National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Fidelis Network™ v9.0.3

Report Number: CCEVS-VR-10884-2018
Dated: 27 August 2018
Version: 1.0

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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Marybeth Panock
Kenneth Stutterheim
The Aerospace Corporation

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Fidelis Network™ v9.0.3 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation of Fidelis Network™ v9.0.3 was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in August 2018. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, and assurance activities specified in *Evaluation Activities for Network Device cPP*, Version 2.0+Errata 20180314, March 2018. The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

Fidelis Network™ v9.0.3 is a network appliance solution for advanced threat detection. It detects inappropriate and malicious network data based on attributes of the network traffic, including content, source, destination, application, and aspects of the communication channel. It analyzes network activity and can issue alerts concerning events of significance.

Fidelis Network™ v9.0.3 is evaluated as a distributed network device TOE consistent with Use Case 3 and Figure 6 presented in *collaborative Protection Profile for Network Devices*, Version 2.0+Errata 20180314, 14 March 2018. The focus of this evaluation is on the TOE functionality supporting the claims in the relevant Protection Profile (PP). The evaluated security functionality includes protection of communications between TOE components and external IT entities, the identification and authentication of administrators, auditing of security-relevant events, and the capability to verify the source and integrity of updates to the TOE.

The Leidos evaluation team determined that the TOE is conformant to *collaborative Protection Profile for Network Devices*, Version 2.0+Errata 20180314, 14 March 2018. The TOE, when configured as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in Fidelis Network™ Security Target, Version 1.0, 24 August 2018. The information in this VR is largely derived from the associated proprietary test reports as summarized in the publicly available Assurance Activities Report (AAR) as produced by the Leidos evaluation team.

The validation team reviewed the evaluation outputs produced by the evaluation team, such as the AAR and associated test reports. The validation team found that the evaluation showed the TOE satisfies the security functional and assurance requirements stated in the ST. The evaluation also showed that the TOE is conformant to *collaborative Protection Profile for Network Devices*, Version 2.0+Errata 20180314, 14 March 2018, and that the assurance activities specified in the Supporting Document had been performed appropriately. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the proprietary Evaluation Technical Report are consistent with the evidence produced.

1.1 Interpretations

The following NIAP Technical Decisions were applied during the evaluation:

- TD0228: NIT Technical Decision for CA certificates - basicConstraints validation
- TD0256: NIT Technical Decision for Handling of TLS connections with and without mutual authentication
- TD0257: NIT Technical Decision for Updating FCS_DTLSC_EXT.x.2/FCS_TLSC_EXT.x.2 Tests 1-4
- TD0262: NIT Technical Decision for TLS server testing – Empty Certificate Authorities list
- TD0289: NIT Technical Decision for FCS_TLSC_EXT.x.1 Test 5e
- TD0290: NIT Technical Decision for physical interruption of trusted path/channel.
- TD0291: NIT Technical Decision for DH14 and FCS_CKM.1
- TD0322: NIT Technical Decision for TLS server testing - Empty Certificate Authorities list
- TD0324: NIT Technical Decision for Correction of section numbers in SD Table 1.

1.2 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

- Threat agents may attempt to gain Administrator access to the network device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
- Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
- Threat agents may attempt to target network devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
- Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
- Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated

using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

- Threat agents may attempt to access, change, and/or modify the security functionality of the network device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
- Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
- Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
- An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

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) use the Common Criteria and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT 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 Product Compliant List (PCL).

Table 1 provides information needed to completely identify the product and its evaluation.

Table 1: Evaluation Details

Evaluated Product:	Fidelis Network™ v9.0.3
Sponsor:	Fidelis Cybersecurity 4500 East West Highway, Suite 400 Bethesda, Maryland 20814
Developer:	Fidelis Cybersecurity 4500 East West Highway, Suite 400 Bethesda, Maryland 20814
CCTL:	Leidos 6841 Benjamin Franklin Drive Columbia, MD 21046
Kickoff Date:	February 28, 2018
Completion Date:	August 2018
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 4, September 2012.
Evaluation Class:	None
PP:	collaborative Protection Profile for Network Devices, Version 2.0+Errata 20180314, 14 March 2018
Evaluation Personnel:	Leidos: Anthony J. Apted, Pascal Patin, Dawn Campbell, Cody Cummins, Heather Hazelhoff, Allen Sant, Kevin Steiner
Validation Body:	National Information Assurance Partnership CCEVS

3 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the Fidelis Network™ Security Target and final Evaluation Technical Report (ETR).

