Fidelis XPS™ Security Target

Version 1.0
3 April 2015

Prepared for:

Fidelis Cybersecurity
4416 East West Highway, Suite 310
Bethesda, Maryland 20814

Prepared by:

Leidos Inc. (formerly Science Applications International Corporation)

Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive, Columbia, Maryland 21046

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is Fidelis XPS ™, provided by Fidelis Cybersecurity. The product is a network security appliance for advanced threat detection. It detects inappropriate and malicious network data based on all aspects of the network traffic including the content, source, destination, application, and all aspects of the communication channel. The TOE is used to prevent the intrusion of attacks and to prevent the transmission of sensitive data, either as a result of an attack or insider threat. The TOE analyzes all network activity and will issue alerts of significant events. The TOE will also collect and store metadata from the network to allow the security analyst to view the context associated with alerts and to analyze all network activity. The focus of this evaluation is on the TOE functionality supporting the claims in the *Protection Profile for Network Devices* (See section 1.2 for specific version information). The security functionality specified in [NDPP] includes protection of communications between TOE components and trusted IT entities, identification and authentication of administrators, auditing of security-relevant events, ability to verify the source and integrity of updates to the TOE, and specifies FIPS-validated cryptographic mechanisms.

The Security Target contains the following additional sections:

1.

- TOE Description (Section 1)

- TOE Description (Section 1)
- Security Problem Definition (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8).

1.1 Security Target, TOE and CC Identification

ST Title – Fidelis XPS™ Security Target

ST Version – Version 1.0

ST Date – 3 April 2015

TOE Identification –

- Fidelis XPS Scout+ v8.0 (includes a CommandPost, a Direct Sensor, and a Collector in one box)

  OR

- One or more Fidelis CommandPost™ v8.0 management console appliances, zero or more Fidelis XPS Collector v8.0 appliances and at least one of the following sensor appliances: Fidelis XPS Direct v8.0, Fidelis XPS Internal v8.0, Fidelis XPS Web v8.0, and Fidelis XPS Mail v8.0.

Some of the appliances include multiple models as listed below:

- Fidelis CommandPost+ and Fidelis CommandPost PlusVM
- Fidelis XPS Direct 50, Fidelis XPS Direct 100, Fidelis XPS Direct 250, Fidelis XPS Direct 500, Fidelis XPS Direct 1000, Fidelis XPS Direct 2500, and Fidelis XPS Direct VM
- Fidelis XPS Internal 50, Fidelis XPS Internal 100, Fidelis XPS Internal 250, Fidelis XPS Internal 500, Fidelis XPS Internal 1000, Fidelis XPS Internal 2500, and Fidelis XPS Internal VM
- Fidelis XPS Web and Fidelis XPS Web VM
- Fidelis XPS Mail and Fidelis XPS Mail VM
- Fidelis XPS Collector SA and Fidelis XPS Collector SA VM
- Fidelis XPS Collector Cluster, which includes one Fidelis XPS Collector Controller, and multiple Fidelis XPS Collector XA nodes. A redundant Fidelis XPS Collector is optional
- Fidelis XPS Blade Array, which may include blades to implement either a Fidelis XPS Direct 2500 sensor or a Fidelis XPS Internal 2500 sensor on each blade. The blade array provides the same function as Direct or Internal sensors at up to 20Gbps throughput capability when fully loaded with blades.

The virtual appliances (designated by "VM" at the end of their names) were tested in a virtual environment consistent with the requirements described in Section 2.2.1.1 of this document, including an Intel i7-4770 processor in the host hardware system. More generally, the virtual appliances are supported on host hardware that includes Intel Core or Xeon processors based on the Ivy Bridge or Haswell microarchitecture, which implement Intel Secure Key.

TOE Developer – Fidelis Cybersecurity

Evaluation Sponsor –Fidelis Cybersecurity

CC Identification – *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012*

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- This ST is conformant to the *Protection Profile for Network Devices*, Version 1.1, 8 June 2012 (NDPP) as amended by Errata #2 dated 13 January 2014, and includes the additional optional SFRs: FCS_HTTPS_EXT.1, FCS_TLS_EXT.1, and FPT_ITT.1.
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.
    - Part 3 Conformant

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number in parentheses placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, (1) and (2).
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …"). Note that 'cases' that are not applicable in a given SFR have simply been removed without any explicit identification.
- The NDPP uses an additional convention – the 'case' – which defines parts of an SFR that apply only when corresponding selections are made or some other identified conditions exist. Only the applicable cases are identified in this ST and they are identified using **bold** text.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.1 Terminology

This section identifies TOE-specific terminology.

Alert	An alert is the recorded and displayed incident of a network event and is generated if the alert action for the rule has been configured to include an alert. Alerts are violations of advanced threat detection policies.

CommandPost™
Unique name for the Fidelis XPS management console appliance of the TOE.

Collector
Unique name for the Fidelis XPS Collector appliance. This may refer to a single appliance configuration (Fidelis XPS Collector SA) or to a cluster of appliances which include a Fidelis XPS Collector Controller and three or more Fidelis XPS Collector XA nodes.

Event
A rule violation. One or more events are reported as an alert if the rule action is configured to alert.

Fidelis Insight Server
A non-TOE component which provides software and policy updates for the TOE.

Fidelis XPS
The TOE, which includes one or more management consoles (CommandPost), and one or more Fidelis XPS sensors. It may also include zero or more Fidelis XPS Collectors.

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’).

ISO
An ISO image (or .ISO file) is a computer file that is an exact copy of an existing file system

MetaData
Data collected by a Fidelis XPS sensor for all network traffic, whether a rule violation occurs or not. Metadata is stored within a Fidelis XPS Collector appliance and is available for analysis by a Fidelis XPS CommandPost.

Milter Protocol
A protocol for e-mail traffic handling that receives e-mail traffic from an external MTA, reassembles the e-mail session and forwards to the next layer for protocol decoding.

Policy
Fidelis XPS policies are composed of one or more rules, which in turn, contain one or more fingerprint definitions.

Postfix
An open source mail server alternative to the Sendmail program.

Rule
A rule is a logical combination of fingerprints that together are used by the event manager to generate alerts based on matches on combinations of fingerprints.

SAMBA
A software re-implementation of the SMB/CIFS networking protocol, providing file and print services for various Microsoft Windows clients.

Sendmail
A general purpose internetwork e-mail routing facility that supports many kinds of mail-transfer and delivery methods.

Sensor
Refers to the Fidelis XPS Direct, Fidelis XPS Internal, Fidelis XPS Web, and Fidelis XPS Mail appliances (hardware or virtual) running the Fidelis XPS software.

1.3.2 Abbreviations

This section identifies abbreviations and acronyms used in this ST.

