP_RDR.1 (EXP): The TSF provides an authorized administrator the capability to read all system data; provides system data in a manner suitable for an authorized administrator to interpret; and prohibits all authorized administrators read access to system data except those that have been granted explicit access.

- FEP_SDC.1 (EXP): The default setting for the TCP session forensics limit is set at 4096 KB because most useful forensic information occurs in the beginning of a recorded session. This setting determines the maximum length (in KB) of data recorded from the TCP session associated with each alert. It is important to keep in mind that a larger limit might substantially increase the size of the database, which will require more available disk space on CommandPost..

- FEP_STG.1 (EXP): The CommandPost protects stored system data from unauthorized deletion by ensuring only authorized administrators granted the authorization may access the data.

- FEP_STG.2 (EXP): The CommandPost data repository overwrites the oldest stored system data if the configured storage capacity has been reached.

6.1.5 Identification and authentication

The TOE provides its own user name and password authentication mechanism. In order to access the TOE, a login account, including a login name and password must be created and privilege must be assigned. Users are granted access to system resources based on user role assignment (a predefined role – System Administrator, Network Admin, Network Admin Supervisor, Policy Author, Policy Author Supervisor, Alert Manager, Alert Manager Supervisor, No Role – or a custom role). Only authorized users granted full access to users privilege 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, the authorized administrator provides the login name (e.g., user identity) and password to the CommandPost. The CommandPost hashes the password with the use of MySQL's embedded "SHA1()" function to hash and store the user password. User password data is stored in a MySQL table protected by access permissions. During user validation, the TOE uses this function to hash the incoming password and then compares the resulting string to that stored in the TOE configuration data. If either the login name or the password is incorrect, the login request will fail and no CommandPost functions will be made available. As a result of a successful login, an interactive session is established that grants the user access to all functionality for which they have been explicitly granted privileges (i.e., Network Admin, Policy Author, Alert Manager, etc.) based on role as the administrator logged on.

Authorized administrators are required to use a valid password that contains at least eight (8) characters; and includes a combination of upper/lower case letters, numbers and special characters. If an authorized administrator attempts to select a password that does not meet the minimum requirements, the TOE will not allow that authorized administrator to log in.

The TOE verifies user credentials for every CommandPost action based on the login name and password to ensure the user is authorized to perform the function based on role assigned. The user name and password are passed to create a session ID so the TOE doesn't have to cache user name and password, and the clock function for session inactivity is mapped to this session ID.

User roles are stored in the database and are verified prior to any action. Each user has one unique user name and password. Users have exactly one role, which defines their access privilege to system functions.

The TOE allows continuous monitoring of the network traffic whether an authorized user (administrator) is logged on or not. Administrators logging on to the CommandPost must be successfully identified and authenticated before any TSF-mediated actions are allowed on behalf of that authorized administrator.

The TOE relies on the hardened CentOS Linux operating system for authentication of users that log on directly to the CommandPost. Only users that are authorized may log on to the CommandPost directly. 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. and while this is the only account on the sensor(s), the CommandPost also has this account with the same access as a sensor. In addition, every CommandPost user has a corresponding Linux account that is used for fingerprint creation and testing. File transfer is done to CommandPost using WinSCP. These accounts have very limited access to the system and system files, and each user gets their own directory on disk and they can only access that data. All GUI interactions are verified as described elsewhere in this ST.

In the evaluated configuration, no additional software is authorized for installation onto the TOE appliances and the appliance devices are locked down such that it is configured to only support TOE functionality.

Refer to Sections 6.1.3, User data protection and 6.1.6, Security management for additional specifics that support the identification and authentication security function.

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 privileges and access) and assignments (alert management group and sensor).

- FIA_UAU.1: The TOE offers no management of security functions until the user is successfully authenticated. Note that management of security functions are identified in the security management function description below.

- FIA_UID.1: The TOE offers no management of security functions until the user is successfully identified. Note that management of security functions are identified in the security management function description below.

6.1.6 Security management

All TOE security management functionality is handled by the CommandPost to authorized administrators. Each CommandPost user is authorized to be assigned one (1) role that determines the parts of the system the user may access (i.e., authorizations)

Alert management groups can be created and used to divide the work of violation review by sensor and to segregate violations by rule, as configured, since rules are associate with an alert management group, based on assignment. When a rule is violated, an alert or a quarantined e-mail may only be managed by persons in the assigned alert management group and once viewed, an alert manager may move the alert or quarantined e-mail to a different alert management group, as needed.

The TOE contains eight (8) built-in, pre-defined roles that cannot be edited or deleted. The System Administrator role has full control over the system and perform all TOE security management functions. Note that only the System Administrator has the Audit privilege and can view audit logs, by default.

Additional authorized users are granted administrator roles based on what they will be performing within the TOE (i.e., sensor(s), policies, alerts, etc.). All other TOE users are Authorized Administrators assigned to one role with privileges to perform security management functions. User(s) assigned to the default System Administrator role have full control over all system privileges (i.e., alerts, quarantine, tickets, reports, policies, users, config, audit, no access).

Authorized Administrator role descriptions:

- System Administrator—complete access to all TOE functionality and components.

- Network Admin—manage sensors; full access to 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 sensors as above Network Admin with full access to the users function. May create new Network Admin users with this role.

- 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 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 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.

In addition to the eight (8) pre-defined roles with default privileges and access levels, an authorized administrator with full access to the users function can create additional roles using any combination of the privileges (i.e., alerts, quarantine, tickets, reports, policies, users, config, audit, no access) with the appropriate access level (i.e., full, view, none) for the desired effect or based on assigned administrative responsibilities, as one privilege has no bearing on others.

Authorized administrators login to the CommandPost to manage TOE security functions via a web-based interface from client workstations simultaneously, thus establishing multiple independent sessions to accommodate concurrent users and transactions are implemented 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 authorized administrators are added to the TOE by user name, password, e-mail address and privileges. Current authorized administrator accounts may be modified to reflect updated personal information (name, e-mail) or to modify privileges assigned and authorized administrators who no longer require access to manage the TOE may be deleted. Only authorized administrators with the full access privilege to the Users screen may query, modify, delete and create user definitions (i.e., user identity, authorizations and privileges) for other users within the group being supervised or by a System Administrator.

The TOE does offer a command line interface to run command line XPS functions, though the available commands are very limited. Furthermore, 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.

