National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

NIKSUN NetDetector/NetVCR 10440

Report Number: CCEVS-VR-VID10869-2018
Version 1.0
August 14, 2018

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

Paul Bicknell
The MITRE Corporation

Patrick Mallett, PhD.
The MITRE Corporation

Sheldon Durrant
The MITRE Corporation

Linda Morrison
The MITRE Corporation

Common Criteria Testing Laboratory

Christopher Gugel, CC Technical Director
Christopher Rakaczky

Booz Allen Hamilton (BAH)
Laurel, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of NIKSUN NetDetector/NetVCR 10440 provided by NIKSUN, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Laurel, Maryland, United States of America, and was completed in August 2018. The information in this report is largely derived from the evaluation sensitive Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements set forth in the Network Device collaborative Protection Profile, version 2.0 + Errata 20180314 (NDcPP).

The Target of Evaluation (TOE) is the NIKSUN NetDetector/NetVCR 10440 appliance, running the NIKSUN NetDetector/NetVCR Everest software version 5.1.2.0. NetDetector's primary functionality is to provide an overview of critical operations of the monitored network. The overview includes monitoring business service disruptions, performance issues, and security incidents. NetDetector accomplishes this by providing security monitoring of network traffic using IDS methods and statistical anomaly detection in order to safeguard networks against cyber-attacks. However, the evaluated TOE functionality includes only the security functional behavior that is defined in the claimed NDcPP.

The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4), as interpreted by the Assurance Activities contained in the NDcPP. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes, and reviewed the individual work units of the ETR for the NDcPP Assurance Activities. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). 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.

The technical information included in this report was obtained from the *NIKSUN NetDetector/NetVCR 10440 Security Target v1.0*, dated June 22, 2018 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

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 Product Compliant 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.
- 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	NIKSUN NetDetector/NetVCR 10440 appliance, running the NIKSUN NetDetector/NetVCR Everest software version 5.1.2.0 Refer to Table 2 for Model Specifications
Protection Profile	Collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018, including all applicable NIAP Technical Decisions and Policy Letters
Security Target	NIKSUN NetDetector/NetVCR 10440 Security Target v1.0, dated June 22, 2018
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "NIKSUN NetDetector/NetVCR 10440" Evaluation Technical Report v1.0 dated June 27, 2018
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	NIKSUN, Inc.
Developer	NIKSUN, Inc.
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Laurel, Maryland
CCEVS Validators	Paul Bicknell, The MITRE Corporation Patrick Mallett, PhD., The MITRE Corporation Sheldon Durrant, The MITRE Corporation Linda Morrison, The MITRE Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

- It is assumed that the TOE is deployed in a physically secured operational environment and not subjected to any physical attacks.
- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- The TOE is not responsible for protecting network traffic that is transmitted across its interfaces that is not related to any TOE management functionality or generated data.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- It is assumed that regular software and firmware updates will be applied by a TOE Administrator when made available by the product vendor.
- Administrator credentials are assumed to be secured from unauthorized disclosure.
- TOE Administrators are trusted to ensure that there is no unauthorized access possible for sensitive residual information on the TOE when it is removed from its operational environment.

3.2 Threats

The following lists the threats addressed by the TOE.