AES	Advanced Encryption Standard
API	Application Programming Interface
CBC	Cipher-Block Chaining
CA	Certificate Authority
CC	Common Criteria for Information Technology Security Evaluation
CIFS	Common Internet File System
CM	Configuration Management
CRL	Certificate Revocation List
DH	Diffie-Hellman
ECB	Electronic Codebook
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
HTTP	Hypertext Transfer Protocol
ICAP	Internet Content Adaptation Protocol
LDAP	Lightweight Directory Access Protocol
MTA	Mail Transfer Agent
MDE	Malware Detection Engine
NDPP	Protection Profile for Network Devices
OS	Operating System
PEM	Privacy Enhanced Email
PGP	Pretty Good Privacy
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMB	Server Message Block
SPAN	Switched Port ANalyzer
SNMP	Simple Network Management Protocol
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
UAU	User Authentication
UDP	User Datagram Protocol
VM	Virtual Machine

2. TOE Description

The Target of Evaluation (TOE) is a combination of Fidelis XPS™ version 8.0 appliances. More specifically, the TOE consists of one or more Fidelis XPS v8.0 management consoles, zero or more Fidelis XPS Collectors v8.0 and at least one of the following sensor appliances: Fidelis XPS Direct v8.0, Fidelis XPS Internal v8.0, Fidelis XPS Web v8.0, and Fidelis XPS Mail v8.0. The TOE also includes Fidelis XPS Scout+ v8.0 which includes a CommandPost; a Direct Sensor; and a Collector in one box.

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

If the configuration includes a Fidelis XPS Collector, the details about every network transaction are captured into metadata and stored on the Collector. The metadata includes all attributes of the analyzed network traffic, but excludes any recording of the data. Metadata includes the identified protocol and application in addition to any attributes detected by the protocol, application, or files transferred. The tag action of a policy can be used to simply tag the metadata without taking any further action on the network data.

The Fidelis XPS sensor software is designed around a series of layers where the first layer receives packets from the attached networks. Unless these packets belong to a session that has already been marked for prevention by the sensor, they would be sent to the next layer for further analysis. The next layer performs session reassembly, organizing the network traffic into streams and then forwards the stream pointer to the next layer where the payload is decoded. This layer identifies protocols and applications and ultimately reveals the contents. Authorized administrators configure policies that delineate exactly what the TOE will capture, analyze and monitor. Once the content is identified, the next layer is invoked to apply a set of rules (e.g., string searches, regular expressions, etc.). These rules can combine content patterns and other attributes (e.g., protocol or application) to form either specific or generic rules. When the rules indicate a violation, the sensor performs the action identified by the rule. The Fidelis XPS Direct, Internal, and Mail sensors also include a Malware Detection Engine (MDE) that can examine files to determine malicious intent. The MDE uses intelligence obtained from the Fidelis Insight Policy server and uses internal and external sources for file examination and the determination of maliciousness. CommandPost also contains the MDE function, which can be applied to data received from Fidelis XPS Web as well as files that are applied through the user interface. MDE performed on CommandPost cannot be used for prevention.

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

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

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

The Fidelis XPS product includes several operational modes that provide full prevention capabilities. This evaluation includes the network device functionality as defined in the NDPP and does not include evaluation of all of the product functionality and therefore all modes of operation as identified in the guidance documentation are acceptable in the evaluated configuration. All intrusion detection and protection functionality may be enabled without affecting the claimed security functionality; however these features have not been evaluated.

CommandPost can communicate with Fidelis Insight Server to download policy and TOE updates. When CommandPost downloads a new policy or update package, it is digitally signed using RSA keys. The signature is verified by using the on-board public keys (PGP public key) on the CommandPost. The server and secure policy download are not included in the TOE. The communication channel between the TOE and the Fidelis Insight Server is protected as described below.

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, CommandPost uses TLS to interact with its associated Sensors for the purposes of configuring the sensors and receiving information back from the sensors. CommandPost also uses TLS/HTTPS for health status and audit notifications. Finally, the TOE uses TLS for communications with trusted external IT entities such as authentication servers, Syslog, and Fidelis Insight Server. The TOE is operated in FIPS mode and includes a NIST validated OpenSSL module.

The TOE provides several system functions that are controlled by an access privilege per user where a role is a collection of these functions. The levels of access are determined for TOE features such as Fidelis XPS appliance configuration and user management. CommandPost includes several predefined roles, but only the System Administrators can manage all of the TOE security functions. Other roles only have a subset of TOE access capabilities.

2.1 TOE Overview

The Target of Evaluation (TOE) is a combination of Fidelis XPS™ version 8.0 appliances. More specifically, the TOE consists of one or more Fidelis XPS v8.0 management consoles, zero or more Fidelis XPS Collector v8.0 and at least one of the following sensor appliances: Fidelis XPS Direct v8.0; Fidelis XPS Internal v8.0; Fidelis XPS Web v8.0; and Fidelis XPS Mail v8.0. The TOE also includes Fidelis XPS Scout+ v8.0 which includes a CommandPost, a Direct Sensor, and a Collector in one box.

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

Each Fidelis XPS appliance includes a hardened CentOS 6.5 with kernel 2.6.32-431.20.3.el6.x86_6, and custom Fidelis XPS applications.

The CommandPost is available in two models: CommandPost Plus (hardware appliance), and CommandPost VM (virtual appliance). A CommandPost is required when using any of the TOE sensors or Collector. Each CommandPost has the same security features, differing only in their form of deployment (hardware or VM). The CommandPost appliance provides the CommandPost Management Console. The Management Console offers a web-based enterprise administrative interface for configuration, and management of the TOE. Additional CommandPosts can be set up to be Masters or Subordinates. All CommandPosts are capable of collecting, aggregating, and storing data from multiple sensors.

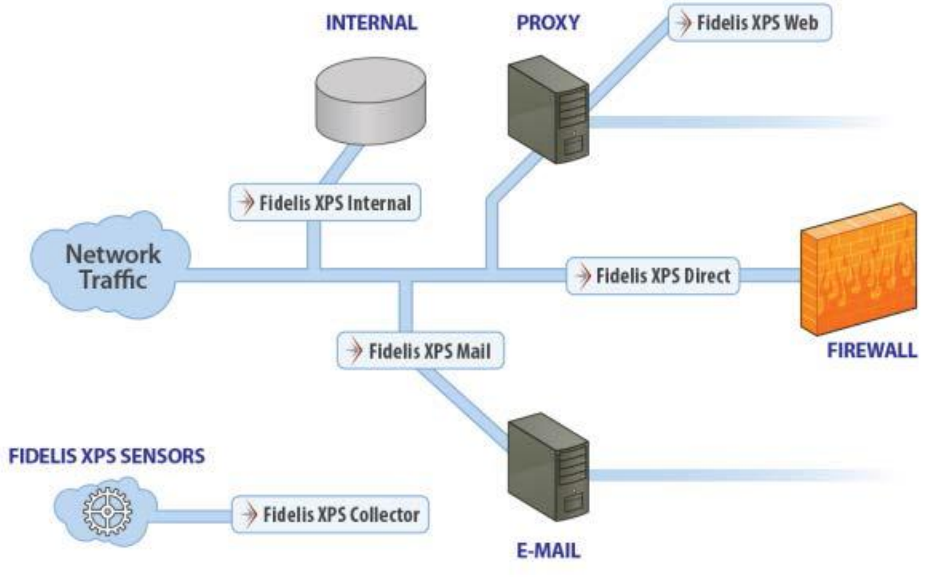
The Fidelis XPS Collector serves as the storage and access point for metadata information. The Collector listens for incoming connections from CommandPost and any sensors configured to use the Fidelis XPS Collector. The Collector is available as a single appliance, Collector SA, and as an extensible combination of a Collector Controller and three or more Collector XA appliances. The Fidelis XPS Collector SA is recommended for connection to a single sensor. The extensible Fidelis XPS Collector Controller plus Fidelis XPS Collector XA is recommended for connecting to multiple sensors.

