# National Information Assurance Partnership


TM

# Common Criteria Evaluation and Validation Scheme Validation Report

# Fidelis XPS 5.0.3

**Report Number:** CCEVS-VR-VID10223-2008
**Dated:** 29 October 2008
**Version:** 1.6

**National Institute of Standards and Technology**
**Information Technology Laboratory**
**100 Bureau Drive**
**Gaithersburg, MD 20899**

**National Security Agency**
**Information Assurance Directorate**
**9800 Savage Road STE 6757**
**Fort George G. Meade, MD 20755-6757**

**ACKNOWLEDGEMENTS**

**Validation Team**

Paul Bicknell
Kenneth Eggers

**Common Criteria Testing Laboratory**

Terrie Diaz, Lead Evaluator
Science Applications International Corporation (SAIC)
Columbia, Maryland

# Table of Contents

# 1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Fidelis XPS, software version 5.0.3 running on Fidelis hardware appliance.

Fidelis XPS 5.0.3 TOE includes four hardware component options where a minimum of one (1) CommandPost appliance is required with up to three (3) sensor options 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):
   - Fidelis XPS Proxy (for Internet Content Adaptation Protocol (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 each is purchased and installed separately (with different license) and 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.

The appliances are running a hardened CentOS Linux 4.4 with MySQL 5.0.28 Enterprise Version and Fidelis XPS version 5.0.3 software.

The Validation Report presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of Fidelis XPS 5.0.3 was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory in the United States and was completed on 21 August 2008.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by SAIC. The ETR and test report used in developing this validation report were written by SAIC. The evaluation team determined the product to be Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL 2 augmented with ALC_FLR.3. The product is not conformant with any published Protection Profiles. All security functional requirements are derived from Part 2 of the Common Criteria or expressed in the form of Common Criteria Part 2 requirements.

The TOE is Fidelis XPS, software version 5.0.3 running on Fidelis hardware appliance versions as identified above. The TOE includes server applications running on the appliance hardware that is supported in the evaluated configuration as well as the appliance hardware itself. The TOE is an Extrusion Prevention System®, that is focused on network data leakage prevention where TOE appliances detect attempts to send inappropriate information, based on configuration, from one network to another; raises alarms and reacts to extrusion attempts to prevent an attack.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced.

During this validation, the Validators determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the Validator concludes that the SAIC findings are accurate, the conclusions justified, and the conformance claims correct.

# 2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products, desiring a security evaluation, contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant; and
- The organizations and individuals participating in the evaluation.

**Table 1: Evaluation Identifiers**

| Item | Identifier |
|---|---|
| **Evaluation Scheme** | United States NIAP Common Criteria Evaluation and Validation Scheme |
| **TOE**: | Fidelis XPS, software version 5.0.3 running on Fidelis hardware appliance: The hardware options include the following options:<br>• CommandPost:<br>o CommandPost (for one (1) to five (5) sensors), or<br>o CommandPost Plus (for six (6) or more sensors)<br>• Fidelis XPS Direct Sensor(s):<br>o Fidelis XPS Direct 100 (for networks up to |