Extrusion Policies—configured by authorized administrator granted the Policy manager privilege. Extrusion policies are based on:

- Policy (comprised of a set of rules that guide business practices within the enterprise and when a policy is violated where a Fidelis Fidelis XPS sensor will perform an action in response) and a

- Rule (comprised of a subset of a policy that has five components: rule expression, rule summary, severity, action, and alert management group).

A rule is defined by the rule expression which includes at least one fingerprint representing content, channel and location, but may contain any combination of multiple conditions of each. A rule is a single entity. Every rule will have one associated action. Rules can be created using any logical expression, combining conditions using AND, OR, and NOT statements. Fidelis Fidelis XPS sensors employ several data analyzers that detect policy violations within transmissions and the analyzers can be configured to generate violations based on the sender or receiver of the data, the type of transmission, or the content of the data in the transmission. If network traffic violates the rule, it is a violation and the action taken for a violation is defined in the rule. For Extrusion Policy definition, fingerprints are described as:

- Content is defined as the data within transmissions;

- Channel is defined as the type of transmission including the application protocol, the length of the transmission, and other characteristics of the channel; and

- Location is defined as the sender and receiver of the transmission where these can be created in groups, or locations, such as Human Resources, Development, or Accounting.

Any event that occurs in the network traffic can be programmed to carry out one of the following possible rule actions:

- <u>Alert</u>—generated upon rule violation. All information about the violating transmission will be sent to the CommandPost and can be accessed by authorized administrators through the Alert Screen.

- <u>Prevent</u>—the data transmission is prevented. Prevent takes the following actions, based on Fidelis Fidelis XPS sensor type and how the sensor is configured:

    - Fidelis Fidelis XPS Direct:

        - In sniffing mode with active mode enabled—sensor issues TCP reset packets to kill the session.

        - In in-line mode with active mode enabled—sensor drops all incoming packets for the TCP session and the sensor also issues TCP reset packets to both endpoints to cleanly terminate the session.

        - With active mode disabled—prevent action has not effect.

      Note that when a transmission is prevented by this sensor, statistics are stored in CommandPost and can be viewed via the Session or Channel Compliance reports.

    - Fidelis Fidelis XPS Proxy—end user will be redirected to the provided URL or to the TOE default URL. If a URL is not provided, the end user will receive an HTTP Error 403 (not permitted) in their browser.

    - Fidelis Fidelis XPS Mail—the e-mail message will not be accepted and the user who sent the e-mail will be notified that the message was not delivered. E-mail handling only applies if the rule is assigned to this type of sensor and an authorized administrator may specify handling as either: Notify Sender Message (entering a message for the sender and the sensor sends the message to the sender of the violating e-mail even if the original e-mail is prevented or quarantined); or Append Message (selecting this option enables an authorized administrator to enter a message in the text box and this message is appended to the original e-mail that caused the violation.

- <u>Alert and Prevent</u>—the data transmission is prevented and an alert is generated. The above descriptions of both alert and prevent apply.

- <u>Throttle</u>—offers the ability to reduce the network bandwidth consumed by certain network user behavior. Throttle is typically used to identify applications (such as peer-to-peer or instant messenger) that are allowed on

the network, but to control their use by throttling activity to an acceptable level. Throttle can be applied to any rule and the following applies:

- Throttle is performed by reducing the TCP window size of sessions matching this rule and by dropping packets at a fixed rate (depending on configuration parameters).

- Throttle will only work on a Fidelis Fidelis XPS Direct sensor that is configured for inline mode. The action will be ignored in all other cases.

- Throttle settings can be modified in a configuration file.

- Alert and Throttle—the session is throttled and an alert is generated. The descriptions of both alert and throttle apply. Selecting the alert and throttle action enables an authorized administrator to view throttle statistics and statistics are available only if an alert was also generated.

- E-Mail Actions—Alert and Quarantine, Alert and Reroute, and Reroute only pertain to the Fidelis Fidelis XPS Mail sensor(s).

A single e-mail may violate multiple rules and in this case, the Fidelis Fidelis XPS Mail sensor will take one action for the entire e-mail based on the priority listed below:

- Quarantine takes first priority—any e-mail that violates one or more rules with the quarantine action will be quarantined.

- Prevent has second priority—any e-mail that violates one or more rules with the Prevent action will be prevented (unless it violates one or more rules with the Quarantine action).

- Reroute is the third priority—if other actions such as quarantine are detected, they are taken.

Note: E-mail actions are ignored by Fidelis Fidelis XPS Proxy and Fidelis Fidelis XPS Direct sensors.

The following table describes the E-mail actions.

ACTION	DESCRIPTION
Alert and Quarantine	Provides an alert of the violation and quarantines the offending e-mail. When this action is selected by an authorized administrator, the Quarantine Expiry Action appears in the Email Handling section of the rules screen with options to either discard or deliver for the quarantined e-mails. The selected quarantine Expiry action affects all e-mails found to be in violation of this rule after a given amount of time has passed (default is two (2) weeks) to prevent quarantined e-mails from taking up increasing amounts of disk space. Authorized administrators can manually take action on e-mail before the expiration time passes by accessing the Quarantine Management screen.
Reroute	Reroutes the offending e-mail to the specified mail server and no alert is provided.
Alert and Reroute	Provides an alert of the violation and reroutes the offending e-mail to the mail server specified during configuration.

Table 7 E-mail Actions

Each rule is associated with one alert management group. When the rule is violated, the alert will be visible to authorized administrators who have been assigned to the alert management group. The alert management group is used to segregate alert information by rule among several authorized alert administrators.

When a rule or a policy is added, deleted or changed on the CommandPost, all affected sensors are updated via a manual push. Note that only the Administrator or Authorized Administrators granted the Policy Manager privilege may manage extrusion policies only to sensors to which they are assigned.

The TOE ships with pre-built policies, rules, content, channels and locations and new policies can be defined. The following pertains to the pre-built policies, rules, content, channels and location content:

- Managing insider use of the Internet—the TOE can be used to enforce corporate policy pertaining to the acceptable use of internet resources where the policies in this category include:

  - Application Management (AM)—allows enforcement of unauthorized applications such as peer-to-peer file sharing, instant messenger, access to web-based e-mail systems, etc.

