National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Klas Telecom, Inc.

VoyagerTDC 10G Switch v2.0

Report Number: CCEVS-VID10911-VR-2018
Dated: November 19, 2018
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Acknowledgements

Validation Team

Michelle Carlson

MITRE Corporation, Bedford, MA

Sheldon Durrant

MITRE Corporation, Bedford, MA

Patrick Mallett, PhD

MITRE Corporation, McLean, VA

Common Criteria Testing Laboratory

Michael Baron

Gerrit Kruitbosh

UL Verification Services, Inc.

San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report documents the NIAP validators' assessment of the CCEVS evaluation of the VoyagerTDC 10G Switch, version 2.0.

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 evaluated.

The Klas Voyager TDC Switch running KlasOS firmware provides connectivity to multiple devices into the same network segment. Authentication can be provided locally or over a trusted channel using SSH and all logs can be securely sent to a syslog server, protected using an SSH tunnel.

Table 1 identifies components that must be present in the Operational Environment to support the operation of the TOE.

Component	Description
Syslog Server	RFC 5424 compliant syslog server
Local Console	The local console must provide a DB-9 serial port and be capable of supporting a VT-100 compatible terminal or emulator

SSH Client (remote administration of the TOE)	An administrative remote console may be used to administer the TOE over SSH. The remote console must implement SSH conformant to RFCs 4251, 4252, 4253, 4254, 5656, and 6668, and provide the following algorithms and parameters:
	• Password authentication.
	  ○ Optionally, ECDSA public key authentication using NIST curves P-256 or P-384.
	  ○ Optionally, RSA public key authentication using 2048, 3072, or 4096-bit keys
	• AES-CBC-128 or AES-CBC-256 encryption.
	• HMAC-SHA1, HMAC-SHA2-256, or HMAC-SHA2-512 for message authentication.
	• Key exchange using Diffie-Hellman Group 14, ECDH over NIST P-256, or ECDH over NIST P-384.

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	VoyagerTDC 10G Switch, version 2.0
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, dated March 14, 2018
Security Target	Klas Telecom VoyagerTDC 10G Switch v2.0 Security Target, v1.1.2, November 16, 2018
Dates of Evaluation	March 2018 – October 2018
Conformance Result	Pass
Common Criteria Version	3.1r4
Common Evaluation Methodology (CEM) Version	3.1r4
Evaluation Technical Report (ETR)	18-4188-R-0024 V1.2
Sponsor/Developer	Klas Telecom, Inc.
Common Criteria Testing Lab (CCTL)	UL Verification Services, Inc.
CCTL Evaluators	Michael Baron
CCEVS Validators	Michelle Carlson, Sheldon Durrant, Patrick Mallett

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 May 30, 2018.

4 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:

- Audit
- Cryptography
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

4.1 Audit

- The TOE will audit all events and information defined in Table 3: Auditable Events of the ST.
- 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 deletion.
- The TOE can transmit audit data to an external IT entity using SSH protocol.

4.2 Cryptography

The TSF performs the following cryptographic operations:

- SSHv2 using
    - AES-CBC-128 or AES-CBC-256 for encryption;
    - DH Group 14, or NIST P-256 / P-384 for key exchange;
    - HMAC SHA1, HMAC-SHA2-256, or HMAC-SHA2-512 for message authentication;
    - RSA public key authentication using 2048, 3072 or 4096-bit keys & EC public key authentication using NIST P-256 or P-384.

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

4.3 Identification and Authentication

- The TSF 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 TSF supports public key-based authentication methods.
- The TSF requires all administrative-users to authenticate before allowing the user to perform any actions other than:
    - Viewing the warning banner.

4.4 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs via a local serial console connection or remote SSH session. The TOE provides the ability to securely manage:

- All TOE administrative users, including identification and authentication parameters and credentials.
- Timestamps maintained by the TOE.
- Updates to the TOE.

Only one administrative user can be created on the TOE, and the administrative user can perform all of the above security relevant management functions. Administrators can create configurable login banners to be displayed at time of login and can also define an inactivity timeout to terminate sessions after a set period of inactivity.

4.5 Protection of the TSF

- The TSF prevents the reading of secret and private keys.
- The TOE provides reliable time stamps for itself.
- The TOE runs a suite of self-tests during the initial start-up (upon power on) to demonstrate the correction operation of the TSF.
- The TOE provides a means to verify firmware/software updates to the TOE using a digital signature mechanism prior to installing those updates.

4.6 TOE Access

- The TOE, for local interactive sessions, shall terminate the session after an Authorized Administrator-specified period of session inactivity.
- The TOE terminates a remote interactive session after an Authorized Administrator-configurable period of session inactivity.
- The TOE allows Administrator-initiated termination of the Administrator's own interactive session.
- Before establishing an administrative user session, the TOE is capable of displaying an Authorized Administrator-specified advisory notice and consent warning message regarding unauthorized use of the TOE.