| Item | Identifier |
|---|---|
| | 100Mbps)<br>o Fidelis XPS Direct 1000 (for networks up to 1Gbps)<br>• Fidelis XPS Proxy Sensor(s):<br>o Fidelis XPS Proxy (for ICAP integration with proxy servers up to 100Mbps)<br>o Fidelis XPS Proxy Plus (for ICAP integration with proxy servers up to 1Gbps)<br>• Fidelis XPS Mail Sensor<br>The evaluated configuration includes at least one CommandPost and at least one sensor. |
| **Protection Profile** | Not applicable |
| **ST** | Fidelis XPS 5.0.3 Security Target, Version 1.0, 29 October 2008 |
| **Evaluation Technical Report** | Evaluation Technical Report For Fidelis XPS 5.0.3, Part 1 (Non-Proprietary), Version 1.5 10 September 2008, Part 2 (Proprietary), Version 1.0 10 September 2008 |
| **CC Version** | Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 |
| **Conformance Result** | CC Part 2 extended and Part 3 conformant, EAL 2 augmented with ALC_FLR.3 |
| **Sponsor** | Fidelis Security Systems, Inc. |
| **Developer** | Fidelis Security Systems, Inc. |
| **Common Criteria Testing Lab (CCTL)** | Science Applications International Corporation<br>7125 Columbia Gateway Drive, Suite 300<br>Columbia, MD 21046 |
| **Evaluation Personnel** | Science Applications International Corporation:<br>Terrie Diaz, Quang Trinh |
| **Validation Body** | NIAP CCEVS: Paul Bicknell, Kenneth Eggers |

# 3 Organizational Security Policy

This section summarizes the security functions provided by Fidelis XPS that are evident at the various identified network interfaces. It is based on information provided in the Security Target.

## 3.1 Security audit

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

## 3.2 Cryptographic support

The TOE uses the MySQL's embedded Secure Hash Algorithm (SHA-1) function to hash and store user passwords. The TOE implements an RFC 1321-based free implementation of the RSA MD5 checksum library function to hash file contents for Exact Content analyzer fingerprint comparison.

## 3.3 User data protection

The TOE enforces an access control list (ACL) based access control mechanism to control users' access to Fidelis XPS objects and administrative interfaces.

## 3.4 Fidelis XPS Component Requirements (EXP)

The TOE uses a set of rules to inspect (e.g., sense via the Fidelis XPS Sensor) network traffic and collect extrusion data based on potentially inappropriate content detected using configured rules. The TOE contains a set of default rules and policies and allows an authorized administrator to customize these rules and policies. The TOE uses these rules and policies to analyze the collected data and identify data leakage events, to which the TOE provides the appropriate response. The TOE collects extrusion data and restricts review of this data to authorized administrators. 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.

## 3.5 Identification and authentication

The CommandPost requires that all administrative users be identified and authenticated before access is allowed to perform security-relevant management functions. The CommandPost maintains the administrator accounts, which 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 compliance and rejects passwords that do not comply.

## 3.6 Security management

The CommandPost is accessed via its web-based Graphical User Interface (GUI), which 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) for each system function.

CommandPost is delivered with three 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 the applicable group may view the associated 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 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.

## 3.7 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 to ensure that all data is protected from both disclosure and modification. The Sensors monitor network traffic and send the information to the registered CommandPost. Each TOE appliance provides protection from outside attacks by being a self-contained device that only provides TOE functionality.

To provide non-bypassability and domain separation, all users must be properly identified and authenticated and then only authorized administrators may access TOE security functions. Additionally, the CommandPost hardware provides a reliable time stamp for

security audit generation and collected system event data. The evaluation configuration of the TOE does not support any additional software to be installed on the appliance devices.

### 3.8 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.

# 4 Assumptions and Threats

The statement of TOE security environment describes the security aspects of the environment in which it is intended that the TOE will be used and the manner in which it is expected to be deployed. The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the intended method for the product, defines the threats that the product is designed to counter and the organizational security policies which the product is designed to comply.

Following are the assumptions identified in the Security Target:

- It is assumed the TOE is appropriately scalable to the IT System the TOE monitors and has access to all network data for collection and analysis.
- It is assumed the processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- It is assumed those responsible to manage the TOE are competent individuals, that only authorized users can gain access to the TOE, and that they are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

Following are the threats levied against the TOE and its environment as identified in the Security Target. The threats that are identified are mitigated by the TOE and its environment. All of the threats identified in the ST are addressed.

- An authorized administrator may attempt to use an unapproved channel or non-standard ports to circumvent the security functionality of the TOE.
- An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
- An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
- Unauthorized attempts to access TOE data or security functions may go undetected.
- 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.