- Unauthorized Traffic (UT)—the detection and prevention of users who circumvent corporate security measures by using unauthorized proxies, defeating firewall rules, and using unauthorized encryption methods.
- Inappropriate Content—enforces policies regarding offensive material or language on the network.

- Protection of digital assets and sensitive information—the TOE can be used to enforce policies pertaining to sensitive information where the policies included are:

  - Digital Asset Protection (DAP) provides the capability to detect and prevent sensitive materials being leaked through the network; and
  - Sensitive U.S. government information (as configured/defined).

- Compliance with federal and state privacy laws; and

- File transfer management.

The CommandPost is accessed through a web-based GUI to:

- Visually monitor network alerts in real time (i.e., drops traffic and/or sends a TCP reset based on configuration immediately upon detection of the violation in the network session)
- Collect, aggregate and store data from multiple sensors
- Examine and analyze data, down to packet contents
- User Alert Radar to monitor groups of related alerts
- Access the web-based CommandPost GUI from anywhere on the network
- Enable/disable particular fingerprints and alerts in real time
- Add, configure and manage sensors and the console itself

Policies contain rules that are assigned to sensors manually. When a policy is assigned (e.g., pushed) to a sensor, all rules that are part of the policy are assigned (pushed) to the sensor. There is only one action done by the user and it is at the policy level, not the rule level. Fingerprints and policies are automatically managed between the TOE sensors and the console. When a fingerprint or a policy is added, deleted or changed on the console by an authorized administrator, all affected sensors are updated by a push from the CommandPost. The push is initiated manually by the user using the CommandPost GUI. First, the policy file is being sent to the sensor using TLS-secured session. Then, sensor connects back to the CommandPost through separate TLS-secured connection, requesting MD5 hashes of all fingerprints used in the policy. After receiving MD5 checksums, it determines all fingerprints that need to be updated/added/deleted, then retrieves all necessary fingerprints from the CommandPost, each over separate TLS-secured connection. Finally, the sensor restarts all necessary components to accommodate the new policy.

The authorized administrator manages policies and can assign them to sensors from the console by using the Add, New or Edit buttons to add or change a policy.

The TOE allows an authorized administrator to create and configure fingerprints, rules, and policies. The authorized administrator may also assign and un-assign policies to sensors – but only to those sensors to which the authorized administrator has been explicitly assigned.

As the TOE searches network traffic for events, each event is mapped to a specific threat or violation. Each rule violation creates a mapping between the violated rule and the network session that caused the violation. If the rule action specified an alert, each event will be sent to CommandPost as an alert.

Network statistics about dataflow and application protocols by sensor can be monitored by an authorized administrator by:

- Sensor type
- Total processed packets since last restart
- Sample (size by time, showing when taken)
- Packets by protocol (a graphical display and a numerical breakdown)
- Bytes by protocol (graphic display and a numerical breakdown in bits/second)
- Packets per second by service, graphically

- Bytes per second by service, graphically
- Volume of packets by size, graphically
- Wire statistics (NIC errors, dropped and individual packets)
- History, showing total number of packets processed since sensor start

Reports can be generated by an authorized administrator with reporting privilege. Tabular reports are called Queries in CommandPost; Graphical reports are called Reports. Tabular reports (queries) can be searched by: description; sensor(s); interval; date; priority; source IPs; destination IPs; alert type(s); alert #(s); show (results); assigned to; ticket status; ticket resolution; save as; and/or save report. Tabular reports can be saved an executed periodically with results delivered by e-mail, SNMP, or syslog. Graphical reports are available in eight forms: Alerts by Channel, Alerts by IP, Alerts by IP Pair, Alerts by Policy, Alerts by Severity, Channel Compliance, Session Compliance, and Policy Summery. Graphical reports can be scheduled to run periodically with results delivered by e-mail.

TOE alert decoding path application protocols are provided for all available protocols.   The TOE uses this path of decoding to extract content for analysis where an example decoding path is: HTTP : YAHOOMAIL : mime(filename.doc) : ms-word. In this example, a Word document was found in a Mime attachment to a Yahoo web mail session. Any of the words in the decoding path (HTTP, YAHOOMAIL, mime, ms-word) may be selected by an authorized administrator. Protocols are always CAPITALIZED in the decoding path.

TOE protocol decoders come in two forms: detection and inspection. The majority of protocol decoders allow inspection of the content. These decoders will extract the content, which will be passed on to other decoders in the path. For inspection-capable decoders, all elements of the decoding path are clickable. Detection decoders are capable of identifying the application protocol, but not capable of extracting the content. These decoders will not be clickable in the decoding path.

The 'Config' Screen of the CommandPost enables an authorized administrator to manage the configuration of connected sensors.

For additional details on TOE policies, rules and fingerprint management, refer to the "Fidelis Fidelis XPS User Manual, Version 3.12" and the "Fidelis Fidelis XPS Guide to Prebuilt Policies[11], Version 3.1.1."

Refer to Section 6.1.1 for additional audit information; Section 6.1.4 for additional FEP information; Section 6.1.5 for additional identification and authentication information; and Section 6.1.7 for additional protection of the TSF information that impacts on security management.

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

- FMT_MOF.1: Only the System Administrator and an Authorized Administrators granted the Policies privilege, by role can modify the behavior of the functions related to system data collection, analysis and reaction.

- FMT_MSA.1: Only the System Administrator, Authorized Administrators granted the Users privileges, by role can assign users to roles/groups, by security functional area.

- FMT_MSA.3: Only the System Administrator can specify alternative initial values to override the default values for role privileges and access levels.

- FMT_MTD.1a: Only the System Administrator and an Authorized Administrators granted the Users privileges, by role can query, modify, delete or create user definitions.

- FMT_MTD.1b: Only the System Administrator and an Authorized Administrators granted the Audit privileges, by role can query audit data records.

- FMT_MTD.1c: Only the System Administrator and an Authorized Administrators granted the Reports privilege, by role can query alert reports within the Alert Manager role.

- FMT_MTD.1d: Only the System Administrator and an Authorized Administrators granted the Policies privilege, by role can query, modify, delete and create extrusion policies within the Policy Author role.

---

[11] This guide has been provided as part of the Administrators Guide for evaluation.

- FMT_MTD.1e: Only the System Administrator and an Authorized Administrators granted the Ticketing privilege, by role can query , modify and assign alerts within the Alert Manager role.

