National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Fidelis Network and Fidelis Deception v9.3.3

Report Number: CCEVS-VR-11128-2021
Dated: 15 April 2021
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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Marybeth Panock
Swapna Katikaneni
Jerome Myers
Aerospace Corporation

Anne Gugel
Peter Kruus
Johns Hopkins University Applied Physics Laboratory

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™ and Fidelis Deception™ v9.3.3 (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™ and Fidelis Deception™ v9.3.3 was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in March 2021. 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 2.2e, December 2019. 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™ and Fidelis Deception™ v9.3.3 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 of significant events.

Fidelis Network™ and Fidelis Deception™ v9.3.3 is evaluated as a distributed network device TOE consistent with Use Case 3 and Figure 7 presented in *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020. The focus of this evaluation is on the TOE functionality supporting the claims in that Protection Profile (PP). The evaluated security functionality includes protection of communications between TOE components and with external IT entities, identification and authentication of administrators, auditing of security-relevant events, and ability 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 2.2e, 23 March 2020. The TOE, when configured as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in Fidelis Network™ and Fidelis Deception™ Security Target, Version 1.0, 26 March 2021. The information in this VR is largely derived from the Assurance Activities Report (AAR) and associated test reports produced by the Leidos evaluation team.

The validation team reviewed the evaluation outputs produced by the evaluation team, in particular the AAR and associated test reports. The validation team found that the evaluation showed that the TOE satisfies all of 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 2.2e, 23 March 2020, 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 Evaluation Technical Report are consistent with the evidence produced.

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™ and Fidelis Deception™ v9.3.3
Sponsor:	Fidelis Cybersecurity Inc. 4500 East West Highway, Suite 400 Bethesda, Maryland 20814
Developer:	Fidelis Cybersecurity Inc. 4500 East West Highway, Suite 400 Bethesda, Maryland 20814
CCTL:	Leidos 6841 Benjamin Franklin Drive Columbia, MD 21046
Kickoff Date:	October 26, 2020
Completion Date:	March 2021
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017.
Evaluation Class:	None
PP:	collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020
Evaluation Personnel:	Leidos: Pascal Patin, Dawn Campbell, 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 and Fidelis Deception 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 CommandPost appliance so they can be accessed by an administrator and can also be configured to export the audit records to an external audit server.

3.2 Cryptographic Support

The TOE implements NIST-approved 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 as a distributed configuration. Initial configuration for each of the appliances is performed by directly attaching a keyboard and monitor to the appliance. The System Setup is used to set network parameters and certificate files. After initial configuration and connection of each appliance to the network, the administrator adds each appliance to CommandPost to register them. After registration, CommandPost communicates to each newly registered appliance at its configured IP address using TLS/HTTPS.

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 CommandPost web-based GUI accessed via HTTPS or locally using the CLI by a directly connected USB keyboard and a monitor to the appliance VGA connector. The TOE supports the local (i.e., on device) definition of administrators with usernames and passwords on all of the TOE components. Additionally, the TOE can be configured to authenticate remote administrators to use the services of trusted LDAP servers in the operational environment.

3.5 Security Management

Administrators manage the TOE remotely using the CommandPost web-based GUI accessed via HTTPS or locally through the Command Line Interface using a keyboard and a monitor directly connected to the appliance's VGA connector.

The TOE also provides the ability to manage the TOE locally using the CLI by directly attaching a keyboard and monitor to the appliance. However, the TOE is designed to be managed using the CommandPost GUI 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 [CPP_ND_V2.2E] Security Administrator.

3.6 Protection of the TSF

In the distributed deployment, the TOE protects communication between its components using HTTPS/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 2.2e, 23 March 2020

That information has not been reproduced here and the cPPND 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 cPPND 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.

Only Rev J hardware for all hardware-based components, featuring 2nd Generation Intel® Xeon® Scalable Processors based on Cascade Lake microarchitecture are covered within the scope of the evaluation.

Virtual appliances within the scope of the evaluation include all VM-based components running on VMware ESXi 6.7 hypervisor on host hardware with Intel Xeon Gold 6248 processors based on the Cascade Lake microarchitecture, that implement Intel Secure Key.

