National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

3eTI 3e-636 Series Network Security Devices

Report Number: **CCEVS-VR-VID10580**
Dated: **March 25, 2015**
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

Mr. Paul A. Bicknell

The MITRE Corporation

Bedford, MA

Mr. Luke A Florer

The Aerospace Corporation

Los Angeles, CA

Mr. Jay Vora

The MITRE Corporation

Fort Meade, MD

Common Criteria Testing Laboratory

Mr. Herb Markle

Ms. Nandini Pathmanathan

CygnaCom Solutions

McLean, Virginia

Much of the material in this report was extracted from evaluation material prepared by the CCTL. The CCTL team deserves credit for their hard work in developing that material. Many of the product descriptions in this report were extracted from the 3eTI-636 Series Network Security Device Security Target.

Table of Contents

List of Figures and Tables

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of the 3eTI 3e-636 Series Network Security Devices as defined in the *3eTI 3e-636 Series Network Security Devices v1.0.*

The 3e-636 Series Network Security Devices share the identical hardware platform. Both devices provide the same functionalities of access control, traffic filter and data packet inspection for network data traffic between the private networks. GUI Management interfaces over TLS/HTTPS.

The Target of Evaluation (TOE) is a Network Device as defined by the *U.S. Government Standard Protection Profile for Network Devices*, 08 June 2012, Version 1.1: "*A network device is a device composed of hardware and software that is connected to the network and has an infrastructure role in the overall enterprise".*

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed in January 2015. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is:

- Common Criteria version 3.1 R4 Part 2 extended and Part 3 conformant, and
- Demonstrates exact compliance to *U.S. Government Standard Protection Profile for Network Devices*, 08 June 2012, Version 1.1 as changed/clarified by *Security Requirements for Network Devices Errata #3 and all applicable Technical Decisions*.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site www.niap-ccevs.org.

2. Identification

Target of Evaluation: 3eTI 3e-636 Series Network Security Devices

The TOE consists of the following 636 Series product:

- 3e-636L3 Network Security Device; Hardware Version 1.0, Firmware Version 5.1 build 73
- 3e-636L2 High Speed Encryption Network Security Device, Hardware Version 1.0, Firmware Version 5.1 build 62

ST Title: *3eTI 3e-636 Series Network Security Device Security Target V1.0 Revision J*

Developer:	3e Technologies International
CCTL:	CygnaCom Solutions 7925 Jones Branch Dr, Suite 5400 McLean, VA 22102-3321
Evaluators:	Herb Markle Nandini Pathmanathan
Validation Scheme:	National Information Assurance Partnership CCEVS
Validators:	Paul A. Bicknell, Luke Florer, Jay Vora
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1 R4, Sept 2012
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 3.1 R4, Sept 2012
PP Identification:	US Government Protection Profile for Network Devices, Version 1.1, 8 June 2012 with Errata 3

3. Security Policy

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

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted path/Channel

3.1. Security Audit

The TOE generates auditable events for actions on the TOE with the capability of selective audit record generation. The records of these events can be viewed within the TOE Management Interface or they can be exported to audit systems in the Operational Environment. The TOE generates records for its own actions, containing information about the user/process associated with the event, the success or failure of the event, and the time that the event occurred. Additionally, all administrator actions relating to the management of TSF data and configuration data are logged by the TOE's audit generation functionality.

3.2. Cryptographic Support

The TOE uses a random number generator and secures communication channels with the following cryptographic algorithms: AES, RSA, ECDSA, SHA, HMAC. The TOE is designed to zeroize Critical Security Parameters (CSPs) to mitigate the possibility of disclosure or modification.

3.3. User Data Protection

The TSF ensures that network packets sent from the TOE do not include data "left over" from processing the previous network information.

3.4. Identification and Authentication

The TOE provides Identification and Authentication security functionality to ensure that all users are properly identified and authenticated before accessing TOE functionality. The TOE enforces a local password-based authentication mechanism to perform administrative user authentication. Passwords are obscured when being displayed during any attempted login.

3.5. Security Management

The Web Management Application of the TOE provides the capabilities for configuration and administration. The Web Management Application can be accessed via the dedicated local Ethernet port configured for "out-of-band" management. There is no local access such as a serial console port. Therefore, the local and remote management is considered the same for this evaluation.

An authorized administrator has the ability to modify, edit, and delete security parameters such as audit data, configuration data, and user authentication data. The Web Management Application also offers an authorized administrator the capability to manage how security functions behave. For example an administrator can enable/disable certain audit functions query and set encryption/decryption algorithms used for network packets.

3.6. Protection of the TSF

Internal testing of the TOE hardware, software, and software updates against tampering ensures that all security functions are running and available before the TOE accepting any communications. The TSF prevents reading of pre-shared keys, symmetric keys, and private keys, and passwords. The TOE uses electronic signature verification before any firmware/software updates are installed.