- FMT_SMF.1: The TOE offers a wide range of security management functions including managing audit functions; user security attributes; alert reports; and functions related to system data collection, analysis and reaction.

- FMT_SMR.1: The TOE supports pre-defined Authorized Administrator roles (i.e., System Administrator, Network Admin, Network Admin Supervisor, Policy Author, Policy Author Supervisor, Alert Manager, Alert Manager and No Role) that can be granted up to nine (9) privileges (i.e., Alerts, Quarantine, Tickets, Reports, Policies, Users, Config, Audit, No Access) to perform security management functions on the TOE as assigned. All TOE users are authorized administrators.

6.1.7 Protection of the TSF

The TOE restricts access to its interfaces by requiring authorized administrators to log into the CommandPost component and commands sent from the console component to the Fidelis XPS sensors are encrypted via protected communications channel. Commands sent between TOE components are encrypted and decrypted by use of the included FIPS 140-2 certified OpenSSL, Version 1.1.2 (certificate 918) over TLS, Version 1 encrypted communications channel and the sensors are configured to accept packets only from a specific network address (e.g., CommandPost).

Communication between TOE components 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 8 TOE Cipher Suite Details

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

Each TOE component 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 the addition of 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 IT environment.

TOE sensors must be registered to 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 TOE 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. Communications between the sensors and the CommandPost is via the TLS/OpenSSL encrypted link and communications between the console and the web browser client is accomplished via the web-based GUI. The appliance hardware provides reliable time stamps for collected data and TOE auditing purposes.

TOE functionality is accessible by requiring users to log in to the TOE application as described in Section 6.1.5, Identification and authentication.

Refer to Sections 6.1.4, Fidelis XPS component requirements; and 6.1.6, Security management for additional protection of TSF functions.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_ITT.1: The TSF protects security management data from disclosure when transmitted between separate parts of the TOE via SSL/TLS encryption/decryption.

- FPT_RVM.1: The TSF ensures the TOE security management functions are invoked and succeed before each function within the TOE is allowed to proceed.

- FPT_SEP.1: The TSF maintains a security domain for its own execution that provides protection form interference and tampering by untrusted subjects and separation between the security domains of subjects in the TOE are enforced by requiring registration of sensors to CommandPost.

- FPT_STM.1: The TOE appliance hardware provides a reliable time stamp for TOE use.

6.1.8 Session Locking (FTA)

An authorized administrator can access the CommandPost from multiple web-based client workstations via an authorized browser simultaneously by logging in successfully; however, session(s) will timeout after 15 minutes without activity and clears the display devices making the current contents unreadable. In order to re-establish a browser session from a client to the CommandPost, the disconnected administrator must successfully log back in. All user credentials (e.g., assigned role with granted privileges and access) are verified on every CommandPost action on a per user basis. Every user access requires a privilege lookup before the requested action is granted and this is accomplished within the CommandPost.

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

- FTA_SSL.1: The TOE provides automatic, hard-coded, session locking after 15 minutes of inactivity.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by Fidelis Security Systems ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. Fidelis Security Systems performs configuration management on the TOE implementation representation, design, tests, user and administrator guidance, and the CM documentation.

These activities are documented in:

- Fidelis XPS Configuration Management Plan

The Configuration management assurance measure satisfies the following EAL 2 augmented with ALC_FLR.3 assurance requirement:

- ACM_CAP.2

6.2.2 Delivery and operation

Fidelis Security Systems provides delivery documentation and procedures to identify the TOE, secure the TOE during delivery, and provide necessary installation and generation instructions. Fidelis Security Systems delivery procedures describe all applicable procedures to be used to prevent in appropriate access to the TOE. Fidelis Security Systems also provides documentation that describes the steps necessary to install Fidelis XPS in accordance with the evaluated configuration.

These activities are documented in:

- Fidelis XPS Delivery, Installation, Generation and Start-up Procedures

The Delivery and operation assurance measure satisfies the following EAL 2 augmented with ALC_FLR.3 assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

Fidelis Security Systems has documents describing all facets of the design of the TOE. These documents serve to describe the security functions of the TOE, its interfaces both external and between subsystems, the architecture of the TOE (in terms of subsystems), and correspondence between the available design abstractions (including the ST).

These activities are documented in:

- Fidelis XPS Functional Specification
- Fidelis XPS High-level Design
- Fidelis XPS Correspondence Representation
- Fidelis XPS Security Policy Model

The Development assurance measure satisfies the following EAL 2 augmented with ALC_FLR.3 assurance requirements:

- ADV_FSP.1
- ADV_HLD.1
- ADV_RCR.1

6.2.4 Guidance documents

Fidelis Security Systems provides user guidance on how to utilize the TOE security functions and warnings to users about actions that can compromise the security of the TOE. Note that all users of the TOE are considered Administrative, and therefore only one user manual is applicable.

These activities are documented in:

- Fidelis XPS User Manual
- Fidelis XPS Guide to Creating Policies
- Fidelis XPS Guide to Prebuilt Policies

The Guidance documents assurance measure satisfies the following EAL 2 augmented with ALC_FLR.3 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Life cycle support

Fidelis Security Systems has procedures that define the process for accepting and acting upon user reports of security flaws. These procedures describe the acceptance criteria for security flaws, how all security flaws and the status of fixes for each security flaw are tracked, and how corrections and corrective measures are automatically made available as applicable.

These activities are documented in:

- Fidelis XPS Flaw Remediation Procedures

The Life cycle support assurance measure satisfies the following EAL 2 augmented with ALC_FLR.3 assurance requirement:

- ALC_FLR.3

6.2.6 Tests

The test documents describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. In addition, these documents describe how the functional specification has been appropriately tested.

These activities are documented in:

- Fidelis XPS Test Plan
- Fidelis XPS Test Results

The Tests assurance measure satisfies the following EAL 2 augmented with ALC_FLR.3 assurance requirements:

- ATE_COV.1
- ATE_FUN.1
- ATE_IND.2

6.2.7 Vulnerability assessment

Fidelis Security Systems has conducted a Strength of Function (SOF) analysis in which all permutational and probabilistic security mechanisms have been identified and analyzed resulting in a demonstration that all of the relevant mechanisms fulfill the minimum strength of function claim, SOF-Basic.

Fidelis Security Systems performs regular vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE.

