National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

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

Report Number: CCEVS-VR-PP-0063
Dated: 30 December 2020
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

Common Criteria Testing Laboratory
Base and Additional Requirements
UL Verification Services Inc.
San Luis Obispo, California

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the collaborative Protection Profile for Network Devices, Version 2.2E (CPP_ND_V2.2E). It presents a summary of the CPP_ND_V2.2E and the evaluation results.

UL Verification Services Inc. (Formerly InfoGard), located in San Luis Obispo, California, performed the evaluation of CPP_ND_V2.2E concurrent with the first product evaluation against the cPP's requirements. The evaluated product was Bivio 6310-NC.

This evaluation addressed the base requirements of CPP_ND_V2.2E and several of the additional requirements contained in Appendices A and B. The Validation Report (VR) author independently performed an additional review of the cPP as part of the completion of this VR, to confirm it meets the claimed APE assurance requirements. During the evaluation, minor issues were identified with the APE_ECD and APE_REQ work units. Specifically, it was determined that some additional clarity should be provided for some ECDs and some operations were incorrectly performed. However, upon further review, the errors were deemed minor as they would not have any impact on any evaluation. Therefore, the issues identified were forwarded to the Network iTC Interpretation Team (NIT) for future NDcPP revisions and were not considered PP deficiencies.

The evaluation determined that the CPP_ND_V2.2E is both Common Criteria Part 2 Extended and Part 3 Conformant. The cPP identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory (CCTL) using the Common Methodology for IT Security Evaluation (Version 3.1, Release 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Release 5). The Security Target (ST) includes material from the CPP_ND_V2.2E; completion of the ASE work units satisfied the APE work units for CPP_ND_V2.2E.

The evaluation laboratory conducted this evaluation in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence given.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called CCTLs. CCTLs evaluate products against PPs and cPPs that contain Evaluation Activities, which are interpretations of CEM work units specific to the technology described by the PP or cPP.

In order to promote thoroughness and efficiency, the evaluation of CPP_ND_V2.2E was performed concurrent with the first product evaluation against the cPP's requirements. In this case, the Target of Evaluation (TOE) was Bivio 6310-NC, evaluated by UL Verification Services Inc. (Formerly InfoGard), located in San Luis Obispo, California, United States of America. The Validation Report (VR) author independently performed an additional review of the cPP as part of the completion of this VR, to confirm it meets the claimed APE assurance requirements.

These evaluations addressed the base requirements of CPP_ND_V2.2E, and several of the additional requirements contained in Appendices A and B. CPP_ND_V2.2E contains a set of base requirements that all conformant STs must include, and additionally contains optional and selection-based requirements. Optional requirements may or may not be included within the scope of the evaluation, depending on whether the vendor provides that functionality within the tested product and chooses to include it inside the TOE boundary. Selection-based requirements are those that must be included based upon the selections made in other requirements and the capabilities of the TOE.

The initial use of the cPP addresses (in terms of the cPP evaluation) the base requirements and any additional requirements incorporated into the initial ST. The VR authors have evaluated all discretionary requirements that were not claimed in the initial TOE evaluation as part of the evaluation of the APE_REQ work units performed against CPP_ND_V2.2E. When an evaluation laboratory evaluates a TOE against any additional requirements not already referenced in this VR through an existing TOE evaluation, the VR may be amended to include references to this as additional evidence that the corresponding portions of CPP_ND_V2.2E were evaluated.

The following identifies the cPP subject of the evaluation or validation, as well as the supporting information from the evaluation performed against this cPP.

Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2E, 23 March 2020
ST (Base)	Bivio 6310-NC Security Target, Version 0.8, Nov 25, 2020
Assurance Activity Report (Base)	Assurance Activity Report Bivio Networks, Inc., Bivio 6310-NC, Version 1.2, 02 December 2020
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5
Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
CCTL	UL Verification Services Inc. San Luis Obispo, California 93401

3 CPP_ND_V2.2E Description

The CPP_ND_V2.2E specifies information security requirements for network device management, as well as the assumptions, threats, organizational security policies, objectives, and requirements of a compliant TOE.

A Network Device (ND) in the context of this VR is a device that is connected to a network and has an infrastructure role within that network. The TOE may be standalone or distributed, where a distributed TOE is one that requires multiple distinct components to operate as a logical whole in order to fulfil the requirements of the cPP.

4 Security Problem Description and Objectives

4.1 Assumptions

The following table contains applicable assumptions.

Table 1: Assumptions

Assumption Name	Assumption Definition
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.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
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). In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device 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 and PP-Modules for particular types of Network Devices (e.g., firewall).
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 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 does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does 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. For virtual network devices (vNDs), this assumption applies to the physical platform on which the VM runs.
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.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys,

Assumption Name	Assumption Definition
	keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
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 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. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.VS_CORRECT_CONFIGURATION (applies to vNDs only)	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.
A.VS_ISOLATON (applies to vNDs only)	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
A.VS_REGULAR_UPDATES (applies to vNDs only)	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.VS_TRUSTED_ADMINISTRATOR (applies to vNDs only)	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.