- **T.UNAUTHORIZED_ADMINISTRATOR_ACCESS** – Threat agents may attempt to gain administrator access to the TOE's management functionality through nefarious means such as replay, impersonation, or man-in-the-middle attacks.
- **T.WEAK_CRYPTOGRAPHY –** Threat agents may exploit weak keys or cryptographic algorithms to gain unauthorized access to protected data at rest or in transit.
- **T.UNTRUSTED_COMMUNICATION_CHANNELS** – Threat agents may exploit unencrypted communications channels to access sensitive data or manipulate data in transit.
- **T.WEAK_AUTHENTICATION_ENDPOINTS –** Threat agents may take advantage of secure protocols to access a remote endpoint used by the TOE using shared, static, plaintext, or default credentials.
- **T.UPDATE_COMPROMISE –** Threat agents may exploit an unpatched system or provide a malicious update to the TOE in order to cause a known failure.
- **T.UNDETECTED_ACTIVITY** – A malicious administrator may perform improper activities on the TOE and have the ability to prevent audit records of the activity from being generated or to remove all traces of their activities.
- **T.SECURITY_FUNCTIONALITY_COMPROMISE –** A self-protection mechanism of the TOE may fail or be improperly implemented, allowing a threat agent to access functions or data that were meant to be protected.
- **T.PASSWORD_CRACKING –** A weak administrator password may allow a malicious actor to access administrative functionality through password guessing or brute force exhaustion.
- **T.SECURITY_FUNCTIONALITY_FAILURE –** A component of the TOE responsible for implementing security functionality may fail without administrator awareness.

3.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that might benefit from additional clarification. 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 level of assurance for this evaluation is defined within the collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018, including all relevant NIAP Technical Decisions. A subset of the "optional" and "selection-based" security requirements defined in the NDcPP are claimed by the TOE and documented in the ST.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to security functionality 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 functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. The security monitoring of network traffic using IDS methods and statistical anomaly detection in order to safeguard networks against cyber-attacks functionality included in the product and described in Section 1.3 of the Security Target 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.

The evaluated configuration of the TOE is the NIKSUN NetDetector/NetVCR 10440 appliance described in Table 2 running the NIKSUN NetDetector/NetVCR Everest software version 5.1.2.0 software. In the evaluated configuration, the TOE uses TLS/HTTPS to secure remote web-based administration, SSH to secure remote command-line administration, and TLS, HTTPS and SSH to secure transmissions of security-relevant data from the TOE to external entities such as authentication server and syslog. The TOE includes administrative guidance in order to instruct Security Administrators in the secure installation and operation of the TOE. Adherence to this guidance is sufficient to ensure that the TOE is operated in accordance with its evaluated configuration.

4 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

4.1 TOE Introduction

The TOE is a network device as defined in the NDcPP which states: "This is a Collaborative Protection Profile (cPP) whose Target of Evaluation (TOE) is a network device… A network device in the context of this cPP is a device composed of both hardware and software that is connected to the network and has an infrastructure role within the network.". The TOE consists of the NIKSUN NetDetector/NetVCR 10440 model, running the NIKSUN NetDetector/NetVCR Everest software version 5.1.2.0. Thus, the TOE is a network device composed of hardware and software.

4.2 Physical Boundary

The TOE is comprised of both software and hardware. The hardware is comprised of the following:

Property	NetDetector
Model Number	NIKSUN 10440 Platform
Size	10 RUs+
Power	AC
Power Supplies	5 + 5 Redundant
Processor	Intel Xeon E5-2660 v2
Memory (RAM)	256GB (Max)
Storage	160TB
External Storage	Yes
RAID	Yes

Table 2 – Hardware Specifications

The TOE resides on a network and supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Component	Definition
LDAP/AD Server	A system that is capable of receiving authentication requests using LDAP over TLS and validating these requests against identity and credential data that is defined in an LDAP directory. In the evaluated configuration, the TOE connects to a server with OpenLDAP for its remote authentication store.
Management Workstation	Any general-purpose computer that is used by a Security Administrator to manage the TOE. The TOE can be managed remotely, in which case the management workstation requires an SSH client to access the CLI or a web browser (Microsoft Internet Explorer 9.0 or higher and Mozilla Firefox 3.6 or higher) to access the web GUI.
Syslog Server	The Syslog Server connects to the TOE and allows the TOE to send Syslog messages to it for remote storage. This is used to send copies of audit data to be stored in a remote location for data redundancy purposes.
SCP Server	A secure server used to ensure the secure copying of data through an SSH encrypted connection. In the evaluated configuration, the SCP Server is used to transfer software updates to the TOE's software image directory.
CRL Distribution Point	A server deployed within the Operational Environment which confirms the validity and revocation status of certificates.

