National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Allied Telesis, Inc.

Allied Telesis x930 Series Switches

x930 Series Switches with AlliedWare Plus version 5.4.6-1

Report Number: CCEVS-VR-10784-2018
Dated: **May 1, 2018**
Version: **1.1**

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 Panel

Jim Donndelinger

Meredith Hennan

The Aerospace Corporation

Common Criteria Testing Laboratory

Brad Mitchell

Ryan Day

UL Verification Services Inc.

San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both 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 5 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 Common Criteria Evaluation and Validation Scheme (CCEVS) evaluation of the Allied Telesis x930 Series Switches with AlliedWare Plus version 5.4.6-1 Target of Evaluation (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 was completed by UL Verification Services in April 2018. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by UL Verification Services. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements defined in the collaborative Protection Profile for Network Devices, Version 1.0, dated February 27, 2015 [NDcPP].

The Target of Evaluation (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 are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). Based on these findings, 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 Allied Telesis x930 Series Switches are stackable Gigabit layer 3 devices. The Allied Telesis x930 Series Switches come in 28-port and 52-port versions with 10 and 40 Gigabit uplinks.

This table identifies components that must be present in the Operational Environment to support the operation of the TOE.

Component	Description
SSHv2 client	Required for remote administration of the TOE
Syslog Server	Required for remote storage of audit logs
RADIUS server	Optional, but required if the TOE administrator wishes to use RADIUS user authentication.
OCSP responder	Required to provide certificate validity messages to the TOE when presented with x.509v3 certificates.

Table 1: Operational Environment Components

2 Identification of the TOE

Table 2 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 organizations and individuals participating in the evaluation.

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	Allied Telesis x930 Series Switches with AlliedWare Plus version 5.4.6-1
Protection Profile	collaborative Protection Profile for Network Devices, Version 1.0, dated February 27, 2015
Security Target	Allied Telesis x930 Series Switches Security Target, version 1.5, dated April 9, 2018
Dates of Evaluation	October 24, 2016 – April 27, 2018
Conformance Result	PASS
Common Criteria Version	3.1r4
Common Evaluation Methodology (CEM) Version	3.1r4
Evaluation Technical Report (ETR)	17-3347-R-0038 V1.3
Sponsor/Developer	Allied Telesis, Inc.
Common Criteria Testing Lab (CCTL)	UL Verification Services Inc.
CCTL Evaluators	Brad Mitchell, Ryan Day
CCEVS Validators	Jim Donndelinger, Meredith Hennan

Table 2: Product Identification

3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the International interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all international interpretations with effective dates on or before

March 12, 2018.

4 Architectural Information

The TOE is classified as a network device for Common Criteria purposes. The TOE is made up of hardware and software components.

4.1 Architecture Overview

The TOE consists of the following components:

4.1.1 TOE Hardware

The TOE consists of the following hardware. Each hardware model uses a Freescale PowerPC P2040 processor.

- AT-x930-28GTX
- AT-x930-28GPX
- AT-x930-28GSTX
- AT-x930-52GTX
- AT-x930-52GPX

4.1.2 TOE Software

- AlliedWare Plus version 5.4.6-1

The TOE requires the following support from the IT Environment:

4.1.3 TOE IT Environment Hardware/Software/Firmware Requirements

- SSHv2 client
    - Complaint with RFCs 4251, 4252, 4253, 4254, 5656, and 6668
    - Allowing ECDSA P-256 or P-384 Host Authentication
    - Supporting ECDSA P-256, ECDSA P-384, or password based client authentication
    - Supporting ECDH P-256 or ECDH P-384 Key Exchange
    - Supporting AES CBC with 128 or 256 bit keys
    - Supporting HMAC-SHA-256
- Syslog server
    - Compliant with RFCs 5424 and 5425
    - Allowing connections using TLS_RSA_WITH_AES_128_CBC_SHA
- RADIUS server
    - Compliant with RFCs 2865, 6613, and 6614
    - Allowing connections using TLS_RSA_WITH_AES_128_CBC_SHA
- OCSP responder(s)
    - Providing certificate status for the Syslog and RADIUS server certificates

5 Security Policy

This section contains the product features and denotes which are within the logical boundaries of the TOE. The following Security Functions are supported by the TOE:

5.1 Audit

The TOE will audit all events and information defined in **Error! Reference source not found.**. The TOE will also include the identity of the user that caused the event (if applicable), date and time of the event, type of event, and the outcome of the event. The TOE protects storage of audit information from unauthorized access, deletion, or modification. The TOE can transmit audit data to an external IT entity using the Syslog over TLS protocol.

