

Comment Resolution Matrix for Public Review #2 of "Open Command and Control (OpenC2) Profile for Stateless Packet Filtering Version 1.0"

Item #	Source	Email Link	Page	Line	Comment Summary	Resolution Summary	Material?	Pull Request	Consensus?	pinged reviewer
SLPF-201	Berliner, Brian	https://www.oasis-open.org/apps/org/workgroup/openc2/message.php/201904/msg00041.html			Section 1.4, Page 10: Should have a link to the "Active Cyber Defense" paper, which is https://www.semanticscholar.org/paper/Active-Cyber-Defense-%3A-A-Vision-for-Real-Time-Cyber-Herring-Willett/7c128468ae42584f282578b86439dbe9e8c904a8	Discussed at face-to-face, accepted	No	Pull#95	Yes	At face-to-face
SLPF-202	Berliner, Brian	https://www.oasis-open.org/apps/org/workgroup/openc2/message.php/201904/msg00041.html			Section 1.4, Page 10: Should have a link to the "Integrated Adaptive Cyberspace Defense" paper, which is https://www.semanticscholar.org/paper/Integrated-Adaptive-Cyberspace-Defense-%3A-Secure-by-Willett/222841820465728142264	Discussed at face-to-face, accepted	No	Pull#95	Yes	At face-to-face
SLPF-203	Berliner, Brian	https://www.oasis-open.org/apps/org/workgroup/openc2/message.php/201904/msg00041.html			Section 1.5.2, Page 11: The first example shown for OpenC2 in the spec is not compliant with the spec as it refers to a "user_account"	Discussed at face-to-face, accepted	No	Pull#95	Yes	At face-to-face
SLPF-204	Berliner, Brian	https://www.oasis-open.org/apps/org/workgroup/openc2/message.php/201904/msg00041.html			Section 1.6, Page 14: The description for the "Message" layer uses the term "requests" and "responses". In the Terminology section (1.2, Page 8) there is no definition of what a request is; only what a command is. The previous page (13) describes a "Command"	Discussed at face-to-face, accepted	No	Pull#93	Yes	At face-to-face
SLPF-205	Berliner, Brian	https://www.oasis-open.org/apps/org/workgroup/openc2/message.php/201904/msg00041.html			Table 2.1.3-2, Page 22: The "running" field seems oddly named to me. The description explains that normally any config changes are made persistently, but the word used to change this fact is "running". Why wouldn't we choose "persist" as the Boolean or "persistent" instead? So, the default for the "persist" field would be TRUE, but it could	Discussed at face-to-face, accepted	Yes	Pull#86	Yes	At face-to-face
SLPF-206	Berliner, Brian	https://www.oasis-open.org/apps/org/workgroup/openc2/message.php/201904/msg00041.html			Table 2.1.3-2, Page 22: For the "direction" field, I find it odd to use an enumeration here, as there appears to be only two possible things that would be enumerated ("ingress" or "egress". If there are only ever two possible options, a Boolean may make more sense, or the addition of	Discussed at face-to-face, accepted	Yes	Pull#87	Yes	At face-to-face

Comment Resolution Matrix for Public Review #2 of "Open Command and Control (OpenC2) Profile for Stateless Packet Filtering Version 1.0"

Item #	Source	Email Link	Page	Line	Comment Summary	Resolution Summary	Material?	Pull Request	Consensus?	pinged reviewer
SLPF-207	Berliner, Brian	https://www.oasis-open.org/apps/org/workgroup/openc2/message.php/201904/msg00041.html			Table 2.3-1, Page 26: Love the table, and it's a great example for other Profiles to use. However, this particular profile does appear to support OPTIONAL action/target pairs, and it would be nice to indicate the OPTIONAL ones in this table (like with an asterisk [*] or something) instead of having to	Discussed at face-to-face, NOT accepted	Yes		Yes	At face-to-face
SLPF-208	Berliner, Brian	https://www.oasis-open.org/apps/org/workgroup/openc2/message.php/201904/msg00041.html			Section A.1.1, Page 42: The example Command uses an "actuator" with a single field of "slpf: asset_id", but this does not match the exact same example included with the Language Spec PRD-02 Section 3.1.5, Page 28, which shows an example of a higher-level "slpf" field with a sub field of "asset_id"	Discussed at face-to-face, accepted	No	Pull#91	Yes	At face-to-face
SLPF-209	Berliner, Brian	https://www.oasis-open.org/apps/org/workgroup/openc2/message.php/201904/msg00041.html			Section A.1.2, Page 43: The example for deny/ip_connection is specifying a Target of "ip_connection", which is not a valid target in the Language Spec, so this example is invalid and misleading.	Discussed at face-to-face, accepted	No	Pull#88	Yes	At face-to-face
SLPF-210	Berliner, Brian	https://www.oasis-open.org/apps/org/workgroup/openc2/message.php/201904/msg00041.html			Section A.1.3, Page 44: Same comment as above about the use of the "slpf" field in the "actuator" object (the Language spec implies that all these fields should be under the "slpf" field, which is itself under the "actuator" top-level field.	Discussed at face-to-face, accepted	No	Pull#91	Yes	At face-to-face
SLPF-211	Berliner, Brian	https://www.oasis-open.org/apps/org/workgroup/openc2/message.php/201904/msg00041.html			Section A.3, Page 46: The example update/file Command uses an "actuator" with a single field of "slpf: named_group", but this does not match the similar example included with the Language Spec PRD-02 Section 3.1.5, Page 28, which shows an example of a higher-level "slpf" field with a sub field of "asset_id"	Discussed at face-to-face, accepted	No	Pull#91	Yes	At face-to-face
SLPF-212	Berliner, Brian	https://www.oasis-open.org/apps/org/workgroup/openc2/message.php/201904/msg00041.html			Section A.4.1, Page 47: The example included for the "query" Action is using an "openc2" target, which no longer exists. This needs to be changed to "features" to be a compliant example.	Discussed at face-to-face, accepted	No	Pull#90	Yes	At face-to-face

Comment Resolution Matrix for Public Review #2 of "Open Command and Control (OpenC2) Profile for Stateless Packet Filtering Version 1.0"

Item #	Source	Email Link	Page	Line	Comment Summary	Resolution Summary	Material?	Pull Request	Consensus?	pinged reviewer
SLPF-213	Berliner, Brian	https://www.oasis-open.org/apps/org/workgroup/openc2/message.php/201904/msg00041.html			Section A.4.3, Page 48: The example response for the query/features/profiles command implies that a returned profile can have more than 16 characters ("iot-front-door-lock"), though the Language Spec PRD-02 says in Section 4.4.2.10, Page 45, that the NSID for a Profile must not be longer	Discussed at face-to-face, accepted and changed in lang spec only	No	No	Yes	At face-to-face
SLPF-214	Berliner, Brian	https://www.oasis-open.org/apps/org/workgroup/openc2/message.php/201904/msg00041.html			Section A.4.4, Page 49: The example response for the query/features/pairs command is using the wrong JSON response format. The Language Spec PRD-02, Section 3.4.2.1, Page 43, defines the "pairs" field as being a Map where the key is the Action (as a String) and the expected targets for that	Discussed at face-to-face, accepted	No	Pull#92	Yes	At face-to-face
SLPF-215	Berliner, Brian	https://www.oasis-open.org/apps/org/workgroup/openc2/message.php/201904/msg00041.html			Annex C, Page 51: Feel free to add me to the Acknowledgements section if you apply any of these comments to the final version (Thanks!).	Discussed at face-to-face, accepted	No	Pull#89	Yes	At face-to-face