- An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
- An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
- An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
- An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
- Inappropriate network traffic may go undetected and not be subject to analysis.
- Potential audit and system data may not be recorded due to storage loss or overflow.
- A reliable time stamp may not be available for audit purposes

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

# 5 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made; and meets them with only a certain level of assurance (EAL 2 in this case).
- As with all EAL 2 evaluations, this evaluation did not specifically search for vulnerabilities that were not "obvious" (as this term is defined in the CC and CEM); or seriously attempt to find counters to them; nor find vulnerabilities related to objectives not claimed in the ST.
- Encryption of communications using either SSL or SSH between the CommandPost and Fidelis XPS Sensors is required. The evaluation team verified

  a. That the TOE invoked the FIPS 140-2 certified OpenSSL implementation correctly by examining the protocol exchange and

  b. That the resulting data exchange was effectively obscured.

  This indicates that, to a reasonable level of assurance, the information was encrypted as specified. This assurance is based on proper invocation of FIPS 140-2 certified cryptographic functionality and analysis of the resulting data stream.
- All of the claimed security functions are provided by the CommandPost, Fidelis XPS Direct, Fidelis XPS Proxy, and Fidelis XPS Mail sensors running software version 5.0.3.

The Fidelis XPS 5.0.3 suite of products also include the following 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)

These sensor products are not included in the evaluated configuration. Each of these sensors is purchased and installed separately and subject to a different license. The sensors that have been excluded are not required to meet the claimed the SFRs.

# 6 Architectural Information[1]

This section provides a high level description of the TOE and its components as described in the Security Target.

The evaluated configuration of the TOE includes a minimum of one CommandPost (either CommandPost or CommandPost Plus) and one or more Fidelis XPS Sensor (i.e., Fidelis XPS Direct, Fidelis XPS Proxy and/or Fidelis XPS Mail).

CommandPost is accessed via a web browser to enable authorized administrators to configure policies, review audit and alert logs, and to analyze results.

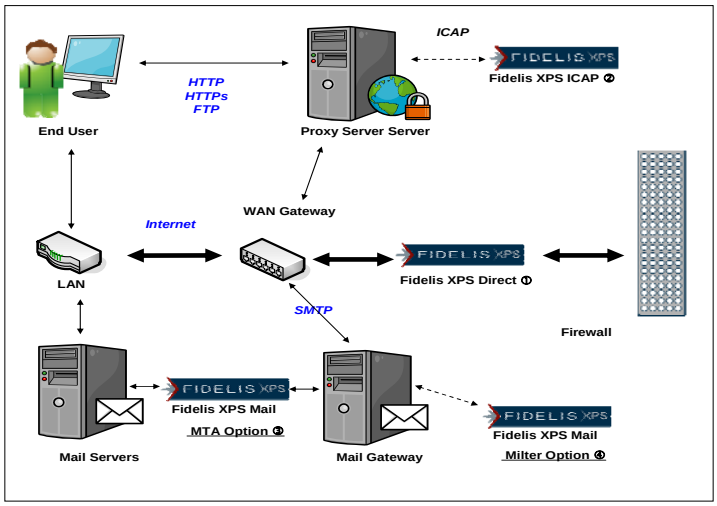
The evaluated configuration of the TOE includes five modes of operation, each providing full prevention capabilities for a specific sensor appliance. The mode of operation is determined and configured by an authorized administrator during initial setup of the TOE on the monitored network. Supported modes of operation include:

- **Fidelis XPS Direct sensor out-of-band**: The Fidelis XPS Direct sensor is connected via a network tap or router SPAN port and implements content-based prevention without requiring an inline network device. Network traffic is passed to the sensor through the network tap or router SPAN port. Prevention is achieved by injecting TCP reset packets that instruct the sender and recipient to reset the network connection.
- **Fidelis XPS Direct sensor inline**: The Fidelis XPS Direct sensor sits in the network path with all network traffic flowing directly through it. Prevention is achieved by dropping any packet or transfer that violates configured polices and sending TCP reset packets.
- **Fidelis XPS Proxy sensor**: The Fidelis XPS Proxy sensor is connected to a third party proxy appliance to provide content inspection. All actions are carried out by

[1] Extracted from SAIC Final ETR Part 1 Version 1.5, 10 September 2008

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, users see an Error 403 on their browser. On redirect, users see a web page informing them that their action was blocked by policy. The redirect page can be customized by an authorized administrator.