NetOmni	NetDetector/NetVCR is a network security and performance monitoring system which sends captured packet data to NetOmni. The NetDetector/NetVCR also receives commands and is managed by NetOmni. The TOE communicates with NetOmni over an encrypted channel.
SMTP Server	A server that forwards an email that is sent from NetDetector/NetVCR when a user utilizes the "Forgot Username/Password" feature on the NetDetector/NetVCR log in screen. The email is protected from unauthorized disclosure using TLS.

Table 3 – IT Environment Components

5 Security Policy

5.1 Security Audit

Audit records are generated for various types of management activities and events. These records include the date and time stamp of the event, the event type, and the subject identity. Audit records are stored as syslog records on the TOE, and can be configured to also be sent to a Syslog Server via a TLS connection. When the storage space allocated to specific audit record types is exhausted, the TOE will overwrite the oldest relevant log file. Administrators are assumed to be trusted users and are not expected to delete or modify the audit records. Applications that run from the CLI keep their own VAR log files, such as Apache, LDAP client, etc. These log files are also sent via TLS to the Syslog Server.

5.2 Cryptographic Support

The TOE relies on its NIKOS FIPS Object Module 2.0.16 (derived from OpenSSL FIPS Object Module 2.0.7) cryptographic module to implement cryptographic methods and trusted channels. X.509v3 certificates are used to support authentication mechanisms. SSH is used to secure the remote CLI interface for remote management of the TOE. SSH is also used to secure the communication with the SCP Server when the TOE receives software image updates. The TOE uses TLS to secure the automatic transfer of syslog audit files and VAR logs to the Syslog Server, and for connection to the LDAP/AD Server for remote authentication. When a user utilizes the "Forgot Username/Password" feature on the NetDetector/NetVCR login screen, NetDetector/NetVCR will send an email to the SMTP Server over a protected TLS channel. TLS/HTTPS is used to secure the connection for remote management of the TOE via the web GUI as well as connections to NetOmni devices. The TOE will deny any connections for disallowed protocols and invalid X.509v3 certificates.

Cryptographic keys are generated using the CTR_DRBG provided through this module. The TOE destroys all plaintext secrets and private keys.

The following table contains the CAVP algorithm certificates:

Algorithm	CAVP Cert. #
AES-128-CBC, AES-256-CBC	5418
RSA (FIPS 186-4 KeyGen, SigGen and SigVer)	2902
CTR_DRBG (AES)	2113
SHA-1, SHA-256, SHA-512	4349
HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512	3588
CVL (FFC 800-56A except key derivation function)	1871
DSA	1394

Table 4 –CAVP References

5.3 Identification and Authentication

The TOE verifies the identity of users connecting to the TOE. All users must be identified and authenticated before being allowed to perform actions on the TOE. This is true of users accessing the TOE via the local console, or through protected paths using the remote CLI via SSH or the web GUI via TLS 1.2. Users can authenticate to the TOE using a username and password. In addition, when authenticating by the remote CLI, users can instead use SSH public-key authentication. LDAP can be configured to provide external authentication. Passwords can

consist of upper case letters, lower case letters, numbers, and a set of selected special characters. Password information is never revealed during the authentication process including during login failures. Before a user authenticates to the device, a customizable warning banner is configured to be displayed. In addition, via the web GUI only, the user has the option to use a "Forgot Username/Password" feature prior to authenticating.

The TOE uses X.509v3 certificates to perform server side authentication of Syslog Server, SMTP Server and LDAP/AD Server and present its certificate to NetOmni for authentication. The TSF determines the validity of the certificates by confirming the validity of the certificate chain, and verifying that the certificate chain ends in a trusted Certificate Authority (CA). The TSF connects with a CRL distribution point through HTTP to confirm certificate validity and to access certificate revocation lists (CRL).