These activities are documented in:

- Fidelis XPS Vulnerability Analysis

The Vulnerability assessment assurance measure satisfies the following EAL2 augmented with ALC_FLR.3 assurance requirements:

- AVA_SOF.1
- AVA_VLA.1

7. Protection Profile Claims

This ST does not claim conformance to any Protection Profile.

8. Rationale

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

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

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

8.1.1 Security Objectives Rationale for the TOE and Environment

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

	O.ACCESS	O.AUDITS	O.CRYPTO	O.EADMIN	O.EPANLZ	O.FIDELISXPSENS	O.IDAUTH	O.INTEGR	O.OFLOWS	O.RESPON	O.TIME	OE.CREDEN	OE.CRYPTO	OE.INSTAL	OE.INTROP	OE.PERSON	OE.PHYCAL
T.CHANNELS				X													
T.COMDIS	X		X				X						X				
T.COMINT	X							X									
T.FACCNT		X								X							
T.FAIL				X													
T.IMPCON	X						X										
T.LOSSOF	X						X	X									
T.NOHALT	X				X	X	X										
T.PRIVIL	X						X										
T.RESPOND				X						X							
T.STORAGE									X								
T.TIME											X						
A.ACCESS															X		
A.ASCOPE															X		
A.LOCATE																	X
A.MANAGE																X	

	O.ACCESS	O.AUDITS	O.CRYPTO	O.EADMIN	O.EPANLZ	O.FIDELISXPSENS	O.IDAUTH	O.INTEGR	O.OFLOWS	O.RESPON	O.TIME	OE.CREDEN	OE.CRYPTO	OE.INSTAL	OE.INTROP	OE.PERSON	OE.PHYCAL
A.NOEVIL												X		X		X	X

Table 9 Environment to Objective Correspondence

8.1.1.1 T.CHANNELS

An authorized administrator may attempt to use an unapproved channel or non-standard ports to circumvent the security functionality of the TOE.

This Threat is satisfied by ensuring that:
- O.EADMIN: This objective requires that administrators are properly trained, not evil and follow all guidance documentation.

8.1.1.2 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: This objective builds upon the O.IDAUTH objective by only permitting authorized administrators to access TOE data.
- O.CRYPTO: This objective ensures data encryption and decryption between components.
- OE.CRYPTO: This objective ensures that sensitive, security-relevant data transferred across a network between itself and other network entities is secure.
- O.IDAUTH: This objective provides for authentication of users prior to any TOE security data access.

8.1.1.3 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: This objective builds upon the O.IDAUTH objective by only permitting authorized administrators to access TOE data.
- O.INTEGR: This objective ensures no TOE data will be modified.

8.1.1.4 T.FACCNT

Attempts to access TOE data or security functions by unauthorized users may go undetected.

This Threat is satisfied by ensuring that:
- O.AUDITS: This objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE security functions.
- O.TIME: This objective helps to counter this threat by requiring the TOE to provide a reliable time stamp for auditing all user actions.

8.1.1.5 T.FAIL

An authorized administrator may not configure the TOE to react to identified/recognized or suspected vulnerabilities and/or inappropriate activity based on network data thus circumventing the purpose of the TOE to protect the network..

This Threat is satisfied by ensuring that:
- O.EADMIN: This objective requires that administrators are properly trained, not evil and follow all guidance documentation.

8.1.1.6 T.IMPCON

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

This Threat is satisfied by ensuring that:
- O.ACCESS: This objective builds upon the O.IDAUTH objective by only permitting authorized administrators to access TOE security functions.
- O.IDAUTH: This objective provides for authentication of users prior to any TOE security function accesses.

8.1.1.7 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: This objective builds upon the O.IDAUTH objective by only permitting authorized administrators to access TOE security functions.
- O.IDAUTH: This objective provides for authentication of users prior to any TOE security function accesses.
- O.INTEGR: This objective addresses this threat by requiring the TOE to ensure the integrity of collected, analyzed and stored audit and system data.

8.1.1.8 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: This objective builds upon the O.IDAUTH objective by only permitting authorized administrators to access TOE security functions.
- O.EPANLZ: This objective addresses this threat by requiring the TOE to analyze system data which includes attempts to halt the TOE.
- O.FIDELISXPSENS: This objective addresses this threat by requiring the TOE to collect system data which includes attempts to halt the TOE.
- O.IDAUTH: This objective provides for authentication of users prior to any TOE security function accesses.

8.1.1.9 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: This objective builds upon the O.IDAUTH objective by only permitting authorized administrator to access TOE security functions.
- O.IDAUTH: This objective provides for authentication of users prior to any TOE security function access.

8.1.1.10 T.RESPOND

Inappropriate network traffic may go undetected and not be subject to analysis.

This Threat is satisfied by ensuring that:
- O.EADMIN: This objective requires all administrators to be trained and to follow the administrator guidance to configure the TOE.
- O.RESPON: This objective requires the TOE to appropriately respond to analytical conclusions where the TOE is the source.

8.1.1.11 T.STORAGE

Potential audit and system data may not be recorded due to storage loss or overflow.

This Threat is satisfied by ensuring that:

- O.FLOWS: This objective ensures the TOE appropriately handles potential audit and system data storage overflows.

8.1.1.12 T.TIME

A reliable time stamp may not be available for audit purposes.

This Threat is satisfied by ensuring that:

- O.TIME: This objective requires the TOE to have a reliable time stamp for audit purposes.

8.1.1.13 A.ACCESS

The TOE has access to all network data for collection and analysis.

This Assumption is satisfied by ensuring that:
- OE.INTROP: This objective ensures the TOE has the needed access.

8.1.1.14 A.ASCOPE

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

This Assumption is satisfied by ensuring that:
- OE.INTROP: This objective ensures the TOE has the needed access.

8.1.1.15 A.LOCATE

The TOE appliances will be located within controlled access facilities, which will prevent unauthorized physical access.

This Assumption is satisfied by ensuring that:
- OE.PHYCAL: This objective provides for the physical protection of the TOE.

8.1.1.16 A.MANAGE

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

This Assumption is satisfied by ensuring that:
- OE.PERSON: This objective ensures all authorized administrators are qualified and trained to manage the TOE.

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:
- O.CREDEN: This objective supports this assumption by requiring protection of the TOE to prevent unauthorized access.
- OE.INSTAL: This objective ensures that the TOE is properly installed and operated.
- OE.PERSON: This objective ensures that personnel working as authorized administrators are carefully selected and trained.
- OE.PHYCAL: This objective provides for the physical protection of the TOE by authorized administrators.