3.1 Security Audit

The TOE generates audit records of security relevant events. Generated audit records include the date and time of the event, the event type, the subject identity and the outcome of the event. For audit events resulting from the actions of identified users, the identity of the user is recorded in the generated audit record. The TOE can be configured to store audit records locally on the K2 appliance or to export the audit records to an external audit server such that the records can be accessed by an administrator.

3.2 Cryptographic Support

The TOE implements NIST-validated cryptographic algorithms that provide 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 TLS and HTTPS.

3.3 Communication

The TOE is deployed in a distributed configuration. Initial configuration for each of the appliances is performed by directly attaching a keyboard and monitor to the appliance to set network parameters and certificate files. After the initial configuration and connection of each appliance to the network, the administrator adds the appliance to the K2 management console to register it. After registration, the K2 communicates with the registered appliance at its configured IP address using TLS.

3.4 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. Administrators manage the TOE remotely using the K2 web-based GUI accessed via HTTPS or locally through the Command Line Interface using a directly connected console. 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.

3.5 Security Management

Administrators can manage the TOE remotely using the K2 web-based GUI accessed via HTTPS or locally using a directly connected console. The evaluation covered the following specific management functions:

- Configuring the TOE access banner
- Configuring cryptographic functionality
- Setting the date and time
- Configuring the reference identifier for an external peer
- Verifying the integrity of a TOE update using the hash comparison capability prior to installing the update
- Updating the TOE
- Configuring authentication failure management
- Configuring session inactivity time-out before session termination
- Re-enabling a disabled administrator account.

3.6 Protection of the TSF

In the distributed deployment, the TOE protects communication between its components using mutually authenticated TLS.

The TOE protects 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 ensures that reliable time information is available (e.g., for log accountability).

The TOE includes a suite of power-on self-tests that confirm the integrity of the TOE software and demonstrate correct operation of the TOE at start up.

The TOE verifies the integrity of updates to the TOE's software and firmware prior to installation by calculating a cryptographic hash of the update and allowing the administrator to confirm its correctness against a hash value published by Fidelis.

3.7 TOE Access

The TOE can be configured to display an administrator-defined advisory banner before establishing an administrative user session and to terminate both local and remote interactive sessions after a configurable period of inactivity. It also provides users the capability to terminate their own interactive sessions.

3.8 Trusted Path/Channels

The TOE protects interactive communication with remote administrators using HTTPS.

The TOE uses TLS v1.2 to protect communications with the following external IT entities: audit server; authentication server; Fidelis Insight Server.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The Security Problem Definition, including the assumptions, can be found in the following document:

- *collaborative Protection Profile for Network Devices*, Version 2.0 +Errata, 14 March 2018

That information has not been reproduced here and the cPPNDv2 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the cPPNDv2 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

4.2 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, with a certain level of assurance (the assurance activities specified in *collaborative Protection Profile for Network Devices* and performed by the evaluation team).
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in *Fidelis Network ™ Security Target*, Version 1.0, 24 August 2018. Any additional security related functional capabilities of the product were not covered by this evaluation.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The TOE appliances consist of software and hardware and do not rely on the operational environment for any supporting security functionality.
- The TOE supports the use of external LDAP authentication servers in the evaluated configuration. Other authentication servers such as RADIUS or TACACS are excluded from the evaluated configuration.
- The TOE must be installed, configured and managed as described in the following guidance documents included in the evaluated configuration:
    a. Fidelis Network™ Common Criteria Configuration Guide, Version 9.0.3, revised August 2018
    b. Fidelis Network™ Enterprise Setup and Configuration Guide, Version 9.0.3, 2017
    c. Fidelis Network™ User Guide, Version 9.0.3, Revised 2017

5 Architectural Information

The Fidelis Network Target of Evaluation (TOE) is a combination of Fidelis Network components in a distributed deployment:

- Fidelis Network v9.0.3 K2 management console component
- Fidelis Network v9.0.3 Collector component
- Fidelis Network v9.0.3 Sensor component
- Fidelis Network v9.0.3 Sandbox component.