5.4 Security Management

The TOE has a role based authentication system where roles (permissions) are assigned to groups for the web GUI. Authorized actions for a particular user are dependent on which group they are assigned to. There are 4 initial groups: Administrator, Account Administrator, Advanced Users, and Users. Only users assigned to the Administrator group are capable of performing SFR related management functions via the web GUI and thus, are Security Administrators in the context of the evaluation. The VCR user is the Security Administrator user for the remote and local CLI, and is able to update the TOE's software and verify it via published hash.

The NDcPP's definition of "role" is synonymous with NIKSUN's definition of "permissions". NIKSUN's terminology fits into the Protection Profiles by using the term "user roles" in place of "user permissions". For the remainder of this document, "user permissions" is used in order to match the terminology used by Common Criteria.

5.5 Protection of the TSF

The TOE stores passwords in a variety of locations depending on their use and encryption. They cannot be viewed by any user regardless of the user's role. The VCR user passwords are stored in the OS hashed by SHA-512. Web GUI passwords are stored in the PostgreSQL Database hashed with SHA-256. Pre-shared keys, symmetric keys, and private keys cannot be accessed in plaintext form by any user. There is an underlying hardware clock that is used for accurate timekeeping and is set by the Security Administrator. Power-on self-tests are executed automatically when the cryptographic module is loaded into memory. It verifies its own integrity using an HMAC-SHA-256 digest computed at build time and also tests all algorithms for integrity. The TOE also performs self-tests on the CPU, RAM, and disk components. The TOE's DRBG also performs its own health tests.

The version of the TOE is verified via the CLI or web GUI. The TOE is updated by the VCR user via the CLI. Updated software images are downloaded to the SCP Server and are transferred to the TOE via the SCP using SSH. The administrator is also capable of copying the image to a CD and manually loading it to the TOE. The TOE conducts a hash verification on the system image using SHA-256 against the known hash to ensure the integrity of the update.

5.6 TOE Access

Before any user authenticates to the TOE, the TOE displays a configurable Security Administrator banner for the web GUI. The local and remote CLI interfaces display the default Linux security banner prior to authentication that is also configurable. The TOE can terminate local CLI, remote CLI, and web GUI sessions after a specified time period of inactivity. Administrator users have the capability to terminate their own sessions.

5.7 Trusted Path/Channels

The TOE connects and sends data to IT entities that reside in the Operational Environment via trusted channels. In the evaluated configuration, the TOE connects to Syslog Server via TLS to send audit data for remote storage. TLS is used for the TOE's connection with the SMTP Server to send secure email. TLS is also used for the TOE's connection with the LDAP/AD Server for its remote authentication store. TLS/HTTPS is used for the transfer of data to the NetOmni appliance. TLS/HTTPS and SSH are used for remote administration of the TOE via the web GUI and remote CLI respectively.

6 Documentation

The vendor provided the following guidance documentation in support of the evaluation:

- NIKSUN NetDetector/NetVCR 10440 Release 5.1.2.0 Supplemental Administrative Guidance for Common Criteria Version 1.0
- NIKSUN NetDetector Release 5.1.2.0 DISA HARDWARE INSTALLATION GUIDE
- NIKSUN NetDetector Release 5.1.2.0 DISA SOFTWARE UPGRADE & REINSTALLATION GUIDE
- NIKSUN Appliance NikOS Everest ADMINISTRATOR GUIDE 5.1.2.0
- NIKSUN Security Configuration & Tools NikOS Everest CONFIGURATION GUIDE 5.1.2.0
- NIKSUN Military Unique Deployment Guide Release 5.1.2.0 Version 1.0

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 as evaluated.