3.7. TOE Access

The TOE will display a customizable banner when an administrator initiates an interactive local or remote session. The TOE also enforces an administrator-defined inactivity timeout after which the inactive session is automatically terminated. Once a session (local or remote) has been terminated, the TOE requires the user to re-authenticate.

3.8. Trusted Path/Channels

The TOE protects interactive communication with administrators using TLS/HTTPS, both integrity and disclosure protection is ensured.

The TOE protects communication with network entities, such as a log server, using TLS connection and optionally using a dedicated physical port to prevent unintended disclosure or modification of logs and management information.

3.9. Secure Usage Assumptions

The ST identifies the following assumptions about the use of the product:

1. 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 hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
2. Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

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

4. Architectural Information

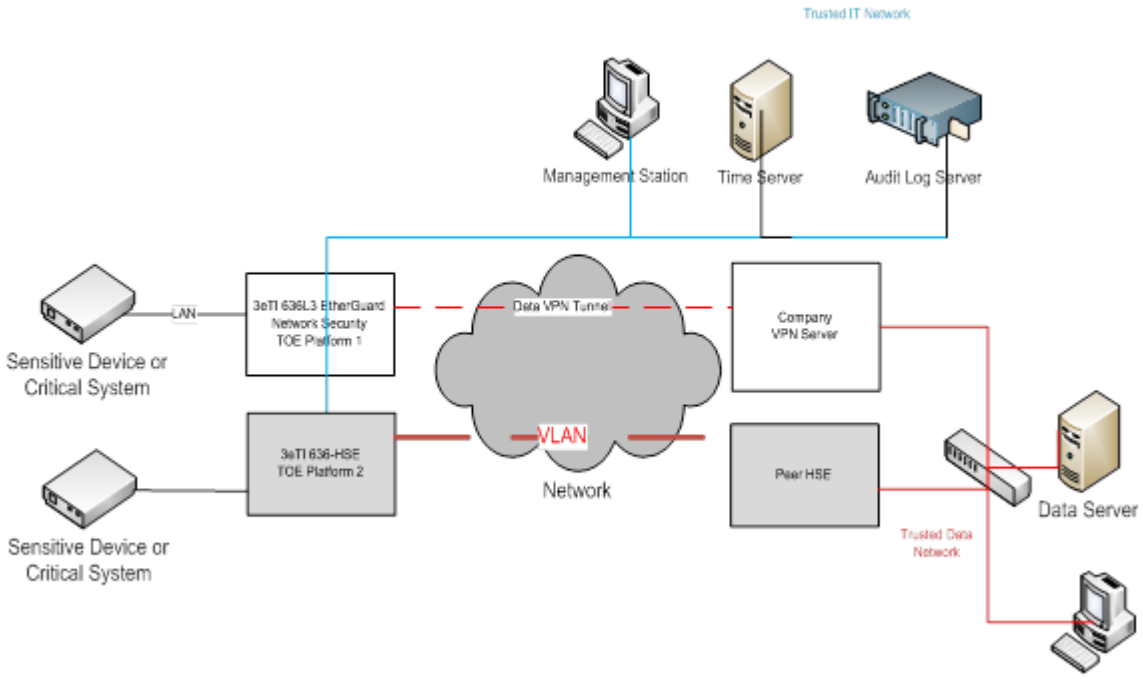
The Target of Evaluation (TOE) is network devices that provide high speed information assurance that combines a number of different capabilities to create a tailored cyber defense.

Acting as an IPsec client, the 3e-636L3 authenticates the IPsec Gateway during IKEv2 negotiation. It provides further data integrity and confidentiality using the ESP mode of the IPsec. AES with 128/256 bits key is used for network data encryption while SHS, CCM or GCM is used for data integrity.

The 3e-636L2 provides high speed IEEE802.3 MAC layer encryption. All 3e-636-HSE devices can communicate securely on the same VLAN using the symmetric encryption key. Data integrity is offered through HMAC-SHS or CCM mode of encryption.

Error! Not a valid bookmark self-reference. depicts a normal operational scenario with the TOE. The 3e-636L3 uses IPSec tunnel while 3e-636L2 operates with symmetric encryption on the VLAN. The TOE relies upon an NTP Server and an Audit Server in its Operational Environment. The TOE may also be configured to communicate with DHCP and SNMP Management Servers in the Operational Environment, but does not depend upon them to support its security functionality.

Figure 1: 3e-636L3/3e-636L2 TOE Operational Configuration



The TOE physical boundary defines all hardware and firmware that is required to support the TOE's logical boundary and the TOE's security functions. The TOE hardware platform uses FreeScale MPC8378E CPU and the TOE's firmware contains embedded

Linux Kernel customized by 3eTI based on kernel version 2.6. In short, the TOE's physical boundary is the physical device/appliance for both models.

