Supporting Document
Mandatory Technical Document

PP-Module for Software Defined Networking Controllers
Version: 1.0
2024-10-31
National Information Assurance Partnership

Foreword

This is a Supporting Document (SD), intended to complement the Common Criteria version 3 and the associated Common Evaluation Methodology for Information Technology Security Evaluation.

SDs may be “Guidance Documents”, that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or “Mandatory Technical Documents”, whose application is mandatory for evaluations whose scope is covered by that of the SD. The usage of the latter class is not only mandatory, but certificates issued as a result of their application are recognized under the CCRA.

Technical Editor:
National Information Assurance Partnership (NIAP)

Document history:

Version	Date	Comment
1.0	2024-10-31	First draft of version 1.0 for comment

General Purpose:
The purpose of this SD is to define evaluation methods for the functional behavior of Software Defined Networking Controller products.

Acknowledgments:
This SD was developed with support from NIAP Software Defined Networking Controllers Technical Community members, with representatives from industry, government agencies, Common Criteria Test Laboratories, and members of academia.

Table of Contents

1 Introduction

1.1 Technology Area and Scope of Supporting Document

The scope of the PP-Module for Software Defined Networking Controllers is to describe the security functionality of Software Defined Networking Controllers products in terms of [CC] and to define functional and assurance requirements for them. The PP-Module is intended for use with the following Base-PP:

- Network Device, version 3.0e.

This SD is mandatory for evaluations of TOEs that claim conformance to a PP-Configuration that includes the PP-Module for :

- Software Defined Networking Controllers, Version 1.0

As such it defines Evaluation Activities for the functionality described in the PP-Module as well as any impacts to the Evaluation Activities to the Base-PP(s) it modifies.

Although Evaluation Activities are defined mainly for the evaluators to follow, in general they also help developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in Evaluation Activities may in some cases clarify the meaning of Security Functional Requirements (SFR), and may identify particular requirements for the content of Security Targets (ST) (especially the TOE Summary Specification), user guidance documentation, and possibly supplementary information (e.g. for entropy analysis or cryptographic key management architecture).

1.2 Structure of the Document

Evaluation Activities can be defined for both SFRs and Security Assurance Requirements (SAR), which are themselves defined in separate sections of the SD.

If any Evaluation Activity cannot be successfully completed in an evaluation, then the overall verdict for the evaluation is a 'fail'. In rare cases there may be acceptable reasons why an Evaluation Activity may be modified or deemed not applicable for a particular TOE, but this must be approved by the Certification Body for the evaluation.

In general, if all Evaluation Activities (for both SFRs and SARs) are successfully completed in an evaluation then it would be expected that the overall verdict for the evaluation is a ‘pass’. To reach a ‘fail’ verdict when the Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

Similarly, at the more granular level of assurance components, if the Evaluation Activities for an assurance component and all of its related SFR Evaluation Activities are successfully completed in an evaluation then it would be expected that the verdict for the assurance component is a ‘pass’. To reach a ‘fail’ verdict for the assurance component when these Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

1.3 Terms

The following sections list Common Criteria and technology terms used in this document.

1.3.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Base Protection Profile (Base-PP)	Protection Profile used as a basis to build a PP-Configuration.
Collaborative Protection Profile (cPP)	A Protection Profile developed by international technical communities and approved by multiple schemes.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).

Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Direct Rationale	A type of Protection Profile, PP-Module, or Security Target in which the security problem definition (SPD) elements are mapped directly to the SFRs and possibly to the security objectives for the operational environment. There are no security objectives for the TOE.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Extended Package (EP)	A deprecated document form for collecting SFRs that implement a particular protocol, technology, or functionality. See Functional Packages.
Functional Package (FP)	A document that collects SFRs for a particular protocol, technology, or functionality.
Operational Environment (OE)	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration (PP-Configuration)	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base-PPs.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of Evaluation (TOE)	The product under evaluation.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.