4.7 Trusted Path/Channels

- The TOE uses SSH to provide a trusted communication channel between itself and all authorized IT entities that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.
- The TOE permits the TSF or the authorized IT entities to initiate communication via the trusted channel.
- The TOE permits remote administrators to initiate communication via the trusted path.

- The TOE requires the use of the trusted path for initial administrator authentication and all remote administration actions.

5 TOE Security Environment

5.1 Secure Usage Assumptions

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

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 a 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 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.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5.2 Threats Countered by the TOE

The TOE is designed to counter the following threats:

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 tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
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 includes 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	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

5.3 Organizational Security Policies

The TOE enforces the following OSPs:

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 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 collaborative Protection Profile for Network Devices.
- Consistent with the expectations of the PP, 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 PP. Any additional security related functional capabilities included in the product were not covered by this evaluation.

7 Architectural Information

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

7.1 Architecture Overview

The TOE consists of a single hardware and software component. The TOE is not a distributed nor a composed TOE. The TOE provides connectivity to multiple devices into the same network segment. Authentication can be provided locally or over a trusted channel using SSH and all logs can be securely sent to a syslog server. The TOE provides a Command Line Interface (CLI) for device configuration as well as TenGigabit Ethernet, and layer 2 high-speed switching and removable storage using the VIK.

7.1.1 TOE Hardware

The TOE consist of the following hardware:

- KLAS-VOY-TDC-R2.0

7.1.2 TOE Software

The TOE runs the following software:

- KlasOS fastnet v5.2.0rc7

8 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the VoyagerTDC 10G Switch. 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 to the user is transport protected packaging. The guidance documents are provided via Klas' user web portal. This guidance documentation applies to the CC Evaluated configuration:

8.1 Design Documentation

Document	Revision	Date
NDcPPv2.0 Assurance Requirements Documentation, Development, Lifecycle, and Entropy Assessment	2	N/A

8.2 Guidance Documentation

Document	Revision	Date
Common Criteria Operational User Guidance	**1.1**	**June 2018**

8.3 Configuration Management and Lifecycle

Document	Revision	Date
NDcPPv2.0 Assurance Requirements Documentation, Development, Lifecycle, and Entropy Assessment	2	N/A

8.4 Test Documentation

Document	Revision	Date
Klas Telecom VoyagerTDC 10G Switch NDcPP 2.0e+20180314 Test Plan	1.7	November 2018

8.5 Vulnerability Assessment Documentation

Document	Revision	Date
18-4188-R-0017 V1.4 Klas AVA_VAN	1.4	November 19, 2018

8.6 Security Target

Document	Revision	Date
Klas Telecom VoyagerTDC 10G Switch v2.0 Security Target	1.1.2	November 16, 2018

9 IT Product Testing

This section describes the testing efforts of the Developer and the Evaluation Team.

9.1 Developer Testing

The developer performed testing on the TOE only to the extent to verify the fulfilment of meeting the SFRs as claimed in the [ST]. No outputs from the developer's testing were included as part of this evaluation. All testing to meet ATE was performed by the CCTL as described in Section 8.2 below.

9.2 Evaluation Team Independent Testing

The evaluation team performed the independent testing activities to confirm the TOE operates to the TOE security functional requirements as specified in the ST for a product claiming conformance to the collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, dated March 14, 2018. The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the NDcPP. The evaluation team, in conjunction with Lightship Security, devised a Test Plan based on the Testing Assurance Activities specified in [NDcPP]. The Test Plan described how each test activity was to be performed. The evaluation team executed the tests specified in the Test Plan and documented the results in the Evaluation Technical Report. The evaluation team consisted of Michael C. Baron from the CCTL and Greg McLearn from Lightship Security.

Testing was performed by Greg McLearn of Lightship Security with support from Michael C. Baron from UL. The test laboratory was configured by UL and physically located at UL San Luis Obispo's office in an access controlled room. Lightship Security was provided VPN access (using IPsec) to this isolated testing environment to execute the test plan. The test plan was reviewed and approved by the CCTL prior to execution by Lightship. The test evidence and report from Lightship were reviewed by the CCTL ensure the test plan was met. The CCTL verified that all test evidence supported the conclusions of the test report.

FTP_ITC.1 Inter-TSF trusted channel, Test 4 was performed by Lightship Security, with support from UL for physical removal of cabling. This testing was performed in real time with both Lightship and UL on the phone to synchronize the testing.

The Test Plan described how each test activity was to be performed. The evaluation team executed the tests specified in the Test Plan and documented the results in a proprietary 'Test Document' listed above in Section 7.3.

The results of the testing are summarized in the publicly available Assurance Activity Report for this evaluation. Independent testing was performed at the UL facility in San Luis Obispo, CA. The hardware/software was provided in the same manner that customers would receive it. The evaluation team installed and configured the TOE in accordance with the vendor provided guidance documentation and performed the testing procedures as described in the Test Documentation.

9.3 Vulnerability Analysis

The evaluator performed the AVA_VAN.1 assurance activities in accordance with Section 5.6 of the [SD]. These assurance activities included developing 'Flaw Hypothesis' based on any findings of the evaluator during testing and searches for publically known vulnerabilities based on keywords derived from components of the evaluation, and any hypothesis derived from specific network packet fuzz testing.