The Fidelis XPS sensors are used to monitor, capture, and examine network traffic sending pertinent findings and other data to the CommandPost, which is used to manage its associated Fidelis XPS sensors and to further analyze the information received from those sensors. In most cases the TOE would be deployed as a single CommandPost associated with one or more sensors. However, two or more CommandPosts can be deployed in a redundant or hierarchical manner. Several models exist for the Fidelis XPS Sensors to address a variety of network architectures, including IPv4 and IPv6. Each appliance type is designed to monitor specific types of network traffic. The differences in the models for a given appliance type involve data rate capacities and form of deployment (hardware or VM), but each of the models for a given appliance type has the same security features.

- The Fidelis XPS Direct sensor monitors and enforces extrusion/intrusion policies across all 65,535 Internet Protocol (IP) ports on the network. This sensor is normally placed at the border of a protected network and is optimized to process numerous, relatively short-lived connections.
- The Fidelis XPS Internal sensor is similar to Direct, but supports protocols typically seen only inside the network, including Oracle and DB2 database access, SMB/CIFS/SAMBA file transfers, and directory queries. This sensor is normally placed within a protected network and is optimized to process a relatively small number of longer duration sessions (e.g., SMB) and is also capable of decoding the content of some protocols such as LDAP and SMB.
- The Fidelis XPS Web sensor monitors and enforces policy for traffic flowing through ICAP-enabled proxy servers.
- The Fidelis XPS Mail sensor monitors and enforces policy for Simple Mail Transfer Protocol (SMTP) e-mail traffic.

Note that hereinafter, the Fidelis XPS sensor appliance identification will not include the specific type (Direct, Internal, Web, 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 sensor(s), where all references pertain to the same TOE component providing this functionality.

A sample deployment scenario for the sensors is depicted as follows.



CommandPosts communicate with one or more sensors and one or more Collectors. Collectors communicate with CommandPost and any sensors configured to use the Fidelis XPS Collector. All communication channels between TOE components and with trusted external IT entities are protected via TLS and/or TLS/HTTPS.

2.2 TOE Architecture

The section describes the TOE physical and logical boundaries.

2.2.1 Physical Boundaries

As explained above, a given Fidelis XPS configuration includes one or more Fidelis XPS v8.0 management consoles, zero or more Fidelis XPS Collector v8.0 and at least one of the following sensor appliances: Fidelis XPS Direct v8.0; Fidelis XPS Internal v8.0; Fidelis XPS Web v8.0; and Fidelis XPS Mail v8.0. The TOE also includes Fidelis XPS Scout+ v8.0 which includes a CommandPost, a Direct Sensor, and a Collector in one box. Each Fidelis XPS appliance is a self-contained hardware appliance or VM designed to interact with its environment via network connections.

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

2.2.1.1 Software Requirements

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

- Browser: Microsoft Internet Explorer; Firefox; Google Chrome; or Apple Safari
- Adobe Flash Player

The virtual (VM) appliances are delivered as an installation disk (or ISO image). They require that the following are installed on the host hardware system:

- VMware ESX or ESXi 5.1 and newer
- VMware vSphere 5.1 (and newer) client or VMware VCenter 5.1 and newer.
- The host hardware must be an Intel Core or Xeon processor based on the Ivy Bridge or Haswell microarchitecture that provides Intel Secure Key capability, which is required to meet entropy requirements. The VM must be based on Virtual Hardware version 9 or greater to utilize the Secure Key.

The VM appliances also require the following:

Type of virtual machine	**Number of vCPUs**	**Memory (GB)**	**Disk (GB)**	**Monitoring Virtual Switch**
CommandPost+ VM	8	24	100	N/A
Direct 1000 VM	8	24	30	1
Internal 1000 VM	8	24	30	1
Web VM	4	8	100	N/A
Mail VM	4	8	100	N/A
Collector SA VM	8	32	200	N/A

Use of the optional syslog and external authentication methods require LDAP, and syslog servers. An NTP Server is required for proper clock synchronization for use in creating reliable timestamps.

2.2.1.2 Additional Hardware Requirements

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

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

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

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

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

2.2.2 Logical Boundaries

This section summarizes the security functions provided by the TOE:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

2.2.2.1 Security audit

The TOE is designed to be able to generate logs for a wide range of security relevant events including the events specified in NDPP. The TOE can be configured to store the logs locally so they can be accessed by an administrator and can also be configured to send the logs to a designated external log server.

2.2.2.2 Cryptographic support

The TOE is operated in FIPS mode and includes a NIST-validated OpenSSL cryptographic module. The module provides key management, random bit generation, encryption/decryption, digital signature and cryptographic hashing and keyed-hash message authentication features in support of higher level cryptographic protocols, including HTTP over TLS.

2.2.2.3 User data protection

The TOE is designed to ensure that it does not inadvertently reuse data found in network traffic.

2.2.2.4 Identification and authentication

The TOE requires users (i.e., administrators) to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers a network accessible GUI (HTTP over TLS) for interactive administrator sessions.

The TOE supports the local (i.e., on device) definition of administrators with usernames and passwords. Additionally, the TOE can be configured to use the services of trusted LDAP servers in the operational environment.

2.2.2.5 Security management

The TOE provides a GUI to access the wide range of security management functions. Security management commands are limited to administrators and are available only after they have provided acceptable user identification and authentication data to the TOE.

The TOE also provides the ability to manage the TOE locally. All administrative functionality available from the GUI is also available via a USB keyboard and a monitor to the appliance VGA connector using the special debug account. However, the TOE is designed to be managed using the GUI CommandPost from a remote HTTPS/TLS client. Following the initial configuration, all changes should be performed by an authorized user from CommandPost. The TOE provides the System Administrator role which corresponds to the NDPP Security Administrator.

2.2.2.6 Protection of the TSF

The TOE implements a number of features designed to protect itself to ensure the reliability and integrity of its security features.

It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. The TOE includes a hardware-based real-time clock that in conjunction with an NTP server in the operational environment ensure that reliable time information is available (e.g., for log accountability).

The TOE uses TLS and HTTPS to protect communications between distributed TOE components (FPT_ITT.1).

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

2.2.2.7 TOE access

The TOE can be configured to display an informative banner that will appear prior to an administrator being permitted to establish an interactive session. Prior to a user logging in, the user must indicate whether he/she wants to continue with the authentication process. The TOE subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session will be terminated.

2.2.2.8 Trusted path/channels

The TOE protects interactive communication with remote administrators using HTTP over TLS. TLS ensures both integrity and disclosure protection.

The TOE protects communication with network peers, such as log server, Fidelis Insight Server and authentications servers, using TLS connections to prevent unintended disclosure or modification of the transferred data.

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.

- Fidelis XPS Enterprise Setup and Configuration Guide, Version 8.0, Revised 2015
- Fidelis XPS User Guide, Version 8.0, Revised 2015
- Fidelis XPS Guide to Creating Policies, Version 8.0, Revised 2015
- Fidelis XPS Collector Quick Start Card, 2013
- Fidelis XPS Quick Start Card, 2013
- Fidelis XPS Addendum Versions 8.0 and 8.0.1, March 2015

3. Security Problem Definition

This security target includes by reference the Security Problem Definition (composed of organizational policies, threat statements, and assumptions) from the NDPP.

In general, the NDPP has presented a Security Problem Definition appropriate for network infrastructure devices, and as such is applicable to the Fidelis TOE.

