

Item Title	Supporting document FW – Evaluation Activities for Stateful Traffic Filter Firewalls cPP-V0.3	Reviewer	<i>Eunyoung Yi</i>
Item Identifier	<i>FW-SD</i>	Review Date	<i>2014-11-27</i>
Version; Date:	<i>0.3; 2014-10</i>		

Notes :-

Severity	1	Significant - Conflicts with current CC/CEM/CCRA. Needs a substantial change in the meaning of the document or a related CC/CEM change request and rationale to CCDB/MC
	2	Moderate - Normally clarifications or proposed improvements to the compliance with CC/CEM/CCRA - unlikely to impact other areas.
	3	Minor - Does not affect the correct operation or interpretation of the item. These are usually syntax and format errors which have no effect on the meaning or interpretation of the item.

This is a public commenting process: the text of comments and responses may be distributed, or made available in other ways, without restriction during the process.

No.	Location	Comment	Suggested Change	Severity	Action
1.	<SD> 2. Evaluation Activities for SFRs	Based upon SARs defined in the related cPP, we consider all evaluation activities for SFRs are interpretations to the CEM because there is no extended SAR in the cPP. It is obvious that the SD can provide interpretations to the CEM in accordance with the baseline requirements defined in the Vision Statement.	We suggest that all of the proposed evaluation activities for SFRs need to be referenced using related work units in the CEM so that the evaluator applies them to his/her pass/fail verdict decision.	moderate	An updated Supporting Document template has been created to address this comment. The intent is that the new SD template will be populated and will replace the existing SD for the Firewall. The updated template states that the

No.	Location	Comment	Suggested Change	Severity	Action
		<p>In accordance with the CEM section 8.2.5, the evaluator assigns verdicts to every evaluator action element, assurance component, and assurance class. Also, in accordance with the CEM paragraph 57, the evaluator shall assign 'pass' verdict if and only if all of the constituent work units are satisfied.</p> <p>The proposed evaluation activities for the SFRs are mandatory because they are using auxiliary verb 'shall', but there is no reference to the origin work unit which can be examined or checked together with. This will lead to a situation that the evaluator has a difficulty to assigns pass/fail verdict.</p>			<p>evaluator performs the CEM work units associated with ASE, ALC_CMC.1, ALC_CMS.1, AGD_OPE.1, AGD_PRE.1, and ATE_IND.1. For the ADV_FSP.1 component, the SD template supplements the CEM work units – called Evaluation Activities (EAs) – to capture the intent of the work units. A mapping of work units to EAs is included in the template and is presented at the end of this table for the reader's convenience.</p>
2.	<p><SD> 2. Evaluation Activities for SFRs</p>	<p>To apply evaluation activities for SFRs, first of all the evaluator needs evaluation deliverables provided by the sponsor or developer. And the sponsor or developer provides their evaluation deliverables based upon SARs claimed for the evaluation.</p> <p>In the related cPP, SARs from EAL1 are claimed. It is unclear that the necessary evaluation deliverables for the proposed evaluation activities for SFRs are consistent with Developer Action</p>	<p>We suggest that all of the proposed evaluation activities for SFRs need to be referenced using related work units in the CEM so that the sponsor or developer determines they are consistent with SARs claimed.</p>	moderate	See response #1.

No.	Location	Comment	Suggested Change	Severity	Action
		Elements and Content & Presentation of Evidence Elements for each SARs claimed in the cPP.			
3.	<cPP> 2. CC Conformance	The current version of the CC/CEM doesn't provide 'Exact Conformance' yet.	The CCMB is now under reviewing process to incorporate 'Exact conformance' into the CC/CEM, so we expect that this comment will be resolved sooner or later.	Significant	For this reason, elements for determining exact conformance are included in section 3.1 of the Network Device Supporting Document ('Evaluation Activities for Network Device cPP'), as referenced from section 1.1 of the Firewall Supporting Document.
4.	<cPP> C. Extended Component Definitions	<p>There are a lot of extended functional components in the cPP.</p> <p>In accordance with the CC part 1 paragraph 271, we can define extended components with following cases:</p> <p>a) there are security objectives for the TOE that can not be translated to Part 2 SFRs, or there are third party requirements (e.g., laws, standards) that can not be translated to Part 3 SARs (e.g. regarding evaluation of cryptography);</p> <p>b) a security objective can be translated, but only with great difficulty and/or complexity based on components in CC</p>	We suggest that the cPP authors consider to use existing CC part2 SFRs to express their security objectives as possible.	moderate	We have carefully considered the use of extended components in the cPP. We believe that they overcome a number of significant difficulties in being precise and specific about security properties (such as the use of particular choices for secure channel protocols) required in particular technology domains. This also helps when defining specific and repeatable Evaluation