The evaluation of security functionality of the product was limited to the functionality specified in *Fidelis Network and Fidelis Deception Security Target*, Version 1.0, 26 March 2021. Any additional security related functional capabilities of the product were not covered by this evaluation. In particular, there are functional capabilities of the product that are described in the "Product Overview" section (2.1) of the ST that are not included in the scope of the 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 product supports the use of external authentication servers, but only LDAP servers are supported in the evaluated configuration. The use of other authentication servers such as RADIUS or TACACS is excluded from the evaluated configuration.

Appendix B of the "Enterprise Setup and Configuration Guide", section "Appliance Configuration Console (ACC)", describes the Appliance Configuration Console (ACC), which is an optional feature

that disables shell access to the appliance operating system and replaces it with an interactive text-based user interface. The evaluation did not cover use of the ACC.

The TOE must be installed, configured and managed in accordance with the instructions and Common Criteria restrictions specified in the following guidance documents included in the evaluated configuration:

Fidelis Network® Fidelis Deception Common Criteria Configuration Guide, version 9.3.3, Revised 2021

Fidelis Network® Fidelis Deception® Enterprise Setup and Configuration Guide, Version 9.3.3

Fidelis Network® Fidelis Deception® User Guide, Version 9.3.3

The Common Criteria Configuration Guide documents all the necessary instructions to install, configure, monitor and maintain the TOE in the evaluated configuration. Any other sections of the user documentation which are not referenced in the Common Criteria Configuration Guide should be considered outside the scope.

5 Architectural Information

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

- Fidelis Network v9.3.3 CommandPost management console
- Fidelis Network Collector v9.3.3
- Fidelis Network Sensor component v9.3.3
- Fidelis Sandbox appliance v9.3.3
- Decoy Server appliance v9.3.3.

The CommandPost, Collector, Sensor, and Decoy Server components are identfied in the following table:

Component	Appliance Models (Revision J)	Virtual Models
CommandPost	CommandPost appliance	CommandPost 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 5000	Mail VM 250 Mail VM 500 Mail VM 1000 Mail VM 5000
Decoy Server	Decoy Server FDH-3000 FDH-1000	Decoy Server VM

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

Virtual models were tested in an environment comprising CentOS 7.7 on VMware ESXi 6.7 on Intel Xeon Gold 6248 (Cascade Lake) in the host hardware system.

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

A sample deployment scenario for the sensors is depicted as follows. TOE components are depicted in the green.

- Fidelis CommandPost appliance or Fidelis CommandPost VM
- Fidelis Sandbox
- Fidelis Collector – (one or more)
  - Collector SA2
  - Collector XA2
  - Collector XA4
  - Collector Controller 2
  - Collector SA VM
  - Collector Controller 10G
- Fidelis Sensor – (one or more)
  - Fidelis Direct 50, Fidelis Direct 100, Fidelis Direct 250, Fidelis Direct 500, Fidelis Direct 1000, Fidelis Direct 2500, Fidelis Direct 5000, Fidelis Direct 10G, or Fidelis Direct VM
  - Fidelis Internal 1000, Fidelis Internal 2500, Fidelis Internal 5000, Fidelis Internal 10G, or Fidelis Internal VM
  - Fidelis Web, Fidelis Web VM
  - Fidelis Mail 250, Fidelis Mail 500, Fidelis Mail 1000, Fidelis Mail 5000, Fidelis Mail VM 250, Mail VM 500, or Mail VM 1000
  - Decoy Server - FDH-3000, FDH-1000.