4. Security Objectives

Like the Security Problem Definition, this security target includes by reference the Security Objectives from the NDPP. The NDPP security objectives for the operational environment are reproduced below, since these objectives characterize technical and procedural measures each consumer must implement in their operational environment.

In general, the NDPP has presented a Security Objectives statement appropriate for network infrastructure devices, and as such is applicable to the Fidelis TOE.

4.1 Security Objectives for the Operational Environment

OE.NO_GENERAL_PURPOSE
There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

OE.PHYSICAL
Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

OE.TRUSTED_ADMIN
TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

5. IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the Protection Profile (PP): *Protection Profile for Network Devices, Version 1.1, 8 June 2012* (NDPP), as amended by Errata #2. As a result, refinements and operations already performed in that PP are not identified (e.g., highlighted) here, rather the requirements have been copied from that PP and any residual operations have been completed herein. Of particular note, the NDPP made a number of refinements and completed some of the SFR operations defined in the CC and that PP should be consulted to identify those changes if necessary.

The SARs are the set of SARs specified in NDPP.

5.1 Extended Requirements

All of the extended requirements in this ST have been drawn from the NDPP. The NDPP defines the following extended SFRs and since they are not redefined in this ST, the NDPP should be consulted for more information in regard to those CC extensions.

- FAU_STG_EXT.1: External Audit Trail Storage
- FCS_CKM_EXT.4: Cryptographic Key Zeroization
- FCS_HTTPS_EXT.1: Extended: HTTP Security (HTTPS)
- FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)
- FCS_TLS_EXT.1: Extended: Transport Layer Security (TLS)
- FIA_PMG_EXT.1: Password Management
- FIA_UAU_EXT.2: Extended: Password-based Authentication Mechanism
- FIA_UIA_EXT.1: User Identification and Authentication
- FPT_APW_EXT.1: Extended: Protection of Administrator Passwords
- FPT_SKP_EXT.1: Extended: Protection of TSF Data (for reading of all symmetric keys)
- FPT_TST_EXT.1: TSF Testing
- FPT_TUD_EXT.1: Extended: Trusted Update
- FTA_SSL_EXT.1: TSF-initiated Session Locking

5.2 TOE Security Functional Requirements

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

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit Data Generation
	FAU_GEN.2: User identity association
	FAU_STG_EXT.1: External Audit Trail Storage
FCS: Cryptographic support	FCS_CKM.1: Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM_EXT.4: Cryptographic Key Zeroization
	FCS_COP.1(1): Cryptographic Operation (for data encryption/decryption)
	FCS_COP.1(2): Cryptographic Operation (for cryptographic signature)
	FCS_COP.1(3): Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(4): Cryptographic Operation (for keyed-hash message authentication)
	FCS_HTTPS_EXT.1: Extended: HTTP Security (HTTPS)
	FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)
	FCS_TLS_EXT.1: Extended: Transport Layer Security (TLS)
FDP: User data protection	FDP_RIP.2: Full Residual Information Protection
FIA: Identification and authentication	FIA_PMG_EXT.1: Password Management
	FIA_UAU.7: Protected Authentication Feedback
	FIA_UAU_EXT.2: Extended: Password-based Authentication Mechanism
	FIA_UIA_EXT.1: User Identification and Authentication
FMT: Security management	FMT_MTD.1: Management of TSF Data (for general TSF data)
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.2: Restrictions on Security Roles
FPT: Protection of the TSF	FPT_APW_EXT.1: Extended: Protection of Administrator Passwords
	FPT_ITT.1: Basic Internal TSF Data Transfer Protection
	FPT_SKP_EXT.1: Extended: Protection of TSF Data (for reading of all symmetric keys)
	FPT_STM.1: Reliable Time Stamps
	FPT_TST_EXT.1: TSF Testing
	FPT_TUD_EXT.1: Extended: Trusted Update
FTA: TOE access	FTA_SSL.3: TSF-initiated Termination
	FTA_SSL.4: User-initiated Termination
	FTA_SSL_EXT.1: TSF-initiated Session Locking
	FTA_TAB.1: Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1: Trusted Channel
	FTP_TRP.1: Trusted Path

Table 1 TOE Security Functional Components

5.2.1 Security audit (FAU)

5.2.1.1 Audit Data Generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shut-down of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All administrative actions;
d) Specifically defined auditable 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, information specified in column three of **Table 2**.

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	
FAU_GEN.2	None.	
FAU_STG_EXT.1	None.	
FCS_CKM.1	None.	
FCS_CKM_EXT.4	None.	
FCS_COP.1(1)	None.	
FCS_COP.1(2)	None.	
FCS_COP.1(3)	None.	
FCS_COP.1(4)	None.	
FCS_HTTPS_EXT.1	Failure to establish a HTTPS session. Establishment/Termination of a HTTPS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures
FCS_RBG_EXT.1	None.	
FCS_TLS_EXT.1	Failure to establish a TLS session. Establishment/Termination of a TLS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures
FDP_RIP.2	None.	
FIA_PMG_EXT.1	None.	
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	
FMT_MTD.1	None.	
FMT_SMF.1	None.	
FMT_SMR.2	None.	
FPT_APW_EXT.1	None.	
FPT_ITT.1	None.	
FPT_SKP_EXT.1	None.	
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).
FPT_TUD_EXT.1	Initiation of update.	No additional information.
FPT_TST_EXT.1	None.	
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	No additional information.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	No additional information.
FTA_SSL.4	The termination of an interactive session.	No additional information.
FTA_TAB.1	None.	
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.

Requirement	Auditable Events	Additional Audit Record Contents
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.

Table 2 Auditable Events

5.2.1.2 User identity association (FAU_GEN.2)

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.2.1.3 External Audit Trail Storage (FAU_STG_EXT.1)

FAU_STG_EXT.1.1 The TSF shall be able to [***transmit the generated audit data to an external IT entity***] using a trusted channel implementing the [***TLS***] protocol.

5.2.2 Cryptographic support (FCS)

5.2.2.1 Cryptographic Key Generation (for asymmetric keys) (FCS_CKM.1)

FCS_CKM.1.1 Refinement: The TSF shall generate asymmetric cryptographic keys used for key establishment in accordance with [

- ***NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” for elliptic curve-based key establishment schemes and implementing “NIST curves” P-256, P-384 and [no other curves] (as defined in FIPS PUB 186-3, “Digital Signature Standard”)***
- ***NIST Special Publication 800-56B, 'Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography' for RSA-based key establishment schemes***]

and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.

5.2.2.2 Cryptographic Key Zeroization (FCS_CKM_EXT.4)

FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

5.2.2.3 Cryptographic Operation (for data encryption/decryption) (FCS_COP.1(1))

FCS_COP.1(1).1 Refinement: The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm [AES operating in [***CBC, GCM***]] and cryptographic key sizes 128-bits and 256-bits that meets the following:

- FIPS PUB 197, 'Advanced Encryption Standard (AES)'
- [***NIST SP 800-38A, NIST SP 800-38D***].

5.2.2.4 Cryptographic Operation (for cryptographic signature) (FCS_COP.1(2))

FCS_COP.1(2).1 Refinement: The TSF shall perform cryptographic signature services in accordance with a [

(1) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater, or

(2) Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 bits or greater]

that meets the following:

Case: RSA Digital Signature Algorithm

- FIPS PUB 186-2 or FIPS PUB 186-3, “Digital Signature Standard”

Case: Elliptic Curve Digital Signature Algorithm

- FIPS PUB 186-3, “Digital Signature Standard”
- The TSF shall implement “NIST curves” P-256, P-384 and [***no other curves***] (as defined in FIPS PUB 186-3, “Digital Signature Standard”).