4.2 Threats

The following table contains applicable threats.

Table 2: Threats

Threat Name	Threat Definition
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_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

Threat Name	Threat Definition
	an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
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.
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.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.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.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.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.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.

4.3 Organizational Security Policies

The following table contains applicable organizational security policies.

Table 3: Threats

Threat Name	Threat Definition
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.

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 4: Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
The TOE does not list and security objectives other than the operation environment objectives.	

The following table contains security objectives for the Operational Environment.

Table 5: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
OE.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs, the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.
OE.NO_GENERAL_PURPOSE	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. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures 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. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.

Environmental Security Objective	Environmental Security Objective Definition
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.VM_CONFIGURATION (applies to vNDs only)	For vNDs, the Security Administrator ensures that the VS and VMs are configured to • reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and • correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting). The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualisation features such as cloning, save/restore, suspend/resume, and live migration. If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.

5 Functional Requirements

As indicated above, requirements in the CPP_ND_V2.2E are comprised of the "base" requirements and additional requirements that are optional or selection-based. The following table contains the "base" requirements that were validated as part of the evaluation activities referenced above.

Table 6: Base Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	Bivio 6310-NC
	FAU_GEN.2: User Identity Association	Bivio 6310-NC
	FAU_STG_EXT.1: Protected Audit Event Storage	Bivio 6310-NC
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation	Bivio 6310-NC
	FCS_CKM.2: Cryptographic Key Establishment	Bivio 6310-NC
	FCS_CKM.4: Cryptographic Key Destruction	Bivio 6310-NC
	FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)	Bivio 6310-NC
	FCS_COP.1/Hash: Cryptographic Operation (Hash Algorithm)	Bivio 6310-NC
	FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)	Bivio 6310-NC
	FCS_COP.1/SigGen: Cryptographic Operation (Signature Generation and Verification)	Bivio 6310-NC
	FCS_RBG_EXT.1: Random Bit Generation	Bivio 6310-NC
FIA: Identification and Authentication	FIA_AFL.1: Authentication Failure Management	Bivio 6310-NC
	FIA_PMG_EXT.1: Password Management	Bivio 6310-NC
	FIA_UAU.7: Protected Authentication Feedback	Bivio 6310-NC
	FIA_UAU_EXT.2: Password-Based Authentication Mechanism	Bivio 6310-NC
	FIA_UIA_EXT.1: User Identification and Authentication	Bivio 6310-NC
FMT: Security Management	FMT_MOF.1/ManualUpdate: Management of Security Functions Behavior	Bivio 6310-NC
	FMT_MTD.1/CoreData: Management of TSF Data	Bivio 6310-NC
	FMT_SMF.1: Specification of Management Functions	Bivio 6310-NC
	FMT_SMR.2: Restrictions on Security Roles	Bivio 6310-NC
FPT: Protection of the TSF	FPT_APW_EXT.1: Protection of Administrator Passwords	Bivio 6310-NC
	FPT_SKP_EXT.1: Protection of TSF Data (for Reading of all Pre-Shared, Symmetric and Private Keys)	Bivio 6310-NC

Requirement Class	Requirement Component	Verified By
	FPT_STM_EXT.1: Reliable Time Stamps	Bivio 6310-NC
	FPT_TST_EXT.1: TSF Testing	Bivio 6310-NC
	FPT_TUD:_EXT.1 Trusted Update	Bivio 6310-NC
FTA: TOE Access	FTA_SSL.3: TSF-Initiated Termination	Bivio 6310-NC
	FTA_SSL.4: User-Initiated Termination	Bivio 6310-NC
	FTA_SSL_EXT.1: TSF-Initiated Session Locking	Bivio 6310-NC
	FTA_TAB.1: Default TOE Access Banners	Bivio 6310-NC
FTP: Trusted Path/Channel	FTP_ITC.1: Inter-TSF Trusted Channel	Bivio 6310-NC
	FTP_TRP.1/Admin: Trusted Path	Bivio 6310-NC

The following table contains the "**Optional**" requirements contained in Appendix A, and an indication of how those requirements were evaluated (from the list in the *Identification* section above). If no completed evaluations have claimed a given optional requirement, the VR author has evaluated it through the completion of the relevant APE work units and has indicated its verification through "cPP Evaluation."

Table 7: Optional Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_STG.1: Protected Audit Trail Storage	Bivio 6310-NC
	FAU_STG_EXT.2/LocSpace: Counting Lost Audit Data	PP Evaluation
	FAU_STG_EXT.3/LocSpace: Action in Case of Possible Audit Data Loss	Bivio 6310-NC
FCO: Communication	FCO_CPC_EXT.1: Component Registration Channel Definition	PP Evaluation
FCS: Cryptographic Support	FCS_DTLSC_EXT.2: DTLS Client Support for Mutual Authentication	PP Evaluation
	FCS_DTLSS_EXT.2: DTLS Server Support for Mutual Authentication	PP Evaluation
	FCS_TLSC_EXT.2: TLS Client Support for Mutual Authentication	PP Evaluation
	FCS_TLSS_EXT.2: TLS Server Support for Mutual Authentication	PP Evaluation
FIA: Identification and Authentication	FIA_X509_EXT.1/ITT: X.509 Certificate Validation	PP Evaluation
FPT: Protection of the TSF	FPT_ITT.1 Basic Internal TSF Data Transfer Protection	PP Evaluation
FTP: Trusted Path/Channels	FTP_TRP.1/Join: Trusted Path	PP Evaluation

The following table contains the "**Selection-Based**" requirements contained in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the

Identification section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant APE work units and has indicated its verification through "cPP Evaluation."