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

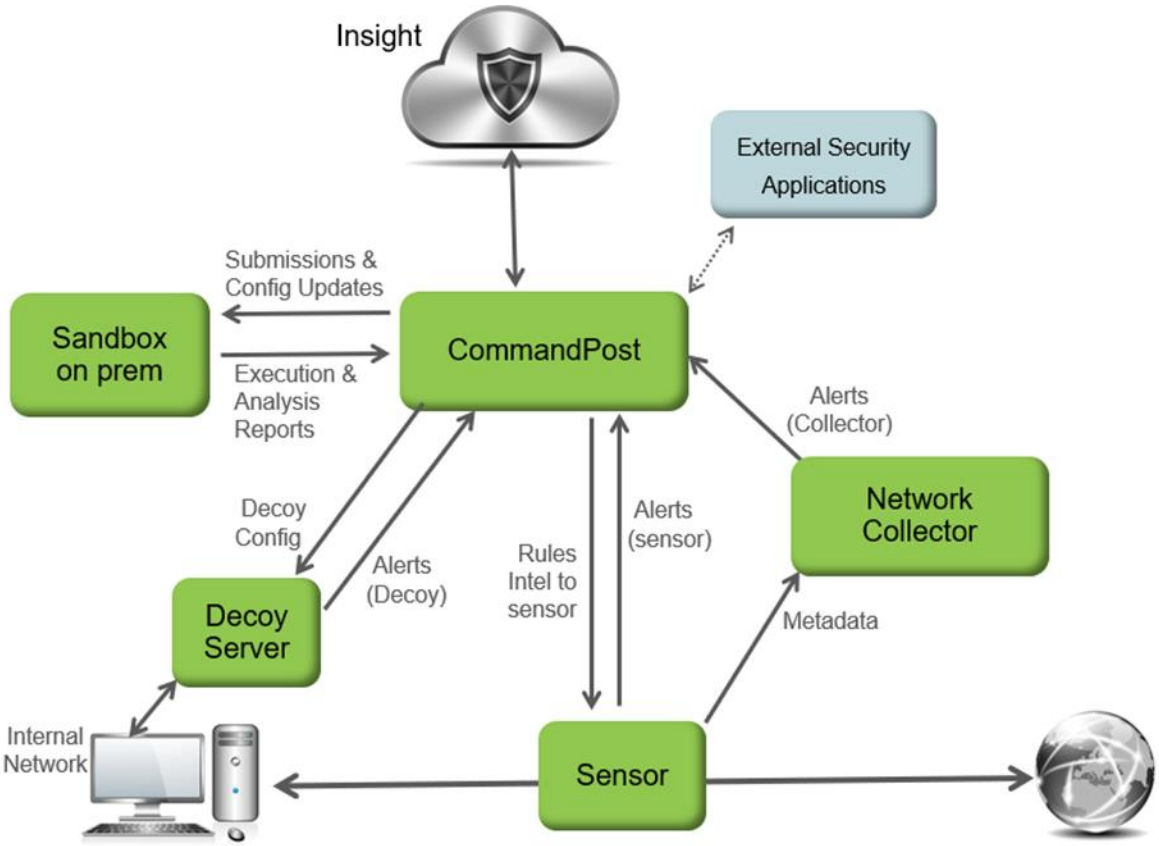

Figure 1: Example Deployment

Initial configuration for each of the appliances is performed by directly attaching a USB keyboard and VGA monitor to the appliance. The System Setup is used to set network parameters: the host name, IP address, IP mask, gateway, and primary (and secondary, if applicable) DNS, and the NTP server. Certificate files, CA-certificate files, CRL files are required to be installed on the Collector, Sensor, Sandbox, and Decoy Server components before proceeding with registration to the CommandPost.

After initial configuration and connecting each component to the network, the administrator adds all the components (Sensors, Collectors, Sandboxes, Decoy Servers) to the CommandPost to register them. The component name, IP address and description are entered into the CommandPost. The component IP address must match the address established in the initial configuration and setup. After registration, the CommandPost attempts to communicate to the newly registered component at the specified IP address over a secure TLS tunnel.

The virtual appliances are delivered as an installation disk (or ISO image). The virtual systems were tested by the evaluation team with CentOS 7.7 on VMware ESXi 6.7 on Intel Xeon Gold 6248 (Cascade Lake). 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	Capacity	Number of vCPUs	Memory	Disk	Operating System / Software
CommandPost VM	Up to 4 alerts/sec Up to total 5 million alerts	Regular[1] 16	64 GB	1500 GB	CentOS 7.7 on VMware ESXi 6.7 on Intel Xeon Gold 6248 (Cascade Lake) Linux kernel 3.10.0-1062.9.1.el7.x86_64 httpd 2.4.41 tomcat 9.0.33 syslog-ng 3.7.3 MariaDB 10.4.8 OpenSSL 1.0.2k-fips
	Up to 10 alerts/sec Up to total 10 million alerts	Heavy[2] 32	128 GB	3000GB	
Direct/Internal VM	100Mbps	8	16 GB	40 GB	CentOS 7.7 on VMware ESXi 6.7 on Intel Xeon Gold 6248 (Cascade Lake) Linux kernel 3.10.0-1062.9.1.el7.x86_64 httpd 2.4.41 tomcat 9.0.33 syslog-ng 3.7.3 MariaDB 10.4.8 OpenSSL 1.0.2k-fips
	500Mbps (70k pps)	14	24 GB	80GB	
	1Gbps (125k pps)	24	32Gb	100GB	
	2Gbps (300K pps)	48	64	200 GB	
Web VM	100Mbps	8	16 GB	40 GB	CentOS 7.7 on VMware ESXi 6.7 on Intel Xeon Gold 6248 (Cascade Lake) Linux kernel 3.10.0-1062.9.1.el7.x86_64 httpd 2.4.41 tomcat 9.0.33 syslog-ng 3.7.3 MariaDB 10.4.8 OpenSSL 1.0.2k-fips
	500Mbps	14	24	80 GB	CentOS 7.7 on VMware ESXi 6.7 on Intel Xeon Gold 6248 (Cascade Lake)