The K2, Collector and Sensor components are available in various form factors, as outlined in the following table:

Component	Appliance Models	Virtual Models
K2	K2 appliance	K2 VM
Collector	Collector SA2 Collector XA2 Collector XA4 Collector Controller 2 Collector Controller 10G	Collector SA VM
Sensor	Direct 50 Direct 100 Direct 250 Direct 500 Direct 1000 Direct 2500 Direct 5000 Direct 10G	Direct VM
	Internal 1000 Internal 2500 Internal 5000 Internal 10G	Internal VM
	Web	Web VM
	Mail 250 Mail 500 Mail 1000	Mail VM 250 Mail VM 500 Mail VM 1000

The Sandbox component is available in a single appliance form factor.

Two further form factors combine three virtual models in a single hardware appliance:

- Fidelis XPS Scout+ AP v9.0.3 (includes a K2 VM, a Direct 1000 VM, and a Collector SA VM in one box)
- Fidelis XPS Scout+ IR v9.0.3 (includes a K2 VM, a Direct 1000 VM, and a Collector SA VM in one box).

Virtual models were tested in an environment comprising an Intel E7-4890 v2 @ 2.80G CPU, DDR3 memory and 7200 RPM 2.5" SATA HDD in the host hardware system. More generally, the virtual models 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.

A Fidelis Network system can be deployed entirely as hardware appliances, VM appliances, or a mixture, as long as there is one K2 and at least one Collector and one Sensor.

The Fidelis Network K2 is the management system for the Fidelis solution. It provides the capability to add, configure, and manage Sensors, Collectors, Sandboxes and additional K2 components.

A sample deployment scenario for the TOE is depicted as follows (TOE components are identified in the green boxes).