Evaluation Clarification: The TOE components use IPSec to provide transport layer security as VPN Client. While the TOE meets (vendor assertion) the FCS_IPSEC_EXT.1 SFR, the NDPP states "The intent of the above requirement is to use a cryptographic protocol to protect external communications with authorized IT entities that the TOE interacts with to perform its functions. This is not, however, to be used to specify VPN Gateway functionality; a separate VPN Protection Profile should be used in these instances." Therefore, the VPN IPSec feature is not evaluated.

The TOE relies upon the Operational Environment for the following security functionality:

- Audit storage
- Reliable time stamps from a Network Time Protocol (NTP) server

5. Documentation

The following documents, in addition to the ST referenced above, were available for the evaluation. These documents are developed and maintained by 3eTI and delivered to the end user of the TOE:

5.1. User Documentation

Reference Title
3eTI 3e-636-series User's Guide, Jan 2015, Revision B, 29000533-002

6. IT Product Testing

This section describes the testing efforts of the Evaluation Team. The information is derived from the *Evaluator Test Report for 3e-636 Series Network Security Device* document. The purpose of this activity was to confirm that the TOE behaves in accordance with security functional requirements specified in the ST.

6.1. Developer Testing

NDPP evaluations do not require developer testing evidence for assurance activities.

6.2. Evaluator Independent Testing

A test plan was developed in accordance with the Testing Assurance Activities specified in the NDPPv1.1 with Errata 3.

Testing was conducted Testing was conducted January 6-8, 2015 at the 9715 Key West Avenue, Suite 500, Rockville, Maryland, USA, 20850.

The Evaluator successfully performed the following activities during independent testing:

- Placed TOE into evaluated configuration by executing the preparative procedures
- Successfully executed the NDPP Assurance-defined tests including the optional TLS tests
- Planned and executed a series of vulnerability/penetration tests

It was determined after examining the Test Report and full set of test results provided by the evaluators the testing requirements for NDPPv1.1 with Errata #3 are fulfilled.

7. Results of Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.

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 version 3.1 R4 of the CC and the CEM. Additionally the evaluators performed the assurance activities specified in the Protection Profile *U.S. Government Standard Protection Profile for Network Devices*, 08 June 2012, Version 1.1 with Errata 3.

The evaluation determined the TOE meets the SARs contained the PP.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL (proprietary).

Below lists the assurance requirements the TOE was required to be evaluated at Evaluation Assurance Level 1. All assurance activities and work units received a passing verdict. The following components are taken from CC part 3:

- ADV_FSP.1 Basic functional specification
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ALC_CMC.1 Labelling of the TOE
- ALC_CMS.1 TOE CM coverage
- ASE_CCL.1 Conformance claims
- ASE_ECD.1 Extended components definition
- ASE_INT.1 ST Introduction
- ASE_OBJ.1 Security objectives
- ASE_REQ.1 Derived security requirements
- ASE_TSS.1 TOE summary specification
- ATE_IND.1 Independent testing – conformance
- AVA_VAN.1 Vulnerability survey

The evaluators concluded that the overall evaluation result for the target of evaluation is PASS. The validators reviewed the findings of the evaluation team, and have concurred that the evidence and documentation of the work performed support the assigned rating.

7.1. 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:

1. 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 the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PP. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. 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.

8. Validators Comments/Recommendations

The validators were satisfied with the evaluation team's evaluation and testing efforts. The validators did not identify any gaps or missing information.

9. Glossary

9.1.Acronyms

The following are product specific and CC specific acronyms. Not all of these acronyms are used in this document.

BGP	Border Gateway Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	HyperText Transmission Protocol
HTTPS	HyperText Transmission Protocol, Secure
IP	Internet Protocol
IPS	Intrusion Protection System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OSPFv2	Open Shortest Path First
PDF	Portable Document Format
RADIUS	Remote Authentication Dial-In User Service
RIP	Routing Information Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer,
ST	Security Target
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security,
UDP	User Datagram Protocol
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network

10. Bibliography

URLs

[1] Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).

[2] CygnaCom Solutions CCTL (http://www.cygnacom.com).

CCEVS Documents

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, July 2009 Version 3.1 Revision 4 Final, CCMB-2012-09-001.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, July 2009 Version 3.1 Revision 4 Final, CCMB-2012-09-002.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, July 2009, Version 3.1 Revision 4 Final, CCMB-2012-09-003.

[4] Common Methodology for Information Technology Security Evaluation - Evaluation methodology, July 2009, Version 3.1 Revision 4 Final, CCMB-2012-09-004.