- **Fidelis XPS Mail sensor inline**: When connected inline, the Fidelis XPS Mail sensor acts as an 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 (milter mode)**: 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.




The physical boundary of the TOE is the Fidelis XPS appliance. 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.

The TOE requires a U. S. Government Department of Defense (DOD) approved External Certificate Authority (ECA) in the IT environment for Public Key Infrastructure (PKI) to import certificates into the TOE. (The ECAs currently DOD-approved for U. S. Government environments are operated by Operational Research Consultants, Inc. (ORC);

VeriSign, Inc. and IdenTrust, Inc.) In addition, 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

Network taps are required by Fidelis XPS Direct sensor for lossless network monitoring because taps replicate all network traffic with no data loss or performance degradation. Network taps guarantee complete traffic replication. 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.

If desired, a proxy server in which the Fidelis XPS Proxy appliance is connected may be included to analyze proxied traffic.

If desired, a Mail Transfer Agent (MTA) in which the Fidelis XPS Mail appliance is connected may be included to analyze e-mail. 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.

# 7 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor).

Design documentation

| Document | Version | Date |
|---|---|---|
| Fidelis XPS System Security Functional Specification | Revision 1.3 | 9/9/2008 |
| Fidelis XPS System Security Design Specification | Revision 1.5 | 10/29/2008 |
| Fidelis XPS Correspondence Representation | Revision 1.0 | 4/10/2008 |

Guidance documentation

| Document | Version | Date |
|---|---|---|
| Fidelis XPS User Guide | Version 5.0.3 | July 2008 |
| Fidelis XPS Enterprise Setup and Configuration Guide | Version 5.0.3 | October 2008 |
| Fidelis XPS Guide To Creating Policies | Version 5.0.3 | July 2008 |
| Fidelis XPS Guide To Prebuilt Policies | Version 5.0.3 | July 2008 |

Configuration Management documentation

| Document | Version | Date |
|---|---|---|

| Document | Version | Date |
|---|---|---|
| Fidelis Security Systems Configuration Management Plan | Version 1.0 | 5/16/2008 |
| Fidelis Security Systems Configuration Items List | Version 1.0 | 9/9/2008 |

Delivery and Operation documentation

| Document | Version | Date |
|---|---|---|
| Fidelis Security Systems Product Delivery Process | Version 1.0 | 07/31/2007 |
| Fidelis XPS Enterprise Setup and Configuration Guide | Version 5.0.3 | July 2008 |

Life Cycle Support documentation

| Document | Version | Date |
|---|---|---|
| Fidelis Security Systems Defect Tracking and Resolution Procedures | Revision 1.0 | January 11 2008 |

Test documentation

| Document | Version | Date |
|---|---|---|
| Fidelis XPS Security Test Plan | Revision 1.2 | 9/8/2008 |
| Fidelis XPS Security System Test Results | | 5/5/2008 |

The actual test results have been submitted to the evaluation team in various log files.