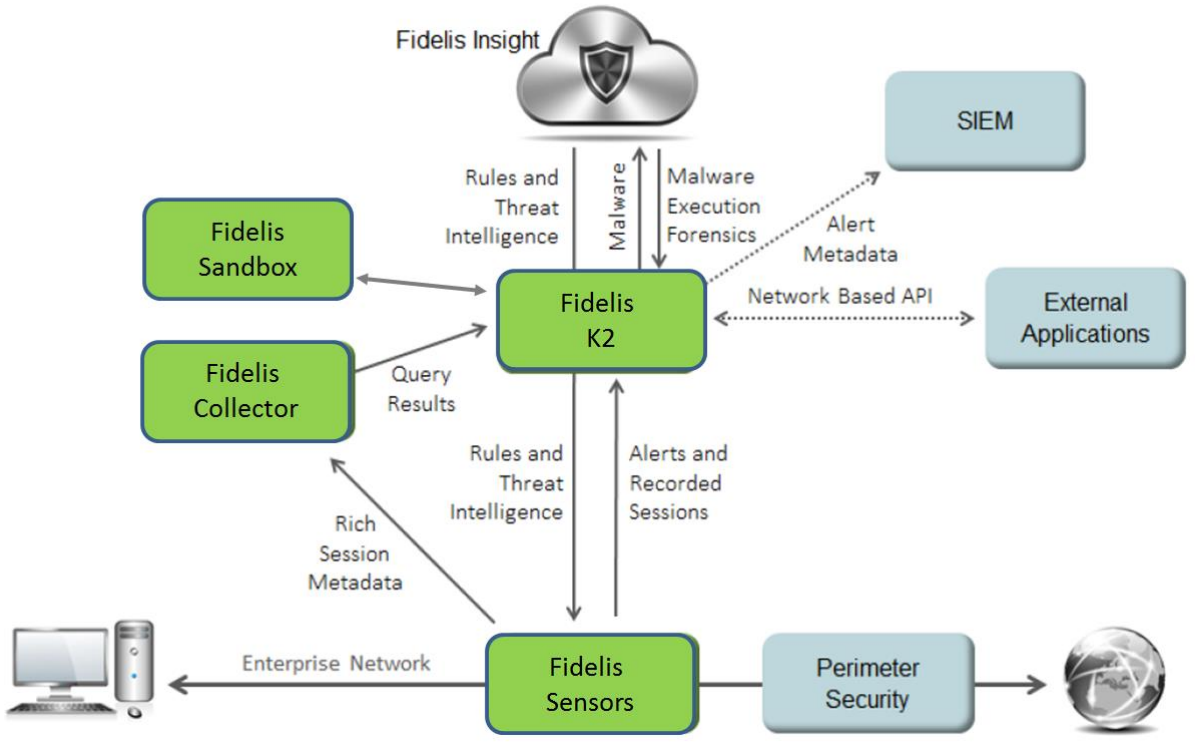

Figure 1: Example Deployment

Initial configuration for each of the appliances is performed by directly attaching a keyboard and monitor to the appliance. The command line interface is used to set network parameters: the host name, IP address, IP mask, gateway, and primary (and secondary, if applicable) DNS, and the clock. Certificate files, CA-certificate files, CRL files are required be installed on each of the appliances before proceeding with

registration to the K2. For administrators to remotely access the K2 GUI requires a client computer with a web browser and Adobe Flash Player.

After initial configuration and the connection of the appliances to the network, the administrator adds those components (Sensors, Collectors, Sandboxes) to the K2 to register them.

The virtual appliances are delivered as an installation disk (or ISO image). The virtual systems were tested by the evaluation team with VMWare ESXi / vSphere 6.5 installed.

Each virtual model in its evaluated configuration is installed on a hardware platform that includes VMware ESXi with vSphere 5.1, 5.5, 6.0 or 6.5 and an Intel Core or Xeon processor based on the Ivy Bridge or Haswell microarchitecture, which implement Intel Secure Key. The virtual module must be the only guest running in the virtual environment.

The following components are supported in the operational environment of the TOE :

- External authentication methods require the use of LDAP servers
- External audit storage requires the use of syslog servers
- An NTP Server is required for proper clock synchronization for use in creating reliable timestamps
- Fidelis Insight Server, which provides software and policy updates for the TOE.

The VM appliances have the following resource requirements:

Device	Number of vCPUs	Memory	Disk	Operating System / Software
K2 VM	8	24 GB	100 GB	CentOS 6.8 with Linux kernel 2.6.32-642.13.1.el6.x86_64 - Apache httpd 2.4.25 - Apache tomcat 8.5.11 - Syslog-ng 3.7.3 - Mysql 5.6.36 - OpenSSL 1.0.1e-fips
Direct VM	14	24 GB	40 GB	CentOS 6.8 with Linux kernel 2.6.32-642.13.1.el6.x86_64 - OpenSSL 1.0.1e-fips
Internal VM	14	24 GB	40 GB	CentOS 6.8 with Linux kernel 2.6.32-642.13.1.el6.x86_64 - OpenSSL 1.0.1e-fips
Web VM	4	8 GB	40 GB	CentOS 6.8 with Linux kernel 2.6.32-642.13.1.el6.x86_64

Device	Number of vCPUs	Memory	Disk	Operating System / Software
				- OpenSSL 1.0.1e-fips
Mail 250 VM	4	8 GB	100 GB	CentOS 6.8 with Linux kernel 2.6.32-642.13.1.el6.x86_64 - OpenSSL 1.0.1e-fips
Mail 500 VM	6	12 GB	120 GB	CentOS 6.8 with Linux kernel 2.6.32-642.13.1.el6.x86_64 - OpenSSL 1.0.1e-fips
Mail 1000 VM	8	14 GB	150 GB	CentOS 6.8 with Linux kernel 2.6.32-642.13.1.el6.x86_64 - OpenSSL 1.0.1e-fips
Collector SA VM	8	32 GB	200 GB	CentOS 6.8 with Linux kernel 2.6.32-642.13.1.el6.x86_64 - OpenSSL 1.0.1e-fips

Initial configuration of the TOE appliances requires local access. A keyboard and monitor are connected to the appliances for initial network setup via the command line interface.