Table 8: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN_EXT.1: Security Audit Data Generation for Distributed TOE Component	PP Evaluation
	FAU_STG_EXT.4: Protected Local Audit Event Storage for Distributed TOEs	PP Evaluation
	FAU_STG_EXT.5: Protected Remote Audit Event Storage for Distributed TOEs	PP Evaluation
FCS: Cryptographic Support	FCS_DTLSC_EXT.1: DTLS Client Protocol Without Mutual Authentication	PP Evaluation
	FCS_DTLSS_EXT.1: DTLS Server Protocol Without Mutual Authentication	PP Evaluation
	FCS_HTTPS_EXT.1: HTTPS Protocol	PP Evaluation
	FCS_IPSEC_EXT.1: IPsec Protocol	PP Evaluation
	FCS_NTP_EXT.1: NTP Protocol	Bivio 6310-NC
	FCS_SSHC_EXT.1: SSH Client Protocol	Bivio 6310-NC
	FCS_SSHS_EXT.1: SSH Server Protocol	Bivio 6310-NC
	FCS_TLSC_EXT.1: TLS Client Protocol Without Mutual Authentication	PP Evaluation
	FCS_TLSS_EXT.1: TLS Server Protocol Without Mutual Authentication	Bivio 6310-NC
FIA: Identification and Authentication	FIA_X509_EXT.1/Rev: X.509 Certificate Validation	Bivio 6310-NC
	FIA_X509_EXT.2: X.509 Certificate Authentication	Bivio 6310-NC
	FIA_X509_EXT.3: X.509 Certificate Requests	Bivio 6310-NC
FMT: Security Management	FMT_MOF.1/AutoUpdate: Management of Security Functions Behaviour	PP Evaluation
	FMT_MOF.1/Functions: Management of Security Functions Behaviour	Bivio 6310-NC
	FMT_MOF.1/Services: Management of Security Functions Behaviour	Bivio 6310-NC
	FMT_MTD.1/CryptoKeys: Management of TSF Data	Bivio 6310-NC
FPT: Protection of the TSF	FPT_TUD_EXT.2: Trusted Update Based on Certificates	PP Evaluation

6 Assurance Requirements

The following are the assurance requirements contained in the CPP_ND_V2.2E.

Table 10: Assurance Requirements

Requirement Class	Requirement Component	Verified By
ADV: Development	ADV_FSP.1 Basic Functional Specification	Bivio 6310-NC
AGD: Guidance Documents	AGD_OPE.1: Operational User Guidance	Bivio 6310-NC
	AGD_PRE.1: Preparative Procedures	Bivio 6310-NC
ALC: Life-cycle Support	ALC_CMC.1: Labelling of the TOE	Bivio 6310-NC
	ALC_CMS.1: TOE CM Coverage	Bivio 6310-NC
ASE: Security Target	ASE_CCL.1: Conformance Claims	Bivio 6310-NC
	ASE_ECD.1: Extended Components Definition	Bivio 6310-NC
	ASE_INT.1: ST Introduction	Bivio 6310-NC
	ASE_OBJ.1: Security Objectives for the Operational Environment	Bivio 6310-NC
	ASE_REQ.1: Stated Security Requirements	Bivio 6310-NC
	ASE_SPD.1: Security Problem Definition	Bivio 6310-NC
	ASE_TSS.1: TOE Summary Specifications	Bivio 6310-NC
ATE: Tests	ATE_IND.1: Independent Testing – conformance	Bivio 6310-NC
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	Bivio 6310-NC

7 Results of the Evaluation

Note that for APE elements and work units that are identical to ASE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

Table 11: Evaluation Results

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	PP Evaluation
APE_ECD.1	Pass	PP Evaluation
APE_INT.1	Pass	PP Evaluation
APE_OBJ.1	Pass	PP Evaluation
APE_REQ.1	Pass	PP Evaluation
APE_SPD.1	Pass	PP Evaluation

8 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology as interpreted by the supplemental guidance in the CPP_ND_V2.2E Evaluation Activities to determine whether or not the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

9 Bibliography

The Validation Team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, dated: April 2017.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 5, dated: April 2017.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 5, dated: April 2017.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, dated: April 2017.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 3.0, May 2014.

[6] collaborative Protection Profile for Network Devices, Version 2.2E, 23 March 2020.

[7] Bivio 6310-NC Security Target, Version 0.8, Nov 25, 2020

[8] Assurance Activity Report Bivio Networks, Inc., Bivio 6310-NC, Version 1.2, 02 December 2020