Vulnerability Assessment documentation

| Document | Version | Date |
|---|---|---|
| Fidelis XPS Security, Vulnerability Analysis | Version 1.0 | 5/12/2008 |
| Fidelis XPS Security, Strength of Fidelis XPS Security Evaluation | Revision 1.0 | 5/5/2008 |

Security Target

| Document | Version | Date |
|---|---|---|
| Fidelis XPS 5.0.3 Security Target | Version 1.0 | 29 October 2008 |

# 8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

## 8.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function tested. The scope of the developer tests included all the TSFI. The testing covered the security functional requirements in the ST including: Security audit, Cryptographic support, User data protection, Functional XPS Component Requirements (EXP), Identification and authentication, Security management, Protection of the TSF, and Session Locking (EXP). All security functions were tested and the TOE behaved as expected. The evaluation team determined that the developer's actual test results matched the vendor's expected results.

## 8.2 Evaluation Team Independent Testing

The evaluation team re-ran the entire automated test suite and a subset of the of the vendor's manual tests. In addition to re-running the vendor's tests, the evaluation team developed a set of independent team tests to address areas of the ST that did not seem completely addressed by the vendor's test suite, or areas where the ST did not seem completely clear. All were run as manual tests.

The vendor provided a CommandPost; appliances to support the Fidelis XPS Direct, Fidelis XPS Proxy, and Fidelis XPS Mail sensors; and the necessary computers, hubs, and cabling for the test environment.

The following hardware is necessary to create the test configuration:

- Four Fidelis XPS appliances with the operating system (one CommandPost, one Fidelis XPS Direct, one Fidelis XPS Proxy, and one Fidelis XPS Mail),
- TOE software (version 5.0.3),
- External serial console – for installation, generation, and startup of TOE and for specified administrative maintenance activities,
- Computer/Workstation on which the authorized administrator's Web browser runs to present the CommandPost GUI, Mail Server, Proxy server, Hub, Ethernet router, CAT 5e cabling, and
- any other items required to create a functional Ethernet network environment.

The following software is required to be installed on the machines used for the test: Fidelis XPS version 5.0.3 (TOE software), appropriate PKI certificates, and WinSCP on the client workstation.

In addition to developer testing, the evaluation team conducted its own suite of tests, which were developed independently of the sponsor. These also completed successfully.

## 8.3 Vulnerability Testing

The evaluators developed vulnerability tests to address the Protection of the TSF security function, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE.

# 9 Evaluated Configuration

The evaluated configuration requires one CommandPost and a separate sensor appliance (i.e., Fidelis XPS Direct, Fidelis XPS Proxy, and/or Fidelis XPS Mail) for each mode of operation. The Fidelis XPS Sensors collect and conduct 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 is designed to operate continuously, observing network traffic as it is perceived on the attached networks.

The CommandPost is accessed via its web-based Graphical User Interface (GUI) that provides the interface to manage: Fidelis XPS Sensors (i.e., all functions related to system data collection, analysis, and reaction), audit functions, users, and alert reports. The TOE is shipped with pre-built policies, rules, content, channels, and locations. The TOE also provides the authorized administrator with the ability to define new policies. All users of the TOE are considered authorized Administrators.

The TOE supports a third-party Certificate Authority (CA) to provide Public Key Infrastructure (PKI) functionality 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 IT environment.

For specific configuration settings required in the evaluated configuration see Fidelis XPS Enterprise Setup and Configuration Guide and the Fidelis XPS User Guide.

# 10 Results of the Evaluation

The evaluation was conducted based upon the Common Criteria (CC), Version 2.3, dated August 2005; the Common Evaluation Methodology (CEM), Version 2.3, dated August 2005; and all applicable International Interpretations in effect on March 2007. The evaluation confirmed that the Fidelis XPS 5.0.3 product is compliant with the Common Criteria Version 2.3, functional requirements (Part 2), Part 2 extended, and assurance requirements (Part 3) for EAL2 Augmented with ALC_FLR.3. The details of the evaluation are recorded in the CCTL's evaluation technical report; Evaluation Technical Report for Fidelis XPS 5.0.3, Part 1 (Non-Proprietary) and Part 2 (Proprietary). The product was evaluated and tested against the claims presented in the Fidelis XPS 5.0.3 Security Target, Version 1.0, 29 October 2008.