1.3.2 Technical Terms

Address Space Layout Randomization (ASLR)	An anti-exploitation feature which loads memory mappings into unpredictable locations. ASLR makes it more difficult for an attacker to redirect control to code that they have introduced into the address space of a process.
	An administrator is responsible for management activities, including setting policies that are applied by the enterprise on the operating system. This administrator could be acting

Administrator	remotely through a management server, from which the system receives configuration policies. An administrator can enforce settings on the system which cannot be overridden by non-administrator users.
Application (app)	Software that runs on a platform and performs tasks on behalf of the user or owner of the platform, as well as its supporting documentation.
Application Programming Interface (API)	A specification of routines, data structures, object classes, and variables that allows an application to make use of services provided by another software component, such as a library. APIs are often provided for a set of libraries included with the platform.
Control Plane	A logical entity that receives instructions or requirements from the SDN application layer through its northbound interface and relays them to the data plane through its southbound interface. The controller extracts information about the network from the data plane and communicates back to the SDN application layer with an abstract view of the network, including statistics and events about what is happening.
Credential	Data that establishes the identity of a user (e.g., a cryptographic key or password).
Critical Security Parameters (CSP)	Information that is either user or system defined and is used to operate a cryptographic module in processing encryption functions including cryptographic keys and authentication data, such as passwords, the disclosure or modification of which can compromise the security of a cryptographic module or the security of the information protected by the module.
DAR Protection	Countermeasures that prevent attackers, even those with physical access, from extracting data from non-volatile storage. Common techniques include data encryption and wiping.
Data Execution Prevention (DEP)	An anti-exploitation feature of modern operating systems executing on modern computer hardware, which enforces a non-execute permission on pages of memory. DEP prevents pages of memory from containing both data and instructions, which makes it more difficult for an attacker to introduce and execute code.
Data Plane	Controls the forwarding and data processing capabilities for the network. This includes forwarding and processing of the data path.
Developer	An entity that writes OS software. For the purposes of this document, vendors and developers are the same.
Host-based Firewall	A software-based firewall implementation running on the OS for filtering inbound and outbound network traffic to and from processes running on the OS.
Hybrid Authentication	A hybrid authentication factor is one where a user has to submit a combination of a cryptographic token and a PIN or password and both must pass. If either factor fails, the entire attempt fails.
Management Plane	Composed of programs that communicate behaviors and needed resources with the SDN controller via application programming interfaces (APIs). In addition, the applications can build an abstracted view of the network by collecting information from the controller for decision-making purposes. These applications could include networking management, analytics, or business applications used to run large data centers. For example, an analytics application might be built to recognize suspicious network activity for security purposes. This is sometimes also referred to as the Orchestration Layer.
Northbound	Communications between an SDN and applications in the management plane.
Operating System (OS)	Software that manages physical and logical resources and provides services for applications. The terms TOE and OS are interchangeable in this document.
Personal Identification Number (PIN)	An authentication factor that is comprised of a set of numeric or alphabetic characters that may be used in addition to a cryptographic token to provide a hybrid authentication factor. At this time it is not considered as a stand-alone authentication mechanism. A PIN is distinct from a password in that the allowed character set and required length of a PIN is typically smaller than that of a password as it is designed to be input quickly.
Personally Identifiable Information (PII)	Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.
Sensitive Data	Sensitive data may include all user or enterprise data or may be specific application data such as PII, emails, messaging, documents, calendar items, and contacts. Sensitive data must minimally include credentials and keys. Sensitive data shall be identified in the OS's TSS by the ST author.

Southbound	Communications between an SDN and network devices in the data plane.
User	A user is subject to configuration policies applied to the operating system by administrators. On some systems, under certain configurations, a normal user can temporarily elevate privileges to that of an administrator. At that time, such a user should be considered an administrator.

2 Evaluation Activities for SFRs

The EAs presented in this section capture the actions the evaluator performs to address technology specific aspects covering specific SARs (e.g. ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, and ATE_IND.1) – this is in addition to the CEM workunits that are performed in Section 3 Evaluation Activities for SARs.

Regarding design descriptions (designated by the subsections labeled TSS, as well as any required supplementary material that may be treated as proprietary), the evaluator must ensure there is specific information that satisfies the EA. For findings regarding the TSS section, the evaluator's verdicts will be associated with the CEM workunit ASE_TSS.1-1. Evaluator verdicts associated with the supplementary evidence will also be associated with ASE_TSS.1-1, since the requirement to provide such evidence is specified in ASE in the PP.