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is NIKSUN NetDetector/NetVCR 10440 appliance, running the software: NIKSUN NetDetector/NetVCR Everest software version 5.1.2.0. Section 4.2 describes the TOE's physical configuration as well as the operational environment components to which it communicates. In its evaluated configuration, the TOE is configured to communicate with the following environment components:

- Management Workstation for local and remote administration
- Syslog Server for recording of syslog data
- OpenLDAP Server for remote authentication
- SMTP Server for sending email
- Certificate Authority/CRL Distribution Point
- SCP server for receiving software updates
- NetOmni for NetDetector/NetVCR's primary functionality

To use the product in the evaluated configuration, the product must be configured as specified in the *NIKSUN NetDetector/NetVCR 10440 Release 5.1.2.0 Supplemental Administrative Guidance for Common Criteria Version 1.0* document.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the *Assurance Activity Report for a Target of Evaluation "NIKSUN NetDetector/NetVCR" Assurance Activities Report v1.0 dated June 29, 2018*.

8.1 Test Configuration

The evaluation team configured the TOE for testing according to the *NIKSUN NetDetector/NetVCR 10440 Release 5.1.2.0 Supplemental Administrative Guidance for Common Criteria Version 1.0* (AGD) document. The evaluation team set up a test environment for the independent functional testing that allowed them to perform the assurance activities against the TOE over the SFR relevant interfaces. The evaluation team conducted testing in the Booz Allen CCTL facility on an isolated network. Testing was performed against all three management interfaces defined in the ST (local CLI, remote CLI, and web GUI).

The TOE was configured to communicate with the following environment components:

- Management Workstation for local and remote administration
- Syslog Server for recording of syslog data
- OpenLDAP Server for remote authentication
- SMTP Server for sending email
- Certificate Authority/CRL Distribution Point
- SCP server for receiving software updates
- NetOmni for NetDetector/NetVCR's primary functionality

The following test tools were installed on a separate workstation (management workstation)

- WireShark: version 2.4.2
- Bitvise SSH Client: version 7.15

*Only the test tools utilized for functional testing have been listed.