5.2 Cryptographic Operations

The TOE uses cryptographic algorithms and protocols to protect Syslog server communication, RADIUS sever communications, remote administrator sessions, test the TOE itself, and verify the integrity of updates to the TOE.

The TSF zeroizes all plaintext secret and private cryptographic keys and CSPs once they are no longer required.

5.3 Identification and Authentication

The TOE supports passwords consisting of alphanumeric and special characters. The TSF also allows administrators to set a minimum password length and support passwords with 15 characters or more.

The TOE requires all administrative-users to authenticate. The TOE allows the following unauthenticated actions:

- Viewing the warning banner
- Responding to ICMP echo requests
- Performing ARP
- Performing routing services (e.g. RIP, OSPF)

5.4 Security Management

The TOE can be administered via a local console port or remotely over SSH. Both methods of administration present the user with a CLI. Authorized administrators are assigned the Security Administrator role when they login.

5.5 Protection of the TSF

The TOE protects itself by:

- Preventing the reading of plaintext passwords.
- Preventing the reading of secret and private keys.
- Providing reliable time stamps for itself.
- Running a suite of self-tests during the initial start-up (upon power on) to demonstrate the correction operation of the TSF.

- Verifying firmware updates to the TOE using a published hash prior to installing those updates.

5.6 TOE Access

For local console sessions and remote SSH sessions, the TSF terminates sessions after an administrator configured inactivity period. Before establishing an administrative user session, the TOE is capable of displaying a configurable advisory notice and consent warning message regarding unauthorized use of the TOE.

5.7 Trusted Path/Channels

The TOE uses TLS to provide a trusted communication channel with the Syslog server and RADIUS server.

The TOE permits remote administrators to connect using SSH.

6 TOE Security Environment

6.1 Secure Usage Assumptions

The following assumptions are made about the usage of the TOE:

Table 3: Assumptions

Assumption	Description
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose Applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g, firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack

Table 3: Assumptions	
Assumption	Description
	malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.

6.2 Threats Countered by the TOE

The TOE is designed to counter the following threats:

Table 4: Threats	
Threat	Description
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle

Table 4: Threats	
Threat	Description
	attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_FAILURE	A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers.

6.3 Organizational Security Policies

The TOE enforces the following OSPs:

Table 5: Organizational Security Policies	
OSP	Description
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

6.4 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 level of assurance for this evaluation is defined within the NDcPP.

- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- 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 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs and applicable Technical Decisions. Any additional security related functional capabilities included in the product were not covered by this evaluation and shall not be used in the evaluated configuration, including:
    - Allied Telesis Management Framework
    - VCStack (Virtual Chassis Stacking)
    - Long-distance Stacking

7 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the Allied Telesis x930 Series Switches. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with **bold** titles.
- Documentation that was used as evidence but is not delivered is shown in a normal typeface.
- Documentation that is delivered as part of the product but was not used as evaluation is shown with a hashed background.

The TOE is shipped directly to the end-user. The guidance documents are provided inside the packaging, and on the vendor website, and apply to the CC Evaluated configuration:

7.1 Design Documentation

Document	Revision	Date
Allied Telesis x930 Series Switches Basic Functional Specification	C613-05048-00 REV A	

7.2 Guidance Documentation

Document	Revision	Date
Common Criteria Operational User Guidance and Preparative Procedures	**C613-02065-00 REV K**	

Document	Revision	Date
Command Reference for AlliedWare Plus™ Version 5.4.6-1.x	**C613-50100-01 REV C**	**2016**
Installation Guide for Stand-alone Switches	**C613-002100 REV C**	**2015**
AlliedWare Plus™ Best Practice Guide		
AlliedWare Plus™ Operating System Log Message Reference	**C613-50013-00 REV G**	**2016**
Bootloader and Start-Up Feature Overview and Configuration Guide	**C613-22003-00 REV A**	
Logging Feature Overview and Configuration Guide	**C613-22059-00 REV A**	
RADIUS Feature Overview and Configuration Guide	**C613-22056-00 REV A**	
Secure Shell (SSH) Feature Overview and Configuration Guide	**C613-22051-00 REV A**	

7.3 Configuration Management and Lifecycle

Document	Revision	Date
Allied Telesis x930 Series Switches Labelling of the TOE	C613-05046-00 REV A	October 18, 2016

7.4 Test Documentation

Document	Revision	Date
17-3347-R-0001 V1.6 Allied Telesis x930 Test Report	V1.6	April 27, 2018

7.5 Vulnerability Assessment Documentation

Document	Revision	Date

17-3347-R-0001 V1.6 Allied Telesis x930 Test Report	V1.6	April 27, 2018

7.6 Security Target

Document	Revision	Date
Allied Telesis x930 Series Switches Security Target	1.5	April 9, 2018

To use the product in the evaluated configuration, the product must be configured as specified in the guidance documentation listed in Section 7.2, and specifically follow the guidance in the Common Criteria Operational User Guidance and Preparative Procedures. 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. Consumers are encouraged to download this CC configuration guide from the NIAP website.