No.	Location	Comment	Suggested Change	Severity	Action
		<p>Part 2 and/or CC Part 3.</p> <p>We couldn't find any good reason to define extended components for some of them (e.g., FIA_PMG_EXT, FIA_UIA_EXT, FIA_UAU_EXT, and FTA_SSL_EXT).</p>			<p>Activities for the SFRs. Based on experience of using such extended SFRs in other PPs, and the experience of involving developers and other subject matter experts in the creation of the recent cPPs, we believe that the use of these components is justified. The particular examples listed in the comment are all examples of where we believe that precision is gained and ambiguity is avoided by using an extended SFR in order to specify exactly what is required in the particular context of administrator sessions that these SFRs relate to. They aim to state specific requirements, and omit some parts of closely related SFRs that we do not consider necessary for the administrator sessions for these devices.</p>

The following table comes from the new SD template and shows how the ADV_FSP.1 work units are covered by the Evaluation Activities.

CEM ADV_FSP.1 Work Units	Evaluation Activities
<p>ADV_FSP.1-1 The evaluator shall examine the functional specification to determine that it states the purpose of each SFR-supporting and SFR-enforcing TSFI.</p>	<p>5.2.1.1 Evaluation Activity: <i>The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.</i></p>
<p>ADV_FSP.1-2 The evaluator shall examine the functional specification to determine that the method of use for each SFR-supporting and SFR-enforcing TSFI is given.</p>	<p>5.2.1.2 Evaluation Activity: <i>The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.</i></p>
<p>ADV_FSP.1-3 The evaluator shall examine the presentation of the TSFI to determine that it identifies all parameters associated with each SFR-enforcing and SFR supporting TSFI.</p>	<p>5.2.1.3 Evaluation Activity: <i>The evaluator shall check the interface documentation to ensure it identifies and describes the parameters for each TSFI that is identified as being security relevant.</i></p>
<p>ADV_FSP.1-4 The evaluator shall examine the rationale provided by the developer for the implicit categorisation of interfaces as SFR-non-interfering to determine that it is accurate.</p>	<p>Paragraph 561 from the CEM: “In the case where the developer has provided adequate documentation to perform the analysis called for by the rest of the work units for this component without explicitly identifying SFR-enforcing and SFR-supporting interfaces, this work unit should</p>

	<p>be considered satisfied.”</p> <p>Since the rest of the ADV_FSP.1 work units will have been satisfied upon completion of the EAs, it follows that this work unit is satisfied as well.</p>
<p>ADV_FSP.1-5 The evaluator <i>shall check</i> that the tracing links the SFRs to the corresponding TSFIs.</p>	<p>5.2.1.4 Evaluation Activity: <i>The evaluator shall examine the interface documentation to develop a mapping of the interfaces to SFRs.</i></p>
<p>ADV_FSP.1-6 The evaluator <i>shall examine</i> the functional specification to determine that it is a complete instantiation of the SFRs.</p>	<p>EAs that are associated with the SFRs in Section Error! Reference source not found., and, if applicable, Sections Error! Reference source not found. and Error! Reference source not found., are performed to ensure that all the SFRs where the security functionality is externally visible (i.e., at the TSFI) are covered. Therefore, the intent of this work unit is covered.</p>
<p>ADV_FSP.1-7 The evaluator <i>shall examine</i> the functional specification to determine that it is an accurate instantiation of the SFRs.</p>	<p>EAs that are associated with the SFRs in Section Error! Reference source not found., and, if applicable, Sections Error! Reference source not found. and Error! Reference source not found., are performed to ensure that all the SFRs where the security functionality is externally visible (i.e., at the TSFI) are addressed, and that the description of the interfaces is accurate with respect to the specification captured in the SFRs.</p>

	Therefore, the intent of this work unit is covered.
--	---