Public searches were conducted on all relevant keywords found within the evaluation documentation and the TOE itself. The search was originally performed on September 6, 2018 and again on November 11, 2018. Keywords included the following words derived by the evaluator:

- OpenSSHv7.7
- Klas
- KlasOS
    - Relevant version: KlasOS fastnet v5.2.0rc7
- Voyager
    - Relevant name: VoyagerTDC 10G Switch
- OpenSSL 1.0.1h

The following keywords were mandatory as per [SD] Section A.1.1, #622:

- The terms “router” and “switch” (or similar generic term describing the device type of the TOE)
    - Since the TOE was a network switch, the evaluator searched on the keyword “switch”
- The following protocols:
    - TCP
- Any protocols not listed above supported (through an SFR) by the TOE (these will include at least one of the remote management protocols (IPsec, TLS, SSH))
    - SSH is the only supported management protocol. The evaluator was able to more accurately define the version of SSH being utilized by the TOE using packet analysis. The following search term was utilized:
        - OpenSSHv7.7
- The TOE name (including appropriate model information as appropriate) :
    - KLAS-VOY-TDC-R2.0

Each keyword listed above was used as a search term with each of the following publically available resources:

- http://cve.mitre.org/cve/
- https://www.cvedetails.com/vulnerability-search.php
- http://www.kb.cert.org/vuls/html/search
- www.exploitsearch.net
    - Note: This site was unreachable during the evaluation process
- www.securiteam.com
- http://nessus.org/plugins/index.php?view=search
- http://www.zerodayinitiative.com/advisories

- https://www.exploit-db.com/
- https://www.rapid7.com/db/vulnerabilities

All identified vulnerabilities were mitigated and patched by the vendor. The results of the searches for publically known vulnerabilities can be found in the proprietary Detailed Test Report.

The evaluator also performed the following network packet fuzzing tests:

- Mutated packets carrying each 'Type' and 'Code' value that is undefined in the relevant RFC for each of ICMPv4 (RFC 792)
- Mutated packets carrying each 'Transport Layer Protocol' value that is undefined in the respective RFC for IPv4 (RFC 791)

The evaluator checked that the TOE did not enter into a failure state. The evaluator verified that the TOE was operating as expected after the fuzzing tool completed sending its iterations of IP packets by authenticating to the TOE and running various commands and log output commands, looking at memory levels and processor consumption.

No flaw hypothesis were derived from the results of the fuzz testing.

The evaluator has examined the Type 1 flaw hypotheses specified in the [SD] in section A.1.1 (i.e. the flaws listed in the previous bullet) and the Type 2 flaw hypotheses specified in the [SD] by the iTC in Section A.1.2.

The evaluation team developed Types 3 and 4 flaw hypotheses in accordance with [SD] Sections A.1.3, A.1.4, and A.2. No residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the CB in accordance with the guidance in the CEM.

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.

11 Validator Comments/Recommendations

The evaluation team performed the independent testing activities to confirm the TOE operates to the TOE security functional requirements as specified in the ST for a product claiming conformance to the collaborative Protection Profile for Network Devices, Version 2.0E, March

18, 2018. The Test Plan described how each test activity was to be performed. The evaluation team created and executed the tests specified in the Test Plan and documented the results in the Evaluation Technical Report.

A Lightship Security SSH testing tool was used to execute the test plan. Testing was performed by a Lightship Security testing representative with oversight and support from UL evaluators. The test laboratory was configured by UL at its facility physically located in San Luis Obispo, CA in an access-controlled room. The Lightship tester was provided VPN access (using IPsec) to this isolated testing environment to help execute the test plan. The test plan and evidence and report from Lightship were reviewed by the UL to ensure completeness.

The validation team determined that the test plan and evidence provided was sufficiently detailed. The validators were able to verify the manual interactions of the remote testers at a granularity that showed precisely what the SSH tool was doing. The internal test environment was restricted so the only thing that the Lightship tester could do through the VPN was exercise the TOE test harness. Thus, the validation team verified that all test evidence supported the conclusions of the test report. The validation team judged that UL had full visibility and oversight over testing and process.

Note the following from Labgram #78: “Remote testing is generally not acceptable. It is very difficult for the CCTLs to ensure proper control over a remote test environment, and difficult for validators to ascertain if the proper control was maintained. Therefore, remote testing or remote observation of testing being done by someone other than the evaluators is only acceptable on a CCEVS-approved case-by-case basis.”

12 Security Target

Klas Telecom VoyagerTDC 10G Switch v2.0 Security Target, version 1.1.2, November 16, 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 July 2009, Version 3.1 Revision 4, CCMB-2012-09-001.

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

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

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

[5] collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, March 14, 2018

[6] Supporting Document Mandatory Technical Document Evaluation Activities for Network Device cPP, Version 2.0 + Errata 20180314, March 2018