5.1 Unevaluated Functionality

The following device functionality was not tested as part of the evaluation.

- The Fidelis Network Collector software captures details about network transactions and stores them into metadata. The metadata includes all attributes of the analyzed network traffic, but excludes any recording of the data.
- The Fidelis Network sensor software is a series of layers that receive packets from the attached networks, perform session reassembly, and decode the payload. Authorized administrators can configure policies that delineate exactly what the Fidelis Network will capture, analyze and monitor. The Fidelis Network Direct, Internal, and Mail sensors also include a Malware Detection Engine (MDE) that can examine files to determine malicious intent.
- The Fidelis Network 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.

- The Fidelis Network 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.
- The Fidelis Network 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. 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.
- The Fidelis Sandbox appliance provides a virtual environment that executes files to analyze their behavior. File submissions are based on the Malware Detection Engine and custom rules that use the sandbox action.
- The TOE's (unevaluated) monitoring capability performs differently depending on whether sensors are connected by Network Taps or SPAN Ports.
    - **Network Taps—**required for lossless network monitoring by Fidelis Direct (including Scout) and internal sensors in an out-of-band deployment.
    - **SPAN Ports—**connecting the Fidelis Direct (including Scout) or internal sensors to the SPAN ports on the router or switch can be done, 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.

6 Documentation

Fidelis provides a set of documentation for the end users of the TOE, providing guidance on the installation, configuration and use of the TOE. The following documents were specifically examined in the context of the evaluation:

- Fidelis Network™ Common Criteria Configuration Guide, Version 9.0.3, Revised August 2018
- Fidelis Network™ Enterprise Setup and Configuration Guide, Version 9.0.3, 2017
- Fidelis Network™ User Guide, Version 9.0.3, Revised 2017

To use the product in the evaluated configuration, the product must be configured as specified in those guides. Any additional customer documentation provided with the product, or that which may be available online was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device in its evaluated configuration. Consumers are encouraged to download the CC configuration guides directly from the NIAP website to ensure the device is configured using the evaluated guidance.

7 IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the proprietary *Fidelis Network v9.0.3 Test Report and Procedures*, Version 1.1, 24 August 2018, as characterized in the publicly available *Assurance Activities Report for Fidelis Network*, Version 1.0, 21 August 2018.

7.1 Developer Testing

The assurance activities in *Evaluation Activities for Network Device cPP* do not specify any requirement for developer testing of the TOE.

7.2 Evaluation Team Independent Testing

The evaluation team devised a test plan based on the Test Assurance Activities specified in *Evaluation Activities for Network Device cPP*. The test plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the test plan and documented the results in the team test report identified above.

Testing of the TOE primarily was performed from December 2017 through August 2018 at the Leidos CCTL facility in Columbia, Maryland. For the purposes of that testing, the configuration depicted in Figure 1 was used for testing the TOE hardware appliances.