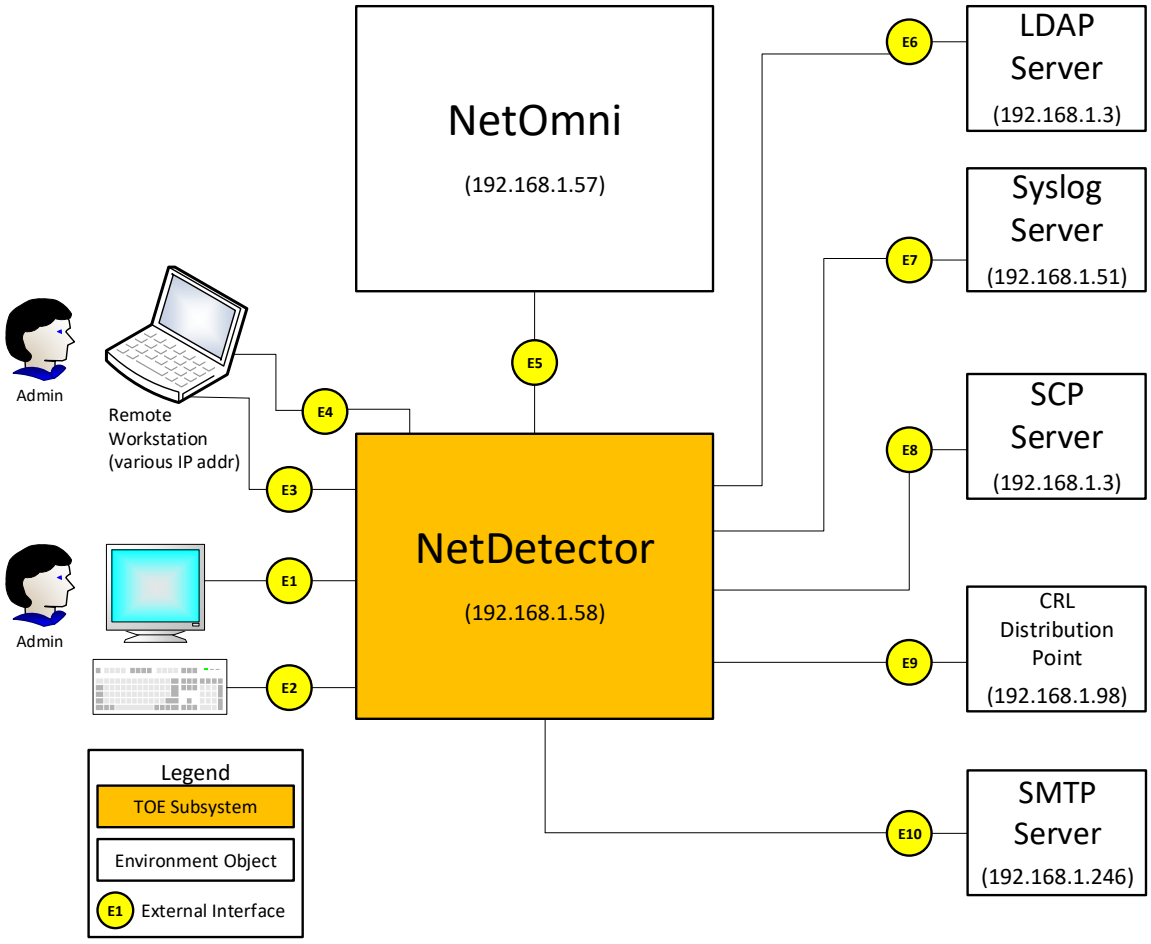

Figure 1 - Test Configuration

8.2 Developer Testing

No evidence of developer testing is required in the Evaluation Activities for this product.

8.3 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the TOE by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the NDcPP for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

8.4 Evaluation Team Vulnerability Testing

The evaluation team reviewed vendor documentation, formulated hypotheses, performed vulnerability analysis, and documented the hypotheses and analysis in accordance with the NDcPP requirements. Keywords were identified based upon review of the Security Target and AGD. The following keywords were identified:

Keyword	Description
NIKSUN	This is a generic term for searching for known vulnerabilities produced by the company as a whole.
NetDetector NetVCR	This is a generic term for searching for known vulnerabilities for the specific product.
10440	This is a generic term for searching for known vulnerabilities for specific model of the specific product line.
Everest	A specific version was not included in the search because this version may be within a range of vulnerable operating system versions and not listed separately.
FreeBSD 11.1	This is a generic term searching for known vulnerabilities for the underlying TOE operating system.
NIKOS (FIPS Object Module 2.0.16)	This is a generic term searching for known vulnerabilities for the TOE's cryptographic module.
TCP, TLS, HTTPS, SSH	These are protocols used by the TOE.

These keywords were used individually and as part of various permutations and combinations to search for vulnerabilities on public vulnerability sources on June 1, 2018. The following public vulnerability sources were searched:

- NIST National Vulnerabilities: https://web.nvd.nist.gov/view/vuln/search
- Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/ https://www.cvedetails.com/vulnerability-search.php
- US-CERT: http://www.kb.cert.org/vuls/html/search
- SecurITeam Exploit Search: www.securiteam.com
- Tenable Network Security http://nessus.org/plugins/index.php?view=search
- Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Port Scanning
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.

- Web Interface Vulnerability Identification (Burp Suite)
  Burp Suite is a web application vulnerability assessment tool. It looks for major vulnerabilities including cross-site scripting, SQL injection, directory traversal, unchecked file uploads, etc. as well as less critical vulnerabilities such as unnecessary information disclosure.

- SSH Timing Attack (User Enumeration)
  This attack attempts to enumerate validate usernames for the SSH interface, by observing the difference in server response times to valid username login attempts.

- Force SSHv1
  This attack determines if the SSH server on the TOE will accept an SSHv1 connection when the TOE claims to only support SSHv2

The evaluation team determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all Evaluation Activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

9.1 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 policies and assumptions, a statement of security requirements claimed to be met by the NetDetector/NetVCR product that is consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Evaluation Activities specified in the NDcPP Supporting Documents in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each 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 contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Documents related to the examination of the information contained in the TOE Summary Specification.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Document related to the examination of the information contained in the operational guidance documents.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work units. The evaluation team found that the TOE was identified.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the NDcPP Supporting Documents and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

The validators reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDcPP Supporting Documents, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The evaluation team also ensured that the specific vulnerabilities defined in the NDcPP Supporting Documents were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis requirements in the NDcPP Supporting Documents, and that the conclusion reached by the evaluation team was justified.