.

5.2.2.5 Cryptographic Operation (for cryptographic hashing) (FCS_COP.1(3))

FCS_COP.1(3).1 Refinement: The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [***SHA-1, SHA-256 and SHA-384***] and message digest sizes [***160, 256, 384***] bits that meet the following: FIPS Pub 180-3, 'Secure Hash Standard.'

5.2.2.6 Cryptographic Operation (for keyed-hash message authentication) (FCS_COP.1(4))

FCS_COP.1(4).1 Refinement: The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-[***SHA-1***], key size [**160 bits**], and message digest sizes [***160***] bits that meet the following: FIPS Pub 198-1, 'The Keyed-Hash Message Authentication Code', and FIPS Pub 180-3, 'Secure Hash Standard.'

5.2.2.7 Extended: HTTP Security (HTTPS) (FCS_HTTPS_EXT.1)

FCS_HTTPS_EXT.1.1

The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2

The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

5.2.2.8 Extended: Cryptographic Operation (Random Bit Generation) (FCS_RBG_EXT.1)

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [***NIST Special Publication 800-90 using [CTR_DRBG (AES)]***] seeded by an entropy source that accumulated entropy from [***a hardware-based noise source***].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength of the keys and hashes that it will generate

5.2.2.9 Extended: Transport Layer Security (TLS) (FCS_TLS_EXT.1)

FCS_TLS_EXT.1.1

The TSF shall implement one or more of the following protocols [***TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)***] supporting the following ciphersuites:

Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA,

Optional Ciphersuites:

[***TLS_RSA_WITH_AES_256_CBC_SHA***,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

].

5.2.3 User data protection (FDP)

5.2.3.1 Full Residual Information Protection (FDP_RIP.2)

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***allocation of the resource to***] all objects.

5.2.4 Identification and authentication (FIA)

5.2.4.1 Password Management (FIA_PMG_EXT.1)

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [***“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(”, “)”,*** [**blank space, and ~`_+-={}|[]:;<>,./**.];
2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater;

5.2.4.2 Protected Authentication Feedback (FIA_UAU.7)

FIA_UAU.7.1 The TSF shall provide only obscured feedback to the administrative user while the authentication is in progress at the local console.

5.2.4.3 Extended: Password-based Authentication Mechanism (FIA_UAU_EXT.2)

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, [***[and access to an external LDAP Server]***] to perform administrative user authentication.

5.2.4.4 User Identification and Authentication (FIA_UIA_EXT.1)

FIA_UIA_EXT.1.1 The TSF shall allow responses to the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [***[Acceptance of the end user license]***].

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

5.2.5 Security management (FMT)

5.2.5.1 Management of TSF Data (for general TSF data) (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to manage the TSF data to the Security Administrators.

5.2.5.2 Specification of Management Functions (FMT_SMF.1)

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

- Ability to administer the TOE locally and remotely;
- Ability to update the TOE, and to verify the updates using the [***digital signature***] capability prior to installing those updates;
- [***Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1***].

5.2.5.3 Restrictions on Security Roles (FMT_SMR.2)

FMT_SMR.2.1 The TSF shall maintain the roles:

- Authorized Administrator.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions

- Authorized Administrator role shall be able to administer the TOE locally;
- Authorized Administrator role shall be able to administer the TOE remotely;

are satisfied.

5.2.6 Protection of the TSF (FPT)

5.2.6.1 Extended: Protection of Administrator Passwords (FPT_APW_EXT.1)

FPT_APW_EXT.1.1 The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext passwords.

5.2.6.2 Extended: Protection of TSF Data (for reading of all symmetric keys) (FPT_SKP_EXT.1)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric key, and private keys.

5.2.6.3 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 Refinement: The TSF shall protect TSF data from disclosure and detect its modification when it is transmitted between separate parts of the TOE through the use **of** [***TLS, TLS/HTTPS***].

5.2.6.4 Reliable Time Stamps (FPT_STM.1)

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

5.2.6.5 TSF Testing (FPT_TST_EXT.1)

FPT_TST_EXT.1.1 The TSF shall run a suite of self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

5.2.6.6 Extended: Trusted Update (FPT_TUD_EXT.1)

FPT_TUD_EXT.1.1 The TSF shall provide security administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide security administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a [***digital signature mechanism***] prior to installing those updates.

5.2.7 TOE access (FTA)

5.2.7.1 TSF-initiated Termination (FTA_SSL.3)

FTA_SSL.3.1 Refinement: The TSF shall terminate a remote interactive session after a Security Administrator-configurable time interval of session inactivity.

5.2.7.2 User-initiated Termination (FTA_SSL.4)

FTA_SSL.4.1 The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

5.2.7.3 TSF-initiated Session Locking (FTA_SSL_EXT.1)

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [***terminate the session***] after a Security Administrator-specified time period of inactivity.

5.2.7.4 Default TOE Access Banners (FTA_TAB.1)

FTA_TAB.1.1 Refinement: Before establishing an administrative user session the TSF shall display a Security Administrator-specified advisory notice and consent warning message regarding use of the TOE.

5.2.8 Trusted path/channels (FTP)

5.2.8.1 Trusted Channel (FTP_ITC.1)

FTP_ITC.1.1 Refinement: The TSF shall use [***TLS***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [***authentication server, [Fidelis Insight Server]***] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2 The TSF shall permit the TSF, or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**transmitting audit records to an audit server, obtaining TOE updates, and external authentication functions**].

5.2.8.2 Trusted Path (FTP_TRP.1)

FTP_TRP.1.1 Refinement: The TSF shall use [***TLS/HTTPS***] **to** provide a communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and detection of modification of the communicated data.

FTP_TRP.1.2 Refinement: The TSF shall permit remote administrators to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial administrator authentication and all remote administrative actions.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are included by reference from the NDPP.

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

Table 3 Assurance Components

Consequently, the assurance activities specified in NDPP apply to the TOE evaluation.

6. TOE Summary Specification

This chapter describes the security functions:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

6.1 Security audit

The TOE is designed to be able to generate log records for a wide range of security relevant and other events as they occur. The events that can cause an audit record to be logged include starting and stopping the audit function, any use of an administrator command via the CommandPost GUI, as well as all of the events identified in **Table 2** (which corresponds to the audit events specified in NDPP). Note that the only protocol (i.e., HTTPS, TLS) failures auditable by the TOE are authentication failures for user-level connections.

The logged audit records identify the date and time, the nature or type of the triggering event, an indication of whether the event succeeded or failed, and the identity of the user responsible for the event. The logged audit records also include event-specific content that includes at least all of the content required in **Table 2**.