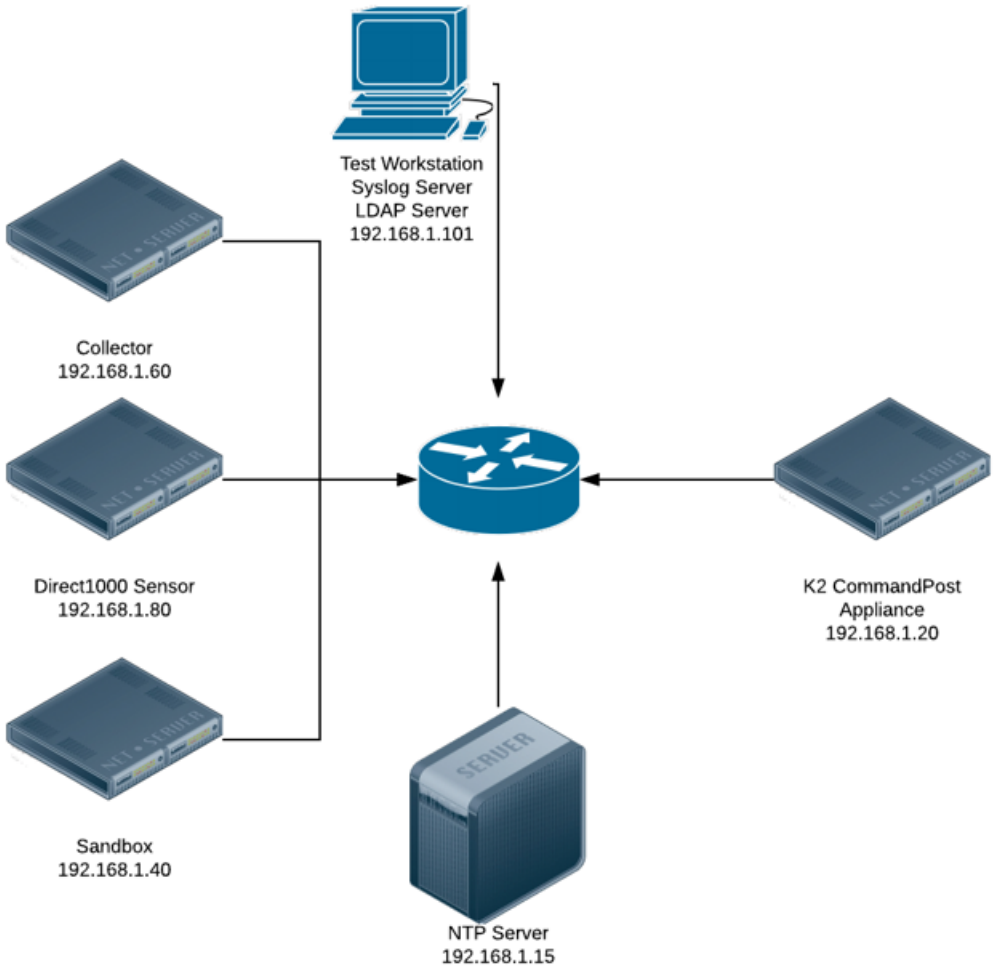

Figure 2: Test Configuration

In addition, the TOE virtual appliances were installed on a Dell Power Edge R920 server with an Intel Ivy Bridge processor with VMWare ESXi/vSphere 6.5 installed. This server was connected to the test network depicted in the above figure.

The following hardware and software components were included in the evaluated configuration during testing:

- Hardware
  - Fidelis K2 appliance
  - Fidelis Collector SA appliance
  - Fidelis Direct 1000 Sensor appliance
  - Fidelis Sandbox appliance
- Virtual Machines
  - Fidelis K2 VM
  - Fidelis Direct 1000 VM
  - Fidelis Collector SA VM
- Software
  - Fidelis Network ™ v9.0.3.

The following components are not part of the TOE but were included in the testing environment:

- Kali Linux 2018.1 rolling release, based on Linux kernel 4.14
- NIAP provided TLS test server tool, updated as of April 1, 2018
- Leidos TLS test client tool, updated as of June 1, 2018
- OpenSSL 1.1.0
- XCA Certificate Authority 1.4.1
- Syslog-ng v3.3.5 running on Debian 7
- OpenLDAP v2.4.31 running on Debian 7
- NTP daemon running on Debian 7
- Google Chrome 67.0.339.6.87 and Microsoft Edge 42.17139.1.0 browsers to remotely access K2 GUI
- Wireshark 2.4.4 to collect and analyze network packets.

The vendor provided the TOE platforms as described above.

The evaluation team followed the installation and configuration procedures documented in the product guidance to install the TOE in the test environment.