The Validators followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The Validators observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The Validators therefore conclude that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL.

### 10.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of threats, policies, and assumptions, a statement of security requirements claimed to be met by the Fidelis XPS 5.0.3 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

### 10.2 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 2 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. In addition, the evaluation team ensured changes to the implementation representation are controlled and that TOE associated configuration item modifications are properly controlled.

### 10.3 Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed identification of the TOE and allows for detection of unauthorized modifications of the TOE. The evaluation team followed the Fidelis XPS Enterprise Setup and Configuration Guide, the Fidelis XPS User Guide, and the Fidelis XPS Security Test Plan to verify the installation of the TOE. Fidelis consultants configure the TOE at the customer site to ensure the TOE is installed and configured in a secure manner that results in the TOE being in the evaluated configuration.

### 10.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and high-level design documents. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

### 10.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 2 AGD CEM work unit. The evaluation team ensured the adequacy of the guidance documents in describing how to securely administer the TOE. The Fidelis XPS Enterprise Setup and Configuration Guide and the Fidelis XPS User Guide were assessed during the design and testing phases of the evaluation to ensure it was complete.

### 10.6 Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation Team applied the ALC_FLR.3 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that systematic procedures exist for managing flaws discovered in the TOE.

### 10.7 Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation Team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team exercised the complete Vendor test suite and devised an independent set of team tests and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

### 10.8 Vulnerability Assessment Activity (AVA)

The Evaluation Team applied each EAL 2 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer vulnerability analysis, the evaluation team's misuse analysis, the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

### 10.9 Summary of Evaluation Results

The Evaluation Team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation Team's performance of the entire set of the vendor's test suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

## 11 Validator Comments/Recommendations

The validation team observed that the evaluation was performed in accordance with the CC, the CEM, and CCEVS practices. The Validation team agrees that the CCTL presented appropriate rationales to support the Results presented in Section 5 of the ETR and the Conclusions presented in Section 6 of the ETR.

The validation team, therefore, recommends that the evaluation and Pass result for the identified TOE be accepted.

## 12 Security Target

The Security Target is identified as Fidelis XPS 5.0.3, Version 1.0, dated 29 October 2008. The document identifies the security functional requirements (SFRs) necessary to

implement the TOE security policies. These include TOE SFRs and IT Environment SFRs. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 2 augmented with ALC_FLR.3.

# 13 Glossary

The following definitions are used throughout this document:

| | |
|---|---|
| CA | Certificate Authority |
| CC | Common Criteria |
| CCEVS | Common Criteria Evaluation and Validation Scheme |
| CLI | Command Line Interface |
| CM | Configuration Management |
| DO | Delivery Operation |
| EAL | Evaluation Assurance Level |
| ECA | External CA |
| GUI | Graphical User Interface |
| HTTP | HyperText Transfer Protocol |
| HTTP(S) | HyperText Transfer Protocol Secure |
| ICAP | Internet Content Adaptation Protocol |
| IDS | Intrusion Detection System |
| I/O | Input/Output |
| IPS | Intrusion Prevention System |
| NIAP | National Information Assurance Partnership |
| PKI | Public Key Infrastructure |
| PP | Protection Profile |
| SF | Security Functions |
| SFR | Security Functional Requirement(s) |
| SSL | Secure Sockets Layer |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Functions |
| TSP | TOE Security Policy |
| TSC | TSF Scope of Control |
| XPS | Extrusion Prevention System |

# 14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 2.3, August 2005.

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

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

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.

[5] Fidelis XPS 5.0.3 FINAL Non-Proprietary ETR – Part 1.

[6] Fidelis XPS 5.0.3 FINAL Proprietary ETR – Part 2 and Supplemental Team Test Report.

[7] Fidelis XPS 5.0.3 Security Target, Version 1.0, 29 October 2008.

[8] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.