The TOE includes an internal log implementation that can be used to store and review audit records locally. The local audit logs are stored on the CommandPost hard drive. The TOE is designed to retain audit records for a configurable number of days (default is 190 days). Any audit record older than this number of days will be removed. The retention of the audit information in the audit database is based on the configurable number of days to keep records for (default is 190). There is no enforced limit on the size of this table, but system disk space is monitored and once disk space becomes limited, the cleanup process is more aggressive than the configured number of days. Aggressive audit cleanup involves a check for disk space at the time of adding an audit event. If disk is low, up to 20 of the oldest audit events are deleted. If any events are deleted due to disk shortage, a status message is sent to the console, and an audit event to the effect is also logged. Authorized administrators can configure the storage time to help control how often audit records get overwritten. Only authorized administrators can access the local audit trail. There are no interfaces to delete individual audit records. The TOE can be configured to send generated audit records to an external Syslog server using TLS. When configured to send audit records to a syslog server, audit records are also written to the external syslog as they are written locally to the CommandPost audit log.

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

- FAU_GEN.1: The TOE can generate audit records for events including starting and stopping the audit function, administrator commands, and all other events identified in **Table 2**. Furthermore, each audit record identifies the date/time, event type, outcome of the event, responsible subject/user, as well as the additional event-specific content indicated in **Table 2**.
- FAU_GEN.2: The TOE associates each auditable event with the identity of the user that caused the event.
- FAU_STG_EXT.1: The TOE can be configured to export audit records to an external Syslog server and can be configured to use TLS for communication with the Syslog server.

6.2 Cryptographic support

The TOE provides a FIPS mode of operation, which must be enabled in the evaluated configuration. The TOE includes NIST-validated cryptographic algorithms providing supporting cryptographic functions. The following functions have been certified in accordance with the identified standards.

Functions	Standards	Certificates
Asymmetric key generation		
• Domain parameter generation (key size 2048 bits)	NIST Special Publication 800-56A NIST Special Publication 800-56B	RSA #1273 ECDSA #413
Encryption/Decryption		
• AES CBC, GCM (128 and 256 bits)	FIPS PUB 197 NIST SP 800-38A	AES #2484
Cryptographic signature services		
• RSA Digital Signature Algorithm (rDSA) (modulus 2048) • ECDSA (256 bit) (P-256, P-384)	FIPS PUB 186-2 FIPS PUB 186-3	RSA #1273 ECDSA #413
Cryptographic hashing		
• SHA-1 (digest sizes 160 bits) • SHA-256 and SHA-384 (digest sizes 256 bits, 384)	FIPS Pub 180-3	SHS #2102
Keyed-hash message authentication		
• HMAC-SHA-1 (key size 160 bits and digest size 160 bits)	FIPS Pub 198-1 FIPS Pub 180-3	HMAC #1526
Random bit generation		
• CTR-DRBG(AES) with one independent hardware-based noise source of 256 bits of non-determinism	NIST Special Publication 800-90A	DRBG #342

Table 4 Cryptographic Functions

The TOE generates asymmetric cryptographic keys for elliptic curve-based key establishment schemes in accordance with Sections 5 and 6 of SP 800-56A.

The TOE generates asymmetric cryptographic keys for RSA-based key establishment schemes in accordance with Sections 5 through 8 of SP 800-56B.

The TOE uses a software-based deterministic random bit generator that complies with NIST SP 800-90, using CTR_DRBG (AES). The entropy source is a 256-bit value derived from hardware based noise source on Intel processors with Intel Secure Key technology. The Entropy Source provided by Intel Ivy Bridge DRNG is assumed to generate at least 0.5 bits of entropy per sample.

The TOE uses the following secret keys, private keys and CSPs.

Key/CSP Name	Algorithm/Key Size	Description
RSA SGK	RSA 2048 bits	RSA signature generation key
RSA KDK	RSA 2048 bits	RSA key decryption (private key transport) key
ECDSA SGK	ECDSA P-256, P-384	ECDSA signature generation key
EC DH Private	EC DH P-256, P-384	EC DH private key agreement key
AES EDK	AES 128, 256 bits	AES encrypt/decrypt key
AES GCM	AES 128, 256 bits	AES encrypt/decrypt/generate/verify key
HMAC Key	HMAC 160 bits	HMAC keyed hash key
CTR_DRBG V	CTR_DRBG 128 bits	Internal CTR_DRBG state variable
CTR_DRBG Key	AES 128, 256 bits	Internal CTR_DRBG key variable

Table 5 Secret keys, Private keys and CSPs

The TOE incorporates OpenSSL, which provides implementation of the cryptographic algorithms specified in Table 4. The TOE operates in FIPS mode and invokes the OpenSSL cryptomodule APIs to set up and maintain the full TLS session, using the underlying cryptographic algorithms as identified in Table 4. Therefore, all key generation, negotiation of session keys, and packet authentication is performed by the cryptomodule. All secret keys, plaintext private keys, and CSPs (see Table 5 above) are managed by the cryptomodule and stored in RAM. The cryptomodule stores CTR_DRBG state values for the lifetime of the DRBG instance and destroys them when the DBRG is uninstantiated. The cryptomodule does not store any other secret or private keys or CSPs persistently (beyond the lifetime of an API call). They are destroyed automatically by the API when no longer required by overwriting once with 0s.

The TOE stores the Certificate files, CA-Certificate files, Private-Key files, and CRL files used in communication between TOE components in encrypted PEM format. The Certificate, CA Certificate, Private-Key and CRL files used for user communication with the CommandPost and for TOE to trusted external IT entities (Syslog, authentication servers, Fidelis Insight Server) are never loaded or stored in memory by the Fidelis code. The files are stored on the file system and in all cases the files are passed to OpenSSL via API calls that pass in the complete filename including full path. Each API call return is checked to make sure there were no errors. The cryptomodule itself does not return sensitive data values and is responsible for ensuring the memory that held those file contents gets zeroized. User passwords for users with local authentication are stored as SHA1 hash in a database located on the CommandPost.

When the CommandPost downloads a new software release package these are digitally signed by RSA keys. The signature is verified by using the on-board public keys (PGP public key) on the CommandPost.

The TOE uses OpenSSL FIPS Object Module version 2.0.9, which is covered by FIPS 140-2 cert number 1747. The algorithms used are AES (CBC, GCM) 128, 256, and 384 bit ciphers, in conjunction with HMAC-SHA-1, SHA-1, SHA-256 and SHA-384 and RSA or ECDSA signature verification. The implementations are in accordance with FIPS PUB 186-3, “Digital Signature Standard”, FIPS Pub 180-3, 'Secure Hash Standard', and FIPS Pub 198-1, 'The Keyed-Hash Message Authentication Code'.

The TOE’s HTTPS protocol complies with RFC 2818 and is implemented using TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), and TLS 1.2 (RFC 5246) supporting the following ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA,
- TLS_RSA_WITH_AES_256_CBC_SHA,
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

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

- FCS_CKM.1: See table above.
- FCS_CKM_EXT.4: See table above.
- FCS_COP.1(1): See table above.
- FCS_COP.1(2): See table above.
- FCS_COP.1(3): See table above.
- FCS_COP.1(4): See table above.
- FCS_HTTPS_EXT.1: The TOE supports HTTPS web-based secure administrator sessions.
- FCS_RBG_EXT.1: See table above.
- FCS_TLS_EXT.1: The TOE supports HTTP over TLS web-based secure administrator sessions.