Subsequently, the evaluators exercised all the test cases. The tests were selected to ensure that each of the test assertions specified in *Evaluation Activities for Network Device cPP* were covered. All tests passed. A summary of the testing performed by the evaluation team is provided in *Assurance Activities Report for Fidelis Network*.

7.3 Test Equivalence Rationale

Each appliance model includes one of the following Intel Xeon Ivy Bridge or Haswell processors with Intel Secure Key:

- E5-2697 v2 (Ivy Bridge)

- E5-2667 v3 (Haswell)
- E5-2697 v3 (Haswell)
- E5-2660 v3 (Haswell)
- E5-4669 v3 (Haswell)
- E5-2687W v3 (Haswell).

For the purposes of testing, each of these processors is deemed equivalent based on the following:

- Within the Ivy Bridge microarchitecture, all processor models (Celeron, Pentium, Core, Xeon) implement the same instruction set. Differences are all associated with performance attributes, based on number of cores, L3 cache size, CPU clock rate, graphics clock rate, and Thermal Design Power (a measure of the heat generated by the CPU).
- Within the Haswell microarchitecture, all processor models (Celeron, Pentium, Core, Xeon) implement the same instruction set. Differences are all associated with performance attributes, based on number of cores, L3 cache size, CPU clock rate, graphics clock rate, and Thermal Design Power (a measure of the heat generated by the CPU).
- The Haswell microarchitecture implements a superset of the Ivy Bridge instruction set. The new instructions are associated with extensions to support vector processing, which in turn improves performance in applications such as floating-point calculations and graphics processing. Haswell is backward compatible with Ivy Bridge, so software that executes on Ivy Bridge will also work on Haswell.

The physical appliance models tested comprised the K2, Fidelis Collector SA2, Fidelis Direct 1000 Sensor, and Fidelis Sandbox.

All Collector appliances are based on the same processor (Intel Xeon E5-2687Wv3) and run the same binary code. The only differences are in terms of storage and physical network ports. In addition, the Collector Controller is a specific physical arrangement of Collector devices with a controller, which does not implement any security functionality. Testing of the Collector SA2 covers all of the Collector appliance models in the TOE.

All Sensor appliances are based on Intel Xeon E5 processors, as follows:

- Intel Xeon E5-4669v3— Direct 10G, Internal 10G
- Intel Xeon E5-2697 v3—Direct 5000, Direct 2500, Internal 5000, Internal 2500
- Intel Xeon E5-2660 v3—Direct 1000, Direct 500, Direct 250, Direct 100, Direct 50, Internal 1000, Mail 1000, Mail 500, Mail 250, Web.

As explained above, each of these processors is deemed equivalent for the purposes of testing.

Each different type of Sensor (i.e., Direct, Internal, Mail, Web) has the same software package loaded and installed on it. The different capabilities of the different Sensors are determined by licensing and configuration. In particular, each Sensor includes the same release of CentOS (CentOS 6.8 with Linux kernel 2.6.32-642.13.1.el6.x86_64) and OpenSSL (1.0.1e-fips) and provides a consistent local management interface. While the different kinds of Sensor are used for monitoring different types of network traffic, each implements the exact same security functionality as called out by the cPP.

The virtual appliance models tested comprised the K2 VM, Collector SA VM, and Direct VM Sensor. The Direct VM Sensor is functionally equivalent to the other virtual Sensor appliances (Internal VM, Web VM, Mail VM 250, Mail VM 500, Mail VM 1000) for the same reasons the physical Direct 1000 Sensor is functionally equivalent to the other physical Sensor appliances, as detailed above.

The Fidelis XPS Scout+ AP v9.0.3 and Fidelis XPS Scout+ IR v9.0.3 each comprise three Fidelis VMs (K2 VM, Direct 1000 VM, and Collector SA VM) running on a single hardware platform. As such, testing by the evaluation team of these VMs was equivalent to testing Scout+ AP v9.0.3 and Scout+ IR v9.0.3.