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 10** 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.AUDITS	O.CRYPTO	O.EADMIN	O.EPANLZ	O.FIDELIS XPSENS	O.IDAUTH	O.INTEGR	O.OFLOWS	O.RESPON	O.TIME	OE.CREDEN	OE.CRYPTO	OE.INSTAL	OE.INTROP	OE.PERSON	OE.PHYCAL
FAU_GEN.1		X															
FAU_SAR.1		X															
FAU_SAR.2		X															
FAU_STG.1		X							X								
FAU_STG.4		X							X								
FDP_ACC.1	X																
FDP_ACF.1	X																
FCS_COP.1a			X														
FCS_COP.1b			X														
FEP_ANL.1 (EXP)					X												
FEP_RCT.1 (EXP)										X							
FEP_RDR.1 (EXP)	X			X													
FEP_SDC.1 (EXP)								X									
FEP_STG.1 (EXP)	X							X	X								
FEP_STG.2 (EXP)								X	X								
FIA_ATD.1								X									
FIA_UAU.1	X							X									
FIA_UID.1	X							X									
FMT_MOF.1	X			X													
FMT_MSA.1	X			X													
FMT_MSA.3	X			X													
FMT_MTD.1a	X			X													
FMT_MTD.1b	X			X													

	O.ACCESS	O.AUDITS	O.CRYPTO	O.EADMIN	O.EPANLZ	O.FIDELIS XPSENS	O.IDAUTH	O.INTEGR	O.OFLOWS	O.RESPON	O.TIME	OE.CREDEN	OE.CRYPTO	OE.INSTAL	OE.INTROP	OE.PERSON	OE.PHYCAL
FMT_MTD.1c	X			X													
FMT_MTD.1d	X			X													
FMT_MTD.1e	X			X													
FMT_SMF.1	X			X													
FMT_SMR.1	X			X			X										
FPT_ITT.1			X					X									
FPT_RVM.1				X				X									
FPT_SEP.1				X				X									
FPT_STM.1		X									X						
FTA_SSL.1							X										
FCS_COP.1c												X	X				
FCS_CKM.4												X	X				
FDP_ITC.2												X	X				X
FMT_MSA.2												X		X		X	
FPT_TDC.1												X			X		
FTP_ITC.1												X			X		

Table 10 Objective to Requirement Correspondence

8.2.1.1 O.ACCESS

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

This TOE Security Objective is satisfied by ensuring that:
- FDP_ACC.1: The TOE identifies the user objects subject to the access control policy.
- FDP_ACF.1: The TOE ensures that the TOE only allows access to user objects based on the defined access control policy.
- FEP_RDR.1(EXP): The system is required to restrict the review of system data to those granted with explicit read access.
- FEP_STG.1(EXP): The system is required to protect system data from modification and unauthorized deletion.
- FIA_UAU.1: Users authorized to access TOE security functions are defined using an authentication process.
- FIA_UID.1: Users authorized to access TOE security functions are defined using an identification process.
- FMT_MOF.1: Only authorized administrators may modify the functions of system data collection, analysis and reaction.
- FMT_MSA.1: Only System Administrators and authorized administrators granted full control of the users privilege may determine who will have access to the objects and the actions the users will be able to perform.
- FMT_MSA.3: The TOE enforces a restrictive access control policy where only System Administrators may override default TOE functions and data values.
- FMT_MTD.1a, b, c, d, e: Only System Administrators and authorized administrators granted specific privileges may query or modify TSF data based on assigned roles.
- FMT_SMF.1: The TOE is required to perform security management functions to manage functions related to system data collection, analysis and reaction , audit data and users.

- FMT_SMR.1: The TOE defines system administrators that have full control and authorized administrators that are based on privileges granted by role (i.e., System Administrator, Network Admin, Network Admin Supervisor, Policy Author, Policy Author Supervisor, Alert Manager, Alert Manager Supervisor, No Role).

8.2.1.2 O.AUDITS

The TOE must record audit records for data accesses and use of the TOE 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_SAR.1: The TOE provides authorized administrators the ability to review and interpret audit records.
- FAU_SAR.2: The TOE prohibits all users read access to the audit records, except those users that have been granted explicit read-access, such that only system administrators may view.
- FAU_STG.1: The TOE provides protected audit storage to prevent unauthorized modification.
- FAU_STG.4: The TOE provides prevention of audit data storage by overwriting the oldest stored audit records if the audit becomes full.
- FPT_STM.1: The TOE hardware provides a reliable time stamp for auditing.

8.2.1.3 O.CRYPTO

The TOE must provide cryptographic encryption and decryption for communications between components.

This TOE Security Objective is satisfied by ensuring that:

- FCS_COP.1a: The CommandPost provides SHA1 password hashing that meets FIPS 180-2.
- FCS_COP.1b: The Exact Content analyzer uses MD5 checksum to match configured fingerprints per RFC 1321.
- FPT_ITT.1: The TOE protects security management data from disclosure and modification when transmitted between separate parts of the TOE via encryption/decryption.

8.2.1.4 O.EADMIN

The TOE must include a set of functions that allow effective management of its functions and data by properly trained administrators who are not evil and follow administrator guidance.

This TOE Security Objective is satisfied by ensuring that:
- FEP_RDR.1: The system is required to restrict the review of system data to those granted with explicit read access.
- FMT_MOF.1: Only authorized administrators granted the Policies privilege (and thus Policy Author role) may modify the functions of system data collection, analysis and reaction.
- FMT_MSA.1: The TOE enforces the Access Control Policy to restrict management functions and data.
- FMT_MSA.3: The TOE provides restrictive default values for management security attributes.
- FMT_MTD.1a, b, c, d, e: Only authorized administrators granted the appropriate privilege(s) by role (i.e., System Administrator, Network Admin, Network Admin Supervisor, Policy Author, Policy Author Supervisor, Alert Manager, Alert Manager Supervisor, No Role) may query or modify TSF data.
- FMT_SMF.1: The TOE is required to provide security management functions.
- FMT_SMR.1: The TOE provides management functions to authorized administrators granted privileges to manage functionality.
- FPT_RVM.1: The TOE must ensure that all functions are invoked and succeed before each function may proceed.
- FPT_SEP.1: The TOE must be protected from interference that would prevent it from performing its functions.