For ensuring the guidance documentation provides sufficient information for the administrators/users as it pertains to SFRs, the evaluator's verdicts will be associated with CEM workunits ADV_FSP.1-7, AGD_OPE.1-4, and AGD_OPE.1-5.

Finally, the subsection labeled Tests is where the authors have determined that testing of the product in the context of the associated SFR is necessary. While the evaluator is expected to develop tests, there may be instances where it is more practical for the developer to construct tests, or where the developer may have existing tests. Therefore, it is acceptable for the evaluator to witness developer-generated tests in lieu of executing the tests. In this case, the evaluator must ensure the developer's tests are executing both in the manner declared by the developer and as mandated by the EA. The CEM workunits that are associated with the EAs specified in this section are: ATE_IND.1-3, ATE_IND.1-4, ATE_IND.1-5, ATE_IND.1-6, and ATE_IND.1-7.

2.1 Network Device

The EAs defined in this section are only applicable in cases where the TOE claims conformance to a PP-Configuration that includes the NDcPP.

2.1.1 Modified SFRs

The PP-Module does not modify any requirements when the NDcPP is the base.

2.2 TOE SFR Evaluation Activities

2.2.1 Security Audit (FAU)

FAU_GEN.1/SDN Audit Data Generation (SDN)

FAU_GEN.1/SDN
TODO: You need to explain the lack of EAs for this component!!!!

2.2.2 User Data Protection (FDP)

FDP_ACC.1 Subset Access Control

FDP_ACC.1
TODO: You need to explain the lack of EAs for this component!!!!

FDP_ACF.1 Security Attribute-Based Access Control

FDP_ACF.1
TODO: You need to explain the lack of EAs for this component!!!!

2.2.3 Security Management (FMT)

FMT_API_EXT.1 Management of API Behavior

FMT_MOF.1/SDN Management of Functions Behavior (SDN)

FMT_SMF.1/SDN Specification of Management Functions (SDN)

FMT_SMR.2/SDN Restrictions on Security Roles (SDN)

2.3 Evaluation Activities for Optional SFRs

The PP-Module does not define any optional requirements.

2.4 Evaluation Activities for Selection-Based SFRs

The PP-Module does not define any selection-based requirements.

2.5 Evaluation Activities for Objective SFRs

The PP-Module does not define any objective requirements.

2.6 Evaluation Activities for Implementation-dependent SFRs

The PP-Module does not define any implementation-dependent requirements.

3 Evaluation Activities for SARs

The PP-Module does not define any SARs beyond those defined within the base NDcPP to which it must claim conformance. It is important to note that a TOE that is evaluated against the PP-Module is inherently evaluated against this Base-PP as well. The NDcPP includes a number of Evaluation Activities associated with both SFRs and SARs. Additionally, the PP-Module includes a number of SFR-based Evaluation Activities that similarly refine the SARs of the Base-PPs. The evaluation laboratory will evaluate the TOE against the Base-PP and supplement that evaluation with the necessary SFRs that are taken from the PP-Module.

4 Required Supplementary Information

This Supporting Document has no required supplementary information beyond the ST, operational guidance, and testing.

Appendix A - References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2022-11-001, CC:2022, Revision 1, November 2022 • Part 2: Security Functional Requirements, CCMB-2022-11-002, CC:2022, Revision 1, November 2022. • Part 3: Security Assurance Requirements, CCMB-2022-11-003, CC:2022, Revision 1, November 2022. • Part 4: Framework for the Specification of Evaluation Methods and Activities, CCMB-2022-11-004, CC:2022, Revision 1, November 2022. • Part 5: Pre-defined Packages of Security Requirements, CCMB-2022-11-004, CC:2022, Revision 1, November 2022.
[CEM]	Common Common Methodology for Information Technology Security Evaluation, CCMB-2022-11-006, CC:2022, Revision 1, November 2022.
[OMB]	Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, OMB M-06-19, July 12, 2006.