7.4 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product. The open source search did not identify any obvious vulnerabilities applicable to the TOE in its evaluated configuration.

A search of public vulnerability databases was conducted on 7 August 2018, using the following search terms:

- "fidelis"
- "openssl"
- "centos"
- "tcp"
- "tls".

The evaluation team searched the National Vulnerability Database (http://web.nvd.nist.gov/view/vuln/search) and the US-CERT Vulnerability Notes Database (https://www.kb.cert.org/vuls/html/search).The evaluation team determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

8 Evaluated Configuration

The TOE is Fidelis Network™ v9.0.3, which is installed and configured according to the product installation guidance identified in Section 6. The TOE appliances are configured to operate in FIPS mode.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in *Evaluation Activities for Network Device cPP*, Version 2.0+Errata 20180314, 14 March 2018, in conjunction with Version 3.1, Revision 4 of the CC and CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all the work units for that component had been assigned a Pass verdict.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the PP, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Final ETR, which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 2: Evaluated Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

10 Validator Comments/Recommendations

It is important to note that the product was evaluated as a network device per the NDcPP V2.0E. The consumer is strongly encouraged to understand the limitations on the network device security functionality as tested. The product(s) perform security related functionality, however that functionality was not evaluated, and no claims can be made regarding their effectiveness and correct operation. For example – considered out of scope are virus and email scanning, intrusion detection / prevention capabilities, Network Address Translation (NAT) as a security function, and virtualized network functions, (except in the case outlined above) as well as the metadata collection performed by the Collector device, the Sensors software and Malware Detection Engines, and other capabilities such as alerting, quarantine, etc.

Administrators must configure the device as specified in the Fidelis Network™ Common Criteria Configuration Guide, Version 9.0.3 revised August 2018.

It is recommended that administrators do not use the Linux command line account for normal system operation after initial setup is complete. Administrators should take note that NTP server services are across an unprotected channel. In the evaluated configuration, LDAP is the only allowable remote authentication method, and neither RADIUS nor TACACS can be used. Administrators must disable automatic updates in order to verify software download hashes before installation.

To ensure adequate entropy for cryptographic operations, 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. The VM must be based on Virtual Hardware version 9 or greater to utilize the Secure Key.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is Fidelis Network v9.0.3 Security Target, Version 1.0, 24 August 2018.

13 Abbreviations and Acronyms

AAR	Assurance Activities Report
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol—a means of synchronizing clocks over a computer network
NVLAP	National Voluntary Laboratory Assessment Program
PCL	Product Compliant List
PP	Protection Profile
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
VR	Validation Report

14 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012. Part 1: Introduction and general model. CCMB-2012-09-001.

[2] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012. Part 2: Security functional components. CCMB-2012-09-002.

[3] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012. Part 3: Security assurance components. CCMB-2012-09-003.

[4] Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012. Evaluation methodology. CCMB-2012-09-004.

[5] collaborative Protection Profile for Network Devices, Version 2.0 + Errata 14-March-2018.

[6] Fidelis Network v9.0.3 Security Target, Version 1.0, 24 August 2018.

[7] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[8] Evaluation Technical Report for Fidelis Network™, Parts 1 and 2 Version 1.0, 24 August 2018. (Proprietary Documents)

[9] Assurance Activities Report for Fidelis Network™, Version 1.0, 24 August 2018.

[10] Fidelis Network v9.0.3 Test Report and Procedures, Version 1.1, 21 August 2018. (Proprietary Document)

[11] Fidelis Network User Guide, Version 9.0.3, Revised 2017

[12] Fidelis Network Enterprise Setup and Configuration Guide, Version 9.0.3, Revised 2017.

[13] Fidelis Network Guide to Creating Policies, Version 9.0.3, Revised 2017

[14] Fidelis Network v9.0.3 Vulnerability Assessment, Version 1.0, 23 August 2018 (Proprietary Document)

[15] Fidelis Network Common Criteria Configuration Guide, Version 9.0.3, Rev. August 2018

[16] Fidelis Network Release Notes, Version 9.0.3, Revised November 2017