6.3 User data protection

A multi-threaded daemon is responsible for packet processing in Fidelis XPS. One of the threads (dispatcher) copies the captured packet in packet ring memory; this copy is performed when there is sufficient space in the ring and is limited to the size of the captured packet. The ring is managed as a linked list and the packet copy always over-writes any previous data in the ring, up to the size of the captured packet. Another thread (processor) would pick up packets from the ring for processing and copying to its local memory. The local memory of the processor thread is the same for all packets, and the packet is copied up to the captured length. Further processing including forwarding of the packet is done on this memory region, always guarded by the size of the packet (same as what was used for the copy). If forwarding is enabled, this memory region up to the size of the packet is written to the outgoing socket. Hence all processing and forwarding of packets is restricted to the data received in the captured packet only.

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

- FDP_RIP.2: The TOE always overwrites resources when allocated for use in objects.

6.4 Identification and authentication

The TOE is designed to require users to be identified and authenticated before they can access any of the TOE functions. Administrators manage the TOE remotely using a web-based GUI accessed via HTTPS. Administrators can also connect to the TOE locally using a directly connected console. However the TOE is not intended to be managed locally. For each session, the user is required to log in prior to successfully establishing a session through which TOE functions can be exercised. Note that the only capabilities allowed prior to users authenticating are the display of the warning banner before authentication, and acceptance of the end-user license. The user only needs to accept the license once for each software release, after which the license acceptance message will not display. The banner is displayed on every login attempt.

In order to log in, the user must provide an identity and also authentication data that matches the provided identity. Users can be defined locally within the TOE with a user identity, password, and user role. Alternately, users can be defined within an external LDAP (e.g. Active Directory) server configured to be used by the TOE, that also defines the user's role in the TOE. Locally defined users are authenticated directly by the TOE, while remotely defined users are authenticated by the external server and the result is enforced by the TOE. In either case, any resulting session is dependent upon successful authentication and established sessions are associated with the role(s) (see Section 6.5) assigned to the user.

When logging in, the TOE will not echo passwords so that passwords are not inadvertently displayed to the user and any other users that might be able to view the login display.

Note also that should a user have their session terminated (e.g., due to inactivity), they are required to successfully authenticate, by reentering their identity and authentication data, in order to establish a new session.

Password requirements can be configured for local user accounts. Passwords can be composed of upper and lower case letters, numbers and special characters, including blank space and ~`!@#$%^&*()_+-={}|[]:;<>,./. Also, new passwords have to satisfy a configurable minimum password length. The administrator can specify a minimum password length of 15 characters with no imposed upper bounds.

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

- FIA_PMG_EXT.1: The TOE implements a rich set of password composition constraints as described above.
- FIA_UAU.7: The TOE does not echo passwords as they are entered.
- FIA_UAU_EXT.2: The TOE provides a local password-based authentication mechanism and can be configured to use an external LDAP authentication server.
- FIA_UIA_EXT.1: The TOE only displays the warning banner and allows for acceptance of the end-user license prior to a user being identified and authenticated.

6.5 Security management

The TOE provides a GUI to access the wide range of security management functions. Security management commands are limited to administrators and are available only after they have provided acceptable user identification and authentication data to the TOE. The TOE controls user access to the TOE and resources based on user role. Users are given permission to access a set of commands and resources based on their user role.

The TOE also provides the ability to manage the TOE locally. All administrative functionality available from the GUI is also available via a USB keyboard and a monitor to the appliance VGA connector using special debug account. However, the TOE is designed to be managed using the GUI CommandPost from a remote HTTPS/TLS client. Following the initial configuration, all changes should be performed by an authorized user from CommandPost.

The TOE includes pre-defined user roles, of which only the user role: System Administrator is considered a ‘Security Administrator’ as defined in the NDPP. Users with the System Administrator role are capable of managing the security functions of the TOE. The security management functions required by the PP are accessible via the GUI, except configuration of the advisory banner, which is done via a USB keyboard and a monitor to the appliance VGA connector during initial configuration. The TOE includes other pre-defined roles that represent logical subsets of the System Administrator role. Only users with the System Administrator role can manage all aspects of the TOE.

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

- FMT_MTD.1: The TOE restricts the access to manage TSF data that can affect the security functions of the TOE to Security Administrators.
- FMT_SMF.1: The TOE includes the functions necessary to enable/disable available network services, to manage the cryptomodule and associated functions, and to manage and verify updates of the TOE software and firmware.
- FMT_SMR.2: The TOE includes predefined roles of which only the System Administrator role has access to all security management functions of the TOE, which corresponds to the required ‘Security Administrator’.

6.6 Protection of the TSF

While the administrative interface is function rich, the TOE is designed specifically to prevent access to locally-stored cryptographically protected passwords and does not disclose any keys stored in the TOE. The TOE protects user passwords by saving a SHA-1 hash of the password. The TOE does not offer any functions that will disclose to any users a stored cryptographic key or password. See Section 6.2 for more information about stored keys and passwords.

The TOE protects TSF data from disclosure and detects its modification when it is transmitted between separate parts of the TOE through the use TLS or TLS/HTTPS. Communication between TOE components uses TLS/HTTPS for health status, and audit notifications; and is always destined for the CommandPost. All other communications among TOE components such as for alerts, forensic, statistics, and configuration use TLS.

The TOE is a hardware appliance or a virtual appliance image installed on a hardware appliance that includes a hardware-based real-time clock. The TOE relies on the use of an NTP server in its operational environment for clock synchronization. The TOE's embedded OS in conjunctions with the NTP Server manages the clock and exposes administrator clock-related functions. The clock is used for audit record time stamps, measuring session activity for termination, and for cryptographic operations based on time/date.

The Fidelis XPS process manager service or 'pman' is responsible for bringing up all relevant Fidelis XPS processes. All the binaries include an embedded integrity checksum that pman verifies before starting the process. The proprietary checksum calculation algorithm is a slight variant of the MD5 hash algorithm. If the checksum is corrupted, the process will not be started and the service will go down. In addition, if a daemon fails to remain functional and keeps restarting frequently, this condition is logged and a message is sent via the system monitor.

CommandPost can be configured to check for software updates available on the Fidelis Insight Server using an HTTPS connection. A software update is available as a tar package along with its digital signature created by Fidelis using a 2048 bit RSA secret key. Fidelis XPS will download both of these via HTTPS and verify the signature using the on-board public key (corresponding to the RSA key used to create the signature). On verification, the tar package is used to do a software upgrade. If the verification fails, it is assumed that the download was corrupted and hence the package and its signature are deleted. Administrators with proper credentials are able to download the update package and its signature manually too. The authorized administrator can manually verify the signature before performing an upload of the update package to Fidelis XPS. The TOE provides functions to query and upgrade the TOE versions.

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

- FPT_APW_EXT.1: The TOE does not offer any functions that will disclose to any user a plain text password. Note that passwords are stored in cryptographically protected form within the TOE.
- FPT_ITT.1: The TOE protects TSF data from disclosure and detect its modification when it is transmitted between separate parts of the TOE through the use of TLS or TLS/HTTPS.
- FPT_SKP_EXT.1: The TOE does not offer any functions that will disclose to any users a stored cryptographic key.
- FPT_STM.1: The TOE includes its own hardware clock.
- FPT_TST_EXT.1: The TOE includes a process manager service that is responsible for bringing up all relevant Fidelis XPS processes and verifying integrity checksums in each binary. This serves to ensure that software checksums are correct and that the TOE is functioning properly.
- FPT_TUD_EXT.1: The TOE provides functions to query and upgrade the TOE versions. Digital signatures are used to ensure the integrity of each upgrade prior to performing the upgrade.