[1] Regular usage is maximum of 10 concurrent users with total alert volume up to 5 million alerts (depending on total average session size and the retention period).
[2] Heavy usage is maximum of 20 concurrent users with total alert volume up to 10 million alerts (depending on total average session size and the retention period).

Device	Capacity	Number of vCPUs	Memory	Disk	Operating System / Software
					Linux kernel 3.10.0-1062.9.1.el7.x86_64 httpd 2.4.41 tomcat 9.0.33 syslog-ng 3.7.3 MariaDB 10.4.8 OpenSSL 1.0.2k-fips
	1Gbps	24	32	100GB	CentOS 7.7 on VMware ESXi 6.7 on Intel Xeon Gold 6248 (Cascade Lake) Linux kernel 3.10.0-1062.9.1.el7.x86_64 httpd 2.4.41 tomcat 9.0.33 syslog-ng 3.7.3 MariaDB 10.4.8 OpenSSL 1.0.2k-fips
Mail 250 VM	250k msg/day	6	12 GB	50 GB	CentOS 7.7 on VMware ESXi 6.7 on Intel Xeon Gold 6248 (Cascade Lake) Linux kernel 3.10.0-1062.9.1.el7.x86_64 httpd 2.4.41 tomcat 9.0.33 syslog-ng 3.7.3 MariaDB 10.4.8 OpenSSL 1.0.2k-fips
Mail 500 VM	500k msg/day	8	16 GB	100 GB	CentOS 7.7 on VMware ESXi 6.7 on Intel Xeon Gold 6248 (Cascade Lake) Linux kernel 3.10.0-1062.9.1.el7.x86_64 httpd 2.4.41 tomcat 9.0.33 syslog-ng 3.7.3 MariaDB 10.4.8 OpenSSL 1.0.2k-fips
Mail 1000 VM	1m msg/day	12	20 GB	200 GB	CentOS 7.7 on VMware ESXi 6.7 on Intel Xeon Gold 6248 (Cascade Lake) Linux kernel 3.10.0-1062.9.1.el7.x86_64 httpd 2.4.41

Device	Capacity	Number of vCPUs	Memory	Disk	Operating System / Software
					tomcat 9.0.33 syslog-ng 3.7.3 MariaDB 10.4.8 OpenSSL 1.0.2k-fips
Mail 5000 VM	5m msg/day	40	32	500 GB	CentOS 7.7 on VMware ESXi 6.7 on Intel Xeon Gold 6248 (Cascade Lake) Linux kernel 3.10.0-1062.9.1.el7.x86_64 httpd 2.4.41 tomcat 9.0.33 syslog-ng 3.7.3 MariaDB 10.4.8 OpenSSL 1.0.2k-fips
Collector SA VM	Minimal	4	28 GB	300 GB	CentOS 7.7 on VMware ESXi 6.7 on Intel Xeon Gold 6248 (Cascade Lake) Linux kernel 3.10.0-1062.9.1.el7.x86_64 httpd 2.4.41 tomcat 9.0.33 syslog-ng 3.7.3 MariaDB 10.4.8 OpenSSL 1.0.2k-fips
	Regular	16	64	1500 GB	CentOS 7.7 on VMware ESXi 6.7 on Intel Xeon Gold 6248 (Cascade Lake) Linux kernel 3.10.0-1062.9.1.el7.x86_64 httpd 2.4.41 tomcat 9.0.33 syslog-ng 3.7.3 MariaDB 10.4.8 OpenSSL 1.0.2k-fips
	Heavy	32	125	3000 GB	CentOS 7.7 on VMware ESXi 6.7 on Intel Xeon Gold 6248 (Cascade Lake) Linux kernel 3.10.0-1062.9.1.el7.x86_64 httpd 2.4.41 tomcat 9.0.33 syslog-ng 3.7.3