9.7 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 test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Evaluation Activities in the NDcPP Supporting Document, and correctly verified that the product meets the claims in the ST.

10 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *NIKSUN NetDetector/NetVCR 10440 Release 5.1.2.0 Supplemental Administrative Guidance for Common Criteria Version 1.0* document. No versions of the TOE and software, either earlier or later were evaluated.

Administrators should take note of the fact that when the product is configured to offload audit files to an audit logging server, if that communications link is interrupted, the audit files generated during the time of the interruption will be captured locally. However, upon resumption of the connectivity, the offload begins with the reconnection and will NOT send those audit files generated during the outage. It will be necessary for the administrator to take steps to offload those files or they will be overwritten when the audit log is full.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the NetOmni, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *NIKSUN NetDetector/NetVCR 10440 Security Target v1.0*, dated June 22, 2018.

13 List of Acronyms

Acronym	Definition
CC	Common Criteria
CLI	Command-Line Interface
cPP	collaborative Protection Profile
CRL	Certificate Revocation List
CVL	Component Validation List
DRBG	Deterministic Random Bit Generator
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IT	Information Technology
LDAP/AD	Lightweight Directory Access Protocol / Active Directory
NDcPP	Network Device collaborative Protection Profile
NIAP	National Information Assurance Partnership
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
RBG	Random Bit Generator
SAR	Security Assurance Requirement
SCP	Secure Copy Protocol
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface

14 Terminology

Term	Definition
Administrator	The web GUI role that is considered a Security Administrator for the evaluation. TOE users with this role will configure and manage the TOE security functions and manages audit records.
NetDetector/NetVCR	The TOE is a monitoring system that captures, records, and analyzes traffic streams on the monitored network for network security and performance. The NetDetector/NetVCR appliance communicates with a NetOmni appliance that is in the Operational Environment. NetDetector/NetVCR provides information on the performance of the network, and NetOmni provides instructions to the NetDetector/NetVCR.
NetOmni	It provides an overview of critical operations of the monitored network.
Security Administrator	The claimed Protection Profile defines a Security Administrator role that is authorized to manage the TOE and its data. For the TOE, this is considered to be any user with the 'Administrator' role in the web GUI and the 'VCR User' in the CLI.
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application a Security Administrator uses to manage it (web browser, terminal client, etc.).
User	In a CC context, any individual who has the ability to access the TOE functions or data.
VAR Log	Log file that contains TOE audit records which is stored in the /var/log directory.
VCR User	The CLI role that is considered to be a Security Administrator for the evaluation. It manages security functions and audit records. The VCR user assumes the Linux root role to perform some of its TOE management functions using the command 'su root'.

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018
6. NIKSUN NetDetector/NetVCR 10440 Security Target v1.0, dated June 22, 2018
7. NIKSUN NetDetector/NetVCR 10440 Release 5.1.2.0 Supplemental Administrative Guidance for Common Criteria Version 1.0
8. NIKSUN NetDetector Release 5.1.2.0 DISA HARDWARE INSTALLATION GUIDE
9. NIKSUN NetDetector Release 5.1.2.0 DISA SOFTWARE UPGRADE & REINSTALLATION GUIDE
10. NIKSUN Appliance NikOS Everest ADMINISTRATOR GUIDE 5.1.2.0
11. NIKSUN Security Configuration & Tools NikOS Everest CONFIGURATION GUIDE 5.1.2.0
12. NIKSUN Military Unique Deployment Guide Release 5.1.2.0 Version 1.0
13. Assurance Activity Report for a Target of Evaluation "NIKSUN NetDetector/NetVCR" Assurance Activities Report v1.0 dated June 29, 2018