8.2.1.5 O.EPANLZ

The TOE console must accept data from sensors and then apply analytical processes and information to derive conclusions about extrusions (past, present, or future).

This TOE Security Objective is satisfied by ensuring that:
- FEP_ANL.1: The CommandPost is required to perform extrusion analysis and generate conclusions.

8.2.1.6 O.FIDELISXPSENS

The sensor must collect all data that is indicative of inappropriate activity that results from misuse, access, or malicious activity of the monitored network and forwards collected data to CommandPost for further analysis, action and storage.

This TOE Security Objective is satisfied by ensuring that:
- FEP_SDC.1: The system sensor is required to collect and store static configuration data as defined in Section 5.1.2.4.

8.2.1.7 O.IDAUTH

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

This TOE Security Objective is satisfied by ensuring that:
- FIA_ATD.1: Security attributes of subjects used to enforce the authentication policy of the TOE must be defined.
- FIA_UAU.1: Users authorized to access TOE security functions are defined using an authentication process.
- FIA_UID.1: Users authorized to access TOE security functions are defined using an identification process.
- FMT_SMR.1: The TOE associates authorized administrators by assigned role based on privileges granted.
- FTA_SSL.1: The TOE locks an authorized administrators interactive session after 15 minutes of inactivity and requires new login with identity and authentication prior to accessing TOE functions and data.

8.2.1.8 O.INTEGR

The TOE must ensure the integrity of all collected, analyzed and stored audit and system data.

This TOE Security Objective is satisfied by ensuring that:
- FEP_STG.1: The system is required to protect system data from any modification and unauthorized deletion.
- FEP_STG.2: The system is required to overwrite the oldest stored system data if storage capacity is reached.
- FPT_ITT.1: The TOE must protect TSF data from disclosure when transmitted between separate parts of the TOE.
- FPT_RVM.1: The TOE must ensure that all functions are invoked and succeed before each function may proceed.
- FPT_SEP.1: The TOE must be protected from interference that would prevent it from performing its functions.

8.2.1.9 O.OFLOWS

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

This TOE Security Objective is satisfied by ensuring that:
- FEP_STG.1: The system is required to protect system data from modification and unauthorized deletion.
- FEP_STG.2: The system is required to overwrite the oldest stored system data if storage capacity is reached.
- FAU_STG.1: The TOE is required to provide protected audit storage.
- FAU_STG.4: The TOE is required to overwrite the oldest stored audit records if audit storage is full.

8.2.1.10 O.RESPON

The TOE must respond appropriately to analytical conclusions where the TOE is the source.

This TOE Security Objective is satisfied by ensuring that:
- FEP_RCT.1: The TOE is required to respond accordingly in the event an extrusion is detected.

8.2.1.11 O.TIME

The TOE must have a reliable time stamp for audit purposes..

This environment Security Objective is satisfied by ensuring that:
- FPT_STM.1: The TOE hardware provides a reliable time stamp for auditing.

8.2.1.12 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..

This IT environment Security Objective is satisfied by ensuring that:
- FCS_COP.1c: The IT environment provides PKI certificates for key exchange encrypted authentication.
- FCS_CKM.4: The IT environment destroys access cryptographic keys.
- FDP_ITC.2: The IT environment enforces the Access Control Policy when importing user data into the TOE.

8.2.1.13 OE.CRYPTO

The IT environment must provide the TOE with a secure and effective capability to protect sensitive, security-relevant data transferred across a network between itself and other network entities.

This IT environment Security Objective is satisfied by ensuring that:
- FCS_COP.1c: The IT environment provides PKI certificates for key exchange and encrypted authentication to protect sensitive security-relevant data transferred.
- FCS_CKM.4: The IT environment destroys access cryptographic keys after use to protect data transferred.
- FDP_ITC.2: The IT environment enforces the Access Control Policy when importing sensitive security-relevant user data.
- FMT_MSA.2: The IT environment ensures that only security values are accepted.
- FPT_TDC.1: The IT environment provides the capability to interpret shared CA certificates.
- FTP_ITC.1: The IT environment provides a trusted communication channel for ECA exchange.

8.2.1.14 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..

This IT environment Security Objective is satisfied by ensuring that:
- FMT_MSA.2: The IT environment ensures that only secure values are accepted for security attributes.

8.2.1.15 OE.INTROP

The TOE is interoperable with the IT systems it monitors.

This IT environment Security Objective is satisfied by ensuring that:
- FPT_TDC.1: The IT environment provides the capability to interpret shared CA certificates.
- FTP_ITC.1: The IT environment provides a trusted communication channel for ECA exchange.

8.2.1.16 OE.PERSON

Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.

This IT environment Security Objective is satisfied by ensuring that:

- FMT_MSA.2: The IT environment ensures that only secure values are accepted for security attributes.

8.2.1.17 OE.PHYCAL

Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

This IT environment Security Objective is satisfied by ensuring that:
- FDP_ITC.2: The IT environment enforces the Access Control Policy when importing user data into the TOE.

8.3 Security Assurance Requirements Rationale

EAL2 was chosen as the assurance level because the TOE is a commercial product whose users require a low to moderate level of independently assured security. Further, the TOE is augmented with flaw remediation (ALC_FLR.3) because flaw remediation procedures provide greater assurance that security-related bugs will be fixed in a widely distributed commercial product. Fidelis Fidelis XPS is targeted at a relatively benign environment with good physical access security and competent administrators. Within such environments, it is assumed that attackers will have little attack potential. The chosen assurance level is appropriate with the threats and assumptions defined for the environment. As such, EAL2, augmented with ALC_FLR.3 is appropriate to provide the assurance necessary to counter the limited potential for attack.

8.4 Strength of Functions Rationale

The TOE minimum Strength of Function (SOF) is Basic (SOF-Basic). The rationale for the SOF is based on the low attack potential and the need to protect against the relatively benign environment with good physical access security and competent administrators. SOF-Basic is therefore selected. This security function is in turn consistent with the security objectives described in Section 4. Further, SOF-Basic was chosen to address the password mechanism that implements the FIA_UAU.1 (Timing of authentication) requirement that contains the only permutational mechanism in the TOE. FIA_UAU.1 instantiated by the identification and authentication function is the only requirement in the TOE that necessitates a SOF claim.