Device	Capacity	Number of vCPUs	Memory	Disk	Operating System / Software
					MariaDB 10.4.8 OpenSSL 1.0.2k-fips
Decoy Server	Low-End Virtual Machine	8 cores, 2.1 GHz and up	16 GB	250 GB	CentOS 7.7 on VMware ESXi 6.7 on Intel Xeon Gold 6248 (Cascade Lake) Linux kernel 3.10.0-1062.9.1.el7.x86_64 httpd 2.4.41 tomcat 9.0.33 syslog-ng 3.7.3 MariaDB 10.4.8 OpenSSL 1.0.2k-fips
	High End Virtual Machine	24 cores, 2.4 GHz and up	32 GB	500 GB	CentOS 7.7 on VMware ESXi 6.7 on Intel Xeon Gold 6248 (Cascade Lake) Linux kernel 3.10.0-1062.9.1.el7.x86_64 httpd 2.4.41 tomcat 9.0.33 syslog-ng 3.7.3 MariaDB 10.4.8 OpenSSL 1.0.2k-fips

There are additional hardware requirements depending on the deployment that are for functionality that is outside the scope of the evaluation but does not interfere with the evaluated functionality.

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

Additional information on how the TOE was configured during testing can be found in section 2.1.4 of the AAR.

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 Fidelis Deception Common Criteria Configuration Guide v9.3.3, Revised 2021
- Fidelis Network Fidelis Deception Enterprise Setup and Configuration Guide, Version 9.3.3
- Fidelis Network Fidelis Deception User Guide, Version 9.3.3

The above documents are the only documents that should be trusted for installation, administration, and use of the TOE in its evaluated configuration.

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 and Fidelis Deception v9.3.3 Common Criteria Test Report and Procedures For Network Device collaborative PP Version 2.2e, Version 1.2, April 7, 2021, as characterized in the publicly available Assurance Activities Report for Fidelis Network and Fidelis Deception v9.3.3, Version 1.0, 26 March 2021.

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 was performed at the Leidos Accredited Testing and Evaluation Lab located in Columbia, Maryland from July 1, 2020 to December 23, 2020. With the physical devices being tested on-site at the clients location on 9/14/2020 to 9/17/2020, 10/20/2020 to 10/22/2020, 11/5/2020 to 11/6/2020 and 11/19/2020. For the purposes of that testing, the configuration depicted in Figure 1 was used as a basis for testing. Figure 2 depicts the actual configuration for the TOE hardware appliances and Figure 3 depicts the virtual devices configuration.