6.7 TOE access

The TOE can be configured by an administrator to display advisory banners prior to allowing an administrator to establish an administrative user session. The banner will be displayed when accessing the TOE locally or via the GUI.

The TOE can be configured by an administrator to set an interactive session timeout value (any integer value greater than zero in minutes). The default timeout is 15 minutes and the feature can be disabled. A remote session that is inactive (i.e., no commands issuing from the remote client) for the defined timeout value will be terminated. A local session that is similarly inactive for the defined timeout period will be terminated. The user will be required to re-enter their user id and their password so they can establish a new session once a session is terminated. If the user id and password match those of the user that was locked, the session is reconnected and normal input/output can again occur for that user.

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

- FTA_SSL.3: The TOE terminates remote sessions that have been inactive for an administrator-configured period of time.
- FTA_SSL.4: The TOE provides the function to logout (or terminate) both local and remote user sessions as directed by the user.
- FTA_SSL_EXT.1: The TOE terminates local sessions that have been inactive for an administrator-configured period of time.
- FTA_TAB.1: The TOE can be configured to display administrator-defined advisory banners before establishing an administrative user session.

6.8 Trusted path/channels

The TOE can be configured to export audit records to an external Syslog server. The TOE uses TLS to protect communications between itself and components in the operational environment including Fidelis Insight Server, Syslog and authentication servers (LDAP).

To support secure remote administration, the TOE includes an implementation of TLS. An authorized administrator can establish secure remote connections with the TOE using HTTP over TLS. To successfully establish an interactive administrative session, the administrator must be able to provide acceptable user credentials (e.g., user id and password), after which they will be able to access the GUI features.

The secure protocols are supported by NIST-validated cryptographic mechanisms included in the TOE implementation.

The Trusted path/channels function is designed to satisfy the following security functional requirements:

- FTP_ITC.1: The TOE can be configured to use TLS to ensure that any authentication operations, and exported audit records, are sent only to the configured Syslog or authentication servers so they are not subject to inappropriate disclosure or modification. TLS is also used to ensure TOE updates are transmitted securely.
- FTP_TRP.1: The TOE provides TLS to support secure remote administration. Administrators can initiate a remote session that is secured (from disclosure and modification) using NIST-validated cryptographic operations, and all remote security management functions requires the use of this secure channel.

7. Protection Profile Claims

The ST conforms to the *Protection Profile for Network Devices, Version 1.1, 8 June 2012* (NDPP), as amended by Errata #2 – with the optional HTTPS and TLS requirements.

As explained in Section 3, Security Problem Definition, the Security Problem Definition of the NDPP has been included by reference into this ST.

As explained in Section 4, Security Objectives, the Security Objectives of the NDPP have been included by reference into this ST.

The following table identifies all the Security Functional Requirements (SFRs) in this ST. Each SFR is reproduced from the NDPP and operations completed as appropriate.

Requirement Class	Requirement Component	Source
FAU: Security audit	FAU_GEN.1: Audit Data Generation	NDPP
	FAU_GEN.2: User identity association	NDPP
	FAU_STG_EXT.1: External Audit Trail Storage	NDPP
FCS: Cryptographic support	FCS_CKM.1: Cryptographic Key Generation (for asymmetric keys)	NDPP
	FCS_CKM_EXT.4: Cryptographic Key Zeroization	NDPP
	FCS_COP.1(1): Cryptographic Operation (for data encryption/decryption)	NDPP
	FCS_COP.1(2): Cryptographic Operation (for cryptographic signature)	NDPP
	FCS_COP.1(3): Cryptographic Operation (for cryptographic hashing)	NDPP
	FCS_COP.1(4): Cryptographic Operation (for keyed-hash message authentication)	NDPP
	FCS_HTTPS_EXT.1: Extended: HTTP Security (HTTPS)	NDPP
	FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)	NDPP
	FCS_TLS_EXT.1: Extended: Transport Layer Security (TLS)	NDPP
FDP: User data protection	FDP_RIP.2: Full Residual Information Protection	NDPP
FIA: Identification and authentication	FIA_PMG_EXT.1: Password Management	NDPP
	FIA_UAU.7: Protected Authentication Feedback	NDPP
	FIA_UAU_EXT.2: Extended: Password-based Authentication Mechanism	NDPP
	FIA_UIA_EXT.1: User Identification and Authentication	NDPP
	FMT_MTD.1: Management of TSF Data (for general TSF data)	NDPP
	FMT_SMF.1: Specification of Management Functions	NDPP
	FMT_SMR.2: Restrictions on Security Roles	NDPP
FPT: Protection of the TSF	FPT_SKP_EXT.1: Extended: Protection of TSF Data (for reading of all symmetric keys)	NDPP
	FPT_APW_EXT.1: Extended: Protection of Administrator Passwords	NDPP
	FPT_ITT.1: Basic Internal TSF Data Transfer Protection	NDPP
	FPT_STM.1: Reliable Time Stamps	NDPP
	FPT_TST_EXT.1: TSF Testing	NDPP
	FPT_TUD_EXT.1: Extended: Trusted Update	NDPP
FTA: TOE access	FTA_SSL.3: TSF-initiated Termination	NDPP
	FTA_SSL.4: User-initiated Termination	NDPP
	FTA_SSL_EXT.1: TSF-initiated Session Locking	NDPP
	FTA_TAB.1: Default TOE Access Banners	NDPP
FTP: Trusted path/channels	FTP_ITC.1: Trusted Channel	NDPP
	FTP_TRP.1: Trusted Path	NDPP

Table 6 SFR Protection Profile Sources

8. Rationale

This security target includes by reference the NDPP Security Problem Definition, Security Objectives, and Security Assurance Requirements. The security target makes no additions to the NDPP assumptions. NDPP security functional requirements have been reproduced with the Protection Profile operations completed. Operations on the security requirements follow NDPP application notes and assurance activities. Consequently, NDPP rationale applies but is incomplete. The TOE Summary Specification rationale below serves to complete the rationale required for the security target.

8.1 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 security functions work together to satisfy all of the security functional 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 7 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Security audit	Cryptographic support	User data protection	Identification and authentication	Security management	Protection of the TSF	TOE access	Trusted path/channels
FAU_GEN.1	X							
FAU_GEN.2	X							
FAU_STG_EXT.1	X							
FCS_CKM.1		X						
FCS_CKM_EXT.4		X						
FCS_COP.1(1)		X						
FCS_COP.1(2)		X						
FCS_COP.1(3)		X						
FCS_COP.1(4)		X						
FCS_HTTPS_EXT.1		X						
FCS_RBG_EXT.1		X						
FCS_TLS_EXT.1		X						
FDP_RIP.2			X					
FIA_PMG_EXT.1				X				
FIA_UAU.7				X				
FIA_UAU_EXT.2				X				
FIA_UIA_EXT.1				X				
FMT_MTD.1					X			
FMT_SMF.1					X			
FMT_SMR.2					X			
FPT_APW_EXT.1						X		
FPT_ITT.1						X		
FPT_SKP_EXT.1						X		
FPT_STM.1						X		
FPT_TST_EXT.1						X		
FPT_TUD_EXT.1						X		
FTA_SSL.3							X	
FTA_SSL.4							X	
FTA_SSL_EXT.1							X	
FTA_TAB.1							X	
FTP_ITC.1								X
FTP_TRP.1								X

Table 7 Security Functions vs. Requirements Mapping