8.5 Requirement Dependency Rationale

The following table demonstrates that all dependencies among the claimed security requirements are satisfied with the exception of those in bracket's and bolded red where the rationale follows the table, and therefore the requirements work together to accomplish the overall objectives defined for the TOE.

ST Requirement	CC Dependencies	ST Dependencies
TOE SFRs		
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_SAR1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FCS_COP.1a	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 and FMT_MSA.2	**None * see note below**
FCS_COP.1b	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 and FMT_MSA.2	**None * see note below**
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.1 and FMT_MSA.3
FEP_ANL.1 (EXP)	none	none

ST Requirement	CC Dependencies	ST Dependencies
FEP_RCT.1 (EXP)	none	none
FEP_RDR.1 (EXP)	none	none
FEP_SDC.1 (EXP)	none	none
FEP_STG.1 (EXP)	none	none
FEP_STG.2 (EXP)	none	none
FIA_ATD.1	none	none
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UID.1	none	none
FMT_MOF.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MSA.1	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1, FMT_SMF.1 and FDP_ACC.1
FMT_MSA.3	FMT_MSA.1 and FMT_SMF.1	FMT_MSA.1 and FMT_SMF.1
FMT_MTD.1a	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1b	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1c	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1d	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1e	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.1
FPT_ITT.1	none	none
FPT_RVM.1	none	none
FPT_SEP.1	none	none
FPT_STM.1	none	none
FTA_SSL.1	FIA_UAU.1	FIA_UAU.1
IT Environment SFRs		
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 and FMT_MSA.2	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 and FMT_MSA.2
FCS_COP.1c	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 and FCS_CKM.4 and FMT_MSA.2	FDP_ITC.1 and FCS_CKM.4 and FMT_MSA.2
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1 and FMT_MSA.3	FDP_ACC.1 and FMT_MSA.3
FMT_MSA.2	ADV_SPM.1 and FDP_ACC.1 or FDP_IFC.1 and FMT_MSA.1 and FMT_SMR.1	FDP_ACC.1 and FMT_MSA.1 and FMT_SMR.1
FPT_TDC.1	none	none
FTP_ITC.1	none	none
SARs		
ACM_CAP.2	none	none
ADO_DEL.1	none	none
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1	ADV_RCR.1
ADV_HLD.1	ADV_FSP.1 and ADV_RCR.1	ADV_FSP.1 and ADV_RCR.1
ADV_RCR.1	none	none
AGD_ADM.1	ADV_FSP.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1	ADV_FSP.1
ALC_FLR.3	none	none
ATE_COV.1	ADV_FSP.1 and ATE_FUN.1	ADV_FSP.1 and ATE_FUN.1
ATE_FUN.1	none	none

ST Requirement	CC Dependencies	ST Dependencies
ATE_IND.2	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1
AVA_SOF.1	ADV_FSP.1 and ADV_HLD.1	ADV_FSP.1 and ADV_HLD.1
AVA_VLA.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1

Table 11 Requirement Dependency Mapping

Note: FCS_COP.1 has dependencies on FDP_ITC.1 (import of user data without security attributes), FDP_ITC.2 (import of user data with security attributes) or FCS_CKM.1 (key generation); FCS_CKM.4, (key destruction), and FMT_MSA.2 (secure data). The FCS_COP.1 claim is included in this ST to support the use of cryptographic hashing functions only. The specified FCS_COP.1 dependency requirements do not pertain to hashing functions where no cryptographic key sizes are applicable. The TOE uses the SHA1() function of the embedded MySQL for user password hashing and uses an RSA MD5 library to hash administrator-configured fingerprints for the Exact Content analyzer. The TOE was not developed with any mechanisms to support any of the dependency functions, as the TOE has adopted identified libraries only. Note that the TOE does include FMT_MSA.3; however, it is satisfying the dependency for FDP_ACF.1 and has nothing to do with the FCS_COP.1 requirements.

ADV_SPM.1 is not included in this ST since it was only added as a dependency requirement to the IT environment SFR, FMT_MSA.2 to support the TOEs use of an External Certificate Authority (ECA). As the FMT_MSA.2 SFR pertains to a required certificate authority in the IT environment for the TOEs use, a vendor security policy model for the certificate authority is not appropriate.

8.6 Explicitly Stated Requirements Rationale

A class of functional Extrusion Prevention System component requirements (FEP) was created to specifically address the data collected and analyzed by the TOE's extrusion prevention system capabilities. The explicitly IDS family of the CC (IDS) was used as a model for creating these requirements, although it must be noted that the TOE is not an IDS and as such does not claim conformance to the IDSSPP. However, the TOE is similar to the technology afforded by and IDS in that it contains sensors and provides analysis of system data, but the TOE provides extrusion prevention capabilities to an infrastructure and contains sniffers as part of the sensors. Whereas the IDS family is inappropriate, this ST has used a number of the IDS functional requirements as a baseline, but only as they pertain to an Extrusion Prevention System.

The purpose of this family of requires is to address the unique nature of Fidelis XPS data and provide for requirements about collecting, reviewing and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

8.7 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 12 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Security audit	Cryptographic support	User data protection	Fidelis XPS Component Requirements (FEP) (EXP)	Identification and authentication	Security management	Protection of the TSF	Session Locking
FAU_GEN.1	X							
FAU_SAR.1	X							
FAU_SAR.2	X							
FAU_STG.1	X							
FAU_STG.4	X							
FCS_COP.1a		X						
FCS_COP.1b		X						
FDP_ACC.1			X					
FDP_ACF.1			X					
FEP_ANL.1 (EXP)				X				
FEP_RCT.1 (EXP)				X				
FEP_RDR.1 (EXP)				X				
FEP_SDC.1 (EXP)				X				
FEP_STG.1 (EXP)				X				
FEP_STG.2 (EXP)				X				
FIA_ATD.1					X			
FIA_UAU.1					X			
FIA_UID.1					X			
FMT_MOF.1					X			
FMT_MSA.1						X		
FMT_MSA.3						X		
FMT_MTD.1a						X		
FMT_MTD.1b						X		
FMT_MTD.1c						X		
FMT_MTD.1d						X		
FMT_MTD.1e						X		
FMT_SMF.1						X		
FMT_SMR.1						X		
FPT_ITT.1							X	
FPT_RVM.1							X	
FPT_SEP.1							X	
FPT_STM.1							X	
FTA_SSL.1								X

Table 12 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.