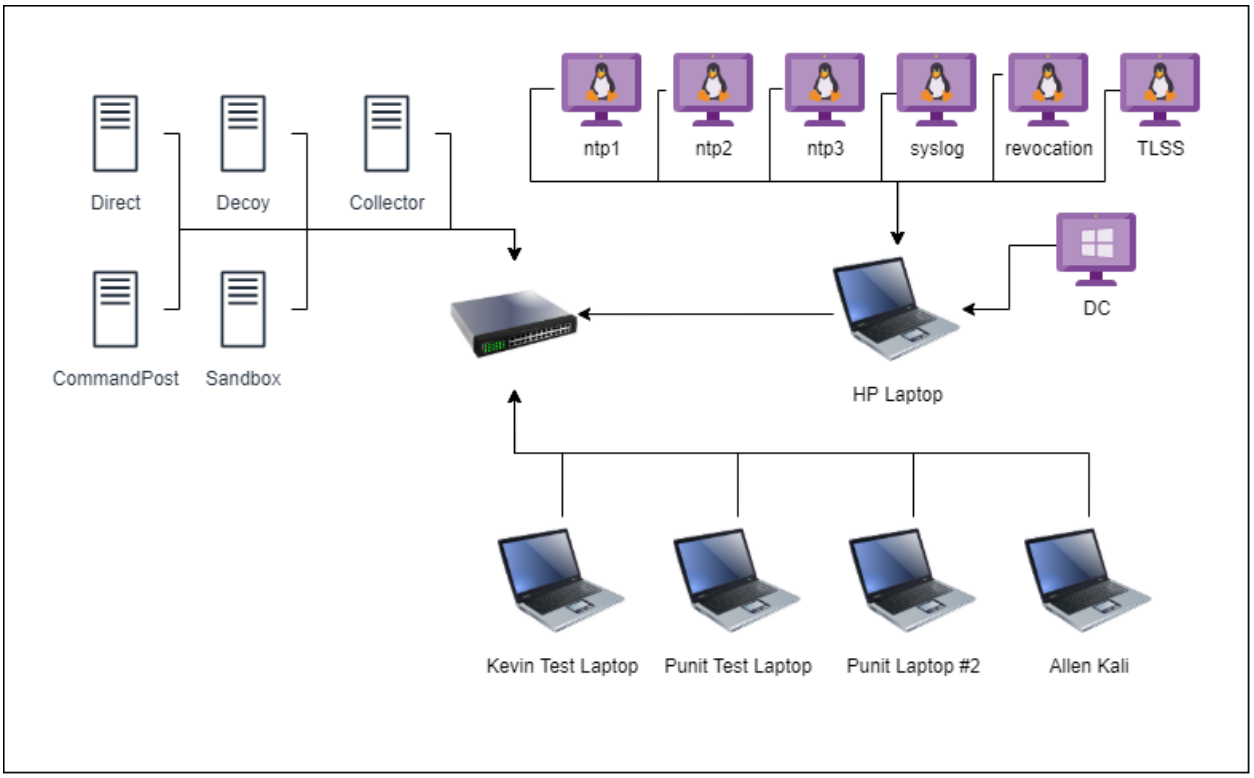

Figure 2: Physical Devices Configuration

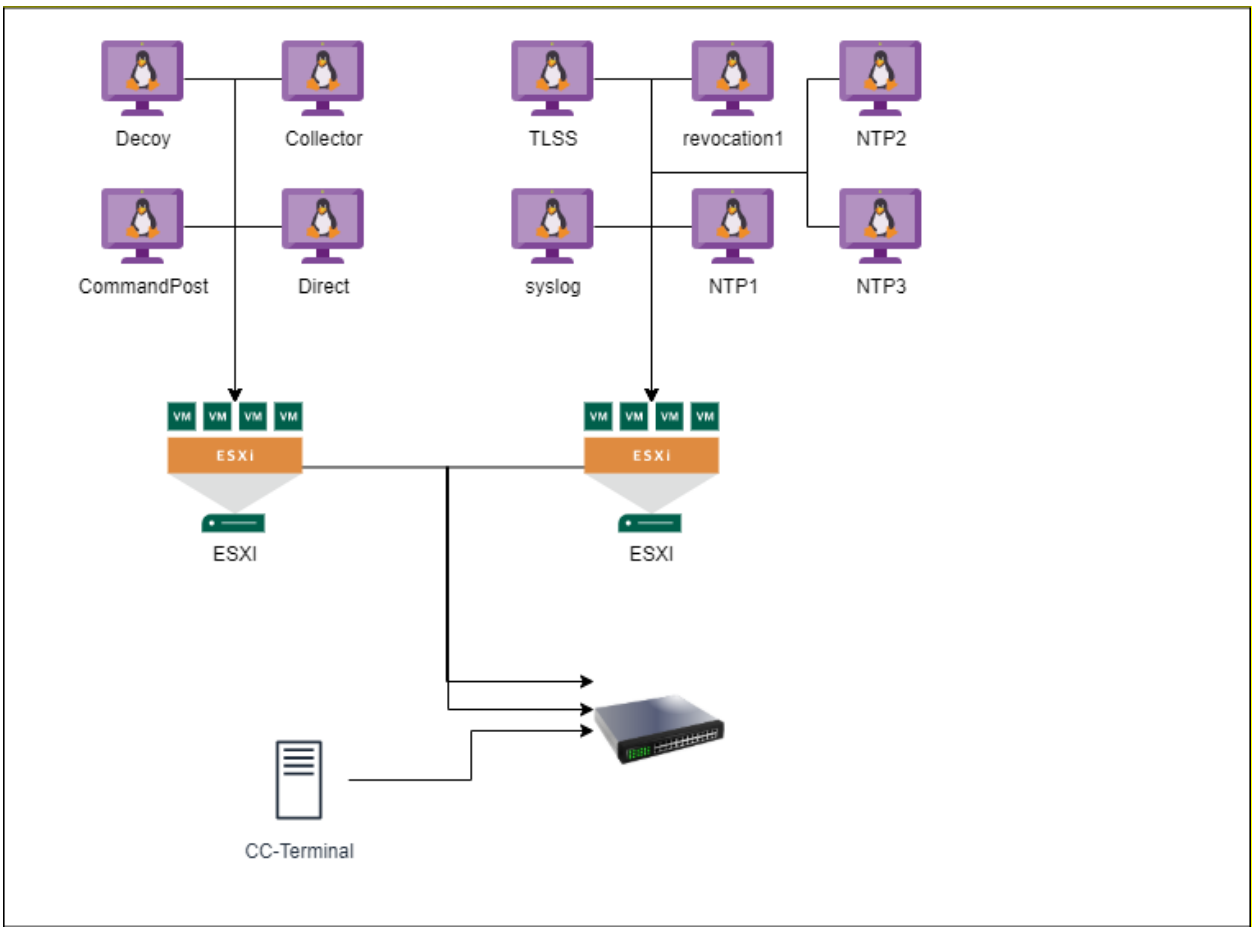

Figure 3: Virtual Devices Configuration

The TOE virtual appliances were installed on a server including CentOS 7.7 on VMware ESXi 6.7 on Intel Xeon Gold 6248 (Cascade Lake). 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 CommandPost appliance
  - Fidelis Collector SA2 appliance
  - Fidelis Direct 1000 Sensor appliance
  - Fidelis Sandbox appliance
  - Fidelis Decoy FDH-1000
- Virtual Machines
  - Fidelis CommandPost VM
  - Fidelis Direct VM
  - Fidelis Collector SA VM
  - Fidelis Decoy Server VM
- Software

- Fidelis Network ™ v9.3.3.

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

- Syslog Server: rsyslogd running on Ubuntu 18.04
- Test laptops with Kali Linux or Windows 10
- TLS Server on Ubuntu 18.04
- Windows AD server on Windows Server 10 DC (physical); Windows Server 2016 (virtual)
- 3 NTP v4.2.8P10 daemons each running on Ubuntu 18.04

The vendor provided the TOE platforms for the appliances as described above. A more detailed description of the platforms for the virtual machine instances tested and the other test tools are in Section 2.1.4 for the AAR.

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 in order 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 and Fidelis Deception v9.3.3*.

7.3 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 list of the search terms, databases searched, and dates of the searches may be found in Section 4.6.1 of the AAR.

8 Evaluated Configuration

The TOE is Fidelis Network and Fidelis Deception v9.3.3, 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 2.2e, 23 March 2020, in conjunction with Version 3.1, Revision 5 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 of 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

All of the validators' comments are covered in the *Clarification of Scope* section (4.2) of this report. There are no additional validator comments or recommendations.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is Fidelis Network and Fidelis Deception v9.3.3 Security Target, Version 1.0, 26 March 2021.

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 5, April 2017. Part 1: Introduction and general model.

[2] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017. Part 2: Security functional components.

[3] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017. Part 3: Security assurance components.

[4] Common Methodology for Information Technology Security Evaluation, Version 3.1, 5, April 2017. Evaluation methodology.

[5] collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020.

[6] Fidelis Network and Fidelis Deception v9.3.3 Security Target, Version 1.0, 26 March 2021.

[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 and Fidelis Deception v9.3.3, Parts 1 and 2 Version 1.0, 31 March 2021.

[9] Assurance Activities Report for Fidelis Network and Fidelis Deception v9.3.3, Version 1.0, 26 March 2021.

[10] Fidelis Network and Fidelis Deception v9.3.3 Common Criteria Test Report and Procedures For Network Device collaborative PP Version 2.2e, Version 1.2, 7 April 2021.