8 Evaluated Configuration

The TOE consists of the following Allied Telesis x930 Series Switch network device models running AlliedWare Plus version 5.4.6-1 software with a Freescale PowerPC P2040 processor as configured in accordance with the Common Criteria Operational User Guidance and Preparative Procedures:

- AT-x930-28GTX
- AT-x930-28GPX
- AT-x930-28GSTX
- AT-x930-52GTX
- AT-x930-52GPX

8.1 Excluded Functionality

The following functionality is excluded from the evaluated configuration:

- Allied Telesis Management Framework
- VCStack (Virtual Chassis Stacking)
- Long-distance Stacking

9 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. This information is derived from the proprietary Evaluation Test Report for the TOE, as characterized in the Assurance Activity Report for Allied Telesis x930 Series Switches, version 1.5, April 30, 2018, which is publicly available.

9.1 Developer Testing

The Vendor performed basic functional regression testing.

9.2 Evaluation Team Independent Testing

The CCTL performed common criteria testing according to the requirements of the Security Assurance Activities in the collaborative Protection Profile for Network Devices, Version 1.0, Feb. 27, 2015. The results of that testing were provided to NIAP in the form of the evaluation technical report. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here. Section 1 of the AAR may be referenced for a more detailed overview of the test bed configuration and software tools used during the testing activities.

10 Results of the Evaluation

The results of the assurance requirements are generally described in this section and in the AAR and presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that 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 in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDcPP.

10.1 Evaluation of Security Target

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 TOE that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the NDcPP 1.0.

The validator 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.

10.2 Evaluation of Development Documentation

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 Assurance Activities specified in the NDcPP 1.0 related to the examination of the information contained in the TOE Summary Specification.

The validator 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.

10.3 Evaluation of Guidance Documents

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 Assurance Activities specified in the NDcPP 1.0 and related to the examination of the information contained in the operational guidance documents.

The validator 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.

10.4 Evaluation of Life Cycle Support Activities

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

The validator 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.

10.5 Evaluation of Test Documentation and the Test Activity

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 1.0 and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validator 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 1.0, and that the conclusion reached by the evaluation team was justified.

10.6 Vulnerability Assessment Activity

The evaluators searched for vulnerabilities known to exist in the product by searching the NVD and CVEDetails for the following keywords:

- Allied Telesis
- Allied Telesys
- X930

The evaluator received results that were not the TOE and worked with the vendor engineering team to ensure that one result related to a non-TOE version of firmware was not present in the TOE.

In addition, the evaluators performed searches of the NVD and CVEDetails.com between December 10, 2016 and January 17, 2017, and again on April 27, 2018, searching for vulnerabilities associated with the third-party modules known to be in use in the TOE. The evaluator worked with the vendor engineers to ensure that all detected vulnerabilities were patched, not applicable to the common criteria evaluated configuration, or not applicable to the TOE.

The validator 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 Assurance Activities in the NDcPP 1.0, and that the conclusion reached by the evaluation team was justified.

10.7 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 Assurance Activities in the NDcPP 1.0 and correctly verified that the product meets the claims in the ST.

11 Validator Comments/Recommendations

All validator comments are covered in the Clarifications of Scope section.

12 Security Target

Allied Telesis x930 Series Switches Security Target, V1.5, April 9, 2018

13 Terms

13.1 Acronyms

CC	Common Criteria
CSP	Critical Security Parameters
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication 140-2
IDS	Intrusion Detection System
IPS	Intrusion Prevention System

I/O	Input/Output
MIB	Management Information Base
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PP	Protection Profile
SF	Security Functions
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

14 Bibliography

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

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

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

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

[5] collaborative Protection Profile for Network Devices, Version 1.0, February 27, 2015

[6] Supporting Document Mandatory Technical Document Evaluation Activities for Network Device cPP, Version 1.0, February 2015